Programa de Mestrado Profissional em Matemática em Rede Nacional
Coordenação do PROFMAT

WANDERLAN CARMINATTI DE OLIVEIRA

ELEMENTOS DA ARITMÉTICA MODULAR E O SEU PAPEL NOS ANOS FINAIS DO ENSINO FUNDAMENTAL E NO ENSINO SUPERIOR

Orientador: Prof. Dr. Aldo Amilcar Bazan Pacoricona

NITERÓI
ABRIL/2024

WANDERLAN CARMINATTI DE OLIVEIRA

ELEMENTOS DA ARITMÉTICA MODULAR E O SEU PAPEL NOS ANOS FINAIS DO ENSINO FUNDAMENTAL E NO ENSINO SUPERIOR

Dissertação apresentada por **Wanderlan Carminatti de Oliveira** ao Programa de Mestrado Profissional em Matemática em Rede Nacional - Universidade Federal Fluminense, como requisito parcial para a obtenção do Grau de Mestre.

Orientador: Prof. Dr. Aldo Amilcar Bazan Pacoricona

NITERÓI

2024

Ficha catalográfica automática - SDC/BIME
Gerada com informações fornecidas pelo autor

D278e De Oliveira, Wanderlan Carminatti
ELEMENTOS DA ARITMÉTICA MODULAR E O SEU PAPEL NOS ANOS FINAIS DO ENSINO FUNDAMENTAL E NO ENSINO SUPERIOR : Aritmética Modular na Educação Básica e Superior. / Wanderlan Carminatti De Oliveira. - 2024.
85 f.

Orientador: Aldo Amilcar Bazan Pacoricona.
Dissertação (mestrado profissional)-Universidade Federal Fluminense, Niterói, 2024.

1. Congruência Modular. 2. Educação Básica. 3. Equação Diofantina Linear. 4. Generalização do Teorema Chinês dos Restos. 5. Produção intelectual. I. Pacoricona, Aldo Amilcar Bazan, orientador. II. Universidade Federal Fluminense. Instituto de Matemática e Estatística. III. Título.

CDD - XXX

Bibliotecário responsável: Debora do Nascimento - CRB7/6368

WANDERLAN CARMINATTI DE OLIVEIRA

ELEMENTOS DA ARITMÉTICA MODULAR E O SEU PAPEL NOS ANOS FINAIS DO ENSINO FUNDAMENTAL E NO ENSINO SUPERIOR

Dissertação apresentada por **Wanderlan Carminatti de Oliveira** ao Programa de Mestrado Profissional em Matemática em Rede Nacional - da Universidade Federal Fluminense, como requisito parcial para a obtenção do Grau de Mestre. Linha de Pesquisa: Aritmética modular

Aprovada em: 05 / 04 / 2024

Banca Examinadora

Documento assinado digitalmente
gov.br
ALDO AMILCAR BAZAN PACORICONA
Data: 03/05/2024 16:21:57-0300
Verifique em https://validar.iti.gov.br

Prof. Aldo Amilcar Bazan Pacoricona - Orientador
Doutor – Universidade Federal Fluminense - UFF

Documento assinado digitalmente
gov.br
MARCELO LEONARDO DOS SANTOS RAINHA
Data: 06/05/2024 16:40:15-0300
Verifique em https://validar.iti.gov.br

Prof. Marcelo Leonardo Rainha dos Santos - Membro
Doutor – UNIRIO

Documento assinado digitalmente
gov.br
MIRIAM DEL MILAGRO ABDON
Data: 03/05/2024 16:42:00-0300
Verifique em https://validar.iti.gov.br

Prof. Miriam del Milagro Abdón - Membro
Doutor – Universidade Federal Fluminense - UFF

Documento assinado digitalmente
gov.br
ALEX FARAH PEREIRA
Data: 03/05/2024 17:14:21-0300
Verifique em https://validar.iti.gov.br

Prof. Alex Farah Pereira - Membro
Doutor – Universidade Federal Fluminense - UFF

NITERÓI

2024

Aos meus pais, a minha esposa e ao meu filho, que foram essenciais para a realização deste trabalho.

AGRADECIMENTOS

A Deus por me ajudar a transpor todas as barreiras encontradas ao longo da realização deste trabalho.

Agradeço a minha esposa, Katiluscia, que esteve comigo em todo momento, apoiando, encorajando e dando o amparo necessário para que hoje pudesse usufruir desta conquista.

Ao meu filho, Guilherme, que é a razão da minha vida e proporciona força para ir além dos meus limites.

Meus agradecimentos e meu carinho aos meus pais, Alcides e Maria Clara, pelo seu amor incondicional e incentivo.

Ao professor Roberval da Costa Lima que deu todo suporte intelectual desde o início das primeiras disciplinas, até a preparação do Exame Nacional de Qualificação.

Ao professor orientador, Doutor Aldo Almicar Bazan Pacoricona, que tornou possível a realização deste trabalho, com toda serenidade e apoio.

A todos os professores do PROFMAT - UFF que conosco compartilham seus conhecimentos, e com isso acarretando nosso desenvolvimento acadêmico.

Aos meus colegas de turma, em especial Maurício Celso que sempre me incentivou e foi um companheiro incansável de estudos.

A todos que, de alguma forma, contribuíram para esta construção.

Palavras são poucas para expressar minha gratidão por vocês.

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Nesta dissertação fazemos uma abordagem da aritmética modular em dois pontos principais: as equações Diofantinas Lineares e o Teorema Chinês do Resto Generalizado. O primeiro versa sobre as definições e resultados associados ao conceito de equação diofantina linear, e fazemos uma digressão sobre este assunto nos anos finais do ensino fundamental. O segundo refere-se a uma generalização do Teorema Chinês dos Resto, e o seu papel no ingresso na educação superior. Apresentamos a fundamentação teórica com conceitos da Teoria dos Números como múltiplos e divisores de um número inteiro, Algoritmo da Divisão de Euclides, Máximo Divisor Comum, Mínimo Múltiplo Comum, Equações Diofantinas Lineares, Congruências Lineares, Teorema Chinês dos Restos Generalizado e, em especial, o assunto de Congruência Modular. Nessa parte expomos um breve histórico de como surgiu esse objeto de estudo, descrevendo sua origem, definições, demonstrações de suas principais propriedades e , ainda, aplicações de Congruências Modulares no concurso Colégio Naval, na OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas), na OBM (Olimpíada Brasileira de Matemática) e no ENQ (Exame Nacional de Qualificação do Mestrado PROFMAT). Este trabalho foi produzido para facilitar o acesso a diversos temas, visando transmitir o conhecimento de uma maneira prática e de fácil entendimento.

Palavras-chave: Congruência Modular, Equações Diofantinas Lineares, Teorema Chinês dos Restos Generalizado, Anos finais do ensino fundamental, Educação Superior.

ABSTRACT

This dissertation presents two scientific articles and a common theme to them. The first deals with the concepts of Linear Diophantine Equations in the final years of elementary school. The second refers to the importance of learning the Chinese Generalized Remainder Theorem, upon entry into higher education. We present the theoretical foundation with concepts from Number Theory such as multiples and divisors of an integer, Euclid's Division Algorithm, Greatest Common Divisor, Least Common Multiple, Linear Diophantine Equations, Linear Congruences, Chinese Generalized Remainder Theorem and, in particular, the subject of Modular Congruence. In this part we present a brief history of how this object of study emerged, describing its origin, definitions, demonstrations of its main properties and, also, applications of Modular Congruences in the Colégio Naval competition, at OBMEP (Brazilian Mathematical Olympiad for Public Schools), in the OBM (Brazilian Mathematics Olympiad) and in the ENQ (PROFMAT Master's National Qualification Exam). This work was produced to facilitate access to various topics, aiming to transmit knowledge in a practical and easy-to-understand way.

Keywords: Modular Congruence, Linear Diophantine Equations, Chinese Generalized Remainder Theorem, Final years of elementary school, Higher Education.

SUMÁRIO

1 INTRODUÇÃO

A maioria dos alunos do ensino fundamental II não possuem uma visão de qual carreira vão seguir. Com isso, os professores terão um papel essencial, proporcionando informações de como funciona a matemática em certames e assim despertando o interesse nos jovens, de forma a estimular os mesmos a estudarem mais a matemática e outros assuntos relacionados a ela. Além disso, os novos universitários, oriundos do Ensino Médio, têm dificuldade em alguns conteúdos de matemática, e especialmente associados à aritmética.

Nesta dissertação propomos um vasto referencial teórico e diversas questões resolvidas passo a passo que incentivem os alunos, dos anos finais do Ensino Fundamental, a se prepararem para concursos para o ensino médio, como o do Colégio Naval, e também oferecemos o mesmo suporte para os estudantes dos cursos universitários que tenham a aritmética em sua grade curricular.

A estrutura deste trabalho é a seguinte. Apresentamos no capítulo 2 um referencial teórico, colocando a ênfase do uso dos restos, na congruência modular e nas suas proposições e teoremas. É notório que inúmeras situações do cotidiano dos discentes estão relacionadas com esse tópico matemático.

A seguir, no capítulo 3 apresentamos diversos exemplos resolvidos, para ratificar a teoria apresentada. Cabe ressaltar que esses problemas podem ser usados nas salas de aula de toda a Educação Básica.

Finalmente no capítulo 4 apresentamos questões e resoluções de inúmeros concursos, olimpíadas e exames de qualificação de mestrado profissional em matemática.

Este trabalho tem a finalidade de expor a relevância do estudo da congruência modular, e quando trazido para a realidade se torna um instrumento indispensável na resolução de problemas desta e de outros ramos que podem conduzir o leitor a um elevado nível de raciocínio e habilidades.

2 REFERENCIAL TEÓRICO

2.1 CONCEITOS BÁSICOS DA TEORIA DOS NÚMEROS

2.1.1 Múltiplos e divisores

Definição 2.1: Dados a, b $\in \mathbb{Z}$ e $a \neq 0$, dizemos que a divide b se b = ac para algum c $\in \mathbb{Z}$. Quando isto acontece também se diz que a é um divisor de b (resultará uma divisão exata, ou seja, o resto é zero) ou que b é um múltiplo de a (ou divisível por a).

A partir de agora usaremos a notação a|b para indicar que a divide b e a∤b no caso contrário. O elemento c tal que b = ac é chamado quociente de b por a e indicado por c = $\frac{b}{a}$ (eventualmente b:a).

2.1.2 Algoritmo da Divisão de Euclides

Teorema 2.1**:** Para quaisquer a, b $\in \mathbb{Z}$**, com** b > 0, existe um único par de inteiros q e r, de modo que a = bq + r, onde 0 $\leq$ r < b.

Na igualdade que expressa o teorema, os elementos a, b, q e r são chamados respectivamente dividendo, divisor, quociente e resto na divisão euclidiana de a por b.

2.1.3 Máximo divisor Comum

Nesta parte vamos apresentar a definição de máximo divisor comum de dois números inteiros, e mostrar que é sempre possível encontrar esse número, que é único.

Definição 2.2: Sejam a e b números inteiros quaisquer. Entendemos por máximo divisor comum de a e b e indicamos por mdc (a,b) = d. O maior inteiro que divide a e b, se d satisfazer as seguintes condições:

(1) d é um divisor comum de a e b.

(2) d é divisível por todo divisor comum de a e b, isto é, se c é um divisor comum de a e b então c | d.

2.1.4 Mínimo múltiplo comum

Nesta parte vamos apresentar a definição de mínimo múltiplo comum de dois números inteiros. O mínimo múltiplo comum de a e b, se existe, é denotado por mmc (a,b) = e ou [a,b] = e. Daí, [-a,b] = [a,-b] = [-a,-b] = [a,b]

Proposição 2.1: Dados dois números inteiros a e b, ambos não nulos, temos que [a,b] existe e [a,b] $\cdot$ (a,b) = |a $\cdot$ b|.

2.2 CONGRUÊNCIA MODULAR

Definição 2.3: Seja m um número natural diferente de zero. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b \bmod m.$$

Decorre, imediatamente, da definição dada que a congruência, módulo um inteiro fixado m, é uma relação de equivalência, ou seja, reflexiva, simétrica e transitiva. Vamos enunciar isto explicitamente abaixo.

Proposição 2.2: Seja $m \in \mathbb{N}$. Para todos a, b, $d \in \mathbb{Z}$, tem-se que

(i) $a \equiv a \bmod m$, (reflexiva)

(ii) se $a \equiv b \bmod m$, então $b \equiv a \bmod m$, (simétrica)

(iii) se $a \equiv b \bmod m$, então $b \equiv d \bmod m$, então $a \equiv d \bmod m$. (transitiva)

Demonstração:

(i) Como m | 0, então m | (a – a), o que implica $a \equiv a \bmod m$.

(ii) Se $a \equiv b \bmod m$, então $a = b + k_1 m$, para algum inteiro k_1. Logo, $b = a - k_1 m$, o que implica $b \equiv a \bmod m$.

(iii) Se $a \equiv b \bmod m$, então $b \equiv d \bmod m$, então existem inteiros k_1 e k_2 tais que $a – b = k_1 m$ e $b – d = k_2 m$. Somando, membro a membro, estas últimas equações, obtemos $a – d = (k_1 + k_2)m$, o que implica $a \equiv d \bmod m$.

Para verificar se dois números são congruentes módulo m, não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar os seus restos. É suficiente aplicar o seguinte resultado.

Proposição 2.3: Suponha que a, b, $m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \bmod m$ se, e somente se, m | b – a.

Demonstração.

Sejam $a = mq + r$, com $0 \leq r < m$ e $b = mq' + r'$, com $0 \leq r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b – a = m(q' – q) + (r' – r).$$

Portanto, $a \equiv b \bmod m$ se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente a dizer que $m \mid b - a$, já que $|r - r'| < m$.

A noção de congruência é uma ferramenta muito útil, pois é uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, segundo a proposição a seguir.

Proposição 2.4: Sejam $a, b, c, d, m \in \mathbb{Z}$ com $m > 1$.

(i)Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$.

(ii) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a \cdot c \equiv b \cdot d \bmod m$.

Demonstração.

Suponhamos que $a \equiv b \bmod m$ e $c \equiv d \bmod m$. Logo, temos que $m \mid b - a$ e $m|d - c$.

(i) Basta observar que $m \mid (b - a) + (d - c)$ e, portanto, $m \mid (b + d) - (a + c)$, o que prova essa parte do resultado.

(ii) Basta notar que $bd - ac = d(b - a) + a(d - c)$ e concluir que $m|bd - ac$.

Proposição 2.5: Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$. Tem-se que

$$a + c \equiv b + c \bmod m \Leftrightarrow a \equiv b \bmod m.$$

Demonstração.

Se $a \equiv b \bmod m$, segue-se imediatamente da Proposição 3(i) que $a + c \equiv b + c \bmod m$, pois $c \equiv c \bmod m$.

Reciprocamente, se $a + c \equiv b + c \bmod m$, então $m \mid (b + c) - (a + c)$, o que implica que $m \mid b - a$ e , consequentemente, $a \equiv b \bmod m$.

Proposição 2.6: Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$. Temos que

$$a \cdot c \equiv b \cdot c \bmod m \Leftrightarrow a \equiv b \bmod \frac{m}{(c,m)}.$$

Demonstração.

Como $\frac{m}{(c,m)}$ e $\frac{c}{(c,m)}$ são coprimos, ou seja, mdc entre eles é 1, temos

$$\begin{aligned} & a \cdot c \equiv b \cdot c \bmod m \\ \Leftrightarrow\ & m \mid ((b - a)c \\ \Leftrightarrow\ & \frac{m}{(c,m)} \mid (b - a)\frac{c}{(c,m)} \\ \Leftrightarrow\ & \frac{m}{(c,m)} \mid b - a \\ \Leftrightarrow\ & a \equiv b \bmod \frac{m}{(c,m)}. \end{aligned}$$

Proposição 2.7: Se a, b, c e m são inteiros tais que $a \equiv b \bmod m$, então $ac \equiv bc \bmod m$.

Demonstração.

Como $a - b = km$, $ac - bc = ckm$, o que implica $m \mid (ac - bc)$ e , portanto, $ac \equiv bc \bmod m$.

Proposição 2.8: Sejam a, $b \in \mathbb{Z}$ m, n, m_1, ..., m_r inteiros maiores do que 1. Temos

i) se $a \equiv b \bmod m$ e $n|m$, então $a \equiv b \bmod n$;

ii) $a \equiv b \bmod m_i$, $\forall$ i = 1, ..., r $\Leftrightarrow a \equiv b \bmod [m_1, ..., m_r]$;

iii) se $a \equiv b \bmod m$, então mdc (a,m) = mdc (b,m).

Demonstração.

(i) Se $a \equiv b \bmod m$, então $m \mid b - a$. Como $n \mid m$, segue-se que $n \mid b - a$. Logo, $a \equiv b \bmod n$.

(ii) Se $a \equiv b \bmod m_i$, i = 1, ..., r, então $m_i \mid b - a$, para todo i. Sendo b – a um múltiplo de cada m_i, segue-se que $[m_1, ..., m_r] \mid b - a$, o que prova $a \equiv b \bmod [m_1, ..., m_r]$. A recíproca decorre do item (i)

(iii) Se $a \equiv b \bmod m$, então $m \mid b - a$ e, portanto, $b = a + tm$ com $t \in \mathbb{Z}$. Logo, pelo lema de Euclides, temos que

$$(a,m) = (a + tm,m) = (b,m)$$

Em seguida temos outra afirmação referente a cancelamento multiplicativo.

Corolário 2.1: Sejam a, b, c, $m \in \mathbb{Z}$ com $m > 1$ e (c,m) = 1. Temos

$$a \cdot c \equiv b \cdot c \bmod m \Leftrightarrow a \equiv b \bmod m.$$

Corolário 2.2: Para todos $n \in \mathbb{N}$ e a, $b \in \mathbb{Z}$ se $a \equiv b \bmod m$, então tem-se que $a^n \equiv b^n \bmod m$.

Demonstração.

Isto segue, imediatamente, da identidade:

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + ... + ab^{k-2} + b^{k-1}).$$

Teorema 2.2: (Pequeno Teorema de Fermat)

Se $p > 1$ é um número primo que não divide o inteiro a, então:

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

Demonstração.

Sabemos que o conjunto formado pelos p números 0, 1, 2, ..., p -1 constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p, pode ser colocado em correspondência biunívoca com um subconjunto de {0, 1, 2, ..., p -1}. Vamos, agora, considerar os números a, 2a, 3a, ..., (p – 1)a. Como (a,p) = 1, nenhum destes números ia, $1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak \bmod p$ implica $j \equiv k \bmod p$ e isto só é possível se j = k, uma vez que ambos j e k positivos e menores do que p. Temos, portanto, um conjunto de p – 1 elementos incongruentes módulo p e não-divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos 1, 2, 3, ..., p -1. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a\,(2a)\,(3a)\cdots(p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p$$

Ou seja, $a^{p-1}\,(p-1)! \equiv (p-1)! \bmod p$. Mas, como $((p-1)!, p) = 1$, podemos cancelar o fator (p – 1)! em ambos os lados, obtendo

$$a^{p-1} \equiv 1 \bmod p,$$

o que conclui a demonstração.

Corolário 2.3: Se p é um primo e a é um inteiro positivo, então $a^p \equiv a \bmod p$.

Demonstração.

