Allan Goldner Campos

Divisibilidade e Congruência: Aplicações Didáticas no Ensino Médio

Vitória

2025

Allan Goldner Campos

Divisibilidade e Congruência: Aplicações Didáticas no Ensino Médio

Dissertação de mestrado apresentada ao PROFMAT como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

PROFMAT

Orientador: Prof. Dra. Rosa Elvira Quispe Ccoyllo

Vitória

2025

Ficha catalográfica disponibilizada pelo Sistema Integrado de
Bibliotecas - SIBI/UFES e elaborada pelo autor

G618d

Goldner Campos, Allan, 1997-
Divisibilidade e Congruência: Aplicações Didáticas no Ensino Médio / Allan Goldner Campos. - 2025.
68 p. : il.

Orientadora: Rosa Elvira Quispe Ccoyllo.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal do Espírito Santo, Centro de Ciências Exatas.

1. Congruências e restos. 2. Matemática - Estudo e ensino Análise de erros. 3. Aritmética. 4. Números primos. 5. Ensino médio. I. Quispe Ccoyllo, Rosa Elvira. II. Universidade Federal do Espírito Santo. Centro de Ciências Exatas. III. Título.

CDU: 51

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

Centro de Ciências Exatas

Programa de Pós-Graduação em Matemática em Rede Nacional – PROFMAT

"Divisibilidade e Congruência: Aplicações Didáticas no Ensino Médio"

Allan Goldner Campos

Defesa de Dissertação de Mestrado Profissional submetida ao Programa de Pós-Graduação em Matemática em Rede Nacional da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do título de Mestre em Matemática.

Aprovado em 03/10/2025 por:

____

Profa. Dra Rosa Elvira Quispe Ccoyllo
Orientador – UFES

____

Prof. Dr. Cássio Henrique Vieira Morais
Examinador interno – UFES

____

Profa. Dra. Bruna Zution Dalle Prane
Examinador externo – IFES

folha_de_assinaturas_Allan_Goldner_Campos

Data e Hora de Criação: 29/09/2025 às 08:44:54

Documentos que originaram esse envelope:
- folha_de_assinaturas_Allan_Goldner_Campos.pdf (Arquivo PDF) - 1 página(s)

Hashs únicas referente à esse envelope de documentos

[SHA256]: 6a7f7b4176eaeb210660cd20f3a576a43c9e4d848b5a0c69e5a1ed87d6f4c755
[SHA512]: ac5306f19747864c4632853b7c6a0e3d2e11c29d46e0cc1559b740eded8f20575524f9822749720b24afaac41d7bd99bf02293719f3e5bab7082007e55a2ad65

Lista de assinaturas solicitadas e associadas à esse envelope

ASSINADO - Bruna Zution Dalle Prane (bruna.prane@ifes.edu.br)
Data/Hora: 03/10/2025 - 09:36:52, IP: 200.137.71.158
[SHA256]: 00fcc8badccf0954cf4f8098576b4e65ef04f052cdd226013fc4d896ac473a6e
Assinatura Eletrônica Avançada (Conforme Lei nº 14.063/20, art. 4º, II)

ASSINADO - Cássio Henrique Vieira Morais (cassio.morais@ufes.br)
Data/Hora: 03/10/2025 - 17:34:51, IP: 187.36.173.142
[SHA256]: 5c068ff865fe67d2c7a8e4acd576aa81004eec6490c9e08e6feda9fbb17301e1
Assinatura Eletrônica Avançada (Conforme Lei nº 14.063/20, art. 4º, II)

ASSINADO - Rosa Elvira Quispe Ccoyllo (rosa.ccoyllo@ufes.br)
Data/Hora: 03/10/2025 - 17:31:00, IP: 200.137.65.104
[SHA256]: 2074e474fdfd74f9be26fa42fbba0a91caadf22de65f2a37b69038aeba9883ad
Assinatura Eletrônica Avançada (Conforme Lei nº 14.063/20, art. 4º, II)

Histórico de eventos registrados neste envelope

03/10/2025 17:34:51 - Envelope finalizado por cassio.morais@ufes.br, IP 187.36.173.142
03/10/2025 17:34:51 - Assinatura realizada por cassio.morais@ufes.br, IP 187.36.173.142
03/10/2025 17:31:00 - Assinatura realizada por rosa.ccoyllo@ufes.br, IP 200.137.65.104
03/10/2025 17:30:51 - Envelope visualizado por rosa.ccoyllo@ufes.br, IP 200.137.65.104
03/10/2025 09:36:53 - Assinatura realizada por bruna.prane@ifes.edu.br, IP 200.137.71.158
03/10/2025 09:36:47 - Envelope visualizado por bruna.prane@ifes.edu.br, IP 200.137.71.158
03/10/2025 07:00:19 - Envelope registrado na Blockchain por notificacao@astenassinatura.com.br
03/10/2025 07:00:19 - Envelope encaminhado para assinaturas por notificacao@astenassinatura.com.br
29/09/2025 08:44:54 - Envelope criado por ivan.barbosa@ufes.br, IP 200.137.65.100

Dedico este trabalho à minha esposa, Gabriela, pelo amor, paciência e incentivo diário, e à minha mãe, Arlete, pelo apoio, confiança e inspiração que sempre me acompanharam. A ambas, minha profunda gratidão por tornarem possível cada passo desta trajetória.

Agradecimentos

Primeiramente, agradeço a Deus, por guiar meus passos, me dar força, sabedoria e perseverança ao longo desta trajetória acadêmica.

Agradeço à minha esposa, Gabriela, pelo amor, paciência e apoio incondicional.

À minha mãe, Arlete, por acreditar em mim e inspirar cada conquista.

À minha orientadora, Rosa Elvira, expresso minha profunda gratidão pela orientação, confiança, incentivo e dedicação durante todo o desenvolvimento desta dissertação. Sua experiência, paciência e conhecimento foram fundamentais para a realização deste trabalho.

À escola e aos estudantes que participaram das atividades, meu reconhecimento por contribuírem com dados e experiências que possibilitaram a análise e reflexão sobre práticas de ensino de matemática.

Por fim, agradeço a todos que, direta ou indiretamente, ofereceram apoio, estímulo e motivação, tornando possível a concretização desta dissertação.

"A Matemática é a Linguagem em que Deus escreveu o Universo."
(Galileu Galilei)

Resumo

Esta dissertação investiga a compreensão dos conceitos de divisibilidade e congruências por alunos do Ensino Médio, por meio de uma intervenção didática planejada. Inicialmente, aplicou-se uma atividade diagnóstica com o objetivo de identificar as principais dificuldades e as estratégias utilizadas pelos estudantes na resolução de problemas envolvendo aritmética modular e padrões cíclicos. Com base nos resultados obtidos, elaborou-se uma sequência de quatro aulas de caráter investigativo, voltadas à consolidação dos conceitos fundamentais. Em seguida, realizou-se uma segunda aplicação para avaliar o progresso dos alunos, observando-se aumento no número de acertos em questões relacionadas a congruências simultâneas, ciclos de dias da semana e padrões de restos em potências. Os resultados indicam que a intervenção contribuiu para o aprimoramento da compreensão conceitual e da capacidade de aplicar estratégias adequadas na resolução de problemas, embora algumas questões mais complexas ainda evidenciem desafios significativos. A análise final ressalta a importância de atividades contextualizadas e da prática contínua para a consolidação do raciocínio matemático no Ensino Médio.

Palavras-chave: Divisibilidade; Congruências; Ensino de Matemática; Aritmética Modular; Intervenção Didática e Padrões.

Abstract

This dissertation investigates high school students' understanding of divisibility and congruences through a structured didactic intervention. Initially, a diagnostic activity was applied to identify the main difficulties and strategies used by students when solving problems involving modular arithmetic and cyclic patterns. Based on the results obtained, a sequence of four investigative lessons was designed, aimed at consolidating the fundamental concepts. Subsequently, a second application was conducted to assess students' progress, revealing an increase in correct answers in questions related to simultaneous congruences, day-of-the-week cycles, and patterns of remainders in powers. The results indicate that the intervention contributed to the improvement of conceptual understanding and the ability to apply appropriate problem-solving strategies, although some more complex questions still posed significant challenges. The analysis highlights the importance of contextualized activities and continuous practice for the consolidation of mathematical reasoning at the high school level.

Keywords: Divisibility; Congruences; Mathematics Education; Modular Arithmetic; Didactic Intervention and Patterns.

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

A Base Nacional Comum Curricular (BRASIL, 2018) evidencia que o ensino de Matemática no Ensino Médio brasileiro, em geral, prioriza conteúdos tradicionais como funções, equações e geometria analítica, frequentemente em detrimento de tópicos como divisibilidade e congruência modular. Apesar de constituírem fundamentos essenciais da Teoria dos Números e possuírem aplicações diretas em áreas modernas como segurança digital, algoritmos e criptografia, tais conceitos têm presença tímida no currículo escolar, muitas vezes restritos à memorização de critérios sem aprofundamento conceitual.

Embora a BNCC não mencione explicitamente a congruência modular no Ensino Médio, oferece brechas importantes para sua abordagem. No Ensino Fundamental, habilidades como EF06MA05 (classificar números como primos e compostos), EF07MA01 (resolver problemas envolvendo divisibilidade) e EF08MA05 (explorar propriedades dos números primos) preparam o terreno conceitual. Já no Ensino Médio, habilidades como EM13MAT301 (resolver problemas com o uso de algoritmos em contextos matemáticos, sociais e tecnológicos) e EM13MAT305 (investigar padrões numéricos) são plenamente compatíveis com a exploração de congruência e divisibilidade de forma integrada à resolução de problemas e à formação de pensamento lógico.

Este trabalho de mestrado tem como objetivo investigar o nível de compreensão dos alunos da 3ª série do Ensino Médio sobre divisibilidade e congruência, e observar possíveis avanços após uma intervenção didática planejada. Para isso, foi elaborada e aplicada uma atividade diagnóstica inicial composta por problemas de diferentes níveis de complexidade sobre os temas citados, cujos resultados foram analisados de forma qualitativa e quantitativa. Em seguida, foram ministradas aulas sobre os conceitos fundamentais de divisibilidade e congruência, utilizando estratégias que privilegiam a resolução de problemas, a argumentação matemática e o desenvolvimento de autonomia dos alunos.

Depois dessa sequência de aulas, foi aplicada uma segunda lista de exercícios, com estrutura semelhante à da primeira, visando comparar os resultados e identificar indícios de avanço conceitual e atitudinal.

De forma mais detalhada, este trabalho busca ainda: (i) identificar as principais dificuldades conceituais apresentadas pelos alunos em relação à divisibilidade e à congruência; (ii) analisar em que medida a intervenção didática contribui para superar tais dificuldades e consolidar os conceitos fundamentais; (iii) observar mudanças na postura dos estudantes quanto à resolução de problemas que envolvem argumentação e raciocínio lógico; e (iv) refletir sobre possibilidades de inserção mais efetiva desses conteúdos no currículo do Ensino Médio, em consonância com as orientações da BNCC.

2 Fundamentações teóricas

Nesta seção, apresentamos os conceitos fundamentais da Teoria dos Números que servirão de base para a compreensão e resolução de problemas envolvendo divisibilidade e congruências. O desenvolvimento segue uma ordem progressiva, partindo dos conceitos elementares até resultados mais avançados, como o Teorema Chinês do Resto e o Pequeno Teorema de Fermat.

As principais referências utilizadas nesta seção incluem Niven, Zuckerman e Montgomery (1991), Hefez (2022), além de material do PROFMAT.

2.1 Divisibilidade

Considere $\mathbb{Z}$ o conjunto dos números inteiros e $\mathbb{N}$ o conjunto dos números naturais.

Definição 2.1.1. *Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Dizemos que b divide a, ou que a é divisível por b, se existe $k \in \mathbb{Z}$ tal que*

$$a = b \cdot k.$$

Neste caso, denotamos por $b \mid a$. Caso contrário, escreve-se $b \nmid a$.

Exemplo 2.1.2. *Temos que $3 \mid 12$, pois $12 = 3 \cdot 4$, mas $5 \nmid 12$, pois não existe $k \in \mathbb{Z}$ tal que $12 = 5k$.*

Proposição 2.1.3. *Sejam $a, b, c \in \mathbb{Z}$. Valem as seguintes propriedades fundamentais:*

1. *Se $b \mid a$ e $a \mid c$, então $b \mid c$.*
2. *Se $b \mid a$ e $b \mid c$, então $b \mid (ma + nc)$ para quaisquer $m, n \in \mathbb{Z}$.*

Demonstração.

1. Se $b \mid a$, então existe $k \in \mathbb{Z}$ tal que $a = bk$. Como $a \mid c$, existe $l \in \mathbb{Z}$ tal que $c = al$. Substituindo $a = bk$, obtemos $c = (bk)l = b(kl)$, o que mostra que $b \mid c$.

2. Se $b \mid a$, então existe $k \in \mathbb{Z}$ tal que $a = bk$. Se $b \mid c$, existe $l \in \mathbb{Z}$ tal que $c = bl$. Logo, para quaisquer $m, n \in \mathbb{Z}$:

$$ma + nc = m(bk) + n(bl) = b(mk + nl),$$

de modo que $b \mid (ma + nc)$.

□

2.2 Divisão Euclidiana

Teorema 2.2.1 (Divisão Euclidiana)**.** *Sejam $a \in \mathbb{Z}$ e $b \in \mathbb{Z}$, $b > 0$. Então existem únicos inteiros q (quociente) e r (resto), com $0 \leq r < b$, tais que*

$$a = bq + r.$$

Demonstração. Considere o conjunto

$$S = \{x = a - by;\ y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Existência: Pela Propriedade Arquimediana, existe $n \in \mathbb{Z}$ tal que

$$n(-b) > -a,$$

logo $a - nb > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = a - bq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < b$.

Suponhamos por absurdo que $r \geq b$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = b + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q + 1)b \in S$, com $s < r$.

Unicidade: Suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < b$ e $0 \leq r' < b$. Assim, temos que

$$-|b| < r - r' = b(q' - q) < |b|.$$

Logo, $|r' - r| < |b|$. Por outro lado,

$$b(q - q') = r' - r,$$

o que implica que

$$|b||q - q'| = |r' - r| < |b|.$$

o que só é possível se $q = q'$ e, consequentemente, $r = r'$. (HEFEZ, 2022) □

Exemplo 2.2.2. *A divisão de 23 por 5 pode ser escrita como*

$$23 = 5 \cdot 4 + 3,$$

onde $q = 4$ e $r = 3$.