Temos que analisar dois casos, se p | a e se p ł a. Se p | a, então p | $(a(a^{p-1} – 1)$ e, portanto $a^p \equiv a \bmod p$. Se p ł a, pelo Teorema 1, p | $(a^{p-1} – 1)$ e, portanto p | $(a^p – a)$. Logo, em ambos os casos, $a^p \equiv a \bmod p$.

Observação 2.1: Uma congruência modular pode ser reescrita somando ou subtraindo os múltiplos do módulo, do lado direito da congruência.

2.3 CONGRUÊNCIA LINEAR

Definição 2.4: Uma congruência algébrica do tipo

$$ax \equiv b \pmod m$$

onde a, b, m $\in \mathbb{Z}$, a $\neq$ 0 e m > 0, e x é um número inteiro, recebe o nome de congruência linear ou congruência do primeiro grau.

Proposição 3.2: Dados a, b, m $\in \mathbb{Z}$, com m > 1, a congruência

$$ax \equiv b \pmod{m}$$

possui solução se, e somente se, mdc (a,m) | b.

2.4 EQUAÇÕES DIOFANTINAS LINEARES

Consideremos, pois, uma equação:

$$ax + by = c \quad (1)$$

onde a, b $\in \mathbb{Z}$ e suponhamos a e b não simultaneamente nulos. Uma solução de (1) é, neste contexto, um par $(x_0,y_0) \in \mathbb{Z} \times \mathbb{Z}$, para o qual a igualdade:

$$ax_0 + by_0 = c$$

é verdadeira.

Proposição 2.9: Uma Equação Diofantina ax + by = c, em que a $\neq$ 0 e b $\neq$ 0, admite solução se, e somente se, d = mdc(a,b) divide c.

Proposição 2.10: Seja (x_0,y_0) uma particular solução da equação diofantina ax + by = c, onde mdc (a,b) = 1. Então todas as soluções inteiras x, y da equação são da seguinte forma:

$$x = x_0 - bt,\ y = y_0 + at, \text{ onde } t \in \mathbb{Z}.$$

O número inteiro t vai oferecer uma solução distinta para a equação diofantina.

2.5 GENERALIZAÇÃO DO TEOREMA CHINÊS DO RESTO

Teorema 2.3: O sistema de congruências

$$X \equiv c_i \bmod m_i,\ i = 1, ..., r. \quad (1)$$

Admite solução se, e somente se, $c_i \equiv c_j \bmod (m_i, m_j)$, $\forall$ i, j = 1, . . ., r.

Nesse caso, a solução é única módulo $[m_1, ..., m_r]$.

A seguir vamos generalizar também o algoritmo para determinar as soluções do sistema de congruências.

Antes, porém, vamos estabelecer dois lemas.

Sejam $m_1, ..., m_r$ números inteiros, estabelecemos as seguintes notações:

$M = [m_1, ..., m_r]$ e $M_i = \frac{M}{m_i}$, $i = 1, ..., r$.

Lema 2.1: Com as notações acima, existem inteiros $x_1, ..., x_r$ tais que

$$x_1M_1 + ... + x_rM_r = 1.$$

Lema 2.2: Para todos i, j = 1, . . ., r, tem-se que

$$m_j \mid M_i \ (m_i, m_j).$$

Teorema 2.3: Se o sistema (1) admite soluções, as soluções são dadas por

$$x = c_1x_1M_1 + ... + c_rx_rM_r + tM,$$

onde $t \in \mathbb{Z}$ e $x_1, ..., x_r$ são tais que

$$x_1M_1 + ... + x_rM_r = 1.$$

3 EXEMPLIFICAÇÃO DA TEORIA

A seguir apresentaremos diversos exemplos, para facilitarem o entendimento da teoria apresentada anteriormente.

3.1 MÚLTIPLOS E DIVISORES

Exemplo 3.1:

3|27, 7|49, 9|0, -2|10 e 5∤13.

Em $\mathbb{Z}$ **o conjunto** dos múltiplos de um dado elemento K será indicado por M_k e é assim constituído:

$M_k = \{0, \pm k, \pm 2k, \pm 3k, ...\} = M_{-k}$

Exemplo 3.2:

$M_6 = \{0, \pm 6, \pm 12, \pm 18, ...\} = M_{-6}$

No conjunto acima, onde temos os múltiplos de 6, observamos que o zero é múltiplo de qualquer número, próprio número é múltiplo dele mesmo e o conjunto é infinito.

E ainda do conjunto M_6, temos que:

Se 12 é múltiplo de 6, então, 6 é divisor de 12.

Agora vamos listar o conjunto dos divisores de um determinado número.

Exemplo 3.3:

$D_{20} = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\}$

No conjunto acima, onde temos os divisores de 20, observamos que o número um é divisor de qualquer número, o próprio número é divisor dele mesmo e o conjunto dos divisores é finito.

3.2 ALGORITMO DA DIVISÃO DE EUCLIDES

Exemplo 3.4:

Ache o quociente e o resto na divisão euclidiana de a por b no seguinte caso:

a = 79 e b = 5.

Resolução:

Como o enunciado diz divisão de a por b, a é o dividendo e b o divisor. Assim, vamos aplicar o algoritmo da divisão.

Daí, observamos que o quociente é 15 e o resto é 4. E ainda podemos escrever:

$79 = 5 \cdot 15 + 4$

3.3 MÁXIMO DIVISOR COMUM

Exemplo 3.5:

Sejam a = 12 e b = 4, determine o mdc(12,4).

Resolução:

Sabemos que o divisor de um número inteiro é todo o número inteiro que ao dividir tal número, resultará em uma divisão exata. Com essa informação vamos determinar o conjunto dos divisores de a = 12 e b = 4, sendo denotados por D_{12} = { $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$ e D_4 = { $\pm 1, \pm 2, \pm 4\}$. Como o mdc(12,4) é o maior inteiro que divide 12 e 4, para encontrar o máximo divisor comum entre esses números, basta determinar a interseção $D_{12} \cap D_4$ e tomar o maior número em módulo desse conjunto.

Logo, $D_{12} \cap D_4 = \{\pm 1, \pm 2, \pm 4\}$ $e\ máx(D_{12} \cap D_4) = 4. Portanto, o\ mdc(12,4) = 4.$

3.4 CONGRUÊNCIA MODULAR

Exemplo 3.6:

Note que $33 \equiv 18 \bmod 5$, já que os restos da divisão de 33 e de 18 por 5 são iguais a 3.

Quando a relação $a \equiv b \bmod m$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes, módulo m. Escreveremos, neste caso, $a \not\equiv b \bmod m$.

Exemplo 3.7:

Note que $20 \not\equiv 11 \bmod 2$, pois os restos da divisão de 20 e de 11 por 2 são diferentes.

Exemplo 3.8:

Vamos verificar a congruência $65 \equiv 23 \bmod 7$, sem efetuar a divisão euclidiana. Utilizando a proposição 2 temos: $7 \mid 23 - 65 \Leftrightarrow 7 \mid -42$, que é verdadeiro.

Exemplo 3.9:

Vamos verificar a congruência $18 \equiv 55 \bmod 11$, sem efetuar a divisão euclidiana. Utilizando a proposição 2 temos: $11 \nmid 55 - 18 \Leftrightarrow 11 \nmid 37$. Logo, a congruência é falsa, e deve-se escrita: $18 \not\equiv 55 \bmod 11$.

Exemplo 3.10:

Considere a congruência $54 \equiv 30 \bmod 8$, que pode ser reescrita através da multiplicação $6 \cdot 9 \equiv 6 \cdot 5 \bmod 8$. Ao efetuar o cancelamento teremos a seguinte congruência, que será falsa $9 \not\equiv 5 \bmod 8$, ou seja, o cancelamento na multiplicação, em geral, é falso.

Exemplo 3.11:

Vamos considerar a congruência anterior $54 \equiv 30 \bmod 8 \Leftrightarrow 6 \cdot 9 \equiv 6 \cdot 5 \bmod 8$, onde c = 6 e m = 8. Fazendo o mdc (6,8) = 2. Aplicando a proposição 2.6 e cancelando o número 6, teremos uma nova congruência de módulo igual ao mdc (6,8) = 2. Daí, obtemos: $9 \equiv 5 \bmod 2$, que é verdadeira. Observem que o cancelamento multiplicativo ocorreu devido à nova congruência, que possuirá um novo módulo

Exemplo 3.12:

Analisando a congruência modular $20 \equiv 6 \bmod 7 \Leftrightarrow 2 \cdot 10 \equiv 2 \cdot 3 \bmod 7$, onde c = 2 e m = 7. Como mdc (2,7) = 1, podemos usar o corolário 2.1 e cancelar o fator multiplicativo 2: $10 \equiv 3 \bmod 7$.

Constatem que a proposição 2.5 e o corolário 2.1 se parecem muito, porém temos que nos atentar em algumas coisas. Na proposição 2.5 o mdc entre c e m tem que ser divisor do módulo m, ou seja, o mdc (c,m) pode ser qualquer valor diferente

de zero, e no corolário 2.1 o mdc entre c e m tem que ser 1, não podendo ser outro valor. Logo, essas observações vão diferenciar quando usar a proposição 2.5 e quando aplicar o corolário 2.1.

Exemplo 3.13:

Dada a congruência modular $15 \equiv 2 \bmod 13$, podemos utilizar o mesmo expoente na congruência, que não vai alterar nada. Assim, temos:

$$15^{121} \equiv 2^{121} \bmod 13.$$

Exemplo 3.14:

Considere a congruência $17 \equiv 2 \bmod 5$, que pode ser reescrita de várias maneiras: $17 \equiv 2 + 5 \bmod 5 \Leftrightarrow 17 \equiv 7 \bmod 5$, $17 \equiv 2 - 5 \bmod 5 \Leftrightarrow 17 \equiv -3 \bmod 5$.

Exemplo 3.15:

Dada a congruência modular $13 \equiv 6 \bmod 7$, que será reescrita subtraindo o módulo 7 do lado direito, segue que: $13 \equiv 6 - 7 \bmod 7 \Leftrightarrow 13 \equiv -1 \bmod 7$. Essa ferramenta é muito utilizada, pois ficamos com -1 do lado direito, e com isso é possível aplicar o Corolário 2.1, colocando um expoente com valor alto e não alterará em nada, já que um dos números elevados a esse expoente será -1.

3.4 CONGRUÊNCIA LINEAR

Exemplo 3.16:

Verifique se o inteiro x é solução das congruências lineares a seguir:

$x = 2$ e $8x \equiv 4 \pmod{12}$.

Resolução:

Vamos substituir $x = 2$ na congruência linear, $8 \cdot 2 \equiv 4 \pmod{12} \Leftrightarrow 16 \equiv 4 \pmod{12}$. Agora vamos verificar se a última congruência satisfaz o conceito:

$12 \mid 4 - 16 = -12 \Leftrightarrow 12 \mid -12$, que é verdadeiro. Logo, $x = 2$ é uma solução da congruência linear $8x \equiv 4 \pmod{12}$.

a) $x = 7$ e $3x \equiv 1 \pmod{5}$.

Resolução:

Vamos substituir $x = 7$ na congruência linear, $3 \cdot 7 \equiv 1 \pmod{5} \Leftrightarrow 21 \equiv 1 \pmod{5}$. Agora vamos verificar se a última congruência satisfaz o conceito: $5 \mid 1 - 21$

= -20 $\Leftrightarrow$ 5 | -20, que é verdadeiro. Logo, x = 7 é uma solução da congruência linear $8x \equiv 4 \pmod{12}$.

b) x = 5 e $6x \equiv 15 \pmod{21}$.

Resolução:

Vamos substituir x = 5 na congruência linear, $6 \cdot 5 \equiv 15 \pmod{21} \Leftrightarrow 30 \equiv 15 \pmod{21}$. Agora vamos verificar se a última congruência satisfaz o conceito: 21 |15 - 30= -15 $\Leftrightarrow$ 21 | -15, que é falso, pois $21 \nmid -15$. Logo, x = 5 não é uma solução da congruência linear $6x \equiv 15 \pmod{21}$.

Exemplo 3.17:

Verifique se as congruências lineares possuem soluções.

a) $4x \equiv 5 \pmod{6}$.

Resolução:

Temos a = 4, b = 5 e m = 6 e mdc (4,6) = 2. E, $2 \nmid 5$, então a congruência linear não possui solução,

b) $8x \equiv 4 \pmod{12}$.

Resolução:

Temos a = 8, b = 4 e m = 12 e mdc (8,12) = 4. E, 4 | 4, então a congruência linear possui solução.

Exemplo 3.18:

Resolva as congruências lineares.

a) $4x \equiv 2 \pmod{6}$.

Resolução:

Vamos encontrar um número inteiro x, que ao ser multiplicado por 4, acharemos um valor que ao ser dividido por 6 e deixará resto 2. Primeiro resolveremos por tentativa:

x = 1, $4 \cdot 1 \equiv 2 \pmod{6} \Rightarrow 4 \equiv 2 \pmod{6}$. Verificamos que 4 ao ser dividido por 6, deixa resto 4, porém a congruência mostra o resto 2. Logo, x = 1 não é solução da congruência.

x = 2, $4 \cdot 2 \equiv 2 \pmod 6 \Rightarrow 8 \equiv 2 \pmod 6$. Verificamos que 8 ao ser dividido por 6, deixa resto 2, a congruência também deixa resto 2. Logo, x = 2 é solução da congruência.

b) $6x \equiv 12 \pmod 5$.

Resolução:

Antes de começarmos a resolver a congruência, vamos melhorá-la. Para isso vamos dividir 6 por 5 e o resto encontrado é 1, substituirá o 6 pelo resto 1. E ainda temos 12 dividido por 5 e o resto achado é 2, o 12 será substituído por 2. Observem que a congruência linear pode ter seus números diminuídos através dos restos. Assim, a congruência linear será reescrita: $1x \equiv 2 \pmod 5$. Logo, a solução da congruência linear é x = 2.

c) $14x \equiv 200 \pmod 9$

Resolução:

Antes de começarmos a resolver a congruência, vamos melhorá-la. Para isso vamos dividir 200 por 9 e o resto encontrado é 2, substituirá o 200 pelo resto 2. E ainda temos 14 dividido por 9 e o resto achado é 5, o 14 será substituído por 5. Observem que a congruência linear pode ter seus números diminuídos através dos restos. Assim, a congruência linear será reescrita: $5x \equiv 2 \pmod 9$. Agora fazendo por tentativa:

x = 1, $5 \cdot 1 \equiv 2 \pmod 9 \Rightarrow 5 \equiv 2 \pmod 9$. Verificamos que 5 ao ser dividido por 9, deixa resto 5, porém a congruência é resto 2. Logo, x = 1 não é solução da congruência.

x = 4, $5 \cdot 4 \equiv 2 \pmod 9 \Rightarrow 20 \equiv 2 \pmod 9$. Verificamos que 20 ao ser dividido por 9, deixa resto 2, a congruência também deixa resto 2. Logo, x = 4 é solução da congruência.

d) $5x \equiv 4 \pmod 7$

Resolução:

Para resolver a congruência linear, vamos usar a propriedade 3.6. Multiplicaremos a congruência por 3, pois a propriedade tem a restrição de que o mdc (c,m) = 1. Na congruência m = 7 (mod 7) e o c = 3, número que multiplicará a congruência linear. Daí, mdc (3,7) = 1. Cabe ressaltar que o 3 foi escolhido, pois o

mod 7 deixa resto 1, quando 15x ($5x \cdot 3$) é dividido por 7. Então, uma técnica valiosa é buscar o resto 1 no número com a letra x, assim a congruência linear já terá sua solução.

$5x \cdot 3 \equiv 4 \cdot 3 \pmod 7 \Rightarrow 15x \equiv 12 \pmod 7 \Rightarrow 1x \equiv 5 \pmod 7$. Observem que o 15 e o 12 foram divididos por 7 (mod 7) e substituídos pelos seus respectivos restos, 1 e 5. Logo, a última congruência oferece a solução x = 5.

e) $6x \equiv 5 \pmod{11}$

Resolução:

Para resolver a congruência linear, vamos usar a propriedade 3.6. Multiplicaremos a congruência por 2, pois a propriedade tem a restrição de que o mdc (c,m) = 1. Na congruência m = 11 (mod 11) e o c = 2, número que multiplicará a congruência linear. Daí, mdc (2,11) = 1. Cabe ressaltar que o 2 foi escolhido, pois o mod 11 deixa resto 1, quando 12x ($6x \cdot 2$) é dividido por 11. Então, uma técnica valiosa é buscar o resto 1 no número com a letra x, assim a congruência linear já terá sua solução.

$6x \cdot 2 \equiv 5 \cdot 2 \pmod{11} \Rightarrow 12x \equiv 10 \pmod{11} \Rightarrow 1x \equiv 10 \pmod{11}$. Observem que o 12 e o 10 foram divididos por 11 (mod 11) e substituídos pelos seus respectivos restos, 1 e 10. Logo, a última congruência oferece a solução x = 10.

f) $8x \equiv 4 \pmod{12}$

Resolução:

Observamos que a = 8, b = 4 e m = 12 são múltiplos de 4. Agora vamos reescrever a congruência em forma de multiplicação por 4, que será c = 4. Propriedade 3.7.

$2x \cdot 4 \equiv 4 \cdot 1 \pmod{4 \cdot 3}$. Fazendo o mdc (c,m), temos mdc (4,12) = 4, teremos:

$2x \equiv 1 \pmod 3$. Agora fazendo tentativas na última congruência linear encontrada:

x = 2, $2 \cdot 2 \equiv 1 \pmod 3 \Rightarrow 4 \equiv 1 \pmod 3$. Verificamos que 4 ao ser dividido por 3, deixa resto 1, a congruência também deixa resto 1. Logo, x = 2 é solução da congruência.

Exemplo 3.19: (Colégio Naval – 1984)

O resto da divisão por 11 do resultado da expressão $1211^{20} + 9119^{32} \cdot 343^{26}$ é:

a) 9

b) 1

c) 10

d) 6

e) 7

Resolução:

Primeiro vamos montar as congruências de 1211 e 9119 em módulo 11:

$$1211 \equiv 1 \bmod 11, \quad (2.1)$$

$$9119 \equiv 0 \bmod 11. \quad (2.2)$$

Aplicando o Corolário 2.2 nas congruências (2.1) e (2.2), segue que

$$1211^{20} \equiv 1^{20} \bmod 11, \quad (2.3)$$

$$9119^{32} \equiv 0^{32} \bmod 11. \quad (2.4)$$

Agora vamos escrever a congruência com a pergunta do enunciado, e usando as congruências (2.3) e (2.4), temos que

$$1211^{20} + 9119^{32} \cdot 343^{26} \equiv 1^{20} + 0^{32} \cdot 343^{26} \equiv 1 \bmod 11.$$

O resto da divisão de $1211^{20} + 9119^{32} \cdot 343^{26}$ por 11 é 1. Portanto a resposta correta é a letra b.

Exemplo 3.20: (Colégio Naval – 2011)

É correto afirmar que o número $5^{2011} + 2 \cdot 11^{2011}$ é múltiplo de:

a) 13

b) 11

c) 7

d) 5

e) 3

Resolução:

Como o enunciado da questão não deu um comando específico, vamos partir das alternativas. Daí, vamos calcular inicialmente o resto da divisão por 3, reescrevendo as congruências utilizando a observação 1.

$$5 \equiv 2 \equiv -1 \bmod 3, \quad (2.5)$$

$$11 \equiv 2 \equiv -1 \bmod 3 \quad (2.6)$$

Adotando o Corolário 2 nas congruências (2.5) e (2.6), obtemos:

$$5^{2011} \equiv (-1)^{2011} \bmod 3, \quad (2.7)$$

$$11^{2011} \equiv (-1)^{2011} \bmod 3 \quad (2.8)$$

Escrevendo a congruência com a pergunta da questão, e utilizando as congruências (2.7) e (2.8), temos

$$5^{2011} + 2 \cdot 11^{2011} \equiv (-1)^{2011} + 2 \cdot (-1)^{2011} \equiv -1 - 2 \equiv -3 \equiv 0 \bmod 3.$$

Como o resto encontrado foi zero, portanto $5^{2011} + 2 \cdot 11^{2011}$ é múltiplo de 3. Daí, a resposta correta é a letra e.

Exemplo 3.21: (Colégio Naval – 2012)

Em dois triângulos, T_1 e T_2, cada base é o dobro da respectiva altura. As alturas desses triângulos, h_1 e h_2, são números ímpares positivos. Qual é o conjunto dos valores possíveis de h_1 e h_2, de modo que a área de $T_1 + T_2$ seja equivalente a área de um quadrado de lado inteiro.

a) $\emptyset$

b) unitário

c) finito

d) {3, 5, 7, 9, 11, ...}

e) {11, 17, 23, 29, …}

Resolução:

O triângulo T_1 tem altura h_1 e base correspondente $2 \cdot h_1$. Logo sua área é:

$$S_{T1} = \frac{2 \cdot h1 \cdot h1}{2} = h_1^2.$$

O triângulo T_2 tem altura h_2 e base correspondente $2 \cdot h_2$. Portanto sua área é:

$$S_{T2} = \frac{2 \cdot h2 \cdot h2}{2} = h_2^2.$$

Seja a área $T_1 + T_2$ seja equivalente à área de um quadrado de lado $k \in \mathbb{Z}$, temos que

$$S_{T1} + S_{T2} = k^2 \Leftrightarrow h_1^2 + h_2^2 = k^2.$$

Como h_1 e h_2 são números ímpares positivos, podemos supor $h_1 = 2a + 1$ e $h_2 = 2b + 1$, com $a, b \in \mathbb{Z}_+$. Assim, temos:

$$h_1^2 + h_2^2 = k^2 \Leftrightarrow (2a + 1)^2 + (2b + 1)^2 = k^2 \Leftrightarrow 4(a^2 + b^2 + a + b) + 2 = k^2.$$

A última igualdade mostra que o número k^2, que é um quadrado perfeito, ao ser dividido por 4, deixa resto 2. Entretanto, os restos dos quadrados perfeitos por 4 são 0 ou 1. A seguir vamos provar esse fato.

Suponha o número par $n = 2t$ e o número ímpar $m = 2t + 1$, com $t \in \mathbb{Z}$. Fazendo $(n)^2 = (2t)^2 \Leftrightarrow n^2 = 4t^2$. Logo, n^2, que é um quadrado perfeito, é múltiplo de 4, ou seja, deixa resto zero ao ser dividido por 4. E ainda, $(m)^2 = (2t + 1)^2 \Leftrightarrow m^2 = 4t^2$

$+ 4t + 1 \Leftrightarrow m^2 = 4(t^2 + t) + 1$. Portanto, m^2, que é um quadrado perfeito, deixa resto 1 ao ser dividido por 4.

Assim, o quadrado de qualquer número inteiro deixa resto 0 ou 1, quando dividido por 4. Daí, não existem a e b que satisfaçam a igualdade $4(a^2 + b^2 + a + b) + 2 = k^2$ e, consequentemente, o conjunto dos valores de h_1 e h_2 que satisfazem as condições do enunciado é o conjunto vazio, já que o resto encontrado foi 2.

Logo, a resposta da questão é a letra ª

Exemplo 3.22: (Colégio Naval – 2017)

Os números x e y pertencem ao conjunto C = {17, 20, 23, 26, ..., 2018} e são tais que $x > y$. Sendo assim, pode-se concluir que $2017 \cdot 2^x + 8^y$, na divisão por 7, deixa resto:

a) 0

b) 1

c) 3

d) 4

e) 5

Resolução:

Inicialmente, observamos que todos os números do conjunto C deixam resto 2 na divisão por 3, ou seja, podem ser escritos na forma $3k + 2$, com $k \in \mathbb{N}$. Vamos calcular o resto de 2017 utilizando congruência módulo 7, segue que

$$2017 \equiv 1 \bmod 7. \quad (2.9)$$

Agora vamos encontrar o resto de 8^y usando congruência módulo 7, temos que:

$$8^y \equiv 1^y \equiv 1 \bmod 7. \quad (2.10)$$

Para calcular o resto de 2^x, vamos analisar as potências de 2 módulo 7, obtemos:

$$2^0 \equiv 1 \bmod 7,$$

$$2^1 \equiv 2 \bmod 7,$$

$$2^2 \equiv 4 \bmod 7,$$

$$2^3 \equiv 8 \equiv 1 \bmod 7,$$

$$2^4 \equiv 16 \equiv 2 \bmod 7.$$

Assim, temos um período de repetição do tamanho 3, o que permite concluir o seguinte:

$$2^{3k} \equiv 1 \bmod 7,$$

$$2^{3k+1} \equiv 2 \bmod 7,$$

$$2^{3k+2} \equiv 4 \bmod 7.$$

Onde k é um número natural qualquer. Como $x \in C$ e todo elemento do conjunto C é da forma 3k + 2, com $k \in \mathbb{N}$, então x = 3k + 2, temos que

$$2^x \equiv 2^{3k+2} \equiv 4 \bmod 7. \quad (2.11)$$

Das congruências (2.9), (2.10) e (2.11), segue que

$$2017 \cdot 2^x + 8^y \equiv 1 \cdot 4 + 1 \equiv 5 \bmod 7.$$

Portanto, o resto de $2017 \cdot 2^x + 8^y$ na divisão por 7 é 5. Daí, a resposta da questão é letra e.

Exemplo 3.23: (Colégio Naval – 2018)

Considere a expressão $(2018^{2018})^{2018}$, que é uma potência de uma potência. É correto afirmar que o último algarismo do resultado dessa expressão é:

a) 0

b) 2

c) 4

d) 6

e) 8

Resolução:

Primeiro devemos considerar uma informação importante do enunciado, que é o último algarismo do resultado da expressão, indicando a congruência módulo 10. Agora, vamos encontrar o último algarismo de 2018^{2018}, analisando esse número módulo 10, para isso usamos o Corolário 2, segue que

$$2018 \equiv 8 \bmod 10 \Leftrightarrow 2018^{2018} \equiv 8^{2018} \equiv (2^3)^{2018} \equiv 2^{6054} \bmod 10.$$

Para calcular o resto de 2^{6054}, temos que verificar as potências de 2 módulo 10, obtemos

$$2^1 \equiv 2 \bmod 10,$$

$$2^2 \equiv 4 \bmod 10,$$

$$2^3 \equiv 8 \bmod 10,$$

$$2^4 \equiv 16 \equiv 6 \bmod 10.$$

$$2^5 \equiv 32 \equiv 2 \bmod 10.$$

Assim, temos um período de repetição do tamanho 4, o que permite inferir o seguinte:

$$2^{4k+1} \equiv 2 \bmod 10,$$

$$2^{4k+2} \equiv 4 \bmod 10,$$

$$2^{4k+3} \equiv 8 \bmod 10,$$

$$2^{4k+4} \equiv 16 \equiv 6 \bmod 10.$$

Onde k é um número natural qualquer. Como queremos encontrar $2018^{2018} \equiv 2^{6054} \bmod 10$ (2.12), bastar efetuar a divisão de 6054 por 4, que é o período de repetição das potências de 2, temos que

$$6054 = 4 \cdot 1513 + 2$$

Com isso, 6054 = 4k + 2 (2.13), $k \in \mathbb{N}$. Calculando (2.12), a partir de (2.13), segue que

$$2018^{2018} \equiv 2^{6054} \equiv 2^{4k+2} \equiv 4 \bmod 10. \quad (2.14)$$

E ainda, temos que analisar $(2018^{2018})^{2018}$ módulo 10, usando (2.14), obtemos

$$(2018^{2018})^{2018} \equiv (4)^{2018} \equiv (2^2)^{2018} \equiv 2^{4036} \bmod 10.$$

Fazendo 4036 = 4 ·1009, obtemos

$$(2018^{2018})^{2018} \equiv 2^{4036} \equiv 2^4 \equiv 6 \bmod 10.$$

Logo, o último algarismo de $(2018^{2018})^{2018}$ é 6. Portanto, a resposta é a letra d.

Exemplo 3.24: (Colégio Naval – 2004)

Um número natural N deixa resto 2, quando dividido por 3; resto 3 quando dividido por 7; e resto 19 quando dividido por 41. Qual o resto do número k = (N+1) · (N+4) · (N+22) por 861?

a) 0

b) 13

c) 19

d) 33

e) 43

Resolução:

Inicialmente vamos utilizar o enunciado e montar três congruências, temos que

$$N \equiv 2 \bmod 3, \quad (2.15)$$

$$N \equiv 3 \bmod 7, \quad (2.16)$$

$$N \equiv 19 \bmod 41. \quad (2.17)$$

Das congruências (2.15), (2.16) e (2.17), e usando a proposição 2.4, temos

$$N + 1 \equiv 2 + 1 \equiv 3 \equiv 0 \bmod 3 \Leftrightarrow 3 \mid (N+1), \quad (2.18)$$

$$N + 4 \equiv 3 + 4 \equiv 7 \equiv 0 \bmod 7 \Leftrightarrow 7 \mid (N+4), \quad (2.19)$$

$$N + 22 \equiv 19 + 22 \equiv 41 \equiv 0 \bmod 41 \Leftrightarrow 41 \mid (N+22). \quad (2.20)$$

Como $3 \cdot 7 \cdot 41 = 861 \mid (N+1) \cdot (N+4) \cdot (N+22) = k$. Daí, o resto da divisão de k por 861 é 0. Logo, a resposta é a letra a.

Exemplo 3.25: (ENQ 2019 - 1 – b)

Prove, usando congruências, que $11^{n+2} + 12^{2n+1}$ é divisível por 133, para qualquer número natural n.

Resolução:

Primeiramente escreveremos a congruência de 11 módulo 133, temos que

$$11 \equiv 11 \bmod 133. \quad (2.18)$$

Da congruência (2.18), aplicando o Corolário 2 e a observação 1, obtemos

$$11^2 \equiv 11^2 = 121 \equiv -12 \bmod 133. \quad (2.19)$$

Agora vamos multiplicar ambos os membros da equivalência (2.19) por 11^n, proposição 6, segue que

$$11^2 \cdot 11^n \equiv -12 \cdot 11^n \bmod 133. \quad (2.20)$$

Da congruência (2.20), temos que

$$11^2 \cdot 11^n \equiv -12 \cdot 11^n \bmod 133 \Rightarrow 11^{n+2} \equiv -12 \cdot 11^n \bmod 133. \quad (2.21)$$

Com isso encontramos a primeira parcela da soma. Analisando a potência 12^{2n+1}, podemos notar que

$$12 \equiv 12 \bmod 133. \quad (2.22)$$

Da congruência (2.22), aplicando o Corolário 2.2 e a observação 2.1, obtemos

$$12^2 \equiv 12^2 = 144 \equiv 11 \bmod 133. \quad (2.23)$$

Agora vamos elevar ambos os membros da equivalência (2.23) por n, Corolário 2.2, note que

$$(12^2)^n \equiv 11^n \bmod 133. \quad (2,24)$$

Agora vamos multiplicar ambos os membros da equivalência (2.25) por 12, proposição 2.6, segue que

$$12^{2n} \cdot 12 \equiv 11^n \cdot 12 \bmod 133. \quad (2,25)$$

Da congruência (2.25), temos que

$$12^{2n} \cdot 12 \equiv 11^n \cdot 12 \bmod 133 \Rightarrow 12^{2n+1} \equiv 11^n \cdot 12 \bmod 133. \quad (2.26)$$

Então, encontramos exatamente o valor da segunda parcela da, de acordo com o enunciado da questão. Com esses resultados, obtivemos duas congruências, note que

$$11^{n+2} \equiv -12 \cdot 11^n \bmod 133, \quad (2.27)$$

$$12^{2n+1} \equiv 11^n \cdot 12 \bmod 133. \quad (2.28)$$

Das congruências (2.27) e (2.28), e aplicando a proposição 3 (i), segue que

$$11^{n+2} + 12^{2n+1} \equiv 0 \bmod 133. \quad (2.29)$$

Assim, provamos que $11^{n+2} + 12^{2n+1}$ é divisível por 133.

Exemplo 3.26: (OBMEP – 2017 b – Nível difícil)

Somando 1 a um certo número natural, obtemos um múltiplo de 11, subtraindo 1 desse mesmo número, obtemos um múltiplo de 8. Qual o resto do quadrado desse número por 88.

Resolução:

Seja x o número pedido. De acordo com o enunciado, temos que

$$x + 1 \equiv 0 \bmod 11, \quad (2.30)$$

$$x - 1 \equiv 0 \bmod 8. \quad (2.31)$$

Das congruências (2.30) e (2.31), e usando a proposição 2.4, note que

$$x + 1 - 1 \equiv 0 - 1 \bmod 11 \Leftrightarrow x \equiv -1 \bmod 11, \quad (2.32)$$

$$x - 1 + 1 \equiv 0 + 1 \bmod 8 \Leftrightarrow x \equiv +1 \bmod 8. \quad (2.33)$$

Das congruências (2.32) e (2.33), e aplicando o Corolário 2.2, segue que

$$x^2 \equiv 1 \bmod 11, \quad (2.34)$$

$$x^2 \equiv 1 \bmod 8. \quad (2.35)$$

Das congruências (2.34) e (2.35), e dispondo da proposição 7, obtemos

$$x^2 \equiv 1 \bmod 88. \quad (2.36)$$

Portanto, o resto de x^2 por 88 será 1.

Exemplo 3.27: (OBM – 2000 – 1ª fase – nível 1)

Se os números naturais são colocados em colunas, como se mostra abaixo, debaixo de que letra aparecerá o número 2000?

A	B	C	D	E	F	G	H	I
1		2		3		4		5
	9		8		7		6	
10		11		12		13		14
	18		17		16		15	
19		20		21		...		...

a) F

b) B

c) C

d) D

e) I

Resolução:

Escrevendo a sequência, temos: A, C, E, G, I, H, F, D, B. Já que a sequência se repete a cada 9 termos, para determinar a coluna em que estará o número 2000, devemos encontrar o resto da divisão de 2000 por 9, isto é, o número que é congruente a 2000 módulo 9, temos que

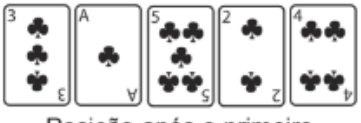
$$2000 \equiv 2 \bmod 9.$$

Logo, o número 2000 estará na mesma coluna que o número 2, ou seja, na coluna C. Assim, a resposta é a letra c.

Exemplo 3.28: (OBMEP – 2012– 1ª fase – nível 2)

Cinco cartas, inicialmente dispostas como na figura, serão embaralhadas. Em cada embaralhamento, a primeira carta passa a ser a segunda, a segunda passa a ser a quarta, a terceira passa a ser a primeira, a quarta passa a ser a quinta e a quinta passa a ser a terceira.

Posição inicial



Posição após o primeiro embaralhamento

Qual será a primeira carta após 2012 embaralhamentos?

A) 

B) 

C) 

D) 

E) 

Resolução:

Considera a disposição inicial das cartas: A, 2, 3, 4, 5.

Após o primeiro embaralhamento, a sequência das cartas será: 3, A, 5, 2, 4.

Após o segundo embaralhamento, a sequência das cartas será: 5, 3, 4, A, 2.

Após o terceiro embaralhamento, a sequência das cartas será: 4, 5, 2, 3, A.

Após o quarto embaralhamento, a sequência das cartas será: 2, 4, A, 5, 3.

Após o quinto embaralhamento, a sequência das cartas será: A, 2, 3, 4, 5.

Podemos perceber que a cada cinco embaralhamentos a sequência de cartas de repete. Então, para determinar a primeira carta da sequência após 2012 embaralhamentos, devemos determinar o número que é congruente a 12 módulo 5, note que

$$2012 \equiv 2 \bmod 5.$$

Portanto, após 2012 embaralhamentos a sequência de cartas será a mesma que depois dois embaralhamentos. Sendo assim, a primeira carta da sequência será o 5. Daí, a resposta é a letra e.

Exemplo 3.29: (ENQ 2023.1 – Questão 8)

Se b é um número inteiro e positivo tal que o mdc (b,17) = 1, prove que 17 divide pelo menos um dos números abaixo: $b^2 - 1$, $b^2 + 1$, $b^4 + 1$, $b^8 + 1$.

Resolução:

Como 17 é primo e mdc (b,17) = 1, usando o Teorema 2.1 e a proposição 2.7, temos que

$$b^{17-1} = b^{16} \equiv 1 \bmod 17.$$

Portanto, pela proposição 2, $17 \mid b^{16} - 1$. Agora, observando que

$$\begin{aligned} b^{16} - 1 &= (b^8 + 1) \cdot (b^8 - 1) \\ &= (b^4 + 1) \cdot (b^4 - 1) \cdot (b^8 + 1) \\ &= (b^2 + 1) \cdot (b^2 - 1) \cdot (b^4 + 1) \cdot (b^8 + 1). \end{aligned}$$

Concluímos que 17 divide pelo menos um dos fatores $b^2 - 1$, $b^2 + 1$, $b^4 + 1$, $b^8 + 1$.

Exemplo 3.30: (ENQ 2021.2 – Questão 1 - a)

Prove que $10^n - 1$ é divisível por 9, para todo $n \geq 1$.

Resolução:

Sabemos que 10 deixa resto 1 na divisão por 9, segue que

$$10 \equiv 1 \bmod 9. \qquad (2.37)$$

Da congruência (2.37), e aplicando o Corolário 2.2, para qualquer $n \geq 1$, temos que

$$10^n \equiv 1^n \bmod 9. \qquad (2.38)$$

Da congruência (2.38), e pela proposição 2.2, note que

$$10^n \equiv 1^n \bmod 9 \Leftrightarrow 9 \mid 10^n - 1.$$

Assim, $10^n - 1$ é divisível por 9.

Exemplo 3.31: (ENQ 2020.2 – Questão 7 - a)

Mostre que se $7 \mid a^2 + b^2$, onde a e b são números inteiros, então $7 \mid a$ e $7 \mid b$.

Resolução:

Dado um número inteiro n, que deixa resto r ao ser dividido por 7, onde $0 \leq r \leq 6$, e usando o Corolário2, segue que

$n \equiv 0 \bmod 7 \Rightarrow n^2 \equiv 0^2 \bmod 7 \Rightarrow n^2 \equiv 0 \bmod 7$,

$n \equiv 1 \bmod 7 \Rightarrow n^2 \equiv 1^2 \bmod 7 \Rightarrow n^2 \equiv 1 \bmod 7$,

$n \equiv 2 \bmod 7 \Rightarrow n^2 \equiv 2^2 \bmod 7 \Rightarrow n^2 \equiv 4 \bmod 7$,

$n \equiv 3 \bmod 7 \Rightarrow n^2 \equiv 3^2 \bmod 7 \Rightarrow n^2 \equiv 9 \bmod 7 \Rightarrow n^2 \equiv 2 \bmod 7$,

$n \equiv 4 \bmod 7 \Rightarrow n^2 \equiv 4^2 \bmod 7 \Rightarrow n^2 \equiv 16 \bmod 7 \Rightarrow n^2 \equiv 2 \bmod 7$,

$n \equiv 5 \bmod 7 \Rightarrow n^2 \equiv 5^2 \bmod 7 \Rightarrow n^2 \equiv 25 \bmod 7 \Rightarrow n^2 \equiv 4 \bmod 7$,

$n \equiv 6 \bmod 7 \Rightarrow n^2 \equiv 6^2 \bmod 7 \Rightarrow n^2 \equiv 36 \bmod 7 \Rightarrow n^2 \equiv 1 \bmod 7$.