A Divisão Euclidiana é a base para o estudo do máximo divisor comum e para o funcionamento do Algoritmo de Euclides (LIMA, 2024).

2.3 Máximo Divisor Comum e Algoritmo de Euclides

Definição 2.3.1. *Diremos que um número inteiro $d > 0$ é um máximo divisor comum (mdc) de a e b, se possuir as seguintes propriedades:*

1. *d é um divisor comum de a e b;*
2. *d é divisível por todo divisor comum de a e b.*

A condição (2) acima pode ser reenunciada como segue:

1. *Se c é um divisor comum de a e b, então $c \mid d$.*

Sejam $a, b \in \mathbb{Z}$. Será denotado o máximo divisor comum de a e b por (a, b).

Teorema 2.3.2 (Algoritmo de Euclides)**.** *Sejam $a, b \in \mathbb{N}$ com $a > b > 0$. O Algoritmo de Euclides consiste em aplicar sucessivamente a divisão euclidiana do dividendo pelo divisor, e em seguida do divisor pelo resto obtido, até que se obtenha resto nulo. Ou seja, realiza-se:*

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b,$$

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2,$$

e assim sucessivamente, até que $r_k = 0$. Então, o último resto não nulo r_{k-1} é precisamente o (a, b).

Exemplo 2.3.3. *Para calcular* $(252, 198)$*:*

$$252 = 198 \cdot 1 + 54, \quad 198 = 54 \cdot 3 + 36, \quad 54 = 36 \cdot 1 + 18, \quad 36 = 18 \cdot 2 + 0.$$

Logo, $(252, 198) = 18$.

O Algoritmo de Euclides estendido permite calcular combinações lineares $ax + by = mdc(a, b)$, fundamentais para o estudo de inversos multiplicativos em congruências (HEFEZ, 2022).

Corolário 2.3.4. *Dados $a, b \in \mathbb{Z}$, não ambos nulos, tem-se que*

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

Teorema 2.3.5 (Lema de Gauss)**.** *Sejam a, b, c números inteiros. Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

2.4 Mínimo Múltiplo Comum (MMC)

Definição 2.4.1. *Diremos que um número inteiro $m > 0$ é um mínimo múltiplo comum (mmc) dos números inteiros a e b, se possuir as seguintes propriedades:*

1. *m é um múltiplo comum de a e b;*
2. *Se c é um múltiplo comum de a e b, então $m \mid c$.*

Sejam $a, b \in \mathbb{Z}$. Será denotado o mínimo múltiplo comum de a e b por $[a, b]$.

Se m e m' são dois mínimos múltiplos comuns de a e b, então, pelo item (2) da definição acima, temos que $m \mid m'$ e $m' \mid m$. Como m e m' são números inteiros não negativos, segue que $m = m'$, o que mostra que o mínimo múltiplo comum, se existe, é único.

Por outro lado, se m é o mmc de a e b e c é um múltiplo comum de a e b, então $m \mid c$. Portanto, se $c > 0$, temos que $m \leq c$, mostrando que m é o menor dos múltiplos comuns positivos de a e b (HEFEZ, 2022).

Proposição 2.4.2. *Dados dois números inteiros a e b, temos que $[a, b]$ existe e*

$$[a, b](a, b) = |ab|.$$

Demonstração. Se $a = 0$ ou $b = 0$, a igualdade acima é trivialmente satisfeita. É também fácil verificar que a igualdade é verificada para a e b se, e somente se, ela é verificada para $\pm a$ e $\pm b$. Então, sem perda de generalidade, podemos supor $a, b \in \mathbb{N}$. Ponhamos

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

Como

$$m = \frac{a}{(a, b)} \cdot b = \frac{b}{(a, b)} \cdot a,$$

temos que $a \mid m$ e $b \mid m$. Portanto, m é um múltiplo comum de a e b.

Seja c um múltiplo comum de a e b; logo, $c = na = n'b$. Segue daí que

$$\frac{na}{(a, b)} = \frac{n'b}{(a, b)}.$$

No entanto, pelo 2.3.4, $\frac{a}{(a, b)}$ e $\frac{b}{(a, b)}$ são primos entre si, segue-se, de 2.3.5, que $\frac{a}{(a, b)}$ divide n', e, portanto,

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

divide $n'b$, que é igual a c. Assim, o resultado está demonstrado (HEFEZ, 2022). $\square$

Exemplo 2.4.3. *Para* $a = 12$ *e* $b = 18$*, temos:*

$$mdc(12, 18) = 6, \quad mmc(12, 18) = \frac{12 \cdot 18}{6} = 36.$$

Corolário 2.4.4. *Se* a *e* b *são números inteiros tais que* $mdc(a, b) = 1$*, então o mínimo múltiplo comum de* a *e* b *é dado por*

$$[a, b] = |ab|.$$

2.5 Números Primos

Definição 2.5.1. *Um número natural* $p > 1$ *é chamado de primo se seus únicos divisores positivos são exatamente* 1 *e* p*. Um número natural maior que* 1 *que não é primo é chamado de composto.*

Exemplo 2.5.2. *Os números* $2, 3, 5, 7, 11$ *são primos. Já* $4, 6, 8, 9, 10, 12$ *são compostos.*

Proposição 2.5.3. *1. O número* 2 *é o único primo par.*

2. Todo número natural $n > 1$ *é divisível por pelo menos um número primo.*

Teorema 2.5.4 (Infinitude dos Primos, Euclides)**.** *Existem infinitos números primos.*

Ideia da prova. Suponha que exista apenas um número finito de primos $p_1, p_2, \ldots, p_n$. Considere o número

$$N = p_1 p_2 \cdots p_n + 1.$$

O número N não é divisível por nenhum dos primos da lista, logo deve ser primo ou possuir um fator primo não listado. Contradição. □

A seguir, estabelecemos um resultado fundamental de Euclides (ALEXANDRIA, 1908), chamado Lema de Euclides.

Proposição 2.5.5 (Lema de Euclides)**.** *Sejam* $a, b, p \in \mathbb{Z}$*, com* p *primo. Se* $p \mid ab$*, então* $p \mid a$ *ou* $p \mid b$*.*

Demonstração. Basta provar que, se $p \mid ab$ e $p \nmid a$, então $p \mid b$.

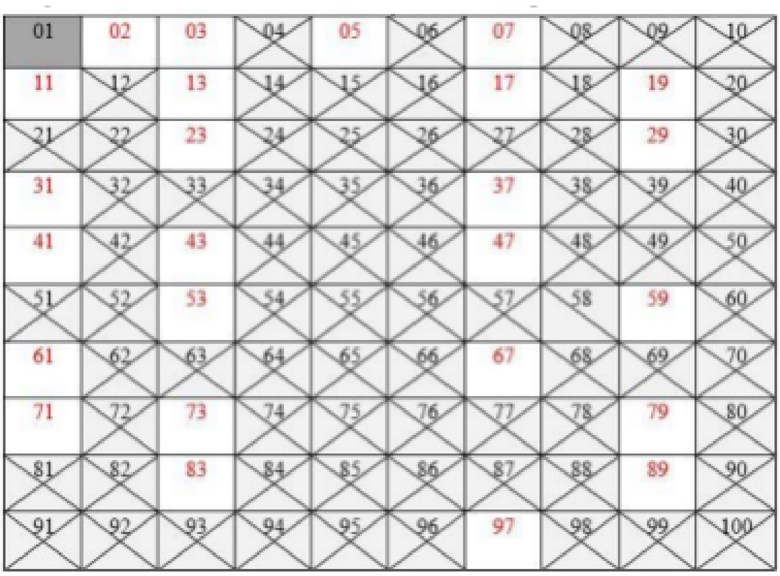
Como $p \nmid a$ e os únicos divisores de p são 1 e o próprio p, então temos que $mdc(p, a) = 1$, e o resultado segue-se do Lema de Gauss (2.3.5). □

Teorema 2.5.6 (Teorema Fundamental da Aritmética)**.** *Todo número inteiro maior que* 1 *ou é primo ou pode ser escrito de maneira única, salvo a ordem dos fatores, como um produto de números primos.*

Dois números inteiros a e b são chamados *primos entre si* ou *coprimos* se seu máximo divisor comum for igual a 1, ou seja, $(a, b) = 1$.

Além dos números primos, é interessante mencionar o *Crivo de Eratóstenes*, um método clássico para identificar números primos de forma sistemática[1]. O procedimento consiste em listar todos os números inteiros de 2 até um limite n e eliminar sucessivamente os múltiplos de cada número primo encontrado, de modo que permanecem apenas os números que não possuem divisores além de 1 e de si mesmos. Trata-se de uma ferramenta simples e eficiente para gerar listas de números primos, com aplicações didáticas em sala de aula e também em problemas de teoria dos números e criptografia básica.

Figura 1 – Crivo de Eratóstenes até 100



01	02	03	~~04~~	05	~~06~~	07	~~08~~	~~09~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Fonte: (LIMA, 2024)

2.6 Congruências

Definição 2.6.1. *Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$, $m > 1$. Dizemos que a é congruente a b módulo m se $m \mid (a - b)$. Escrevemos*

$$a \equiv b \pmod{m}.$$

Proposição 2.6.2. *Seja $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se:*

1. *$a \equiv a \pmod{m}$.*
2. *Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.*
3. *Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.*

[1] Eratóstenes de Cirene, aproximadamente 200 a.C.

Corolário 2.6.3 (Propriedades elementares de congruência)**.** *Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:*

1. $a + c \equiv b + d \pmod{m}$,
2. $a - c \equiv b - d \pmod{m}$,
3. $ac \equiv bd \pmod{m}$.

Exemplo 2.6.4. *Temos $17 \equiv 5 \pmod{12}$, pois $17 - 5 = 12$, que é múltiplo de 12.*

Proposição 2.6.5. *Sejam $a, b \in \mathbb{Z}$ e $n, m_1, \ldots, m_r$ inteiros maiores do que 1. Temos que:*

1. *Se $a \equiv b \pmod{m}$ e $n \mid m$, então $a \equiv b \pmod{n}$;*
2. *Se $a \equiv b \pmod{m_i}$, $i = 1, \ldots, r$, então $a \equiv b \pmod{[m_1, \ldots, m_r]}$;*
3. *Se $a \equiv b \pmod{m}$, então $(a, m) = (b, m)$.*

Demonstração.

1. Se $a \equiv b \pmod{m}$, então $m \mid (b - a)$. Como $n \mid m$, segue-se que $n \mid (b - a)$. Logo, $a \equiv b \pmod{n}$.
2. Se $a \equiv b \pmod{m_i}$, $i = 1, \ldots, r$, então $m_i \mid (b - a)$ para todo i. Sendo $b - a$ múltiplo de cada m_i, segue-se que $[m_1, \ldots, m_r] \mid (b - a)$, o que prova que $a \equiv b \pmod{[m_1, \ldots, m_r]}$.
3. Se $a = b \pmod{m}$, então $m \mid (b - a)$ e, portanto, $b = a + tm$ com $t \in \mathbb{Z}$. Logo, temos

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

□

Proposição 2.6.6. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Temos que*

$$ac \equiv bc \pmod{m} \iff a \equiv b \pmod{\tfrac{m}{(c,m)}}.$$

Demonstração. Como $\frac{m}{(c,m)}$ e $\frac{c}{(c,m)}$ são primos entre si (2.3.4), temos que

$$ac \equiv bc \pmod{m} \iff m \mid (b - a)c \iff \tfrac{m}{(c,m)} \mid (b - a)\tfrac{c}{(c,m)},$$

$$\iff \tfrac{m}{(c,m)} \mid (b - a) \iff a \equiv b \pmod{\tfrac{m}{(c,m)}}.$$

□

2.7 Pequeno Teorema de Fermat

Teorema 2.7.1 (Pequeno Teorema de Fermat)**.** *Seja p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então*

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

Demonstração. Seja p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$. Considere o produto

$$a \cdot 2a \cdot 3a \cdots (p-1)a = a^{p-1} \cdot (p-1)!.$$

Como p é primo e $p \nmid a$, nenhum fator do produto é divisível por p. Além disso, $p \nmid (p-1)!$, portanto podemos escrever a congruência

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}.$$

Cancelando $(p-1)!$ módulo p, em razão de $(p,(p-1)!) = 1$ e pela Proposição 2.6.6, obtemos

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

concluindo a prova. □

Exemplo 2.7.2. *Seja $p = 7$ e $a = 3$. Temos:*

$$3^6 = 729 \equiv 1 \pmod{7}.$$

2.8 Teorema Chinês do Resto

Teorema 2.8.1 (Teorema Chinês do Resto)**.** *Sejam $m_1, m_2, \ldots, m_k$ inteiros positivos dois a dois primos entre si. Então, para quaisquer inteiros $a_1, a_2, \ldots, a_k$, o sistema de congruências*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

possui solução, e essa solução é única módulo $N = m_1 m_2 \cdots m_k$.

Demonstração. Seja $M = m_1 m_2 \cdots m_k$. Para cada i, definimos $M_i = \dfrac{M}{m_i}$. Como m_i é coprimo de M_i, existe $y_i \in \mathbb{Z}$ tal que

$$M_i y_i \equiv 1 \pmod{m_i},$$

isto é, $M_i y_i$ é o inverso de M_i módulo m_i.

Definimos então

$$x = \sum_{i=1}^{k} a_i M_i y_i.$$

Verifiquemos que x satisfaz o sistema:

Para um dado j, temos

$$x \equiv a_j M_j y_j \pmod{m_j},$$

pois todos os outros termos da soma são múltiplos de m_j. E como $M_j y_j \equiv 1 \pmod{m_j}$, segue que

$$x \equiv a_j \pmod{m_j}.$$

Portanto, x é solução do sistema.

A unicidade segue do fato de que, se x e x' são soluções, então $x \equiv x' \pmod{m_i}$ para todo i. Logo, $x \equiv x' \pmod{M}$, já que os m_i são coprimos dois a dois. $\square$

Este capítulo apresentou os principais conceitos de divisibilidade, congruência e aritmética modular, contextualizados a partir das competências e habilidades definidas pela BNCC (BRASIL, 2018). Esses fundamentos fornecem a base teórica necessária para a elaboração das atividades pedagógicas e para a análise de sua efetividade. No capítulo seguinte, serão descritos os procedimentos metodológicos adotados na pesquisa, incluindo instrumentos e estratégias para a coleta e análise dos dados.

3 Metodologia

3.1 Tipo de pesquisa e abordagem

A presente pesquisa caracteriza-se como qualitativa, com suporte de dados quantitativos para análise complementar. Nessa abordagem, o pesquisador participa ativamente da elaboração, aplicação e análise das atividades, articulando intervenção e investigação de forma simultânea. O objetivo central é compreender os conhecimentos prévios dos alunos sobre divisibilidade e congruência, promover uma intervenção didática estruturada e avaliar os efeitos dessa intervenção no contexto real de ensino-aprendizagem.