Suponha que $7 \nmid a$ ou $7 \nmid b$, isto é, $a \not\equiv 0 \bmod 7$ ou $b \not\equiv 0 \bmod 7$. Analisando todas as possibilidades, obtemos

$$a^2 + b^2 \equiv 1, 2, 3, 4, 5, 6 \bmod 7.$$

Logo, $a^2 + b^2 \not\equiv 0 \bmod 7$. Portanto, se $7 \mid a^2 + b^2$, então $7 \mid a$ e $7 \mid b$.

Ainda nessa questão, cabe ressaltar que foi utilizada uma técnica de demonstração, que se chama Contraposição. Essa técnica é aplicada em problemas que apareçam o conectivo “se então”, e é o que ocorre na questão.

A técnica consiste em negar a hipótese e a tese, em seguida, inverter a posição desses elementos.

Se $7 \mid a^2 + b^2$, então $7 \mid a$ e $7 \mid b \Leftrightarrow$ Se $7 \nmid a$ ou $7 \nmid b$, então $a^2 + b^2 \not\equiv 0 \bmod 7$.

Com isso, nossos esforços se limitam em provar a negação da hipótese.

Exemplo 3.32: (ENQ 2020.2 – Questão 8)

Seja m um número natural. Dois números inteiros a e b são ditos congruentes módulo m se os restos da divisão euclidiana de a e b por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b \bmod m$$

Suponha que a, b, $m \in \mathbb{Z}$, com $m > 1$. Prove que $a \equiv b \bmod m$ se, e somente se, $m \mid b - a$.

Resolução:

Sejam $a = mq_1 + r_1$ e $b = mq_2 + r_2$, com $0 \leq r_1, r_2 < m$, as divisões euclidianas de a e b por m, respectivamente.

Suponha que $a \equiv b \bmod m$. Segue, da definição, que $r_1 = r_2$, segue que

$$b - a = m(q_2 - q_1) + r_2 - r_1 = m(q_2 - q_1) + r_2 - r_2 = m(q_2 - q_1).$$

Daí, $m \mid b - a$. Reciprocamente, suponha que $m \mid b - a$. Como $r_2 - r_1 = b - a - m(q_2 - q_1)$ e $m \mid b - a$, concluímos que $m \mid r_2 - r_1$. Sendo $0 \leq r_1, r_2 < m$, temos que $|r_2 - r_1| < m$, assim $r_1 = r_2$. Portanto, $a \equiv b \bmod m$

Exemplo 3.33: (ENQ 2020.1 – Questão 5 – a e b)

a) Quais são possíveis restos da divisão do quadrado de um número inteiro por 5? Uma tripla pitagórica é uma tripla de inteiros positivos a, b e c tais que $a^2 = b^2 + c^2$.

b) Use o item (a) para mostrar que em toda tripla pitagórica sempre há um múltiplo de 5?

Resolução:

a) Todo número inteiro deixa resto 0, 1, 2, 3, ou 4 quando dividido por 5. Desta forma, se n é um inteiro qualquer, temos uma, e apenas uma, das seguintes situações:

$n \equiv 0 \bmod 5 \Rightarrow n^2 \equiv 0^2 \bmod 5 \Rightarrow n^2 \equiv 0 \bmod 5$,

$n \equiv 1 \bmod 5 \Rightarrow n^2 \equiv 1^2 \bmod 5 \Rightarrow n^2 \equiv 1 \bmod 5$,

$n \equiv 2 \bmod 5 \Rightarrow n^2 \equiv 2^2 \bmod 5 \Rightarrow n^2 \equiv 4 \bmod 5$,

$n \equiv 3 \bmod 5 \Rightarrow n^2 \equiv 3^2 \bmod 5 \Rightarrow n^2 \equiv 9 \bmod 5 \Rightarrow n^2 \equiv 4 \bmod 5$,

$n \equiv 4 \bmod 5 \Rightarrow n^2 \equiv 4^2 \bmod 5 \Rightarrow n^2 \equiv 16 \bmod 5 \Rightarrow n^2 \equiv 1 \bmod 5$.

Daí, um quadrado perfeito deixa resto 0, 1 ou 4 quando dividido por 5.

No caso em que um dos inteiros a ou b é múltiplo de 5, não há o q provar. Suponhamos então que nem a nem b sejam múltiplos de 5. Então, deve ocorrer uma das possibilidades abaixo:

$a^2 \equiv 1 \bmod 5$ e $b^2 \equiv 1 \bmod 5 \Rightarrow a^2 + b^2 \equiv 2 \bmod 5 \Rightarrow c^2 \equiv 2 \bmod 5$,

$a^2 \equiv 4 \bmod 5$ e $b^2 \equiv 4 \bmod 5 \Rightarrow a^2 + b^2 \equiv 8 \bmod 5 \Rightarrow c^2 \equiv 3 \bmod 5$,

$a^2 \equiv 1 \bmod 5$ e $b^2 \equiv 4 \bmod 5 \Rightarrow a^2 + b^2 \equiv 5 \bmod 5 \Rightarrow c^2 \equiv 0 \bmod 5$,

$a^2 \equiv 4 \bmod 5$ e $b^2 \equiv 1 \bmod 5 \Rightarrow a^2 + b^2 \equiv 5 \bmod 5 \Rightarrow c^2 \equiv 0 \bmod 5$.

b) Pelo item (a) sabemos que os primeiros casos são impossíveis, já que os restos da divisão por 5 não podem ser 2 nem 3 e os dois últimos casos significam que c^2 e, portanto, c, é múltiplo de 5. Isso mostra que deve haver um múltiplo de 5 entre os inteiros a, b e c.

Exemplo 3.34: (ENQ 2019.2 – Questão 8 – b)

Resolução:

Como p é primo, pelo Corolário 2.3, temos que

$3^p \equiv 3 \bmod p \Leftrightarrow p \mid 3^p - 3$.

Escrevendo $3^p + 382 = 3^p - 3 + 385$, concluímos que $p \mid (3^p + 382)$ se, e somente se, $p \mid 385 = 5 \cdot 7 \cdot 11$. Portanto, p = 5, 7 ou 11.

Exemplo 3.35: (ENQ 2017.2 – Questão 6 – a e b)

Sejam a e b números inteiros e p um número primo. Prove que:

a) Se $p \mid a^p - b^p$, então $p \mid a - b$.

b) Se $p \mid a^p - b^p$, então $p^2 \mid a^2 - b^2$.

Resolução:

Suponha que $p \mid a^p - b^p$. Como p é primo, e aplicando o Corolário 2.3, note que

$a^p \equiv a \bmod p \Leftrightarrow p \mid a^p - a$, (2.39)

$b^p \equiv b \bmod p \Leftrightarrow p \mid b^p - b$. (2.40)

Das congruências (2.39) e (2.40), e pela proposição 2.3, obtemos

$a^p - b^p \equiv a - b \bmod p \Leftrightarrow p \mid a^p - b^p + a - b$.

Agora, como $p \mid a^p - b^p$, concluímos que $p \mid a - b$. Suponha que $p \mid a^p - b^p$. Segue que, usando o item (a),

$$p \mid a - b \Leftrightarrow a \equiv b \bmod p. \quad (2.41)$$

Da congruência (2.41), e aplicando o Corolário 2.2, note que

$$a \equiv b \bmod p \Leftrightarrow a^n \equiv b^n \bmod p.$$

Daí,

$a^{p-1} + a^{p-2}b + ... + ab^{p-2} + b^{p-1} \equiv b^{p-1} + b^{p-2}b + ... + bb^{p-2} + b^{p-1} \equiv pb^{p-1} \equiv 0 \bmod p$.

Como $a^p - b^p = (a - b)(a^{p-1} + a^{p-2}b + ... + ab^{p-2} + b^{p-1})$ e os dois fatores são divisíveis por p, concluímos que $p^2 \mid a^2 - b^2$.

Exemplo 3.36: (ENQ 2016.2 – Questão 8 – a e b)

Dados a, $n \in \mathbb{N}$, $a > 2$ ímpar, mostre que:

a) Se $\frac{a^n - 1}{2}$ é par, então a é da forma 4k + 1 ou n é par.

b) Se a é da forma 4k + 1 ou n é par, então $\frac{a^n - 1}{2}$ é par.

Resolução:

Suponha que $\frac{a^n - 1}{2}$ é par, segue que $\frac{a^n - 1}{2}$ = 2k, daí a^n = 4k + 1 ou equivalente $a^n \equiv 1 \bmod 4$. Como a é ímpar, $a \equiv 3 \equiv -1 \bmod 4$.Logo, n é par pois, caso contrário, teríamos $a^n \equiv -1 \bmod 4$. Suponhamos que a é da forma 4k + 1, segue que

$$a \equiv 1 \bmod 4. \qquad (2.41)$$

Da congruência (2.41), e pelo Corolário 2, note que

$$a^n \equiv 1 \bmod 4.$$

Portanto, $\frac{a^n - 1}{2}$ = 2k é par. Suponhamos eu n é par. Como a é ímpar, temos

$$a \equiv 1 \bmod 4 \text{ ou } a \equiv 3 \equiv -1 \bmod 4.$$

Nos dois casos, $a^n \equiv 1 \bmod 4$. Daí, $\frac{a^n - 1}{2}$ = 2k é par.

Exemplo 3.37: (ENQ 2016.1 – Questão 5)

Se p é um número natural primo, mostre que $2^{(p+1)^3} \equiv 256 \bmod p$.

Resolução:

Como p é primo, e através do Corolário 2.3, segue que

$$2^p \equiv 2 \bmod p. \qquad (2.42)$$

Da congruência (2.42), e aplicando o Corolário 2.2, temos que

$2^{p^2} = (2^p)^p \equiv 2^p \equiv 2 \bmod p$, (2.43)

$2^{p^3} = (2^p)^{p^2} \equiv 2^{p^2} \equiv 2 \bmod p$, (2.44)

$2^{3p^2} = (2^{p^2})^3 \equiv 2^3 \bmod p$, (2.45)

$2^{3p} = (2^p)^3 \equiv 2^3$. (2.46)

Das congruências (2.43), (2.44), (2.45) e (2.46), e sabendo que $(p+1)^3 = p^3 + 3p^2 + 3p + 1$, obtemos

$$2^{(p+1)^3} = 2^{p^3 + 3p^2 + 3p + 1} = 2^{p^3} \cdot 2^{3p^2} \cdot 2^{3p} \cdot 2^1 \equiv 2 \cdot 8 \cdot 8 \cdot 2 \equiv 256 \bmod p.$$

Portanto, $2^{(p+1)^3} \equiv 256 \bmod p$.

Exemplo 3.38: (ENQ 2015.2 – Questão 3 – a e b)

a) Calcule o resto da divisão de 28^{237} por 13.

b) Determine o algarismo das unidades do número $7^{(7^{1^{000}})}$

Resolução:

a) Dividindo 28 por 13 deixa resto 2. Note que

$$28 \equiv 2 \bmod 13. \qquad (2.47)$$

Da congruência (2.47), e pelo Corolário 2.2, segue que

$$28 \equiv 2 \bmod 13 \Rightarrow 28^2 \equiv 2^2 \equiv 4 \bmod 13, \qquad (2.48)$$

$$28 \equiv 2 \bmod 13 \Rightarrow 28^3 \equiv 2^3 \equiv 8 \bmod 13, \qquad (2.49)$$

$$28 \equiv 2 \bmod 13 \Rightarrow 28^4 \equiv 2^4 \equiv 16 \equiv 3 \bmod 13, \qquad (2.50)$$

$$28 \equiv 2 \bmod 13 \Rightarrow 28^6 \equiv 2^6 \equiv 64 \equiv -1 \bmod 13. \qquad (2.51)$$

Das congruências (2.48), (2.49), (2.50) e (2.51), e escrevendo $237 = 6 \cdot 39 + 3$, temos que

$$28^{237} \equiv 28^{6 \cdot 39 + 3} \equiv (28^6)^{39} \cdot 28^3 \equiv (-1) \cdot 8 \equiv -8 \equiv 5 \bmod 13.$$

Portanto, o resto da divisão de 28^{237} por 13 é 5.

(b) Calcular o algarismo das unidades do número $7^{(7^{1000})}$ equivale a encontrar o resto desse número por 10, e ainda temos que nos atentar a observação 1, e por fim do Corolário 2.2, note que

$$7 \equiv 7 \equiv -3 \bmod 10, \qquad (2.52)$$

$$7^2 \equiv (-3)^2 \equiv 9 \bmod 10, \qquad (2.53)$$

$$7^4 \equiv 9^2 \equiv 81 \equiv 1 \bmod 10, \qquad (2.54)$$

$$7^{4q} \equiv (7^4)^q \equiv 1 \bmod 10. \qquad (2.55)$$

Por outro lado, ainda usando a observação 2.1 e o Corolário 2.2, segue que

$$7 \equiv 3 \equiv -1 \bmod 4, \qquad (2.56)$$

$$7^{1000} \equiv (-1)^{1000} \equiv 1 \bmod 4, \qquad (2.57)$$

Da congruência (2.57), obtemos

$$7^{1000} = 4q + 1. \qquad (2.58)$$

Da congruência (2.55) e da igualdade (2.58), temos que

$$7^{(7^{1000})} \equiv 7^{4q+1} \equiv 7^{4q} \cdot 7 \equiv 1 \cdot 7 \bmod 10.$$

Logo, o algarismo das unidades do número $7^{(7^{1000})}$ é 7.

Exemplo 3.39: (ENQ 2015.1 – Questão 6)

Sejam a, b e c inteiros tais que $a^3 + b^3 + c^3$ é divisível por 9. Mostre que pelo menos um dos inteiros a, b ou c é divisível por 3.

Resolução:

Observamos primeiramente que, se um número n não divisível por 3 então ele é da forma 3k + 1 ou 3k + 2, logo n^3 é da forma 9k +1 ou 9k + 8.

Portanto, se n não divisível por 3 então $n^3 \equiv 1 \bmod 9$ ou $n^3 \equiv 8 \bmod 9$.

Suponha que nenhum dos inteiros a, b e c seja divisível por 3. Segue que os cubos desses números são congruentes a 1 ou a 8 módulo 9.

Considerando todas as possibilidades para a soma de três cubos teremos:

$a^3 + b^3 + c^3 \equiv 1 + 1 + 1 \equiv 3 \bmod 9$,

$a^3 + b^3 + c^3 \equiv 1 + 1 + 8 \equiv 10 \equiv 1 \bmod 9$,

$a^3 + b^3 + c^3 \equiv 1 + 8 + 8 \equiv 17 \equiv 8 \bmod 9$,

$a^3 + b^3 + c^3 \equiv 8 + 8 + 8 \equiv 24 \equiv 6 \bmod 9$.

Portanto, obtemos $a^3 + b^3 + c^3$ não é divisível por 9.

Exemplo 3.40: (ENQ 2014.1 – Questão 7)

Mostre que $a^7 \equiv a \bmod 21$, para todo inteiro a.

Resolução:

Sabendo que (3,7) = 1, e pelo Corolário 2.3, seguem as seguintes congruências:

$$a^7 \equiv a \bmod 7, \qquad (2.59)$$

$$a^3 \equiv a \bmod 3. \qquad (2.60)$$

Da congruência (2.60), aplicando o Corolário 2.2, temos

$$a^3 \equiv a \bmod 3 \Rightarrow (a^3)^2 \equiv a^2 \bmod 3 \Rightarrow a^6 \equiv a^2 \bmod 3. \qquad (2.61)$$

Da congruência (2.61), e pela proposição 2.6, obtemos

$$a^6 \equiv a^2 \bmod 3 \Rightarrow a^6 \cdot a \equiv a^2 \cdot a \bmod 3 \Rightarrow a^7 \equiv a^3 \bmod 3. \qquad (2.62)$$

Da congruência (2.62), e pelo a congruência (2.60), segue que

$$a^7 \equiv a^3 \equiv a \bmod 3. \qquad (2.63)$$

Das congruências (2.59) e (2.63), e pela proposição 2.7, note que

$$a^7 \equiv a \bmod [3,7] \Leftrightarrow a^7 \equiv a \bmod 21.$$

Logo, $a^7 \equiv a \bmod 21$.

Exemplo 3.41: (ENQ 2012.3 – Questão 7)

Mostre que, para todo $n \in \mathbb{N}$, é inteiro o número $\frac{1}{7} \cdot n^7 + \frac{1}{5} \cdot n^5 + \frac{23}{35} \cdot n$.

Resolução:

Pelo Corolário 2.3, temos as seguintes congruências

$$n^5 \equiv n \bmod 5, \qquad (2.64)$$

$$n^7 \equiv n \bmod 7. \qquad (2.65)$$

Das congruências (2.64) e (2.65), e usando a proposição 2.2, obtemos

$$n^5 \equiv n \bmod 5 \Leftrightarrow 5 \mid n^5 - n, \qquad (2.66)$$

$$n^7 \equiv n \bmod 7 \Leftrightarrow 7 \mid n^7 - n. \qquad (2.67)$$

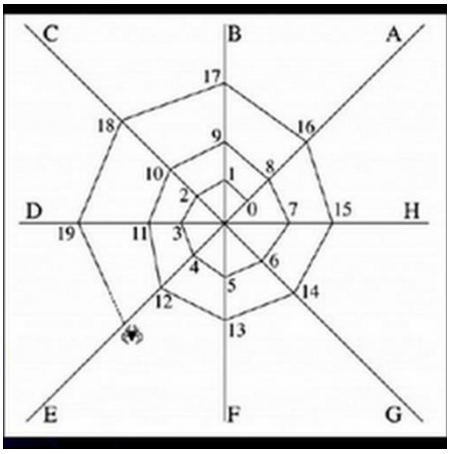
Reescrevendo $\frac{1}{7} \cdot n^7 + \frac{1}{5} \cdot n^5 + \frac{23}{35} \cdot n$, segue que

$$\frac{1}{7} \cdot n^7 + \frac{1}{5} \cdot n^5 + \frac{23}{35} \cdot n = \frac{n^7 - n}{7} + \frac{n^5 - n}{5} + n \qquad (2.68)$$

Das equivalências (2.66) e (2.67), e pela igualdade (2.68), obtemos que $\frac{1}{7} \cdot n^7 + \frac{1}{5} \cdot n^5 + \frac{23}{35} \cdot n$ é um número inteiro. Portanto, é inteiro o número $\frac{1}{7} \cdot n^7 + \frac{1}{5} \cdot n^5 + \frac{23}{35} \cdot n$.

Exemplo 3.42: (Banco de questões da OBMEP – Olimpíada Brasileira de Matemática das Escolas Públicas).

A, B, C, D, E, F, e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118.



Resolução:

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 $118 = 8 \cdot 14 + 6$. 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.

Exemplo 3.43: (ENQ 2021.2 – Questão 8)

Determine o resto da divisão por 19 do número

$S = 1^{18} + 2^{18} + 3^{18} + ... + 95^{18}$.

Resolução:

Primeiramente observamos que a soma possui cinco múltiplos de 19, ou seja, deixam resto zero na divisão por 19. Aplicando o Corolário 2.2, temos que

$$19 \equiv 0 \bmod 19 \Rightarrow 19^{18} \equiv 0^{18} \bmod 19,$$
$$38 \equiv 0 \bmod 19 \Rightarrow 38^{18} \equiv 0^{18} \bmod 19,$$
$$57 \equiv 0 \bmod 19 \Rightarrow 57^{18} \equiv 0^{18} \bmod 19,$$
$$76 \equiv 0 \bmod 19 \Rightarrow 76^{18} \equiv 0^{18} \bmod 19,$$
$$95 \equiv 0 \bmod 19 \Rightarrow 75^{18} \equiv 0^{18} \bmod 19.$$

Logo, das 95 parcelas da soma S, vamos considerar apenas os restos das 90 parcelas restantes, pois 5 parcelas deixam resto zero.

Como 19 é primo e mdc das noventa parcelas restantes com 19 é igual a 1, usando o pequeno Teorema de Fermat, proposição 7, segue que

$$1^{19-1} = 1^{18} \equiv 1 \bmod 19,$$
$$2^{19-1} = 2^{18} \equiv 1 \bmod 19,$$
$$3^{19-1} = 3^{18} \equiv 1 \bmod 19,$$
$$\vdots \qquad \vdots$$
$$94^{19-1} = 94^{18} \equiv 1 \bmod 19.$$

Daí, as noventa parcelas restantes possuem resto 1, cada uma, na divisão por 19. Totalizando noventa restos na divisão por 19, note que

$$S \equiv 1 + 1 + 1 + ... + 1 = 90 \bmod 19.$$

E ainda, o resto na divisão por 19 deve varia entre zero e 18, não podemos adotar 90 como resposta, para finalizar basta verificar o resto de 90 por 19, temos que $S \equiv 14 \bmod 19$. Portanto, o resto é igual a 14.

3.5 EQUAÇÕES DIOFANTINAS LINEARES

Exemplo 3.19:

Considere a equação 2x + 3y = 10, onde a = 2, b = 3 e c = 10. Verificamos que x_0 = 2 e y_0 = 2 é uma solução particular da equação acima. Basta substituir x_0 e y_0 na equação dada: $2 \cdot 2 + 3 \cdot 2 = 10$. Vejamos em que condições (1) admite soluções.

Exemplo 3.20:

Verifique se as equações 2x + 6y = 5 e 5x + 10y = 95 possuem soluções.

Resolução:

Primeiro, considerando 2x + 6y = 5, vamos calcular o mdc(2,6) = 2. Agora observamos que 2 não divide 5, então a equação não possui solução.

Segundo, considerando 5x + 10y = 95, e calculando mdc(5,10) = 5. Como 5 divide 95, a equação possui solução.

Exemplo 3.21:

Encontre a solução geral das equações diofantinas a seguir.

a) 14x + 26y = 48

Resolução:

Primeiro vamos verificar se a equação diofantina possui solução. Sabendo que a = 14, b = 26 e c = 48, temos que mdc (14,26) = 2 e 2|48, então a equação possui solução.

Como a, b e c são múltiplos de 2, podemos dividir a equação diofantina por 2. 14x + 26y = 48 $\Leftrightarrow$ 7x + 13y = 24, considerando a = 7, b = 13 e c = 24. Agora vamos achar uma solução particular, transformando a equação em uma congruência linear, temos: 7x + 13y = 24 $\Leftrightarrow$ $13x \equiv 24 \pmod 7$.

Dividindo 13x e 24 por 7 (mod 7), para substituí-los pelos respectivos restos, que são: 6x e 3. Reescrevendo a congruência linear.

$13x \equiv 24 \pmod 7 \Leftrightarrow 6x \equiv 3 \pmod 7$. Como 6 e 3 são múltiplos de 3, podemos colocá-los em forma de multiplicação: $3 \cdot 2x \equiv 3 \cdot 1 \pmod 7$. Como mdc (3,7) = 1, de acordo com a propriedade 3.6, podemos escrever: $2x \equiv 1 \pmod 7$.

Agora podemos usar as tentativas para a variável x, na última congruência linear encontrada.

x = 1, $2 \cdot 1 \equiv 1 (\text{mod } 7) \Leftrightarrow 2 \equiv 1 (\text{mod } 7)$. Verificamos que 2 ao ser dividido por 7, deixa resto 2, a congruência deixa resto 1. Logo, x = 1 não é solução da congruência linear.

x = 4, $2 \cdot 4 \equiv 1 (\text{mod } 7) \Leftrightarrow 8 \equiv 1 (\text{mod } 7)$. Verificamos que 8 ao ser dividido por 7, deixa resto 1, a congruência também deixa resto 1. Logo, x = 4 é solução da congruência linear.

Assim, $x_0 = 4$ é uma solução particular da equação Diofantina. Substituindo $x_0 = 4$ na equação, temos: $7 \cdot 4 + 13y = 24 \Leftrightarrow 28 + 13y = 24 \Leftrightarrow 13y = 24 - 28 \Leftrightarrow 13y = -4 \Leftrightarrow y = \frac{-4}{13}$.

Logo, o par de inteiros $x_0 = 4$ e $y_0 = \frac{-4}{13}$ é uma solução particular da equação.

Até agora a resolução não foi novidade, pois já efetuamos esses cálculos em exemplos anteriores. Agora, para achar a solução geral, vamos a proposição 3.3:

$$x = x_0 - bt \Leftrightarrow x = 4 - 13t$$

$$y = y_0 + at \Leftrightarrow y = \frac{-4}{13} + 7t$$

onde $t \in \mathbb{Z}$.

Logo, $x = 4 - 13t$ e $y = \frac{-4}{13} + 7t$, com $t \in \mathbb{Z}$. é a solução geral da equação Diofantina Linear.

b) 25x – 28y = 37

Resolução:

Reconhecendo os coeficientes da equação a = 25 b = - 28 e c = 37 e verificando se ela possui solução: mdc (25, -28) = mdc (25,28) = 1 e 1|37. Portanto a equação possui solução.

Reparem que só resolvemos exemplos, que os coeficientes eram positivos. No entanto, temos b = - 28. Quando isso acontecer, encontre uma solução particular colocando os coeficientes todos positivos, na forma ax + by = c.

Encontrando uma solução particular de (i) 25x + 28y = 37. Vamos transformar a equação em uma congruência linear.

$25x + 28y = 37 \Leftrightarrow 28y \equiv 37 (\text{mod } 25)$

Dividindo 28y e 37 por 25 (mod 25), para substituí-los pelos respectivos restos, que são: 3y e 12. Reescrevendo a congruência linear.

28y $\equiv$ 37 (mod 25) $\Leftrightarrow$ 3y $\equiv$ 12 (mod 25). Como 3 e 12 são múltiplos de 3, podemos colocá-los em forma de multiplicação:

3 $\cdot$ 1y $\equiv$ 3 $\cdot$ 4 (mod 25).

Como mdc (3,25) = 1, de acordo com a propriedade 3.6, podemos escrever: 1y $\equiv$ 4 (mod 25).

Dessa última congruência linear, já temos uma solução particular y_0 = 4.

Daí, y_0 = 4 é uma solução particular da equação Diofantina (i). Substituindo y_0 = 4 na equação, temos: 25x + 28 $\cdot$ 4= 37 $\Leftrightarrow$ 25x + 112= 37 $\Leftrightarrow$ 25x = 37 - 112 $\Leftrightarrow$ $25x = -75$ $\Leftrightarrow$ x = - 3.

Logo, o par de inteiros x_0 = - 3 e y_0 = 4 é uma solução particular da equação (i).

Para encontrar uma solução particular de 25x – 28y = 37, devemos usar a seguinte nota:

Quando os coeficientes de x e y numa equação Diofantina linear não são ambos positivos sua resolução pode ser feita mais facilmente observando que:

se (x_0,y_0) é solução de ax + by = c, então $(-x_0,y_0), (x_0,-y_0), (-x_0,-y_0)$ são soluções respectivamente de: -ax + by = c, ax - by = c e -ax - by = c

Ou seja, encontramos uma solução particular, como se a equação possui todos os coeficientes positivos, depois verificamos em qual forma ela se encaixa: -a e b, a e – b e -a e -b.

No nosso exemplo a equação é a e -b, com isso usamos $(x_0,-y_0)$.

Assim, o par de inteiros x_0 = - 3 e y_0 = 4, que é solução da equação com todos os coeficientes positivos, será escrito em $(x_0,-y_0)$, para sabermos uma solução particular de (ii) 25x – 28y = 37.

Portanto, $(-3,-4)$ é uma solução particular de (ii).

Agora, para achar a solução geral da equação 25x - 28y = 37, vamos usar a proposição 3.3

$$x = x_0 - bt \Leftrightarrow x = -3 - (-28)\,t \Leftrightarrow x = -3 + 28t$$

$$y = y_0 + at \Leftrightarrow y = -4 + 25t$$

onde t $\in \mathbb{Z}$.

Logo, x = -3 + 28t e y = -4 + 25t, com t $\in \mathbb{Z}$, é a solução geral da equação

Exemplo 3.22:

Dada a equação 3x + 4y = 20, encontre uma solução particular.

Resolução:

3x + 4y = 20. Inicialmente temos que a = 3, b = 4 e c = 20. O mdc (3,4) = 1 e como 1|20 a equação (i) possui solução.

Escrevendo 1 como multiplicações de 3 e 4 temos:

(ii) 3 · (-1) + 4 · 1 = 1

Multiplicando (ii) por 20, obtemos:

(iii) 3 · (-20) + 4 · 20 = 1 · 20

Logo, o par de inteiros x_0 = -20 e y_0 = 20 é uma solução particular da equação 3x + 4y = 20.

Observamos que esse método é utilizado, pois após escrever as multiplicações com resultado 1, podemos multiplicar a igualdade toda pelo c = 20.

Exemplo 3.23:

Dada a equação 3x + 5y = 50, encontre uma solução particular.

Resolução:

Primeiramente vamos utilizar fatoração por evidência, para escrever (i) 3x + 5y = 50 na forma do algoritmo da divisão euclidiana.

3x + 5y = 50 $\Leftrightarrow$ 3x + 3y + 2y = 50 $\Leftrightarrow$ (ii) 3 · (x+y) + 2y = 50. Percebemos que (ii) está escrito na forma do algoritmo da divisão, onde 50 é o dividendo, 3 o divisor e 2y o resto. Ao dividir 50 por 3, achamos 2 no resto. Daí, podemos escrever 2y = 2 $\Leftrightarrow$ y = 1. Logo, o par de inteiros x_0 = 15 e y_0 = 1 é uma solução particular da equação (i).

Exemplo 3.24: Encontre uma solução particular da equação x + 7y = 19.

Resolução: Inicialmente temos que a = 1, b = 7 e c = 19. O mdc (1,7) = 1 e como 1|19, a equação possui solução.

Agora basta considerar y = 0 e substituindo na equação, temos: x + 7 · 0 = 19 $\Leftrightarrow$ x = 19. Assim, o par de inteiros x_0 = 19 e y_0 = 0 é uma solução particular da equação.

Exemplo 3.25:

Encontre uma solução particular da equação 2x + 5y = 15.

Resolução:

Inicialmente temos que a = 2, b = 5 e c = 15. O mdc (2,5) = 1 e como 1|15, a equação possui solução.

Verificamos que o coeficiente b = 5 é múltiplo de c = 15, pois 5 · 3 = 15. Vamos considerar x = 0 e substituindo na equação, temos: 2 · 0 + 5y= 15 $\Leftrightarrow$ 5y= 15 $\Leftrightarrow$ y = 3. Assim, o par de inteiros x_0 = 0 e y_0 = 3 é uma solução particular da equação.

Exemplo 3.26:

Transforme a equação Diofantina em congruência linear e encontre uma solução particular.

a) 11x + 7y = 58

Resolução:

A equação informada possui a = 11, b = 7 e c = 58. Assim, teremos: 11x + 7y = 58 $\Leftrightarrow$ 11x $\equiv$ 58 (mod 7).

A seguir vamos encontrar uma solução particular da equação Diofantina, resolvendo a congruência linear. Cabe ressaltar que esse método é ensinado, pois a equação do exemplo não se encaixa em nenhum dos quatro métodos anteriores.

Primeiro vamos dividir 11x e 58 por 7 (mod 7), para substituí-los pelos respectivos restos, que são: 4x e 2. Reescrevendo a congruência linear encontrada: 11x $\equiv$ 58 (mod 7) $\Leftrightarrow$ 4x $\equiv$ 2 (mod 7). Agora podemos usar as tentativas para a variável x.

x = 1, $4 \cdot 1 \equiv 2 \pmod 7 \Rightarrow 4 \equiv 2 \pmod 7$. Verificamos que 4 ao ser dividido por 7, deixa resto 4, a congruência deixa resto 2. Logo, x = 1 não é solução da congruência linear.

x = 2, $4 \cdot 2 \equiv 2 \pmod 7 \Rightarrow 8 \equiv 2 \pmod 7$. Verificamos que 8 ao ser dividido por 7, deixa resto 1, a congruência deixa resto 2. Logo, x = 2 não é solução da congruência linear.

x = 3, $4 \cdot 3 \equiv 2 \pmod 7 \Rightarrow 12 \equiv 2 \pmod 7$. Verificamos que 12 ao ser dividido por 7, deixa resto 5, a congruência deixa resto 2. Logo, x = 3 não é solução da congruência linear.

x = 4, $4 \cdot 4 \equiv 2 \pmod 7 \Rightarrow 16 \equiv 2 \pmod 7$. Verificamos que 16 ao ser dividido por 7, deixa resto 2, a congruência também deixa resto 2. Logo, x = 4 é solução da congruência linear.

Assim, x_0 = 4 é uma solução particular da equação Diofantina. Substituindo x_0 = 4 na equação, temos: $11 \cdot 4 + 7y = 58 \Leftrightarrow 44 + 7y = 58 \Leftrightarrow 7y = 58 - 44 \Leftrightarrow 7y = 14 \Leftrightarrow y = 2$. Logo, o par de inteiros x_0 = 4 e y_0 = 2 é uma solução particular da equação.

4 RESOLUÇÃO DE QUESTÕES

Nesta parte apresentamos uma bateria de exercícios e suas respectivas resoluções, extraídos do banco de questões do concurso do Colégio Naval, da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas), da OBM (Olimpíada Brasileira de Matemática) e do ENQ (Exame Nacional de Qualificação do Mestrado PROFMAT). Os enunciados foram transcritos conforme aparecem nos bancos de questões, por este motivo as tabelas e as figuras não foram numeradas.

Diversas situações-problema do cotidiano dos alunos, dos Anos finais do Ensino Fundamental, os quais futuramente estarão no ensino superior, podem ser resolvidas utilizando o conceito de congruência modular, que nada mais é do que trabalhar com os restos achados através da divisão de números inteiros.

4.1 GENERALIZAÇÃO DO TEOREMA CHINÊS DO RESTO.

1) Resolva o sistema

   $X \equiv 2 \pmod 3$, $X \equiv 3 \pmod 4$, $X \equiv 4 \pmod 5$, $X \equiv 2 \pmod 6$.

Resolução:

Primeiro temos que verificar se o sistema possui solução, para isso temos que destacar as congruências lineares duas a duas, que possuem os módulos múltiplos e efetuar o máximo divisor comum entre eles.

$X \equiv 3 \pmod 4$, $X \equiv 2 \pmod 6$

Agora, calculamos (4,6) = 2 e verificamos: $3 \not\equiv 2 \pmod 2$ temos, pelo Teorema do Resto Chinês Generalizado, que o sistema não tem solução.

Observamos que o mdc será o módulo da congruência formada, o 3 e 2 são encontrados nas duas congruências lineares destacadas.

2) Resolva o sistema

   $X \equiv 1 \pmod 4$, $X \equiv 5 \pmod 6$, $X \equiv 2 \pmod 9$, $X \equiv 3 \pmod{10}$.

Resolução:

Primeiro temos que verificar se o sistema possui solução, para isso temos que destacar as congruências lineares duas a duas, que possuem os módulos múltiplos e efetuar o máximo divisor comum entre eles.

$X \equiv 1 \pmod 4$, $X \equiv 5 \pmod 6$

Agora, calculamos (4,6) = 2 e verificamos: $1 \equiv 5 \pmod 2$.

$X \equiv 1 \pmod 4$, $X \equiv 3 \pmod{10}$

Agora, calculamos (4,10) = 2 e verificamos: $1 \equiv 3 \pmod 2$.

$X \equiv 5 \pmod 6$, $X \equiv 2 \pmod 9$

Agora, calculamos (6,9) = 3 e verificamos: $5 \equiv 2 \pmod 3$.

$X \equiv 5 \pmod 6$, $X \equiv 3 \pmod{10}$

Agora, calculamos (6,10) = 2 e verificamos: $5 \equiv 3 \pmod 2$.

Pelo Teorema Chinês dos Restos Generalizado, que o sistema tem solução. Observa-se que as congruências lineares, que os módulos são múltiplos, têm que ser destacadas duas a duas. A solução do sistema será dada por:

$X = C_1 \cdot x_1 \cdot m_1 + C_2 \cdot x_2 \cdot m_2 + C_3 \cdot x_3 \cdot m_3 + C_4 \cdot x_4 \cdot m_4 + [a_1, a_2, a_3, a_4] \cdot n$, com $n \in \mathbb{Z}$, onde $x_1 \cdot m_1 + x_2 \cdot m_2 + x_3 \cdot m_3 + x_4 \cdot m_4 = 1$.

Das congruências lineares do sistema, temos:

$X \equiv 1 \pmod 4$, $C_1 = 1$ e $a_1 = 4$.

$X \equiv 5 \pmod 6$, $C_2 = 5$ e $a_2 = 6$.

$X \equiv 2 \pmod 9$, $C_3 = 2$ e $a_3 = 9$.

$X \equiv 3 \pmod{10}$, $C_4 = 3$ e $a_4 = 10$.

Calculando [4, 6, 9, 10] = 180

E ainda, temos:

$$m_1 = \frac{[a1,a2,a3,a4]}{a1} = \frac{[4,6,9,10]}{4} = \frac{180}{4} = 45.$$

$$m_2 = \frac{[a1,a2,a3,a4]}{a2} = \frac{[4,6,9,10]}{6} = \frac{180}{6} = 30.$$

$$m_3 = \frac{[a1,a2,a3,a4]}{a3} = \frac{[4,6,9,10]}{9} = \frac{180}{9} = 20.$$

$$m_4 = \frac{[a1,a2,a3,a4]}{a4} = \frac{[4,6,9,10]}{10} = \frac{180}{10} = 18.$$

Agora, vamos calcular x_1, x_2, x_3 e x_4, a partir de $x_1 \cdot m_1 + x_2 \cdot m_2 + x_3 \cdot m_3 + x_4 \cdot m_4 = 1$.

Se $x_1 \cdot 45 + x_2 \cdot 30 + x_3 \cdot 20 + x_4 \cdot 18 = 1$, então podemos encontrar $x_1 = x_2 = 1$, $x_3 = -1$ e $x_4 = -3$.

Portanto, a solução é dada por:

$X = C_1 \cdot x_1 \cdot m_1 + C_2 \cdot x_2 \cdot m_2 + C_3 \cdot x_3 \cdot m_3 + C_4 \cdot x_4 \cdot m_4 + [a_1, a_2, a_3, a_4] \cdot n$, com $n \in \mathbb{Z}$.