No presente estudo, a intervenção consistiu em aulas sobre conteúdos matemáticos pouco explorados no currículo tradicional do Ensino Médio, mas de elevada relevância para o desenvolvimento do raciocínio lógico e de habilidades matemáticas aplicadas.

3.2 Contexto da pesquisa

O público-alvo da pesquisa foi composto por 150 estudantes da 3ª série do Ensino Médio, em fase final da educação básica e em preparação para exames como o ENEM e vestibulares. Desse total, 120 pertencem ao turno matutino e 30 ao turno vespertino. É importante destacar que, embora as turmas da 3ª série compreendam mais de 150 alunos, o número considerado foi reduzido em virtude de faltas nos dias de aplicação das atividades. Ainda assim, manteve-se o total de 150 estudantes como referência da amostra, mesmo havendo pequenas variações entre os participantes das atividades diagnóstica e de acompanhamento. A escolha desses estudantes ocorreu por conveniência, uma vez que são alunos regulares do professor-pesquisador responsável pelo estudo, o que favoreceu a implementação das atividades e o acompanhamento sistemático da intervenção.

A pesquisa foi realizada em uma escola estadual de Ensino Médio localizada no bairro Prainha, no município de Vila Velha (ES). Segundo o Índice de Desenvolvimento da Educação Básica (IDEB) de 2023, a instituição ocupa o 1º lugar entre as escolas estaduais de Vila Velha e o 2º lugar entre as escolas estaduais da região da Grande Vitória (INEP, 2023). A escola atende estudantes de diferentes turnos e apresenta um perfil diversificado. Atualmente, a instituição possui 748 estudantes distribuídos nos turnos matutino e vespertino, sendo que 240 estão matriculados nas turmas de 3ª série do Ensino Médio. A escolha da instituição se deu por critérios de conveniência e viabilidade, considerando também o vínculo pré-existente do pesquisador com a escola, o que favoreceu a implementação das atividades e o acompanhamento sistemático da intervenção.

Procedimentos de correção

As respostas dos estudantes foram classificadas em três categorias: corretas, incorretas e em branco. Consideraram-se corretas as respostas que apresentaram o resultado esperado conforme a resolução proposta apresentadas no apêndice; incorretas, aquelas que apresentaram resultado divergente, ainda que demonstrassem algum procedimento de cálculo; e em branco, os casos em que não houve tentativa de resolução. A correção inicial foi realizada pelo pesquisador, com base em uma rubrica previamente definida.

4 Aplicação da Atividade Diagnóstica

Com o intuito de verificar os conhecimentos prévios dos estudantes sobre divisibilidade e congruência, elaborou-se uma atividade diagnóstica de caráter avaliativo-exploratório, disponível no Apêndice A, juntamente com as soluções. A atividade foi aplicada em uma aula com duração de 50 minutos. A proposta contemplou questões de diferentes níveis de complexidade, variando desde o reconhecimento de critérios básicos de divisibilidade até problemas que exigiam raciocínio lógico mais elaborado e a aplicação de propriedades específicas. O estudo desses conteúdos fundamenta-se em conceitos clássicos da Teoria dos Números e da Aritmética, conforme discutido por Ribenboim (2001), Santos (2000) e Hefez (2011), os quais ressaltam a importância do reconhecimento de padrões numéricos, da estrutura algébrica dos inteiros e do domínio das operações fundamentais. Compreender tais propriedades é essencial não apenas para a resolução de problemas complexos, mas também para o desenvolvimento do raciocínio lógico, permitindo aos estudantes generalizar estratégias e aplicar conceitos matemáticos em situações diversas. O objetivo da atividade diagnóstica foi, portanto, levantar dados preliminares sobre o desempenho dos alunos, identificando padrões de raciocínio, lacunas conceituais e atitudes diante de desafios matemáticos.

Durante a aplicação, observou-se uma dificuldade recorrente em lidar com questões discursivas. Essa dificuldade pode ser compreendida à luz do modelo predominante de avaliação da escola e dos exames externos, como SAEB, PAEBES e ENEM, que utilizam majoritariamente o formato objetivo. Nesse contexto, valoriza-se apenas a alternativa correta, sem considerar o percurso cognitivo ou as estratégias adotadas. Na escola em questão, as avaliações oficiais seguem esse mesmo padrão, o que limita a identificação de níveis de habilidade ou inconsistências nos acertos.

Outro aspecto relevante foi a postura dos alunos diante de uma atividade que exigia esforço reflexivo, elaboração de estratégias e autonomia. Parte dos estudantes demonstrou desmotivação, abandonando a atividade mesmo após estímulos do aplicador, o que indica fragilidade no enfrentamento de tarefas desafiadoras. Em contrapartida, um grupo significativo mostrou engajamento, lançando mão de estratégias como tentativa e erro, o que revela disposição para enfrentar o desafio e ampliar o repertório de resolução de problemas.

4.1 Síntese dos Resultados

A Tabela 1 apresenta a distribuição de acertos, erros e questões em branco para cada item da atividade, permitindo uma leitura inicial do desempenho dos estudantes.

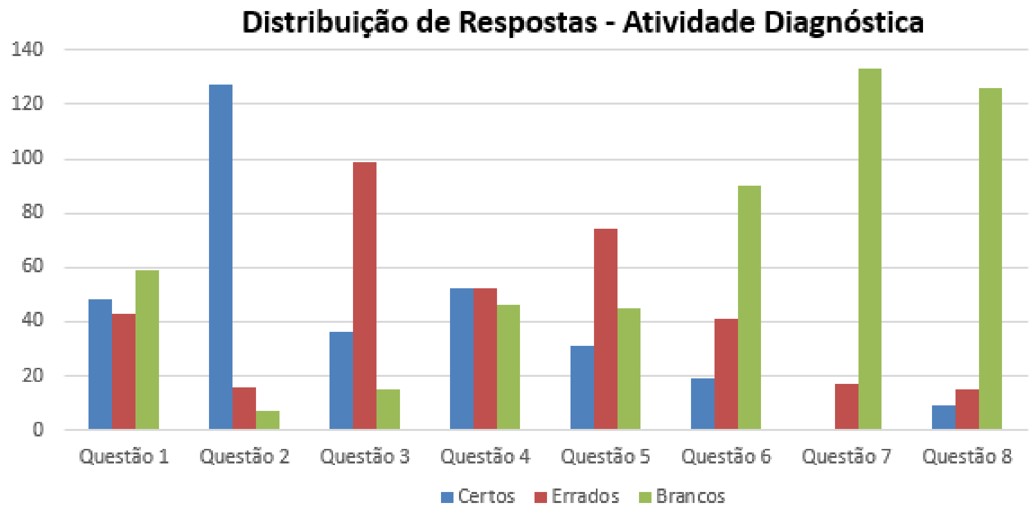
Tabela 1 – Distribuição de resultados da atividade diagnóstica

Questões	Acertos	Erros	Em Branco
Questão 1	48 (32,0%)	43 (28,7%)	59 (39,3%)
Questão 2	127 (84,7%)	16 (10,7%)	7 (4,6%)
Questão 3	36 (24,0%)	99 (66,0%)	15 (10,0%)
Questão 4	52 (34,7%)	52 (34,7%)	46 (30,6%)
Questão 5	31 (20,7%)	74 (49,3%)	45 (30,0%)
Questão 6	19 (12,7%)	41 (27,3%)	90 (60,0%)
Questão 7	0 (0,0%)	17 (11,3%)	133 (88,7%)
Questão 8	9 (6,0%)	15 (10,0%)	126 (84,0%)

Fonte: Autor (2025).

Para complementar a leitura numérica da tabela, a Figura 2 apresenta um gráfico comparativo das quantidades de acertos, erros e omissões por questão, facilitando a visualização das tendências gerais do desempenho dos alunos.

Figura 2 – Distribuição gráfica de acertos, erros e omissões na atividade diagnóstica.



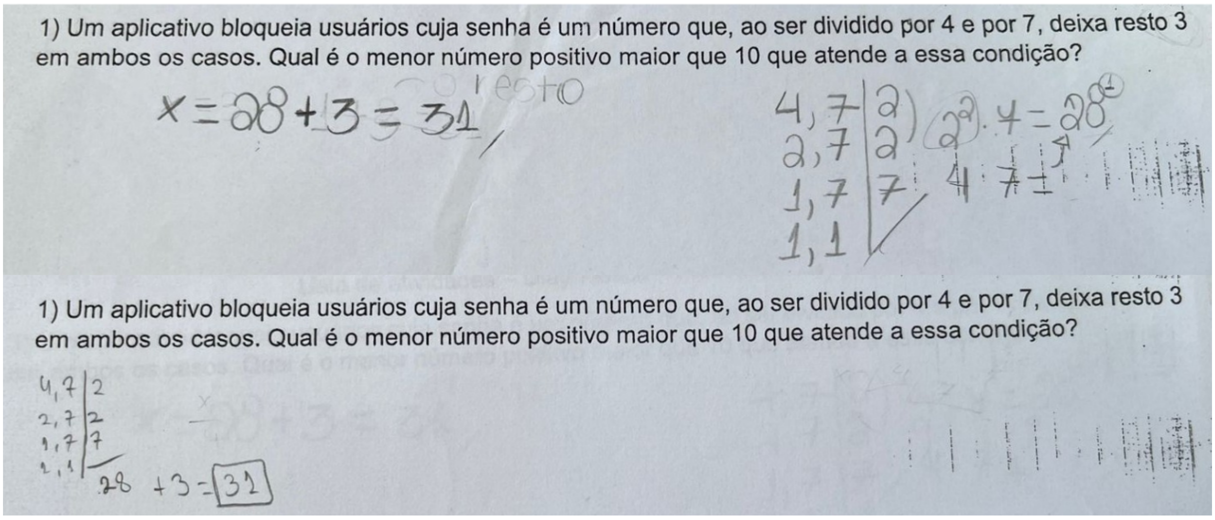
Fonte: Autor (2025).

Questão 1 – Um aplicativo bloqueia usuários cuja senha é um número que, ao ser dividido por 4 e por 7, deixa resto 3 em ambos os casos. Qual é o menor número positivo maior que 10 que atende a essa condição?

Apesar de se tratar de um exemplo das ideias de divisibilidade e congruência, observou-se que a maioria dos estudantes apresentou dificuldades em estruturar um procedimento adequado de resolução. Conforme evidenciado na Tabela 1, verificou-se um número expressivo de omissões, sugerindo que a ausência de familiaridade com o conceito gerou insegurança diante de um enunciado pouco contextualizado. Conforme ilustra a

Figura 3, é possível observar exemplos de resoluções apresentadas pelos estudantes na Questão 1.

Figura 3 – Resoluções de estudantes para a Questão 1 da Atividade Diagnóstica



Fonte: Autor (2025).

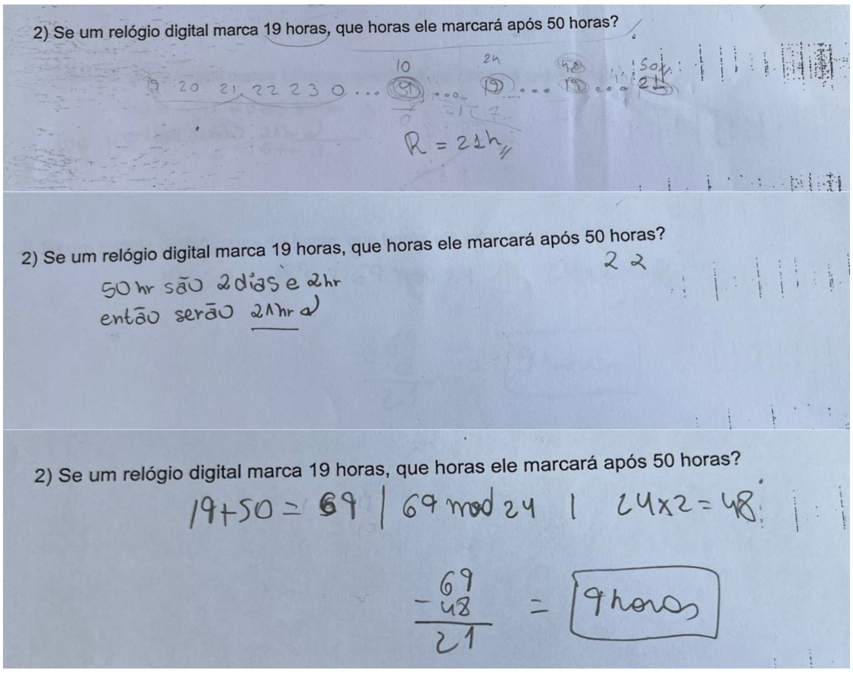
Observa-se que ambas as resoluções apresentaram procedimentos semelhantes, evidenciando que os estudantes recorreram ao conhecimento que tinham disponível, como, por exemplo, a utilização do mínimo múltiplo comum dos números somado ao resto 3. Essas estratégias mostram que eles pensaram de forma simples e correta, embora não generalista, refletindo métodos de resolução que não foram formalmente abordados na escola, mas que permitem chegar ao resultado de maneira adequada.

Questão 2 – Se um relógio digital marca 19 horas, que horas ele marcará após 50 horas?

Por se tratar de um contexto cotidiano e de fácil reconhecimento, constatou-se melhor desempenho em comparação com os demais itens da atividade. Esse resultado, conforme registrado na Tabela 1, reforça a constatação de que os alunos demonstram maior domínio em situações de aplicação direta, em que a congruência aparece de forma explícita e acessível.

Na Figura 4 encontram-se três resoluções distintas elaboradas para a Questão 2. Embora apresentadas de maneiras diferentes, todas se fundamentam no mesmo princípio teórico, o que demonstra que os estudantes compreenderam parcialmente a lógica do problema. Contudo, observa-se que a ausência de rigor formal na escrita matemática compromete a clareza das soluções. Esse aspecto pode ser compreendido à luz da cultura escolar marcada pela predominância de avaliações objetivas, nas quais se valoriza apenas a escolha da alternativa correta. Como consequência, os alunos tendem a registrar seus procedimentos de forma incompleta, muitas vezes restrita ao próprio entendimento, sem a preocupação em comunicar de maneira estruturada o raciocínio desenvolvido.