$X = 1 \cdot 1 \cdot 45 + 5 \cdot 1 \cdot 30 + 2 \cdot (-1) \cdot 20 + 3 \cdot (-3) \cdot 18 + 180 \cdot n = 45 + 150 – 40 – 162 = -7 \equiv 173 \pmod{180}$.

Daí, $X \equiv 173 \pmod{180}$.

E ainda, podemos escrever o conjunto: $S = \{173 + 180n;\ n \in \mathbb{Z}\}$.

3) Ache os inteiros que deixam restos 1, 2, 5, e 5, quando divididos respectivamente por 2, 3, 6 e 12.

<u>Resolução</u>:

Queremos encontrar a solução para o sistema:

$X \equiv 1 \pmod 2$, $X \equiv 2 \pmod 3$, $X \equiv 5 \pmod 6$, $X \equiv 5 \pmod{12}$.

Primeiro temos que verificar se o sistema possui solução, para isso temos que destacar as congruências lineares duas a duas, que possuem os módulos múltiplos e efetuar o máximo divisor comum entre eles.

$X \equiv 1 \pmod 2$, $X \equiv 5 \pmod 6$

Agora, calculamos (2,6) = 2 e verificamos: $1 \equiv 5 \pmod 2$.

$X \equiv 2 \pmod 3$, $X \equiv 5 \pmod 6$

Agora, calculamos (3,6) = 3 e verificamos: $2 \equiv 5 \pmod 3$.

$X \equiv 5 \pmod 6$, $X \equiv 5 \pmod{12}$

Agora, calculamos (6,12) = 6 e verificamos: $5 \equiv 5 \pmod 6$.

Pelo Teorema do Resto Chinês Generalizado, que o sistema tem solução. Observa-se que as congruências lineares, que os módulos são múltiplos, têm que ser destacadas duas a duas. A solução do sistema será dada por:

$X = C_1 \cdot x_1 \cdot m_1 + C_2 \cdot x_2 \cdot m_2 + C_3 \cdot x_3 \cdot m_3 + C_4 \cdot x_4 \cdot m_4 + [a_1, a_2, a_3, a_4] \cdot n$, com $n \in \mathbb{Z}$, onde $x_1 \cdot m_1 + x_2 \cdot m_2 + x_3 \cdot m_3 + x_4 \cdot m_4 = 1$.

Das congruências lineares do sistema, temos:

$X \equiv 1 \pmod 2$, $C_1 = 1$ e $a_1 = 2$.

$X \equiv 2 \pmod 3$, $C_2 = 2$ e $a_2 = 3$.

$X \equiv 5 \pmod 6$, $C_3 = 5$ e $a_3 = 6$.

$X \equiv 5 \pmod{12}$, $C_4 = 5$ e $a_4 = 12$.

Calculando [2, 3, 6, 12] = 12

E ainda, temos:

$m_1 = \frac{[a1,a2,a3,a4]}{a1} = \frac{[2,3,6,12]}{2} = \frac{12}{2} = 6.$

$m_2 = \frac{[a1,a2,a3,a4]}{a2} = \frac{[2,3,6,12]}{3} = \frac{12}{3} = 4.$

$m_3 = \frac{[a1,a2,a3,a4]}{a3} = \frac{[2,3,6,12]}{6} = \frac{12}{6} = 2.$

$m_4 = \frac{[a1,a2,a3,a4]}{a4} = \frac{[2,3,6,12]}{12} = \frac{12}{12} = 1.$

Agora, vamos calcular x_1, x_2, x_3 e x_4, a partir de $x_1 \cdot m_1 + x_2 \cdot m_2 + x_3 \cdot m_3 + x_4 \cdot m_4 = 1$.

Se $x_1 \cdot 6 + x_2 \cdot 4 + x_3 \cdot 2 + x_4 \cdot 1 = 1$, então podemos encontrar $x_1 = x_4 = 1$ e $x_2 = x_3 = -1$.

Portanto, a solução é dada por:

$X = C_1 \cdot x_1 \cdot m_1 + C_2 \cdot x_2 \cdot m_2 + C_3 \cdot x_3 \cdot m_3 + C_4 \cdot x_4 \cdot m_4 + [a_1, a_2, a_3, a_4] \cdot n$, com $n \in \mathbb{Z}$.

$X = 1 \cdot 1 \cdot 6 + 2 \cdot (-1) \cdot 4 + 5 \cdot (-1) \cdot 2 + 5 \cdot 1 \cdot 1 + 12 \cdot n = 6 - 8 - 10 + 5 = -7 \equiv 5 \pmod{12}$.

Daí, $X \equiv 5 \pmod{12}$.

E ainda, podemos escrever o conjunto: $S = \{5 + 12n;\ n \in \mathbb{Z}\}$.

4) Resolva o sistema

$X \equiv 4 \pmod 6$, $X \equiv 13 \pmod{15}$, $X \equiv 8 \pmod{14}$, $X \equiv 1 \pmod 7$.

Resolução:

Primeiro temos que verificar se o sistema possui solução, para isso temos que destacar as congruências lineares duas a duas, que possuem os módulos múltiplos e efetuar o máximo divisor comum entre eles.

$X \equiv 4 \pmod 6$, $X \equiv 13 \pmod{15}$

Agora, calculamos (6,15) = 3 e verificamos: $4 \equiv 13 \pmod 3$.

$X \equiv 4 \pmod 6$, $X \equiv 8 \pmod{14}$

Agora, calculamos (6,14) = 2 e verificamos: $4 \equiv 8 \pmod 2$.

$X \equiv 8 \pmod{14}$, $X \equiv 1 \pmod 7$

Agora, calculamos (7,14) = 7 e verificamos: $8 \equiv 1 \pmod 7$.

Pelo Teorema do Resto Chinês Generalizado, que o sistema tem solução. Observa-se que as congruências lineares, que os módulos são múltiplos, têm que ser destacadas duas a duas. A solução do sistema será dada por:

$X = C_1 \cdot x_1 \cdot m_1 + C_2 \cdot x_2 \cdot m_2 + C_3 \cdot x_3 \cdot m_3 + C_4 \cdot x_4 \cdot m_4 + [a_1, a_2, a_3, a_4] \cdot n$, com $n \in \mathbb{Z}$, onde $x_1 \cdot m_1 + x_2 \cdot m_2 + x_3 \cdot m_3 + x_4 \cdot m_4 = 1$.

Das congruências lineares do sistema, temos:

$X \equiv 4 \pmod 6$, $C_1 = 4$ e $a_1 = 6$.

$X \equiv 13 \pmod{15}$, $C_2 = 13$ e $a_2 = 15$.

$X \equiv 8 \pmod{14}$, $C_3 = 8$ e $a_3 = 14$.

$X \equiv 1 \pmod 7$, $C_4 = 1$ e $a_4 = 7$.

Calculando [6, 7, 14, 15] = 210

E ainda, temos:

$m_1 = \frac{[a1,a2,a3,a4]}{a1} = \frac{[6,7,14,15]}{6} = \frac{210}{6} = 35.$

$m_2 = \frac{[a1,a2,a3,a4]}{a2} = \frac{[6,7,14,15]}{15} = \frac{210}{15} = 14.$

$m_3 = \frac{[a1,a2,a3,a4]}{a3} = \frac{[6,7,14,15]}{14} = \frac{210}{14} = 15.$

$m_4 = \frac{[a1,a2,a3,a4]}{a4} = \frac{[6,7,14,15]}{7} = \frac{210}{7} = 30.$

Agora, vamos calcular x_1, x_2, x_3 e x_4, a partir de $x_1 \cdot m_1 + x_2 \cdot m_2 + x_3 \cdot m_3 + x_4 \cdot m_4 = 1$.

Se $x_1 \cdot 35 + x_2 \cdot 14 + x_3 \cdot 15 + x_4 \cdot 30 = 1$, então podemos encontrar $x_1 = 6$, $x_2 = -1$, $x_3 = 1$ e $x_4 = -7$.

Portanto, a solução é dada por:

$X = C_1 \cdot x_1 \cdot m_1 + C_2 \cdot x_2 \cdot m_2 + C_3 \cdot x_3 \cdot m_3 + C_4 \cdot x_4 \cdot m_4 + [a_1, a_2, a_3, a_4] \cdot n$, com $n \in \mathbb{Z}$.

$X = 4 \cdot 6 \cdot 35 + 13 \cdot (-1) \cdot 14 + 8 \cdot 1 \cdot 15 + 1 \cdot (-7) \cdot 30 + 210 \cdot n = 840 - 182 + 120 - 210 = 568 \equiv 148 \pmod{210}$.

Daí, $X \equiv 148 \pmod{210}$.

E ainda, podemos escrever o conjunto: S = { $148 + 210n;\ n \in \mathbb{Z}$}.

4.2 EQUAÇÕES DIOFANTINAS LINEAREAS

Questão 5 (Colégio Naval – 2009/2010).

Um funcionário usa uma empilhadeira para transportar bobinas de 70 kg ou de 45 kg, sendo uma de cada vez. Quantas viagens com uma carga deverá fazer, no mínimo, para transportar exatamente uma tonelada dessa carga?

(A) 18

(B) 17

(C) 16

(D) 15

(E) 14

Resolução:

Primeiramente vamos identificar as variáveis da questão, seja m o número de viagens com a carga de 70 kg e n o número de viagens com a carga de 45 kg. Dessa forma a equação representativa é: (i) 70m + 45n = 1000

Temos que o mdc(70,45) = 5 e a equação dada tem solução pois 5|1000. Dividindo (i) por 5, obtemos a equação equivalente: (ii) 14m + 9n = 200, onde o mdc (14,9) = 1.

Agora vamos achar uma solução particular, transformando a equação em uma congruência linear, temos:

14m + 9n = 200 $\Leftrightarrow$ 14m $\equiv$ 200 (mod 9).

Dividindo 14m e 200 por 9 (mod 9), para substituí-los pelos respectivos restos, que são: 5m e 2. Reescrevendo a congruência linear.

14m $\equiv$ 200 (mod 9) $\Leftrightarrow$ 5m $\equiv$ 2 (mod 9).

Agora podemos usar as tentativas para a variável m.

m = 1, $5 \cdot 1 \equiv 2$ (mod 9) $\Leftrightarrow$ 5 $\equiv$ 2 (mod 9). Verificamos que 5 ao ser dividido por 9, deixa resto 5, a congruência deixa resto 2. Logo, m = 1 não é solução da congruência linear.

m = 4, $5 \cdot 4 \equiv 2$ (mod 9) $\Leftrightarrow$ 20 $\equiv$ 2 (mod 9). Verificamos que 20 ao ser dividido por 9, deixa resto 2, a congruência também deixa resto 2. Logo, m = 4 é solução da congruência linear.

Assim, m_0 = 4 é uma solução particular da equação Diofantina. Substituindo m_0 = 4 na equação, temos: 14 · 4 + 9n= 200 ⇔ 56 + 9n= 200 ⇔ 9n = 200 – 56 ⇔ 9n = 144 ⇔ n = $\frac{144}{9}$ ⇔ n = 16

Logo, o par de inteiros m_0 = 4 e n_0 = 16 é uma solução particular da equação.

Até agora a resolução não foi novidade, pois já efetuamos esses cálculos em exemplos anteriores. Agora, para achar a solução geral:

$$m = m_0 + bt = 4 + 9t$$
$$n = n_0 - at = 16 - 14t$$

onde t $\in \mathbb{Z}$.

Logo, $m = 4 + 9t$ e $n = 16 - 14t$, com t $\in \mathbb{Z}$. é a solução geral da equação Diofantina.

Na busca de soluções não negativas devem ser satisfeitas as desigualdades:

m $\geq$ 0 e n $\geq$ 0, assim temos que 4 + 9t $\geq$ 0 e 16 – 14t $\geq$ 0

Isto é:

$$t \geq -\frac{4}{9} \approx \text{- 0,4 e t} \leq \frac{16}{14} \approx 1{,}1$$

o que implica que $\{t \in \mathbb{Z};\ 0 \leq t \leq 1\}$, assim t $\in$ {0,1} e temos duas possibilidades para as viagens, a saber:

Para t = 0, temos 4 viagens com a empilhadeira de 70 kg e 16 viagens com a empilhadeira de 45 kg.

Para t = 1, temos 13 viagens com a empilhadeira de 70 kg e 2 viagens com a empilhadeira de 45 kg.

Como foi pedido a quantidade mínima de viagens, devemos considerar t = 1. Assim, o total é de 15 viagens.

Questão 6 (Colégio Naval – 2021/2022).

Um estudante, no retorno às aulas, comprou quatro tipos de materiais escolares em duas lojas diferentes, conforme tabela abaixo.

LOJA	PRODUTO	PREÇO UNITÁRIO (R$)	TOTAL (R$)
PAPEL E	Lápis	3,00	50,00

CIA	Caderno	5,00	
PAPELARIA MIX	Marca texto	4,00	44,00
	Borracha	2,00	

Ao chegar em casa, o estudante percebeu que havia trazido o mesmo número de lápis e marca texto. Assinale a opção que corresponde à quantidade de borrachas compradas, sabendo que o estudante comprou o maior número possível de cadernos.

(A) 8
(B) 9
(C) 10
(D) 11
(E) 12

Resolução:

Seja x a quantidade de lápis e de marca texto, y a quantidade de cadernos e z a quantidade de borrachas.

A partir da tabela do enunciado, podemos escrever:

$$\begin{cases} 3x + 5y = 50 \\ 4x + 2z = 44 \end{cases} \Leftrightarrow \begin{cases} 3x + 5y = 50 \\ 2x + z = 22 \end{cases}$$

Os valores de x, y e z devem ser inteiros e positivos, pois foram comprados quatro tipos de materiais (ou seja, nenhum deles pode ser nulo).

Agora vamos resolver a equação diofantina (i) 3x + 5Y = 50.

Como o mdc(3,5) = 1 e 1|50, a equação (i) possui solução em $\mathbb{Z}$.

Vamos utilizar fatoração por evidência, para escrever (i) na forma do algoritmo da divisão.

3x + 5y = 50 $\Leftrightarrow$ 3x + 3y + 2y = 50 $\Leftrightarrow$ (ii) 3 $\cdot$ (x+y) + 2y = 50. Percebemos que (ii) está escrito na forma do algoritmo da divisão, onde 50 é o dividendo, 3 o divisor e 2y o resto. Ao dividir 50 por 3, achamos 2 no resto. Daí, podemos escrever 2y = 2 $\Leftrightarrow$ y = 1.

Logo, o par de inteiros x_0 = 15 e y_0 = 1 é uma solução particular da equação (i) e as demais soluções são dadas pelas fórmulas:

$$\begin{cases} x = x_0 + bt = 15 + 5t \\ y = y_0 - \text{at} = 1 - 3t \end{cases}, com\ t \in \mathbb{Z}$$

X $\geq$ 0 e y $\geq$ 0, assim temos que 15 + 5t $\geq$ 0 e 1 – 3t $\geq$ 0

Isto é:

t $\geq$ -3 e t $\leq \frac{1}{3} \approx$ 0,3, daí temos que -3 $\leq$ t $\leq$ 0,3. Temos qy=eu observar duas situações: a primeira é que t não pode ser igual a –3, pois ao substituir em x = 15 + 5t, verificamos que x = 0, o que é impossível por causa da natureza da questão. E por fim t $\in \mathbb{Z}$, ou seja, t não pode ser igual a 0,3.

o que implica que $\{t \in \mathbb{Z};\ -3 < t < 0{,}3\}$, assim t $\in$ {-2, -1, 0}. Daí, temos três possibilidades a saber:

Para t = -2, temos 5 lápis e marca texto e 7 cadernos.

Para t = -1, temos 10 lápis e marca texto e 4 cadernos.

Para t = 0, temos 15 lápis e marca texto e 1 caderno.

Como o enunciado informa que foram comprados o maior número possível de cadernos, devemos considerar t = - 2, ou seja, 5 lápis e 7 cadernos.

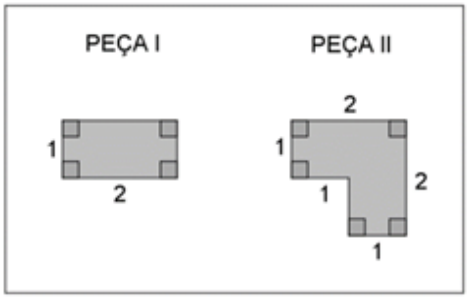
Considerando x = 5 e substituindo em (iii) $2x + z = 22$, obtemos:

$2x + z = 22 \Leftrightarrow$ 2 · (5) + z = 22 $\Leftrightarrow$ z = 12.

Portanto, foram compradas 12 borrachas.

Questão 7 (Colégio Naval – 2011/2012).

Observe a ilustração a seguir.



Qual a quantidade mínima de peças necessárias para revestir, sem falta ou sobra, um quadrado de lado 5, utilizando as peças acima.

(A) 12

(B) 11

(C) 10

(D) 9

(E) 8

Resolução:

Um comentário interessante, antes de iniciar a resolução, é que parece um problema de Geometria Euclidiana Plana, porém vamos usar conhecimento de equação Diofantina Linear.

Primeiramente verificamos que a peça I possui área S1 = 2 e a peça II possui área S2 = 2^2 - 1^2 = 3 e um quadrado de lado 5 possui área S3 = 25.

Supondo que sejam utilizadas x peças do tipo I e y peças do tipo II, para revestir o quadrado, então (i) 2x + 3y = 25.

É fácil perceber que o mdc(2,3) = 1 e a equação (i) tem solução pois 1|25.

Agora vamos achar uma solução particular, transformando a equação em uma congruência linear, temos: 2x + 3y = 25 $\Leftrightarrow$ 3y $\equiv$ 25 (mod 2).

Dividindo 3y e 25 por 2 (mod 2, para substituí-los pelos respectivos restos, que são: 1x e 1. Reescrevendo a congruência linear.

3y $\equiv$ 25 (mod 2) $\Leftrightarrow$ 1y $\equiv$ 1 (mod 2).

Assim, y_0 = 1 é uma solução particular da equação Diofantina. Substituindo y_0 = 1 na equação, temos: 2x + 3 $\cdot$ 1= 25 $\Leftrightarrow$ 2x + 3= 25 $\Leftrightarrow$ 2x = 25 – 3 $\Leftrightarrow$ 2x = 22 $\Leftrightarrow$ x = 11.

Logo, x_0 = 11 e y_0 = 1 é uma solução particular da equação (i) e as demais soluções são dadas pelas fórmulas:

$$\begin{cases} x = x_0 + bt = 11 + 3t \\ y = y_0 - at = 1 - 2t \end{cases}, \text{ com } t \in \mathbb{Z}$$

Na busca de soluções não negativas devem ser satisfeitas as desigualdades:

X $\geq$ 0 e y $\geq$ 0, assim temos que $11 + 3t \geq 0$ e $1 - 2t \geq 0$

Isto é:

t $\geq -\frac{11}{3} \approx -3{,}6\ e$ t $\leq \frac{1}{2}$ = 0,5, daí temos que - $\frac{11}{3} \leq$ t $\leq$ 0,5

o que implica que t $\in$ {-3, -2, -1, 0}. Com isso, temos quatro possibilidades a saber:

Para t = -3, temos 2 peças do tipo I e 7 peças do tipo II.

Para t = -2, temos 5 peças do tipo I e 5 peças do tipo II.

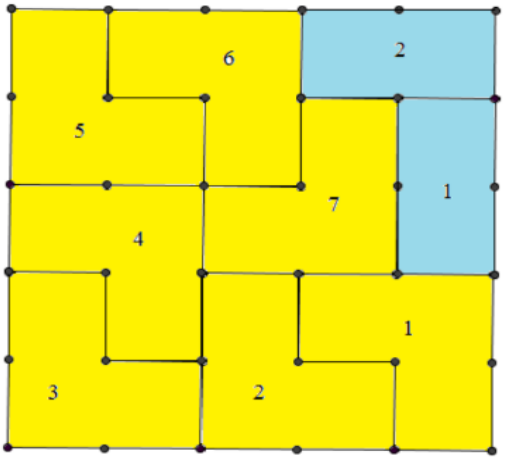
Para t = -1, temos 8 peças do tipo I e 3 peças do tipo II.

Para t = 0, temos 11 peças do tipo I e 1 peça do tipo II.

Para encontrar a quantidade mínima de peças, devemos obter o valor mínimo de x + y.

Logo, x = 2 e y = 7, totalizando nove peças.

A figura a seguir ilustra o caso encontrado acima



Questão 8 (Colégio Naval – 2001/2002).

Marta comprou petecas, bolas e bonecas, pagando por cada unidade, respectivamente, R$ 1,00, R$ 10,00 e R$ 20,00. Gastou R$ 220,00 em um total de 101 unidades de brinquedos. Quantas petecas ela comprou?

(A) 95

(B) 93

(C) 92

(D) 91

(E) 90

Resolução:

Se x denota a quantidade de petecas, y a quantidade de bolas e z a quantidade de bonecas então teremos as seguintes equações:

(i)x+ 10y + 20z = 220 e (ii) x + y + z = 101

Subtraindo (i) de (ii), obtemos uma equação Diofantina: (iii) 9y + 19z = 119

É fácil perceber que o mdc(9,19) = 1 e a equação (iii) tem solução pois 1|119.

Agora vamos achar uma solução particular, transformando a equação em uma congruência linear, temos: 9y + 19z = 119 $\Leftrightarrow$ 19z $\equiv$ 119 (mod 9).

Dividindo 19z e 119 por 9 (mod 9), para substituí-los pelos respectivos restos, que são: 1z e 2. Reescrevendo a congruência linear.

19z $\equiv$ 119 (mod 9) $\Leftrightarrow$ 1z $\equiv$ 2 (mod 9).

Assim, z_0 = 2 é uma solução particular da equação Diofantina. Substituindo z_0 = 2 na equação, temos: 9y + 19 · 2= 119 $\Leftrightarrow$ 9y + 38 = 119 $\Leftrightarrow$ 9y = 119 – 38 $\Leftrightarrow$ 9y = 81 $\Leftrightarrow$ y = 9.

Daí, y_0 = 9 e z_0 = 2 é uma solução particular da equação (iii) e as demais soluções são dadas pelas fórmulas:

$$\begin{cases} y = y_0 + \mathrm{bt} = 9 + 19t \\ z = z_0 - at = 2 - 9t \quad ,com\ t \in \mathbb{Z} \end{cases}$$

Como o número de petecas, bolas e bonecas é um inteiro e positivo devemos restringir a resposta de modo que escolhendo t sejam satisfeitas as desigualdades:

y > 0 e z > 0, assim temos que 9 + 19t > 0 e 2 – 9t > 0

Isto é:

t < $-\frac{9}{19} \approx$ -0,4 t < $\frac{2}{9} \approx$ 0,2, daí temos que t = 0.

O que implica que:

Para t = 0, temos 9 bolas e 2 bonecas.

Para encontrar a quantidade de petecas, que é solicitada no enunciado, vamos substituir a quantidade de bolas e bonecas em (ii).

Substituindo temos: x + 9 + 2 = 101 $\Leftrightarrow$ x = 90.

Assim, o número de petecas é 90.

5 CONSIDERAÇÕES FINAIS

Ainda que alguns elementos da Aritmética Modular, como congruência modular e equações Diofantinas Lineares, não fazerem parte do currículo da Educação Básica o projeto de inserir estes assuntos nessa fase escolar seria muito relevante pois poderia contribuir e incentivar a aprendizagem dos alunos. Reconhecemos que embora o nosso público alvo seja muito jovem, isto é, discentes a partir do 6º ano do ensino fundamental, estas teorias são de fácil assimilação, por isso, poderiam ser praticadas, tanto para a obtenção de novos conhecimentos, que melhorariam o desempenho de atividades cotidianas dos alunos, como para a preparação de concursos públicos.

A metodologia difundida também tem o propósito de disponibilizar conteúdos necessários, para que o universitário possa avançar adquirindo conhecimentos, que muitas das vezes não foram ensinados na Educação Básica, esclarecendo os fundamentos matemáticos utilizados nas escolas. O ensino da generalização do Teorema Chinês do Resto, vem enriquecer a proximidade do aluno com a matemática, no sentido de prepará-los para as disciplinas do Ensino Superior.

Desta maneira, acreditamos que a Teoria da Aritmética Modular, poderia colaborar de forma considerável para a evolução do discente e que a organização que sugerimos, associando conceitos a exemplos e como eles podem ser eficazes na vidas das pessoas, satisfazem a atual predisposição do ensino de matemática, de prevalecer pelo raciocínio e contextualização em vez do processo de decorar e aplicar conceitos em exercícios de fixação.

REFERÊNCIAS

BORGES, Fábio Vieira de Andrade. **Equações Diofantinas Lineares em Duas Incógnitas e Suas Aplicações**. 2013. 67f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Federal de Goiás, Goiás, 2013.

BRAGA, Eliaze da Silva; do CARMO, Renato Cardoso. **Aplicações de Equações Diofantinas**. 2018. 44f. Monografia – Universidade Federal do Amapá, Macapá, 2018.

BRASIL, Casa Civil. **Lei Nº 9.394, de 20 de dezembro de 1996**. Estabelece as diretrizes e bases da educação nacional. Brasília, DF, 20 dez. 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 25 nov. 2023.

BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Versão em revisão, 2017. Disponível em: http://basenacionalcomum.mec.gov.br/. Acesso em: 25 nov. 2023.

CMRJ. **Colégio Militar do Rio de Janeiro**. 2012. Disponível em: https://www.cmrj.eb.mil.br/provas-anteriores . Acesso em: 25 nov. 2023.

Da SILVA, Sandra Elisa Ramalho. **Uma experiência de ensino de matemática usando robótica educacional**. 2023. 94f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Federal Fluminense, Niterói, 2023.

De OLIVEIRA, Luisa Mara Silva. **Estratégias para o ensino e aprendizagem de funções polinomias do 1º e 2º grau em turmas de 9º do ensino fundamental II**. 2023. 125f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Federal Fluminense, Niterói, 2023.

De SOUZA, Letícia Vasconcellos. **Congruência modular nas séries finais do ensino fundamental**. 2015. 41f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Federal de Juiz de Fora, Minas Gerais, 2015.

DOMINGUES, Hygino, H. **Fundamentos de Aritmética**. São Paulo: Editora Atual, 1991.

Dos SANTOS, Filipe da Costa Neves. **Educação financeira dentro do ensino de matemática na educação básica – algumas possíveis abordagens nos anos finais do ensino fundamental 2**. 2023. 141f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Federal Fluminense, Niterói, 2023.

Exame Nacional de Qualificação – PROFMAT. Disponível em: <https://profmat-sbm.org.br/exame-nacional-de-qualificacao/>. Acesso em: 16 fev. 2024.

FERREIRA, Rosiane Barros. **Congruência modular no ensino básico**. 2018. 49f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Federal do Maranhão, São Luis, 2018.

GOMES, Ataniel Rogério Gonçalves. **Uma abordagem do ensino de congruência na educação básica**. 2015. 77f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Federal de Sergipe, Sergipe, 2015.

HEFEZ, A. **Elementos de Aritmética**. 3. Ed. Rio de Janeiro: SBM, 2022.

OBM - Olimpíada Brasileira de Matemática. Disponível em: <https://www.obm.org.br/como-se-preparar/provas-e-gabaritos/>. Acesso em: 16 jan. 2023.

Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP | Somando novos talentos para o Brasil. Disponível em: <https://www.obmep.org.br/provas.htm>. Acesso em: 21 dez. 2023.

POMMER, Wagner M. As Equações Diofantinas Lineares e o novo Ensino médio. **Boletim Grupo de Estudos e Pesquisas em Educação Matemática.** BOLETIM GEPEM, Nº 58 – JAN. / JUN. 2011, 51 – 70.

SILVA, Diego Adriano; BRITO, Arnaldo Silva; de SOUSA Valdirene Gomes. Equações Diofantinas Lineares: um estudo com estudantes do 1º ano do Ensino médio. **Revista Eletrônica da Matemática**. REMAT, Bento Gonçalves, RS, Brasil, V.6, n. 2, p. e2009, 25 de novembro de 2020.

SSPM. **Serviço de Seleção de Pessoal da Marinha**. Disponível em: https://www.marinha.mil.br/sspm/colegionaval/colegio_princ . Acesso em: 25 nov. 2023.

SSPM. **Serviço de Seleção de Pessoal da Marinha**. Disponível em: https://www.marinha.mil.br/sspm/?q=colegionaval/a-cn-provag . Acesso em: 25 nov. 2023.

APÊNDICE

SEQUÊNCIA DIDÁTICA PARA O ENSINO DE TÓPICOS DA ARITMÉTICA MODULAR NOS ANOS FINAIS DO ENSINO FUNDAMENTAL

ORIENTADOR: PROF. DR. ALDO AMILCAR BAZAN PACORICONA

DISCENTE: WANDERLAN CARMINATTI DE OLIVEIRA

NITERÓI
ABRIL/2024

LISTA DE FIGURAS

LISTA DE QUADRO

SUMÁRIO

1 INTRODUÇÃO

Este produto educacional, caderno de atividades, é referente a dissertação intitulada “Elementos da Aritmética Modular e o seu papel nos anos finais do ensino fundamental e no ensino superior”, consequência da pesquisa ligada ao Programa de Mestrado Profissional em Matemática em Rede Nacional, vinculado ao Instituto de Matemática e Estatística, da UFF (Universidade Federal Fluminense).

Este tem como finalidade complementar e sustentar as orientações metodológicas recomendadas na última unidade do trabalho citado acima. Está fracionada em três sequências constituídas por parte teórica, tendo como continuidade recomendações de exercícios do banco de questões do concurso do Colégio Naval, da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas), e da OBM (Olimpíada Brasileira de Matemática), que buscam potencializar a aprendizagem do assunto compreendido.

São elas:

I. Congruências modulares.
II. Equações Diofantinas Lineares.

2 ORIENTAÇÕES AO PROFESSOR

Este material é composto por 10 atividades que abordam a resolução de problemas de congruência modular e equações Diofantinas Lineares. Todas as atividades foram desenvolvidas para aplicação no 8°e 9º ano do Ensino Fundamental. Contudo, dependendo do entusiasmo da turma e do nível de desenvolvimento, o professor pode ficar à vontade para aplicar as atividades em suas turmas.

2.1 ORIENTAÇÕES AO DISCENTE

Este material é composto por 10 atividades que abordam a resolução de problemas de congruência modular e equações Diofantinas Lineares. Todas as atividades foram desenvolvidas para aplicação no 8°e 9º ano do Ensino Fundamental. É importante que os alunos intensifiquem os estudos no conteúdo de algoritmo da divisão de Euclides, pois esse é peça essencial para o entendimento dos problemas propostos.

3 SEQUÊNCIA DIDÁTICA

Nesta, atribui-se que a audiência possua conhecimentos pregressos sobre:

- Múltiplos e divisores de um número inteiro.
- Algoritmo da Divisão de Euclides.
- Máximo Divisor Comum.
- Mínimo Múltiplo Comum.

Na hipótese de os discentes não tenham domínio dos assuntos mencionados, orienta-se que utilizem as unidades 2 e 3 da dissertação citada, com o intuito de auxiliar na resolução das questões.

3.1 CONGRUÊNCIA MODULAR

Objetivo:

- Alcançar os conceitos e definições de congruência modular.
- Apresentar as principais propriedades de congruência modular.

Material necessário: Lousa, pilotos coloridos, videoaulas de sua preferência sobre o tema.

Tipo de atividade: individual.

Duração: 6 aulas de 50 minutos.

Neste primeiro instante é essencial uma aula expositiva, com registros de conceitos e definições. Para isso, pode-se utilizar o próprio quadro da sala de aula com auxílio de pilotos coloridos. Entretanto, se tiver a chance de exibir uma mídia digital, recomenda-se que utilize videoaulas de sua preferência sobre o assunto.

Registros para serem apresentados na lousa:

3.1.1 Introdução ao estudo de congruência modular

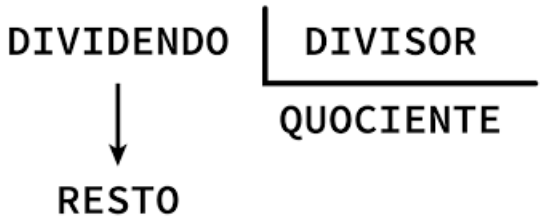
Primeiramente é necessário realizar uma revisão sobre o Algoritmo da Divisão:
Dicas → Deve-se exemplificar oralmente com exemplos lúdicos que façam parte do cotidiano dos alunos, para melhor compreensão.
Tipo:

- Temos 42 frutas que serão divididas entre 6 alunos, quantas frutas cada aluno receberá? (Nesse momento, é interessante usar o nome de seis estudantes presentes na sala de aula). Após a reposta da turma, escrever o Algoritmo da

divisão na lousa: $42 = 6 \cdot 7 + 0$, ressaltando que o zero é o resto da divisão, e com isso temos que 42 é múltiplo de 6.

- A reunião de Paulo receberá 7 convidados, que receberão lembranças confeccionadas por sua mãe. Sabendo que foram produzidos 20 brindes, quantas lembranças cada convidado receberá? E ainda, perguntar se sobrarão lembranças nessa ocasião. Em seguida, espera a resposta dos discentes, e registre o Algoritmo da divisão na lousa: $20 = 7 \cdot 2 + 6$.

Algoritmo da Divisão: É um método para dividir um número por outro, obtendo um quociente como resultado e, algumas vezes, um resto. Além das duas partes citadas, temos o dividendo e o divisor.



Exemplo 3.1:

Efetue a divisão de 17 por 5, utilizando o Algoritmo da divisão. Em seguida, destaque o dividendo, divisor, quociente e o resto

Resolução:

$$17 = 5 \cdot 3 + 2$$

Onde: Dividendo = 17, divisor = 5, quociente = 3 e o resto = 2.

Passada a revisão do conteúdo citado acima, é imprescindível mostrar que o Algoritmo da divisão pode ser reescrito na forma de congruência modular. É importante salientar que essa transformação vai oferecer a utilização de propriedades importantes, primordiais na resolução dos exercícios propostos futuramente.

Dica → Utilize cores diferentes para representar os elementos do Algoritmo da divisão, e use essas mesmas cores para reescrever no formato de congruência modular.

Dado o Algoritmo da divisão $34 = 6 \cdot 5 + 4$, temos: Dividendo = 34, divisor = 6, quociente = 5 e o resto = 4, que será reescrito na forma: $34 \equiv 4 \pmod 6$.

Essa nova forma significa que 34 e 4 deixam o mesmo resto 4, quando são divididos por 6 separadamente. E reparem que ao escrever a congruência modular usamos o dividendo, o resto e o divisor.

Exemplo 3.2:

Dada a divisão de 57 por 9, escreva o Algoritmo da divisão e, em seguida, transforme o algoritmo em congruência modular.

Resolução:

$57 = 9 \cdot 6 + 3$ temos: Dividendo = 57, divisor = 9, quociente = 6 e o resto = 3, que será reescrito na forma: $57 \equiv 3 \pmod 9$.

Após mostrar que o Algoritmo da divisão pode ser reescrito como congruência modular, trabalharemos com algumas propriedades.

Propriedades importantes de congruência modular

Propriedade 3.1: $a \equiv b \pmod m \Leftrightarrow a + c \equiv b + c \pmod m$.

Exemplo 3.3:

Dada a congruência $10 \equiv 3 \pmod 7$. Agora vamos somar 5 a ambos os membros:

$10 + 5 \equiv 3 + 5 \pmod 7 \Leftrightarrow 15 \equiv 8 \pmod 7$.

Propriedade 3.2: $a \equiv b \pmod m \Leftrightarrow a - c \equiv b - c \pmod m$.

Exemplo 3.4**:**

Dada a congruência $10 \equiv 3 \pmod 7$. Agora vamos subtrair 2 a ambos os membros: $10 - 2 \equiv 3 - 2 \pmod 7 \Leftrightarrow 8 \equiv 1 \pmod 7$.

Propriedade 3.3: $a \equiv b \pmod m \Leftrightarrow a \cdot c \equiv b \cdot c \pmod m$.

Exemplo**:**

Dada a congruência $10 \equiv 3 \pmod 7$. Agora vamos multiplicar 2 a ambos os membros:$10 \cdot 2 \equiv 3 \cdot 2 \pmod 7 \Leftrightarrow 20 \equiv 6 \pmod 7$.

Propriedade 2.4: $a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$.

Exemplo 3.5**:**

Dada a congruência $10 \equiv 3 \pmod 7$. Agora vamos elevar ambos os membros da congruência a 11: $10 \equiv 3 \pmod 7 \Rightarrow 10^{11} \equiv 3^{11} \pmod 7$.

Como a propriedade 2.4 é muito importante, vamos a outro exemplo.

Exemplo 3.6:

Ache o resto da divisão de 2^{45} por 7.

Resolução:

Como 8 e 1 deixam o mesmo resto 1, quando divididos por 7, podemos escrever:

$8 \equiv 1 \pmod 7$. E ainda, $2^3 = 8$. Daí, temos:

$2^3 \equiv 1 \pmod 7 \Rightarrow (2^3)^{15} \equiv 1^{15} \pmod 7 \Rightarrow 2^{45} \equiv 1 \pmod 7$.

Portanto, o resto da divisão de 2^{45} por 7 é 1.

Observação 3.1: Uma congruência modular pode ser reescrita somando ou subtraindo os múltiplos do módulo, do lado direito da congruência.

Exemplo 3.7:

Considere a congruência $17 \equiv 2 \bmod 5$, que pode ser reescrita de várias maneiras: $17 \equiv 2 + 5 \bmod 5 \Leftrightarrow 17 \equiv 7 \bmod 5$, $17 \equiv 2 - 5 \bmod 5 \Leftrightarrow 17 \equiv -3 \bmod 5$.

Exemplo 3.8:

Dada a congruência modular $13 \equiv 6 \bmod 7$, que será reescrita subtraindo o módulo 7 do lado direito, segue que: $13 \equiv 6 - 7 \bmod 7 \Leftrightarrow 13 \equiv -1 \bmod 7$. Essa ferramenta é muito utilizada, pois ficamos com -1 do lado direito, e com isso é possível aplicar o Corolário 2, colocando um expoente com valor alto e não alterará em nada, já que um dos números elevados a esse expoente será -1.

A seguir, serão apresentadas questões do assunto congruência modular e suas respectivas resoluções.