Figura 4 – Resoluções de estudantes para a Questão 2 da Atividade Diagnóstica



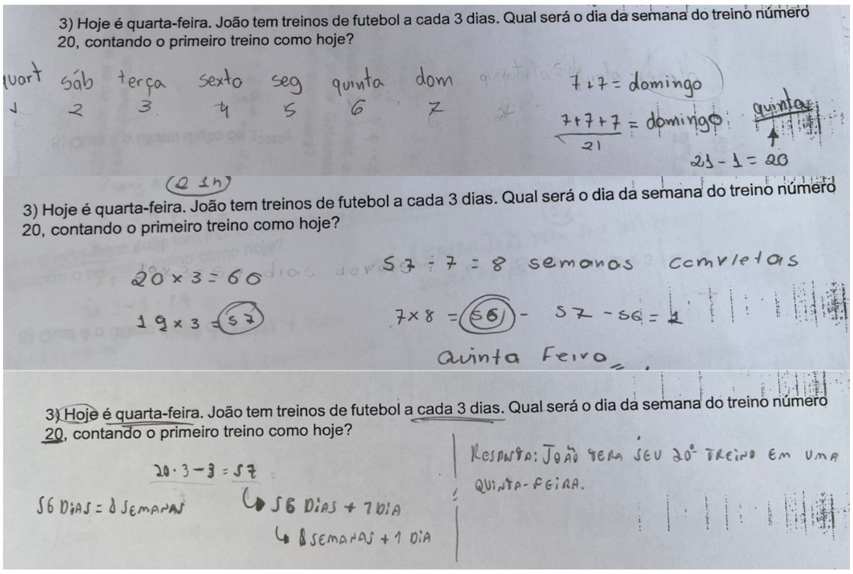
Fonte: Autor (2025).

Questão 3 – Hoje é quarta-feira. João tem treinos de futebol a cada 3 dias. Qual será o dia da semana do treino número 20, contando o primeiro treino como hoje? .

A terceira questão relacionava a contagem de treinos esportivos à repetição dos dias da semana, exigindo implicitamente a utilização do módulo 7. Considerando que os estudantes haviam sido expostos apenas a conceitos de divisibilidade, mas a maioria dos alunos não tinham conhecimento prévio sobre congruências, verificou-se que muitos recorreram a contagens lineares, em vez de mobilizar raciocínio modular de forma sistemática. Os dados da Tabela 1 evidenciam a predominância de erros, indicando que a associação entre periodicidade e congruência ainda não estava consolidada entre os alunos, o que torna compreensível o desempenho observado.

A Figura 5 apresenta três resoluções distintas elaboradas para a Questão 3. Embora todas tenham conduzido ao resultado esperado, observa-se que os estudantes mobilizaram estratégias diferenciadas: uma baseada em tentativa e erro, outra fundamentada no cálculo algébrico correto e uma terceira decorrente do reconhecimento de padrão. Esse conjunto de produções evidencia que, diante de um enunciado de fácil contextualização, os alunos recorrem a diferentes percursos cognitivos, o que reforça a pluralidade de modos de pensar matematicamente.

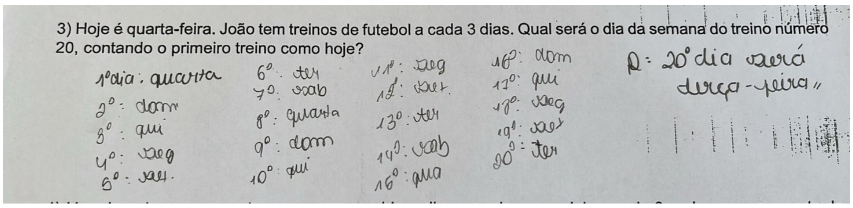
Figura 5 – Resoluções de estudantes para a Questão 3 da Atividade Diagnóstica



Fonte: Autor (2025).

Na análise das respostas à Questão 3 (Figura 6), constatou-se que, embora algumas resoluções estivessem corretas, esta foi a questão com maior incidência de erros. Observou-se um padrão recorrente na tomada de decisão: vários alunos superestimaram a contagem temporal, considerando quatro dias em vez de três, evidenciando dificuldade sistemática na manipulação de unidades temporais, mesmo em um contexto próximo à realidade dos estudantes.

Figura 6 – Erro observado na questão 3 da Atividade Diagnóstica



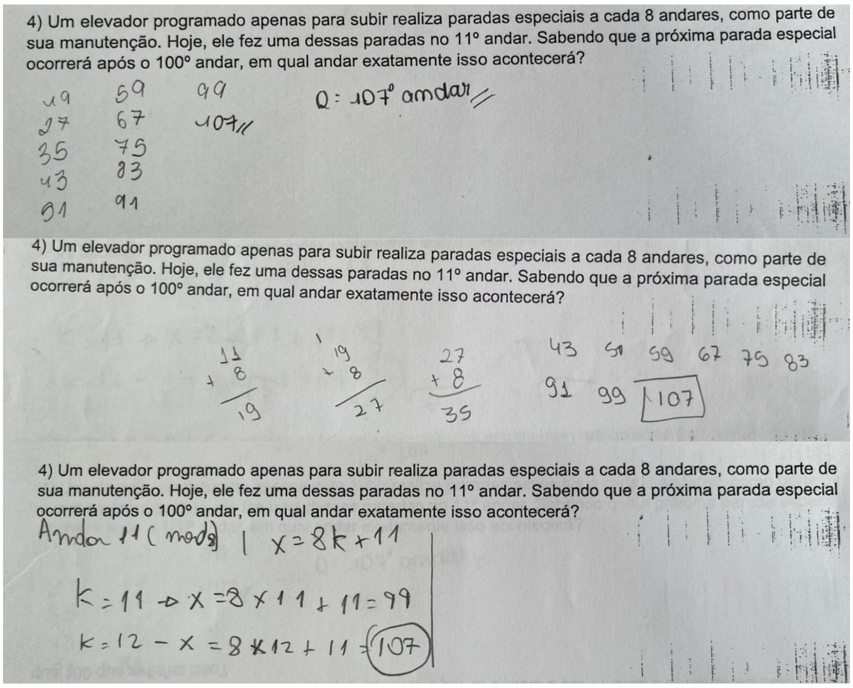
Fonte: Autor (2025).

Questão 4 – Um elevador programado apenas para subir realiza paradas especiais a cada 8 andares, como parte de sua manutenção. Hoje, ele fez uma dessas paradas no 11º andar. Sabendo que a próxima parada especial ocorrerá após o 100º andar, em qual andar exatamente isso acontecerá?

O quarto item solicitava a determinação de um andar em que o elevador realizaria nova parada, considerando intervalos fixos. Conforme a Tabela 1, os resultados se mostraram equilibrados entre acertos, erros e omissões, o que evidencia que parte dos estudantes compreendeu a regularidade envolvida, enquanto outros apresentaram dificuldades na interpretação da regra. Esse equilíbrio sugere que enunciados de complexidade intermediária, que exigem interpretação para além do cálculo direto, ainda provocam insegurança significativa.

A Figura 7 ilustra as resoluções da Questão 4 pelos estudantes. Apesar de existirem diferentes formas de abordagem, a maioria recorreu a soma sucessiva ou a progressão aritmética para chegar ao resultado, evidenciando um equilíbrio entre acertos e erros.

Figura 7 – Resoluções de estudantes para a Questão 4 da Atividade Diagnóstica



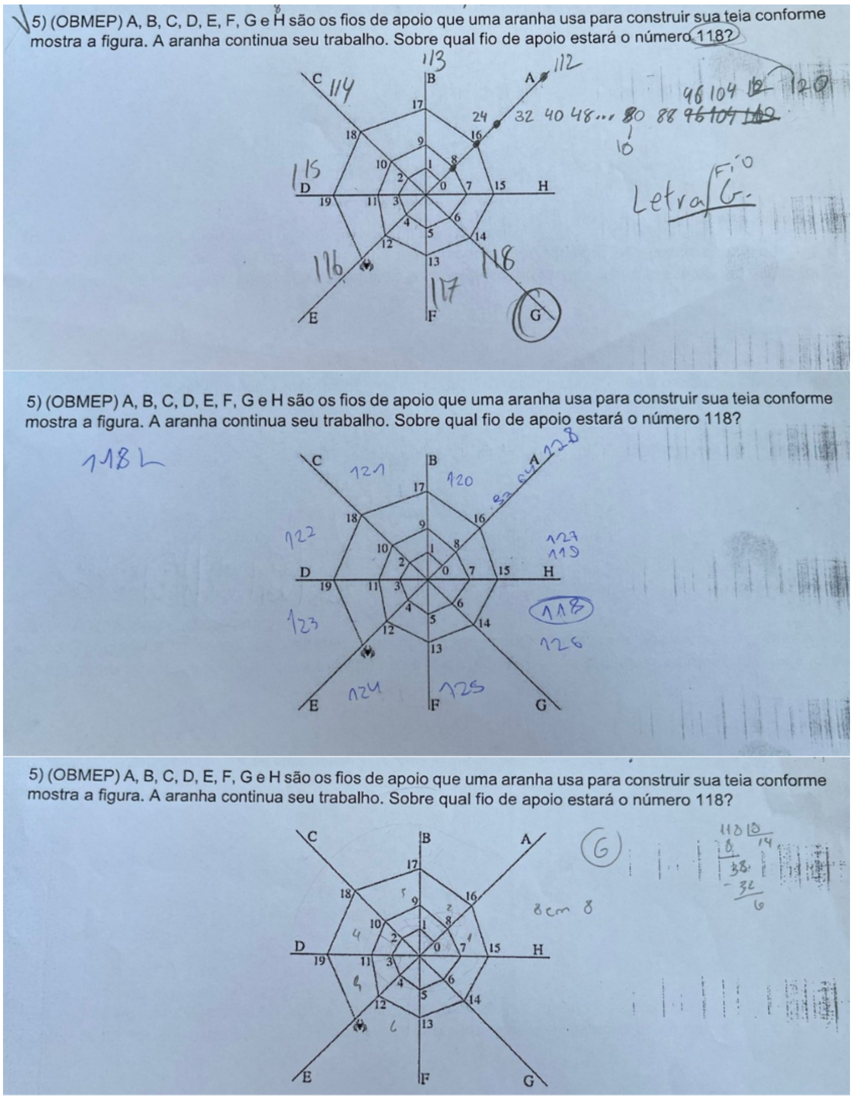
Fonte: Autor (2025).

Questão 5 – (OBMEP) A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?

A quinta questão, adaptada de uma prova da OBMEP, exigia a identificação de padrões em um contexto repetitivo. Os resultados indicam baixo índice de acertos e elevado número de erros, revelando dificuldades em generalizar regularidades cíclicas. Observa-se que muitos estudantes optaram por contagens exaustivas, o que evidencia fragilidade no raciocínio indutivo e ausência de estratégias sistemáticas para lidar com problemas desse tipo.

A Figura 8 ilustra as resoluções da Questão 5 pelos alunos, que, como discutido anteriormente, se apoiam principalmente em estratégias de contagem sucessiva, complementadas pelo uso da ideia de congruência em ciclos.

Figura 8 – Resoluções de estudantes para a Questão 5 da Atividade Diagnóstica



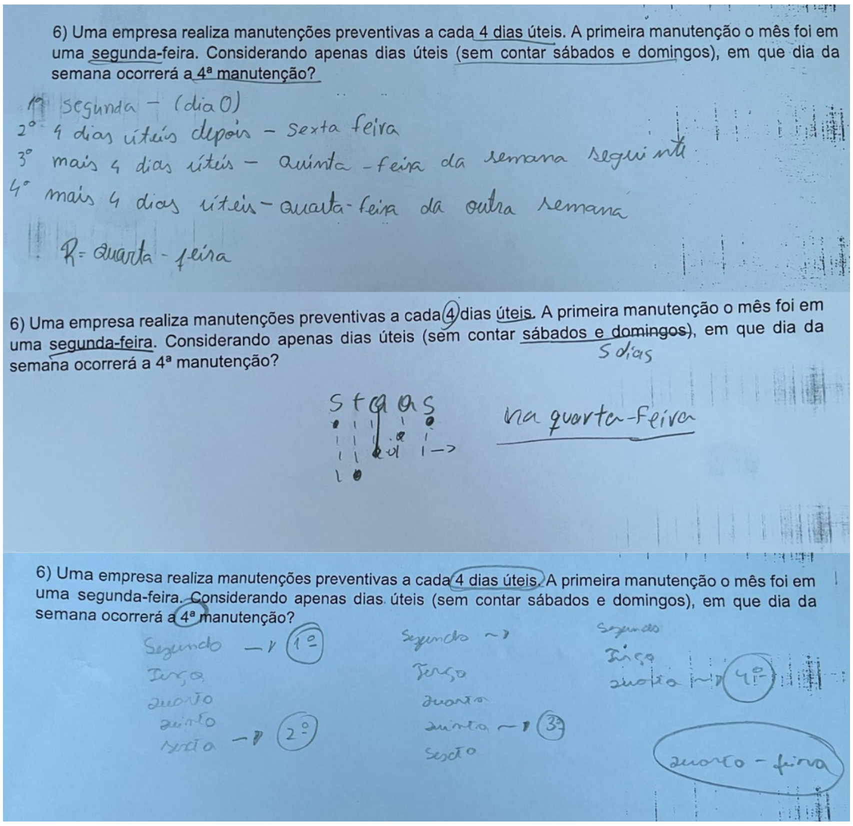
Fonte: Autor (2025).

Questão 6 – Uma empresa realiza manutenções preventivas a cada 4 dias úteis. A primeira manutenção do mês foi em uma segunda-feira. Considerando apenas dias úteis (sem contar sábados e domingos), em que dia da semana ocorrerá a 4ª manutenção?

A sexta questão apresentava a necessidade de considerar apenas dias úteis na contagem periódica, desconsiderando sábados e domingos. Essa condição adicional aumentou a complexidade do problema e resultou em elevado número de omissões, conforme evidenciado na Tabela 1. O desempenho sugere que, ao se depararem com restrições adicionais vinculadas ao calendário, os estudantes apresentam dificuldade em adaptar os procedimentos algorítmicos às condições impostas pela situação.

A Figura 9 ilustra as resoluções da Questão 6 pelos estudantes, evidenciando que eles estruturaram suas soluções com base na contagem e na organização dos dias úteis, demonstrando a utilização consciente de uma estratégia de sistematização temporal para alcançar o resultado

Figura 9 – Resoluções de estudantes para a Questão 6 da Atividade Diagnóstica



6) Uma empresa realiza manutenções preventivas a cada 4 dias úteis. A primeira manutenção o mês foi em uma segunda-feira. Considerando apenas dias úteis (sem contar sábados e domingos), em que dia da semana ocorrerá a 4ª manutenção?