Questão 1 (OBMEP – 2010 – nível 1 – 1ª fase)

Paula iniciou um programa de ginástica no qual os dias de treino são separados por dois dias de descanso. Se o primeiro treino foi em uma segunda-feira, em qual dia da semana cairá o centésimo treino?

a) Domingo
b) Segunda-feira
c) Terça-feira
d) Quinta-feira
e) Sexta-feira

Resolução:

Podemos organizar a sequência de dias da semana em que Paula realizará seus treinos em uma tabela, como mostrado abaixo:

Segunda-feira	1º treino					8º treino
Terça-feira					6º treino	
Quarta-feira				4º treino		
Quinta-feira		2º treino				
Sexta-feira					7º treino	
Sábado				5ºtreino		
Domingo			3ºtreino			

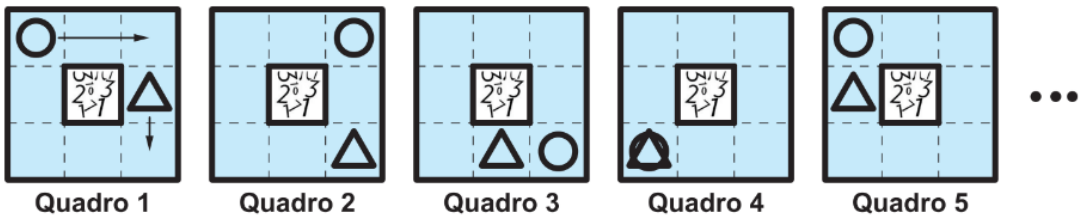
Podemos observar que depois do sétimo treino a ordem dos dias da semana para os próximos treinos se repetirá. Então, devemos encontrar o número que é resto da divisão de 100 por 7, isto é, o número que é congruente a 100 módulo 7. Temos que:

$$100 \equiv 2 \bmod 7.$$

Portanto, podemos concluir que o centésimo treino será no mesmo dia do segundo treino, ou seja, em uma quinta-feira.

Questão 2 (OBMEP – 2015 – nível 1 – 2ª fase)

Na sequência de quadros abaixo, uma bolinha e um triângulo caminham no sentido horário pelas casas sombreadas. De um quadro para o seguinte, o triângulo passa de uma casa para a casa vizinha, e a bolinha pula uma casa. Desenhe a bolinha e o triângulo do quadro 2015.



Resolução:

Podemos perceber pela Figura que a cada 8 quadros, a sequência de desenhos se repete. Como queremos saber o quadro 2015, temos que encontrar o resto da divisão de 2015 por 8, isto é, o número que é congruente a 2015 módulo 8, segue que

$2015 \equiv 7 \bmod 8$.

Logo, concluímos que o quadro 2015 será igual ao quadro 7.

Questão 3 (Olimpíada Regional de Matemática de Santa Catarina – 2017 – Nível Intermediário)

Jucavo propõe o seguinte desafio: “Eu vou pensar em um número. A seguir, darei três dicas e você terá que dizer qual foi o número em que pensei”. Você aceita o desafio? Jucavo, então pensa em um número e fornece as seguintes dicas:

- o número que eu pensei é um múltiplo de 7;
- quando eu subtraio 17 do número que eu pensei, resultado obtido é múltiplo de 4;
- o número que eu pensei é um número natural entre 2000 e 2017.

Assinale a alternativa que corresponde ao número que Jucavo pensou.

a) 2005
b) 2009
c) 2002
d) 2016
e) 2003

Resolução:

Seja x o número que Jucavo pensou. Dadas as três condições, buscamos um número x tal que:

$x \equiv 0 \bmod 7$,

$x - 17 \equiv 0 \bmod 4 \Rightarrow x - 17 + 17 \equiv 0 + 17 \bmod 4 \Rightarrow x \equiv 17 \bmod 4$,

$2000 < x < 2017$.

Primeiramente, vamos obter o resto da divisão de 2002 por 7, isto é, o número que é congruente a 2002 módulo 7, note que

$2002 \equiv 0 \bmod 7$.

Com isso, podemos concluir que 2002 é um múltiplo de 7. Da terceira dicas temos que os próximos múltiplos de 7 são 2009 e 2016. Então, temos três candidatos ao número pensado por Jucavo: 2002, 2009 e 2016.

Agora, de acordo com a segunda dica, vamos verificar qual número deixa resto 17 ao ser dividido por 4, obtemos

$2002 \equiv 2 \bmod 4$,

$2009 \equiv 17 \bmod 4$,

$2016 \equiv 0 \bmod 4$.

Daí, o número pensado é 2009.

Questão 4 (Olimpíada Brasileira de Matemática – 2001 – Nível 2 – 1ª fase)

Contando-se os alunos de uma classe de 4 em 4 sobram 2, e contando-se de 5 em 5 sobra 1. Sabendo -se que 15 alunos são meninas e que nessa classe o número de meninas é maior que o meninos, o número de meninos nessa classe é:

a) 7
b) 8
c) 9
d) 10
e) 11

Resolução:

Sabe-se que 15 é o número de meninas e sendo o número de meninas maior que o de meninos, concluímos que pode haver de 1 a 14 meninos. Portanto, o total de alunos é um número compreendido entre 16 e 29. Denotando x o número total de alunos, segue que

$x \equiv 1 \bmod 5, \quad 16 \leq x \leq 29$

Daí, x pode ser igual a 16, 21 e 26. Além disso, se contarmos o número de 4 em 4 sobram 2. Então, $x \equiv 2 \bmod 4$.

Logo, o único que satisfaz a última condição é o 26.

Portanto, são 26 alunos e o número de meninos é 26 – 15 = 11.

Questão 5 (Colégio Naval 1994)

O resto da divisão do número 743^{48} por 6, é:

a) 1

b) 2

c) 3

d) 4

e) 5

Resolução:

Primeiramente, devemos encontrar o número que é resto da divisão de 743 por 6, isto é, o número que é congruente a 743 módulo 6. Temos que

$$743 \equiv 5 \bmod 6.$$

Um artifício muito utilizado é somar ou subtrair o módulo no resto, para encontramos 1 ou -1, que podem ser elevados a qualquer expoente. Com isso, vamos subtrair 6 ao 5, note que

$$743 \equiv 5 - 6 \bmod 6 \Leftrightarrow 743 \equiv -1 \bmod 6.$$

Por fim, podemos elevar ambos os membros da congruência a 48, obtemos

$$743^{48} \equiv (-1)^{48} \bmod 6 \Rightarrow 743^{48} \equiv 1 \bmod 6.$$

Logo, o resto procurado é 1.

3.2 EQUAÇÕES DIOFANTINAS LINEARES

3.2.1 Introdução ao estudo de equações Diofantinas Lineares

Objetivo:

- Alcançar os conceitos e definições de equações Diofantinas Lineares.
- Encontrar soluções geral e particular das equações Diofantinas Lineares.

Material necessário: Lousa, pilotos coloridos, videoaulas de sua preferência sobre o tema.

Tipo de atividade: individual.

Duração: 9 aulas de 50 minutos.

Neste primeiro instante é primordial uma aula expositiva, com registros de conceitos e definições. Para isso, pode-se utilizar o próprio quadro da sala de aula com auxílio de pilotos coloridos. Entretanto, se tiver a chance de exibir uma mídia digital, recomenda-se que utilize videoaulas de sua preferência sobre o assunto.

Registros para serem apresentados na lousa:

Vamos apresentar a equação Diofantina linear

Dica →Deve-se exemplificar oralmente com exemplos lúdicos que façam parte do cotidiano dos alunos, para melhor compreensão.

Tipo:

- **Temos 14 animais com duas e quatro patas e um total de 22 patas em um zoológico. Sabendo que há animais de duas patas e de 4 patas, qual equação podemos montar para representar o total de animais e qual equação para denotar o total de patas? Após a reposta da turma, escrever a equação na lousa: x + y = 14 e 2x + 4y = 22, ressaltando que x é o número total de animas com duas patas e y o número total de animais de quatro patas.**

A seguir, serão apresentadas questões do conteúdo equações Diofantinas Lineares e suas respectivas resoluções

Questão 1: Prova final da Olimpíada de Matemática de São Paulo

Peça a um amigo que multiplique o dia de seu aniversário por 12, o mês do aniversário por 31 e some os dois resultados. Sabendo que o amigo seguiu as instruções e a soma deu 368. Quando é o aniversário dele?

Resolução:

Sejam d e m, respectivamente, o dia e o mês do nascimento. Então, (i)12d + 31m = 368.

Por inspeção, verificamos que x = 10 e y = 8 é uma das soluções de (i).

Onde x_0 = 10 e y_0 = 8 é uma solução particular da equação (i) e as demais soluções são dadas pelas fórmulas:

$$\begin{cases} x = x_0 + bt = 10 + 31t \\ y = y_0 - at = 8 - 12t \end{cases}, \text{ com } t \in \mathbb{Z}$$

Na busca de soluções não negativas devem ser satisfeitas as desigualdades:

x $\geq$ 0 e y $\geq$ 0, assim temos que 10 $+ 31t \geq 0$ e 8 - 12$t \geq 0$

o que implica que t $\in$ {0}. Com isso, temos uma possibilidade a saber:

Para t = 0, temos o dia 10 e o mês 8.

Portanto, o aniversário do amigo é 10 de agosto.

Questão 2: (Problema do século XVI)

Um total de 41 pessoas entre homens, mulheres e crianças foram a um banquete e juntos gastaram 40 patacas. Cada homem pagou 4 patacas, cada mulher 3 patacas e cada criança um terço de pataca. Quantos homens, quantas mulheres e quantas crianças havia no banquete?

Resolução:

Primeiramente vamos identificar as variáveis do problema, seja H a quantidade de homens, M a quantidade de mulheres e C a quantidade de crianças. Dessa forma as equações representativas são:

(i)H + M + C = 41

(ii)4H + 3M + $\frac{1}{3}$ C = 40

Multiplicando (ii) por 3, obtemos 12H + 9M + C = 120. Entretanto, utilizando (i), obtemos uma equação diofantina de duas variáveis, como segue:

11H + 8M + (H + M + C) = 11H + 8M + 41 = 120 $\Leftrightarrow$ (iii)11H + 8M = 79.

Como o mdc(11,8) = 1, a equação (iii) tem solução pois 1|79.

Por inspeção, verificamos que H = 5 e M = 3 é uma das soluções de (iii).

Onde H_0 = 5 e M_0 = 3 é uma solução particular da equação (i) e as demais soluções são dadas pelas fórmulas:

$$\begin{cases} H = H_0 + bt = 5 + 8t \\ M = M_0 - at = 3 - 11t \end{cases}, \text{ com } t \in \mathbb{Z}$$

Logo, o conjunto solução da equação (iii) é dado por:

S = {(5 + 8t, 3 – 11t) | $t \in \mathbb{Z}$}.

É fato que

5 + 8t > 0 e 3 – 11t> 0.

Daí segue que $-\frac{5}{8}$ < t < $\frac{3}{11}$. Como t é inteiro, o único valor possível é t = 0. Sendo assim, o número de homens e mulheres, respectivamente, presentes no banquete é 5 e 3. Logo o número de crianças é C = 33.

Questão 3

Uma certa quantidade de maças é dividida em 37 montes de igual número. Após serem retiradas 17 frutas, as restantes são acondicionadas em 79 caixas, cada uma com a mesma quantidade. Quantas maças foram colocadas em cada caixa? Quantas maças tinha cada monte?

Resolução: Seja x a quantidade de maças, y o número de maças em cada monte e z número de maças dentro de cada caixa.

Observemos, inicialmente, x foi dividida em 37 monte, ou seja,

(i)x = 37y.

Por outro lado, se forem retiradas do total 17 frutas, restante pode ser acondicionado em 79 caixas, ou seja,

(ii)x – 17 = 79z

Substituindo (i) em (ii), obtemos:

(iii)37y – 79z = 17

Basta agora calcularmos a solução para (iii), uma vez que ela admite solução já que mdc(37,79) = 1.

Por inspeção, verificamos que y = 9 e z = 4 é uma das soluções de (iii).

Onde y_0 = 9 e z_0 = 4 é uma solução particular da equação (iii). Assim a solução geral é dada por:

S = {(9 - 79t, 4 – 37t) | $t \in \mathbb{Z}$}.

Mais uma vez, o único valor possível de t é 0. Logo, em cada monte foram colocadas 9 maças e em cada caixa, 4 maças.

Questão 4

Para o retorno às aulas, a mãe de Maíra, comprou cadernos e jogos de canetas para sua filha. Cada caderno escolhido por Maíra custa R$ 12,00 e os jogos de canetas R$ 8,00. Com R$ 80,00, quais as possíveis quantidades de cadernos e jogos de canetas que ela poderá comprar, sabendo que irá comprar no mínimo 2 cadernos e 3 jogos de canetas?

Resolução:

Vamos identificar as variáveis do problema, seja C a quantidade de cadernos e L a quantidade de jogos de canetas. Dessa forma a equação representativa é: (i) 12C + 8L = 80.

Como o mdc(12,8) = 4 e 4|80, a equação (i) possui solução.

Escrevendo 4 como combinação linear de 12 e 8 temos:

(ii) 12 · (1) + 8 · (-1) = 4

Multiplicando (ii) por 20, obtemos:

(iii) 12 · (20) + 8 · (-20) = 80

Logo, o par de inteiros C_0 = 20 e L_0 = -20 é uma solução particular da equação (i) e as demais soluções são dadas pelas fórmulas:

$$\begin{cases} C = C_0 + \mathrm{bt} = 20 + 8\mathrm{t} \\ L = L_0 - at = -20 - 12t \end{cases}, \text{ com } t \in \mathbb{Z}$$

Observando -se as restrições do problema, para calcular os possíveis valores de $t \in \mathbb{Z}$, teremos:

20 + 8t $\geq$ 2 e -20 -12t $\geq$ 3.

Isto é:

t $\geq -\frac{18}{8}$ e t $\leq -\frac{23}{12}$, daí temos que - $\frac{18}{8} \leq$ t $\leq$ - $\frac{23}{12}$

o que implica que t $\in$ {-2}. Com isso, temos apenas uma possibilidade a saber:

Para t = -2, temos 4 cadernos e 4 jogos de canetas.

Questão 5

Quando 100 quilogramas de grãos são distribuídos entre 100 pessoas, de modo que cada homem recebe 3 quilogramas, cada mulher recebe 2 quilogramas, e cada criança recebe meio quilograma. Quantos homens, mulheres e crianças havia?

Resolução:

Chamando de x, y e z o número de homens, mulheres e crianças, respectivamente, obtemos as seguintes equações:

$3x + 2y + \frac{z}{2} = 100$

$X + Y + Z = 100$

Agora vamos resolver o sistema de equações:

$\begin{cases} X + Y + Z = 100 \\ 3X + 2Y + \frac{z}{2} = 100 \end{cases} \Leftrightarrow \begin{cases} X + Y + Z = 100 \\ 6X + 4Y + Z = 100 \end{cases} \Leftrightarrow$ (i) 5X + 3Y = 100

Sabendo que (i) é uma equação Diofantina, vamos a resolução:

Se mdc(5,3) = 1 e 1|100, então a equação tem solução inteira.

Escrevendo 5 como combinação linear de 2 e 3 temos:

(ii) 3 · (1) + 2 · (1) = 5 $\Leftrightarrow$ 2 = 5 · (1) - 3 · (1)

Multiplicando (ii) por 50, obtemos:

(iii) 5 · (50) + 3 · (-50) = 100

Onde x_0 = 50 e y_0 = -50 é uma solução particular da equação (i).

Assim, a solução geral é da forma x = 50 + 3t, e y = -50 – 5t, com $t \in \mathbb{Z}$. Como os valores de x e y devem ser positivos, pois o problema se refere a homens e mulheres, temos que t $\geq -\frac{50}{3}$ e t $\leq$ -10, daí temos que - $\frac{50}{3} \leq$ t $\leq$ - 10. Daí, t $\in$ {-16, -15, -14, -13, -12, -11, -10}. Com isso, temos sete possibilidades a saber:

Se t = -10, obtemos x = 20 e y = 0, e encontramos z = 80.

Se t = -11, obtemos x = 17 e y = 5, e encontramos z = 78.

Se t = -12, obtemos x = 14 e y = 10, e encontramos z = 76.

Se t = -13, obtemos x = 11 e y = 15, e encontramos z = 74.

Se t = -14, obtemos x = 8 e y = 20, e encontramos z = 72.

Se t = -15, obtemos x = 5 e y = 25, e encontramos z = 70.

Se t = -16, obtemos x = 2 e y = 30, e encontramos z = 68.

Como não foi dada nenhuma restrição no enunciado do problema, devemos considerar as respostas acima.

Questão 6: OBMEP 2018 – NIVEL 3 – 1ª FASE

De quantas maneiras podemos trocar uma nota de R$ 20,00 por moedas de R$ 0,10 e R$ 0,25.

(A) 21

(B) 36

(C) 38

(D) 41

(E) 56

Resolução:

Sejam x e y as quantidades de moedas R$ 0,10 e R$ 0,25, respectivamente, usadas para formar a quantia de R$ 20,00. Assim, temos a equação Diofantina:

(i) 0,10x + 0,25y = 20

Multiplicando (i) por 20, obtemos

(ii) 2x + 5y = 400.

Como mdc(5,2) = 1 e 1|400, a equação tem solução inteira.

O número 400 é múltiplo de 2 e 5, então podemos considerar x_0 = 200 e y_0 = 0 é uma solução particular da equação (ii) e as demais soluções são dadas pelas fórmulas:

$$\begin{cases} x = x_0 + bt = 200 + 5t \\ y = y_0 - at = -2t \end{cases}$$, com $t \in \mathbb{Z}$

x $\geq$ 0 e y $\geq$ 0, assim temos que 200 $+ 5t \geq 0$ e -2$t \geq 0$

o que implica que t $\in$ {-40, -39, -38, ..., -1, 0}. Com isso, temos 41 maneiras de trocar uma nota de R$ 20,00 por moedas de R$ 0,10 e R$ 0,25.

Cabe ressaltar que podemos considerar t = 0, pois não foi dada nenhuma restrição no problema.

REFERÊNCIAS

OLIVEIRA, Wanderlan Carminatti. **Elementos da Aritmética Modular e seu papel nos anos finais do Ensino Fundamental e na Educação superior**. 2024. 125f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Federal Fluminense, Niterói, 2024.

DOMINGUES, Hygino, H. **Fundamentos de Aritmética**. São Paulo: Editora Atual, 1991.

SANTOS, Filipe da Costa Neves. **Educação financeira dentro do ensino de matemática na educação básica – algumas possíveis abordagens nos anos finais do ensino fundamental 2**. 2023. 141f. Dissertação (Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Federal Fluminense, Niterói, 2023.

HEFEZ, A. **Elementos de Aritmética**. 3. Ed. Rio de Janeiro: SBM, 2022.

OBM - Olimpíada Brasileira de Matemática. Disponível em: <https://www.obm.org.br/como-se-preparar/provas-e-gabaritos/>. Acesso em: 16 jan. 2023.

Olimpíada Brasileira de Matemática das Escolas Públicas - **OBMEP | Somando novos talentos para o Brasil.** Disponível em: <https://www.obmep.org.br/provas.htm>. Acesso em: 21 dez. 2023

SSPM. **Serviço de Seleção de Pessoal da Marinha**. Disponível em: https://www.marinha.mil.br/sspm/colegionaval/colegio_princ . Acesso em: 25 nov. 2023.

SSPM. **Serviço de Seleção de Pessoal da Marinha**. Disponível em: https://www.marinha.mil.br/sspm/?q=colegionaval/a-cn-provag . Acesso em: 25 nov. 2023.