1º segunda – (dia 0)
2º 4 dias úteis depois – sexta feira
3º mais 4 dias úteis – quinta-feira da semana seguinte
4º mais 4 dias úteis – quarta-feira da outra semana
R= quarta-feira

6) Uma empresa realiza manutenções preventivas a cada 4 dias úteis. A primeira manutenção o mês foi em uma segunda-feira. Considerando apenas dias úteis (sem contar sábados e domingos), em que dia da semana ocorrerá a 4ª manutenção?

5 dias
S T Q Q S
na quarta-feira

6) Uma empresa realiza manutenções preventivas a cada 4 dias úteis. A primeira manutenção o mês foi em uma segunda-feira. Considerando apenas dias úteis (sem contar sábados e domingos), em que dia da semana ocorrerá a 4ª manutenção?

Segundo → 1º
Terço
quarto
quinto
sexto → 2º
Segundo →
Terço
quarto
quinto → 3º
sexto
Segundo
Terço
quarto → 4º
quarta-feira

Fonte: Autor (2025).

Questão 7 – Um número x deixa resto 2 na divisão por 3, resto 3 na divisão por 5, e resto 2 na divisão por 7. Qual é o menor número maior que 100 que satisfaz essas condições?

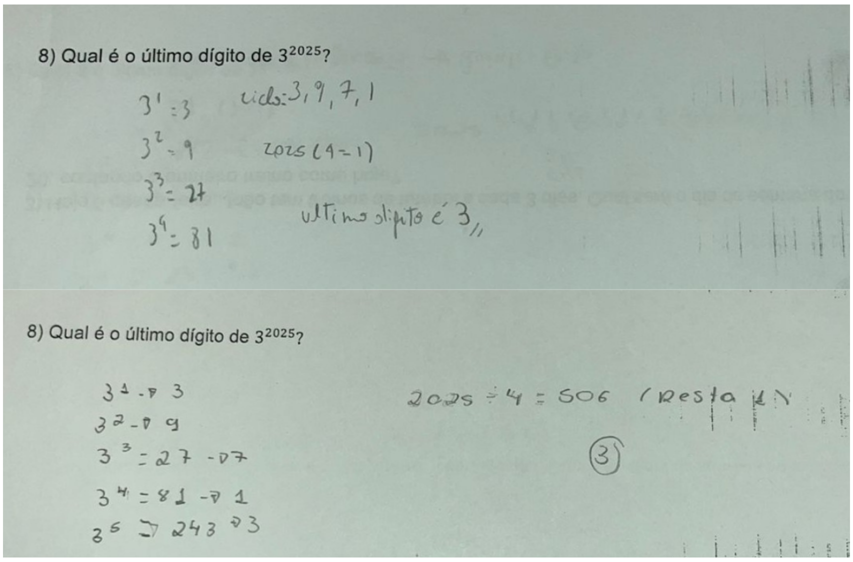
O sétimo item consistia em resolver um sistema de congruências envolvendo três condições distintas. Embora se trate de um problema clássico no campo da aritmética modular, sua resolução exige maior nível de raciocínio articulado. Conforme mostrado na Tabela 1, não foram registradas respostas corretas, sendo predominante a opção pela omissão. Tal resultado indica que os estudantes reconheceram a elevada complexidade da questão, mas não dispunham de repertório conceitual ou heurístico para propor soluções.

Questão 8 – Qual é o último dígito de 3^{2025}?

O último item solicitava a identificação do último dígito de uma potência, tarefa que exige a percepção de padrões modulares em base decimal. Os resultados apontam alto índice de omissões e baixo desempenho geral. Esse dado sugere que, diante de problemas que demandam maior abstração e reconhecimento de regularidades não evidentes, os estudantes tendem a desistir da tentativa, revelando fragilidades tanto conceituais quanto atitudinais.

A Figura 10 ilustra as resoluções dos estudantes para a Questão 8, destacando que ambos empregaram a mesma estratégia, sendo, no entanto, entre os poucos a utilizá-la, o que evidencia uma abordagem menos frequente dentro do grupo.

Figura 10 – Resoluções de estudantes para a Questão 8 da Atividade Diagnóstica



Fonte: Autor (2025).

Resumo da análise individual

A análise individualizada das questões evidencia três aspectos centrais no desempenho dos estudantes:

- Segurança em situações de aplicação imediata – Nos problemas de caráter mais direto e contextualizados em situações familiares, observou-se bom desempenho, o que indica domínio de procedimentos básicos.
- Dificuldades em problemas de complexidade intermediária – Em questões que exigiam a identificação de ciclos ou regularidades, verificou-se maior proporção de erros, revelando fragilidade no raciocínio indutivo e na generalização.
- Resistência diante de problemas mais complexos – Nas questões que demandavam abstração mais elevada, predominou o abandono da resolução, evidenciado pelo número elevado de omissões.

Constata-se, portanto, que os estudantes apresentam relativo domínio dos procedimentos algorítmicos mais diretos, mas encontram limitações progressivas à medida que o nível de complexidade aumenta. Esse cenário reforça a necessidade de práticas pedagógicas que ultrapassem a mecanização de algoritmos e favoreçam o desenvolvimento de competências cognitivas mais amplas, como a persistência, a autonomia e a capacidade de lidar com situações desafiadoras.

5 Intervenção Didática

A partir da aplicação da atividade diagnóstica realizada com os estudantes, elaborou-se uma sequência de quatro aulas, de caráter investigativo, com o objetivo de superar as principais dificuldades identificadas e promover a consolidação dos conceitos fundamentais relacionados à divisibilidade e às congruências. O planejamento detalhado das quatro aulas, incluindo a distribuição do tempo, as estratégias didáticas e as atividades propostas, está apresentado no Apêndice B.

5.1 Aula 1: Divisão Euclidiana e Números Primos

Uma das primeiras dificuldades constatadas referia-se à compreensão da divisão euclidiana e, em especial, à noção de "resto". Observou-se que muitos alunos, ao efetuar divisões, prolongavam o processo até obter quocientes decimais ou insistiam na continuação do cálculo até que o resto fosse nulo. Essa lacuna conceitual remete a conteúdos do Ensino Fundamental, particularmente à habilidade EF06MA03 (BRASIL, 2018), que orienta o estudante a resolver e elaborar problemas com números naturais, envolvendo adição, subtração, multiplicação, divisão, potenciação e radiciação, utilizando estimativas, o cálculo mental e algoritmos.

Com base nesse diagnóstico, a aula foi dedicada à retomada da divisão euclidiana, com exemplos práticos e exercícios introdutórios. Observou-se também fragilidade na definição de números primos, conceito essencial para a compreensão de diversos procedimentos. Por isso, foi relembrada a definição de primos e, em seguida, revisados os critérios de divisibilidade por 2, 3, 5, 7, 9 e 11, com exemplos e atividades de fixação. Esses elementos serviram de base para a transição ao estudo do máximo divisor comum (MDC) e do mínimo múltiplo comum (MMC).

Durante essa etapa, constatou-se que o conceito de MMC tende a ser mais familiar aos alunos, uma vez que é frequentemente utilizado em situações cotidianas, especialmente na adição e subtração de frações com denominadores diferentes. Em contrapartida, o MDC costuma gerar maior dificuldade de compreensão, por aparecer com menor frequência em contextos escolares e práticos. Essa diferença de familiaridade foi considerada na organização das atividades e na mediação das discussões em sala.

A sequência de conteúdos está em consonância com a habilidade EM13MAT102, que propõe a resolução e elaboração de problemas envolvendo divisibilidade, múltiplos, divisores, números primos e compostos, além do cálculo do MDC e do MMC, com ou sem recursos tecnológicos.(BRASIL, 2018)

5.2 Aula 2: Introdução às Congruências Lineares e Pequeno Teorema de Fermat

Na segunda aula, introduziu-se o estudo das congruências lineares. Embora a BNCC (BRASIL, 2018) não faça referência explícita às congruências modulares, é possível articulá-las às habilidades EF06MA03, EF07MA01, EM13MAT102 e EM13MAT301, que preveem a análise e utilização de procedimentos algorítmicos em diferentes contextos, inclusive em investigações matemáticas e aplicações em outras áreas do conhecimento.

Além disso, foi apresentado o Pequeno Teorema de Fermat, relacionando-o à resolução de congruências, seguido de exercícios práticos que permitiram verificar a compreensão inicial dos estudantes.

5.3 Aula 3: Resolução de Exercícios e Consolidação dos Conceitos

A terceira aula concentrou-se na resolução de exercícios envolvendo congruências modulares, congruências lineares e aplicações do Pequeno Teorema de Fermat. Nessa etapa, verificou-se avanço progressivo na aprendizagem, ainda que acompanhado de dúvidas pontuais, que foram trabalhadas ao longo da aula, contribuindo para a consolidação gradual dos conceitos.

5.4 Aula 4: Sistemas de Congruências Lineares e Teorema Chinês do Resto

A quarta aula foi destinada ao estudo dos sistemas de congruências lineares, com a introdução do Teorema Chinês do Resto. Foram apresentados exemplos e aplicações em situações cotidianas, estabelecendo vínculos entre a teoria e o uso prático dos conteúdos. Devido à complexidade do tema, a duração dessa aula foi estendida para 100 minutos, em contraste com os 50 minutos das aulas anteriores.

Como fechamento da intervenção, aplicou-se uma segunda lista de exercícios, cujo objetivo foi comparar o desempenho dos estudantes em relação à atividade diagnóstica inicial, possibilitando avaliar a evolução da aprendizagem ao longo da sequência didática.

6 Aplicação Final

Com o objetivo de verificar a assimilação dos conteúdos trabalhados nas aulas destinadas ao aprofundamento dos conceitos de divisibilidade e congruência, aplicou-se uma segunda atividade aos estudantes. Esta etapa configurou-se como a avaliação final da proposta didática, funcionando também como instrumento comparativo em relação à atividade diagnóstica apresentada no Capítulo 4. As questões desta segunda aplicação, disponíveis no Apêndice C, foram elaboradas a partir dos mesmos eixos conceituais da diagnóstica, mas reformuladas e complementadas, de modo a permitir uma análise mais precisa da evolução dos estudantes.

As questões propostas exigiam não apenas a aplicação de algoritmos e propriedades de divisibilidade, mas também a interpretação dos enunciados e a justificativa das estratégias utilizadas, possibilitando avaliar tanto a dimensão procedimental quanto a argumentativa. A elaboração da atividade levou em conta a relevância do estudo de divisibilidade e congruência para a formação do pensamento aritmético, em consonância com os princípios discutidos por Hefez (2011).

Na análise dos resultados, constatou-se que a maior parte dos estudantes apresentou avanços na compreensão e no uso das propriedades de congruência. Em comparação com a atividade diagnóstica, houve redução dos erros relacionados à interpretação de restos e ao uso inadequado do algoritmo da divisão. Além disso, observou-se maior frequência de resoluções em que os alunos explicitaram de forma clara e coerente o raciocínio adotado, indicando progresso conceitual. Persistiram, contudo, dificuldades em situações que exigiam generalizações ou manipulação de expressões algébricas no contexto das congruências, o que reforça a necessidade de continuidade no trabalho pedagógico voltado à transição entre cálculo numérico e formalização algébrica.

A Tabela 2 apresenta a distribuição dos resultados obtidos na segunda aplicação, permitindo uma leitura detalhada do desempenho em cada questão.

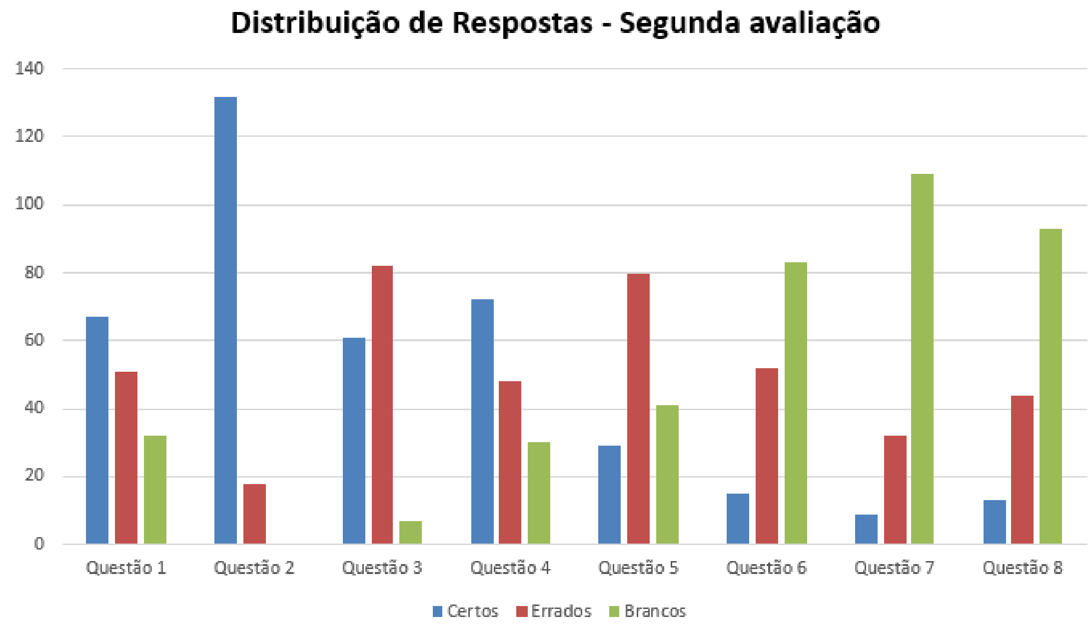
Tabela 2 – Distribuição de resultados por questão da segunda aplicação

Questões	Acertos	Erros	Em Branco
Questão 1	67 (44,7%)	51 (34,0%)	32 (21,3%)
Questão 2	132 (88,0%)	18 (12,0%)	0 (0,0%)
Questão 3	61 (40,7%)	82 (54,7%)	7 (4,7%)
Questão 4	72 (48,0%)	48 (32,0%)	30 (20,0%)
Questão 5	29 (19,3%)	80 (53,3%)	41 (27,3%)
Questão 6	15 (10,0%)	52 (34,7%)	83 (55,3%)
Questão 7	9 (6,0%)	32 (21,3%)	109 (72,7%)
Questão 8	13 (8,7%)	44 (29,3%)	93 (62,0%)

Fonte: Autor (2025).

Para complementar a leitura numérica da tabela, a Figura 11 sintetiza graficamente a distribuição de acertos, erros e omissões por questão, permitindo uma visualização imediata das tendências gerais do desempenho dos estudantes após a intervenção.

Figura 11 – Distribuição gráfica de acertos, erros e omissões na segunda aplicação.



Fonte: Autor (2025).

6.1 Síntese dos Resultados.

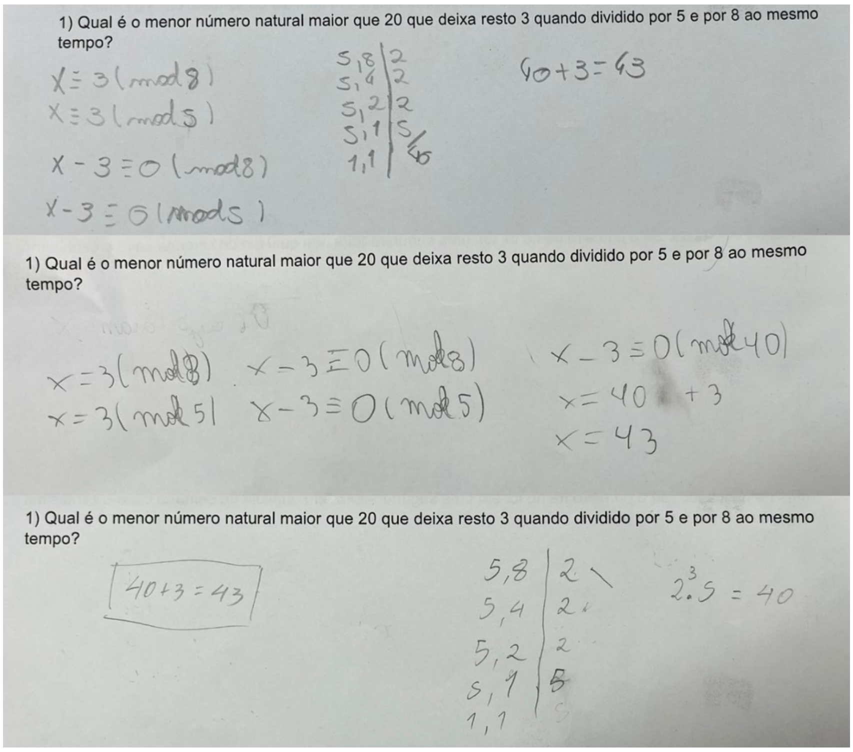
A seguir, são examinadas detalhadamente as respostas apresentadas pelos estudantes na segunda atividade, buscando identificar padrões de raciocínio, estratégias utilizadas, acertos e dificuldades persistentes. Esta análise permite compreender de que maneira os conteúdos trabalhados nas aulas foram assimilados e como os alunos aplicaram conceitos de divisibilidade e congruência na resolução dos problemas propostos.

Questão 1 – Qual é o menor número natural maior que 20 que deixa resto 3 quando dividido por 5 e por 8 ao mesmo tempo?

O índice de acertos mostra que parte dos alunos conseguiu compreender a ideia de congruências simultâneas, mas os erros e omissões ainda revelam dificuldades mesmo após as aulas de intervenção.

Um aspecto relevante é a diversidade de estratégias utilizadas: alguns estudantes buscaram soluções por tentativa, outros recorreram ao mínimo múltiplo comum, e houve ainda respostas incompletas ou incoerentes. Essa variedade de caminhos será ilustrada na figura 12, que sintetiza as formas de resolução mais recorrentes entre os alunos.

Figura 12 – Resoluções de estudantes para a Questão 1 da Segunda Aplicação



Fonte: Autor (2025).

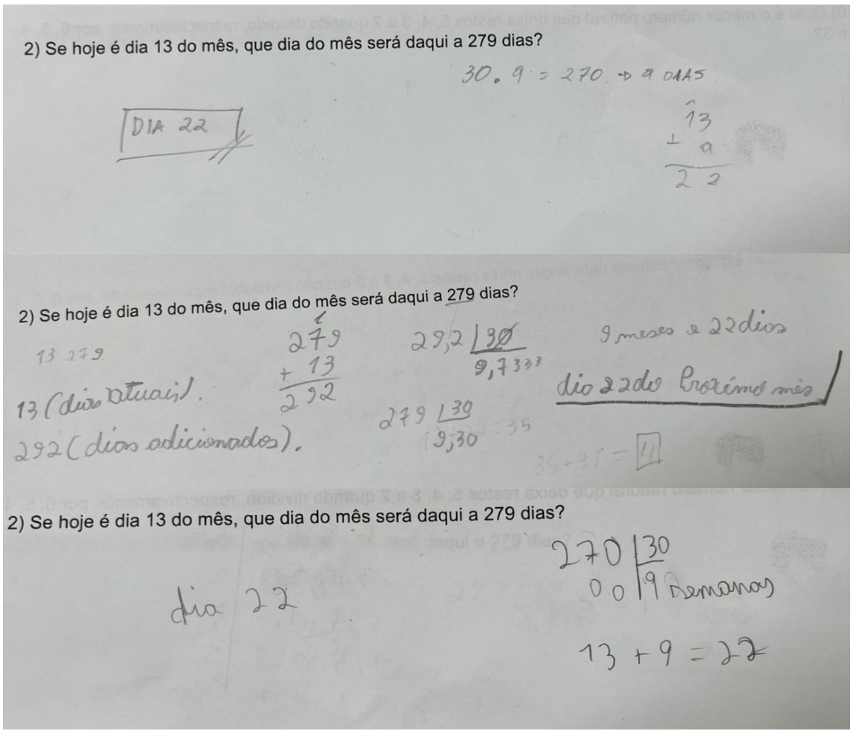
Questão 2 – Se hoje é dia 13 do mês, que dia do mês será daqui a 279 dias?

O problema envolve o uso de congruências no calendário, em especial a identificação do resto da divisão de 279 por 30 (considerando meses de 30 dias como padrão simplificado, o que foi destacado e discutido nas aulas de intervenção).

O desempenho foi bastante satisfatório sendo que não houve respostas em branco. Esse dado sugere que o contexto da questão, relacionado ao calendário e, portanto, mais próximo do cotidiano dos estudantes, contribuiu para que todos tentassem uma resolução.

As resoluções apresentadas revelam que alguns alunos utilizaram diretamente o cálculo do quociente e do resto, enquanto outros optaram por estratégias mais informais, como somas sucessivas ou aproximações sucessivas. Essas diferentes formas de abordagem são apresentadas na figura 13, que sintetiza as estratégias mais recorrentes entre os estudantes.

Figura 13 – Resoluções de estudantes para a Questão 2 da Segunda Aplicação



Fonte: Autor (2025).

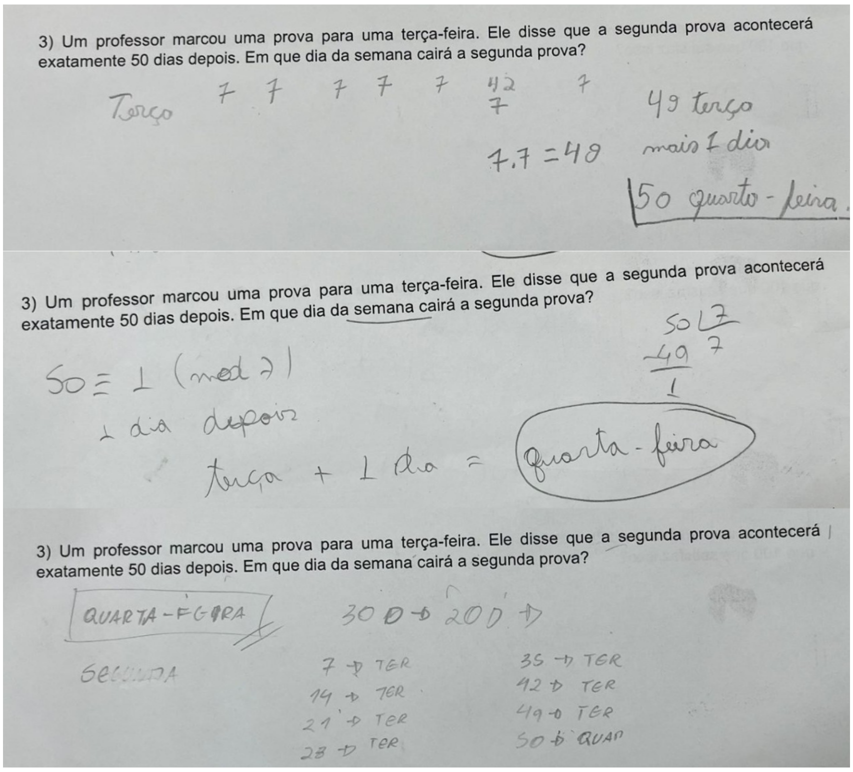
Questão 3 – Um professor marcou uma prova para uma terça-feira. Ele disse que a segunda prova acontecerá exatamente 50 dias depois. Em que dia da semana cairá a segunda prova?

Para resolvê-la corretamente, seria necessário considerar o ciclo semanal e, portanto, calcular o resto da divisão de 50 por 7.

Os resultados mostraram maior dificuldade pois o número expressivo de erros revela uma interpretação equivocada recorrente. Muitos estudantes aplicaram a congruência em relação a 30, associando 30 dias com a ideia de um "mês completo", e concluíram incorretamente que após 30 dias a prova voltaria a cair em uma terça-feira. Essa confusão entre o ciclo semanal (módulo 7) e o ciclo mensal (módulo 30) foi a principal responsável pelo alto índice de respostas incorretas.

As diferentes estratégias de resolução estão sintetizados na figura 14, que reúne os tipos de respostas apresentados pelos estudantes.

Figura 14 – Resoluções de estudantes para a Questão 3 da Segunda Aplicação



Fonte: Autor (2025).

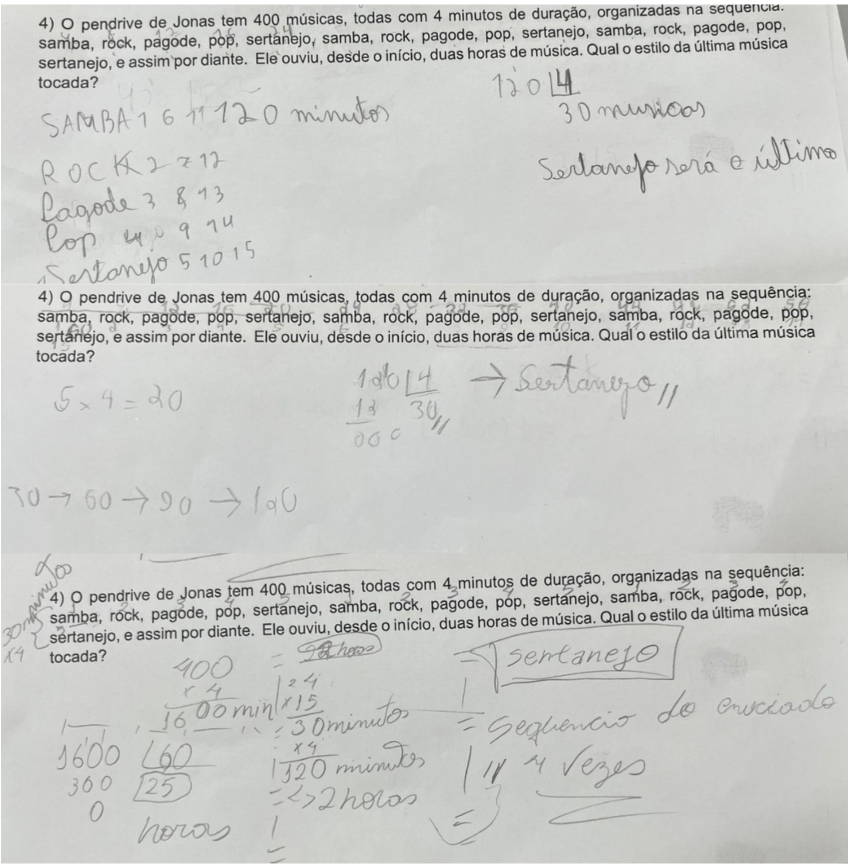
Questão 4 – (OBMEP) O pendrive de Jonas tem 400 músicas, todas com 4 minutos de duração, organizadas na sequência: samba, rock, pagode, pop, sertanejo, samba, rock, pagode, pop, sertanejo, samba, rock, pagode, pop, sertanejo, e assim por diante. Ele ouviu, desde o início, duas horas de música. Qual o estilo da última música tocada?.

Para a resolução correta, era necessário transformar o tempo total em número de músicas, e em seguida aplicar a ideia de congruência em relação à sequência de cinco estilos.

Apesar de uma quantidade relevante de acertos, os erros e omissões revelam que muitos estudantes se confundiram com os diferentes dados do enunciado, em especial com a presença de “400 músicas”, “4 minutos por música” e “duas horas de reprodução”. Essa multiplicidade de informações levou parte dos alunos a se perder nos cálculos preliminares, sem sequer chegar à etapa de aplicação da congruência por 5.

As soluções apresentadas evidenciam tanto estratégias corretas quanto raciocínios incompletos ou baseados em interpretações equivocadas dos dados. Algumas abordagens são apresentadas na figura 15, que sintetiza os principais caminhos percorridos pelos alunos.

Figura 15 – Resoluções de estudantes para a Questão 4 da Segunda Aplicação



Fonte: Autor (2025).

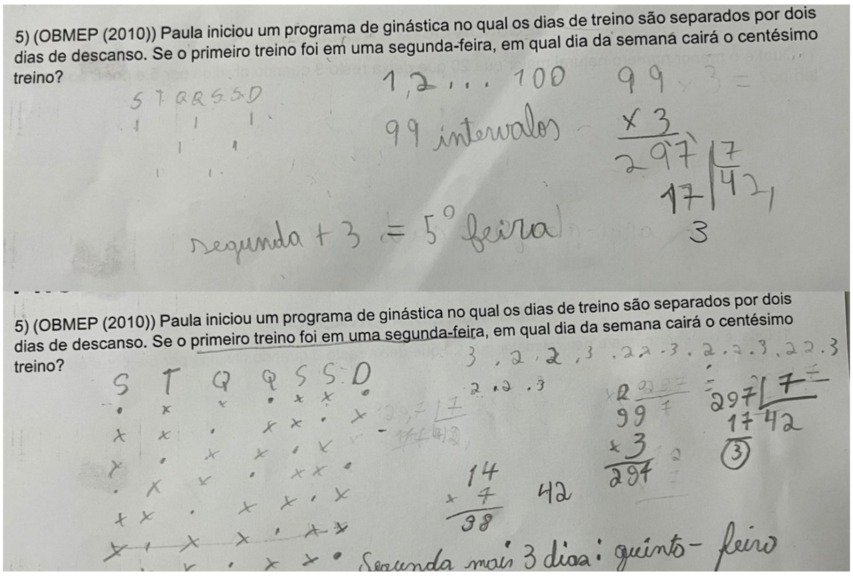
Questão 5 – Paula iniciou um programa de ginástica no qual os dias de treino são separados por dois dias de descanso. Se o primeiro treino foi em uma segunda-feira, em qual dia da semana cairá o centésimo treino?

A quinta questão propunha determinar o dia da semana correspondente ao centésimo treino de Paula, considerando que os treinos ocorrem com intervalo de dois dias de descanso e que o primeiro treino foi em uma segunda-feira. Para resolver corretamente, seria necessário aplicar raciocínio modular, considerando o ciclo de treino e descanso, e calcular o resto da divisão dos dias por 3 dias.

O elevado número de erros e respostas em branco indica que muitos estudantes se sentiram intimidados pelo grande número de treinos (100) e tiveram dificuldade em visualizar ou aplicar sistematicamente o padrão cíclico.

As soluções apresentadas revelam tanto abordagens corretas quanto tentativas incompletas ou interrupções na resolução devido à magnitude do número de treinos. Essas diferentes estratégias são sintetizadas na figura 16.

Figura 16 – Resoluções de estudantes para a Questão 5 da Segunda Aplicação



Fonte: Autor (2025).

Questão 6 – Qual é o menor número natural que deixa restos 5, 4, 3 e 2 quando dividido, respectivamente, por 6, 5, 4 e 3?

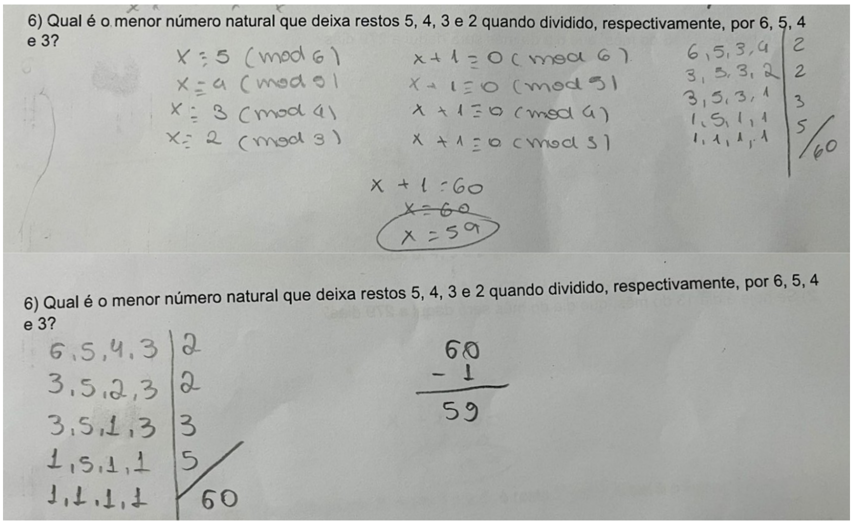
Para resolvê-la corretamente, seria necessário aplicar conceitos de congruências simultâneas ou, equivalentemente, buscar um número que satisfaça todas as condições de divisibilidade impostas.

Os resultados evidenciam a complexidade percebida pelos estudantes, Apesar de os alunos terem participado de aulas sobre os assuntos abordados, muitos se sentiram desmotivados diante de uma questão direta, sem contextualização, que aparentava maior dificuldade.

Por outro lado, alguns estudantes conseguiram relacionar o enunciado a exemplos trabalhados em sala de aula, utilizando estratégias informais ou aproximações intuitivas, mesmo que não tenham formalizado completamente a resolução. Esse contraste entre desmotivação e lembrança parcial de conceitos evidencia a importância do contexto para engajamento e aplicação dos conhecimentos adquiridos.

As diferentes estratégias, bem como os tipos de respostas apresentadas, estão sintetizadas na figura 17.

Figura 17 – Resoluções de estudantes para a Questão 6 da Segunda Aplicação



Fonte: Autor (2025).

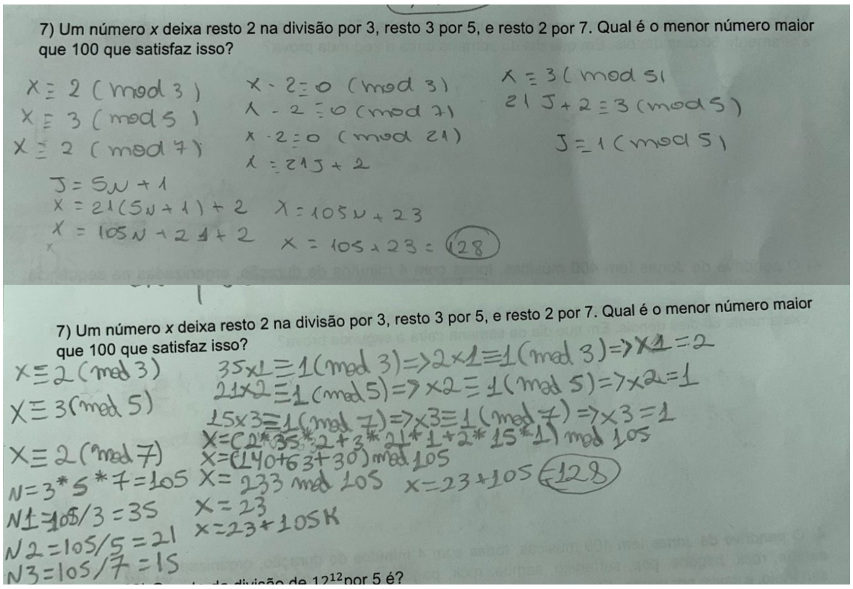
Questão 7 – Um número x deixa resto 2 na divisão por 3, resto 3 na divisão por 5 e resto 2 na divisão por 7. Qual é o menor número *maior que* 100 que satisfaz essas condições?

Trata-se de um problema de congruências simultâneas, que pode ser resolvido utilizando o Teorema Chinês dos Restos ou por métodos de substituição e tentativa sistemática.

Os resultados indicam grande dificuldade. Essa questão havia sido aplicada anteriormente na atividade diagnóstica, quando nenhum aluno conseguiu resolvê-la. A repetição permitiu observar um efeito interessante: alguns estudantes, motivados pela curiosidade despertada na primeira aplicação, buscaram aplicar o Teorema Chinês dos Restos, mesmo antes das aulas sobre o tema. Outros alunos utilizaram estratégias baseadas em congruências parciais, combinadas com substituição de variáveis, conseguindo chegar à solução de forma mais informal.

A figura 18 apresenta as diferentes estratégias de resolução observadas, evidenciando tanto os caminhos formais quanto as aproximações intuitivas utilizadas pelos estudantes.

Figura 18 – Resoluções de estudantes para a Questão 7 da Segunda Aplicação



Fonte: Autor (2025).

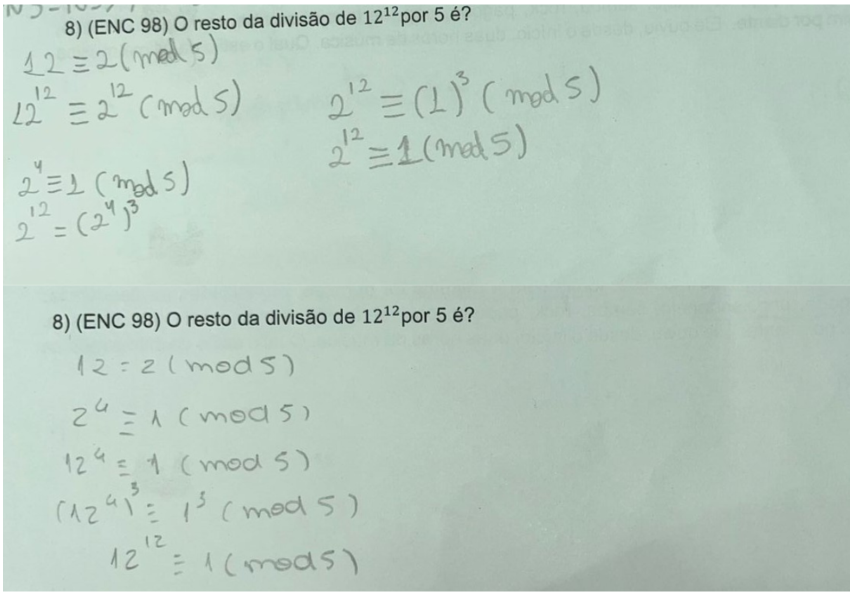
Questão 8 – (ENQ98) O resto da divisão de 12^{12} por 5 é?

Para resolvê-la corretamente, era necessário identificar padrões nas potências de 12 módulo 5 ou aplicar propriedades de congruências.

Os resultados indicam que a maioria dos alunos encontrou dificuldades na resolução. Entre os acertos, alguns estudantes observaram corretamente o padrão do algarismo das unidades, enquanto outros aplicaram diretamente a congruência e suas propriedades para chegar à resposta correta.

As estratégias e abordagens utilizadas pelos alunos estão sintetizadas na figura 19, que evidencia tanto os métodos formais quanto as soluções baseadas em padrões observados.

Figura 19 – Resoluções de estudantes para a Questão 8 da Segunda Aplicação



Fonte: Autor (2025).

Resumo da análise individual

A análise das respostas da segunda lista revela avanços significativos em relação à atividade diagnóstica, embora ainda persistam dificuldades em questões que exigem maior abstração ou ausência de contexto. Questões envolvendo congruências simples ou situações próximas do cotidiano, como datas e ciclos semanais, apresentaram alto índice de acertos, enquanto problemas mais complexos ou sem contextualização direta, como congruências simultâneas e potências modulares, resultaram em maior número de erros e respostas em branco.

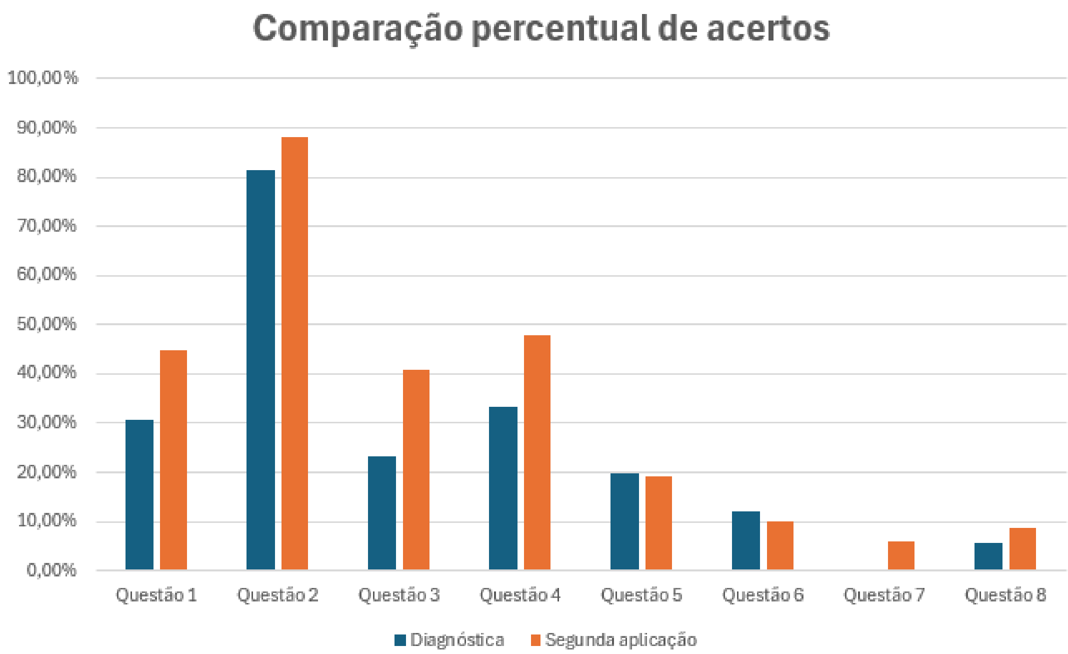
Observa-se que, mesmo quando não resolveram formalmente, muitos alunos recorreram a estratégias intuitivas ou lembraram de exemplos trabalhados em sala, demonstrando assimilação parcial dos conceitos. Além disso, a repetição de questões da atividade diagnóstica permitiu verificar o impacto da familiaridade com o problema e o despertar da curiosidade em alguns estudantes, evidenciando a importância de intervenções graduais e contextualizadas para o desenvolvimento do raciocínio matemático.

7 Comparação de Resultados

Este capítulo tem como objetivo comparar os resultados obtidos pelos estudantes na atividade diagnóstica e na segunda lista aplicada após a intervenção didática. A análise busca evidenciar os avanços alcançados, as dificuldades persistentes e as mudanças de abordagem na resolução dos problemas, de modo a compreender em que medida o processo de ensino contribuiu para a aprendizagem dos conteúdos de divisibilidade e congruência.

Para visualizar de forma mais clara a evolução do desempenho dos estudantes entre a atividade diagnóstica e a segunda aplicação, a Figura 20 apresenta um gráfico comparativo com os percentuais de acertos em cada questão.

Figura 20 – Comparação percentual de acertos entre a atividade diagnóstica e a segunda aplicação.



Fonte: Autor (2025).

7.1 Comparação questão a questão

Questão 1

Na atividade diagnóstica, 48 alunos acertaram, 43 erraram e 59 deixaram em branco. Na segunda aplicação, observou-se um aumento no desempenho: 67 acertos, 51 erros e 32 em branco.

Apesar de os enunciados não serem idênticos, ambos exigem compreensão de congruências simultâneas. A intervenção didática favoreceu um maior número de estudantes a resolver problemas desse tipo, refletido no aumento dos acertos e na redução das respostas em branco. As estratégias identificadas incluem tentativas sucessivas, uso implícito do mínimo múltiplo comum e abordagens por congruências formais; os erros mais frequentes derivaram de interpretações incorretas dos restos ou procedimentos aritméticos incompletos. Esses aspectos serão aprofundados nas análises qualitativas das respostas exemplares.

Questão 2

Na atividade diagnóstica, 127 alunos acertaram, 16 erraram e 7 deixaram em branco. Na segunda aplicação, o número de acertos aumentou para 132, com 18 erros e nenhuma resposta em branco.

Embora os contextos tenham diferido, ambos exigiam o uso da aritmética modular em situações cotidianas. O conceito já era amplamente dominado na primeira aplicação, mas a intervenção contribuiu para reduzir omissões e manter elevado o índice de acertos. O fato de nenhum estudante ter deixado a questão em branco na segunda lista sugere maior engajamento, possivelmente devido à familiaridade com o contexto.

Questão 3

Na atividade diagnóstica, 36 alunos acertaram, 99 erraram e 15 deixaram em branco. Na segunda aplicação, os acertos subiram para 61, com 81 erros e 27 respostas em branco.

Os contextos diferentes envolveram ciclos de dias da semana, exigindo aritmética modular. Observa-se progresso na compreensão dos ciclos, refletido no aumento dos acertos. Entretanto, o aumento das respostas em branco indica que alguns estudantes ainda hesitaram, sugerindo a necessidade de maior consolidação do conteúdo.

Questão 4

Na atividade diagnóstica, 52 alunos acertaram, 52 erraram e 46 deixaram em branco. Na segunda aplicação, 72 alunos acertaram, 48 erraram e 30 deixaram em branco.

Apesar das diferenças contextuais — uma questão sobre ciclos de andares de elevador e outra sobre reprodução de músicas em sequência —, ambas exigiam aplicação de padrões cíclicos. Houve melhora no desempenho, com aumento dos acertos e redução das respostas em branco, indicando que a intervenção ajudou a consolidar a habilidade de identificar padrões em situações práticas.

Questão 5

Na atividade diagnóstica, 31 alunos acertaram, 74 erraram e 45 deixaram em branco. Na segunda aplicação, houve leve queda nos acertos (29), aumento de erros (80) e pequenas variações nas respostas em branco (41).

Os contextos diferiram — construção de uma teia de aranha versus determinação do dia da semana de um treino —, mas ambos exigiam padrões cíclicos. O desempenho similar sugere que os alunos ainda enfrentam dificuldades na aplicação consistente desses conceitos em contextos variados.

Questão 6

Na atividade diagnóstica, 19 alunos acertaram, 41 erraram e 90 deixaram em branco. Na segunda aplicação, 15 acertaram, 52 erraram e 83 deixaram em branco.

As questões envolveram previsões em dias úteis e determinação do menor número natural que satisfaz restos específicos, exigindo aritmética modular e raciocínio lógico. O desempenho permaneceu baixo, com predomínio de erros e omissões, indicando necessidade de intervenções mais direcionadas para consolidar a habilidade de manipular restos e divisões sucessivas.

Questão 7

A sétima questão foi idêntica nas duas aplicações. Na primeira, nenhum aluno acertou, 17 erraram e 133 deixaram em branco; na segunda, 9 acertaram, 32 erraram e 109 deixaram em branco.

A questão exigia resolução de sistemas de congruências. Apesar da melhora nos acertos, o desempenho geral permaneceu baixo, com predominância de respostas em branco. Os resultados indicam dificuldades significativas na compreensão e aplicação de conceitos de congruência em problemas com múltiplos restos, reforçando a necessidade de práticas graduais e exercícios mais complexos.

Questão 8

Na atividade diagnóstica, 9 alunos acertaram, 15 erraram e 126 deixaram em branco. Na segunda aplicação, houve melhora: 13 acertos, 44 erros e 93 respostas em branco.

As questões envolveram padrões de restos em potências diferentes (3^{2025} e 12^{12}), exigindo aritmética modular. Observa-se leve melhora no desempenho, mas o baixo número de acertos evidencia dificuldade na identificação de padrões de restos, indicando a necessidade de estratégias pedagógicas que reforcem cálculos modulares em situações variadas.

7.2 Resumo comparativo

A comparação entre as oito questões da atividade diagnóstica e da segunda aplicação permitiu traçar um panorama geral do desempenho dos estudantes em relação aos conceitos de aplicação de padrões, aritmética modular e congruências.

De modo geral, observou-se que, em ambas as aplicações, os índices de erros e de respostas em branco foram elevados, evidenciando dificuldades persistentes na compreensão e aplicação desses conteúdos. Em algumas questões, notou-se discreta melhora no número de acertos, sugerindo efeito positivo das intervenções didáticas, enquanto em outras o desempenho se manteve baixo, indicando que determinados obstáculos conceituais permanecem pouco superados.

Os resultados mostram, portanto, que a evolução foi pontual e concentrada em problemas mais simples, ao passo que tarefas que exigiam maior articulação de operações modulares ou raciocínios envolvendo sistemas de congruências continuaram a apresentar elevado grau de dificuldade.

8 Conclusão

A análise das atividades aplicadas revelou que os estudantes apresentam dificuldades significativas na aplicação da aritmética modular, especialmente em problemas que exigem múltiplas operações de congruência ou identificação de padrões mais complexos. Como o tema não é abordado no Ensino Básico, a avaliação diagnóstica tinha como objetivo verificar como os alunos se sairiam ao enfrentar conceitos até então não explorados formalmente. Apesar das limitações do conhecimento prévio, observou-se um avanço relevante em tarefas envolvendo ciclos simples, refletido na redução de omissões (de 521 para 395, aproximadamente 24,2%) e no aumento agregado de acertos (de 322 para 398, aproximadamente 23,6%). Esses resultados indicam que a intervenção realizada teve impacto positivo, ainda que limitado, reforçando a importância de estratégias pedagógicas progressivas, que avancem de situações elementares para contextos mais elaborados, consolidando gradualmente habilidades essenciais ao raciocínio lógico e à resolução de problemas.

Outro aspecto evidenciado é a relevância de propor atividades contextualizadas. Problemas que envolveram situações práticas, como rotinas de treino ou ciclos naturais, mostraram-se mais acessíveis e favoreceram a percepção de padrões, sugerindo que conteúdos tradicionalmente tratados de forma abstrata podem ganhar em significatividade quando associados à realidade dos estudantes. De modo mais amplo, os resultados indicam que o ensino de congruências e da aritmética modular, ainda pouco explorados no Ensino Médio brasileiro, pode contribuir não apenas para a resolução de problemas aritméticos, mas também para o desenvolvimento do pensamento algorítmico, competência valorizada em um cenário de crescente integração entre Matemática, Computação e Tecnologia. Além disso, o estudo da divisibilidade e da congruência favorece a compreensão da estrutura e da lógica subjacentes a diversos algoritmos trabalhados no Ensino Médio, auxiliando o estudante a compreender, de forma mais consciente, os passos envolvidos em sua aplicação.

Em síntese, este trabalho evidencia, de um lado, as dificuldades enfrentadas pelos alunos diante da aritmética modular e, de outro, as possibilidades didáticas que emergem quando a formalização matemática é associada à resolução de problemas contextualizados. Para pesquisas futuras, sugerem-se intervenções mais longas, o uso de softwares educacionais e jogos digitais, bem como estratégias de ensino colaborativo, ampliando recursos disponíveis para a aprendizagem de divisibilidade, congruência e padrões numéricos. Dessa forma, reforça-se a necessidade de inserir tais conceitos de forma mais estruturada no currículo do Ensino Médio, em favor de uma formação matemática mais crítica, significativa e alinhada às demandas contemporâneas.

Referências

ALEXANDRIA, E. de. *Os Elementos*. 2. ed. Cambridge, UK: Cambridge University Press, 1908. Traduzido do grego por Thomas L. Heath. Citado na página 19.

BRASIL. *BNCC*. 1. ed. Brasília, DF: Ministério da Educação, 2018. Disponível em: <http://basenacionalcomum.mec.gov.br/>. Citado 4 vezes nas páginas 14, 23, 36 e 37.

ENQ. *Exame Nacional de Qualificação – 1998*. 1998. Brasil. Prova disponibilizada pelo Ministério da Educação - PROFMAT. Citado na página 66.

HEFEZ, A. *Elementos de aritmética*. 2.. ed. Rio de Janeiro: Sociedade Brasileira de Matemática (SBM), 2011. (Textos Universitários). Citado 2 vezes nas páginas 26 e 38.

HEFEZ, A. *Aritmética*. 3. ed. Rio de Janeiro, RJ: Sociedade Brasileira de Matemática, 2022. 306 p. (Coleção PROFMAT). ISBN 978-85-8337-181-6. Citado 4 vezes nas páginas 15, 16, 17 e 18.

INEP. *IDEB 2023 – Índice de Desenvolvimento da Educação Básica*. 2023. <http://www.ideb.inep.gov.br>. Acesso em: 06 set. 2025. Citado na página 24.

LIMA, F. A. d. Números primos e algumas curiosidades históricas: Da proposição infinita de euclides ao crivo de eratóstenes. *Revista História da Matemática para Professores*, p. 11, 2024. Citado 2 vezes nas páginas 16 e 20.

NIVEN, I.; ZUCKERMAN, H. S.; MONTGOMERY, H. L. *A Matemática dos Números Inteiros*. [S.l.]: Guanabara Dois, 1991. Citado na página 15.

OBMEP. *Prova da OBMEP 2010*. 2010. Disponível em: <https://www.obmep.org.br/banco.htm> (acesso em: 3 set. 2025). Citado na página 64.

OBMEP. *Módulo 23 – Portal da OBMEP*. 2011. <https://portaldaobmep.impa.br/index.php/modulo/ver?modulo=23>. Acesso em: 3 set. 2025. Citado na página 64.

OBMEP. *Prova da OBMEP 2018*. 2018. Disponível em: <https://www.obmep.org.br/banco.htm> (acesso em: 3 set. 2025). Citado na página 56.

RIBENBOIM, P. *Números primos: mistérios e recordes*. 1.. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada (IMPA), 2001. (Coleção Matemática Universitária). Citado na página 26.

SANTOS, J. P. O. *Introdução à teoria dos números*. 2.. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada (IMPA), 2000. (Coleção Matemática Universitária). Citado na página 26.

APÊNDICE A – Atividade diagnóstica e sua solução.

Este apêndice apresenta as soluções das questões aplicadas na atividade diagnóstica. As resoluções incluem os procedimentos matemáticos corretos e destacam os conceitos de divisibilidade e congruência.

As soluções passo a passo permitem a verificação do desempenho dos alunos e servem como referência para futuras intervenções pedagógicas.

Atividades

1. Um aplicativo bloqueia usuários cuja senha é um número que, ao ser dividido por 4 e por 7, deixa resto 3 em ambos os casos. Qual é o menor número positivo maior que 10 que atende a essa condição?

Solução: Queremos encontrar o menor número positivo $x > 10$ tal que:

$$x \equiv 3 \pmod 4 \quad \text{e} \quad x \equiv 3 \pmod 7.$$

Observamos que x deixa resto 3 quando dividido por 4 e por 7. Assim, podemos escrever:

$$x = 4k + 3 \quad \text{para algum inteiro } k \geq 0,$$

e

$$x = 7m + 3 \quad \text{para algum inteiro } m \geq 0.$$

Igualando as duas expressões (já que são o mesmo número x):

$$4k + 3 = 7m + 3 \implies 4k = 7m.$$

Como 4 e 7 são coprimos, 4 deve dividir m, isto é, $m = 4n$ para algum inteiro $n \geq 0$ (2.3.5). Então:

$$x = 7m + 3 = 7(4n) + 3 = 28n + 3.$$

O menor n que produz um $x > 10$ é $n = 1$, pois:

$$x = 28 \cdot 1 + 3 = 31 > 10.$$

2. Se um relógio digital marca 19 horas, que horas ele marcará após 50 horas?

Solução: Queremos determinar o horário x após 50 horas, sabendo que o relógio marca 19 horas e funciona em ciclo de 24 horas. Podemos escrever uma congruência linear:

$$x \equiv 19 + 50 \pmod{24}.$$

Somando os números:

$$x \equiv 69 \pmod{24}.$$

Agora resolvemos a congruência linear:

$$69 \div 24 = 2 \text{ com resto } 21 \implies 69 \equiv 21 \pmod{24}.$$

3. Hoje é quarta-feira. João tem treinos de futebol a cada 3 dias. Qual será o dia da semana do treino número 20, contando o primeiro treino como hoje?

Solução: Seja x o dia da semana do treino número 20, considerando quarta-feira como o dia 0. Cada treino ocorre a cada 3 dias, então podemos escrever a congruência linear:

$$x \equiv 0 + 3 \cdot (20 - 1) \pmod{7}.$$

Calculando o deslocamento total:

$$3 \cdot 19 = 57.$$

Agora, reduzimos módulo 7:

$$57 \div 7 = 8 \text{ com resto } 1 \implies 57 \equiv 1 \pmod{7}.$$

Como definimos quarta-feira como 0, somando o resto:

$$x \equiv 0 + 1 \equiv 1 \pmod{7}.$$

Se a quarta-feira é 0, então:

$$0 = \text{quarta-feira}, \quad 1 = \text{quinta-feira}.$$

4. Um elevador programado apenas para subir realiza paradas especiais a cada 8 andares, como parte de sua manutenção. Hoje, ele fez uma dessas paradas no 11º andar. Sabendo que a próxima parada especial ocorrerá após o 100º andar, em qual andar exatamente isso acontecerá?

Solução: Seja x o andar da próxima parada especial do elevador. Sabemos que as paradas especiais ocorrem a cada 8 andares. Assim, podemos escrever a congruência linear:

$$x \equiv 11 \pmod{8}.$$

Além disso, sabemos que $x > 100$. Para encontrar o menor número que satisfaça essas condições, podemos escrever:

$$x = 11 + 8k, \quad k \in \mathbb{Z}^+.$$

Queremos o menor k tal que $x > 100$:

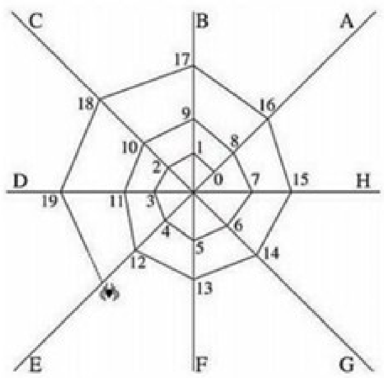
$$11 + 8k > 100 \implies 8k > 89 \implies k > 11{,}125.$$

O menor número inteiro k que atende é $k = 12$. Então:

$$x = 11 + 8 \cdot 12 = 11 + 96 = 107.$$

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

Figura 21 – Representação da questão 5



Fonte: (OBMEP, 2018)

Solução: Seja x o fio de apoio correspondente ao número 118. Como os fios se repetem ciclicamente de A a H, temos 8 fios, então podemos escrever a congruência:

$$x \equiv 118 \pmod{8}.$$

Calculando o resto da divisão:

$$118 \div 8 = 14 \text{ com resto } 6 \implies 118 \equiv 6 \pmod{8}.$$

o resto 6 corresponde ao fio G.

6. Uma empresa realiza manutenções preventivas a cada 4 dias úteis. A primeira manutenção do mês foi em uma segunda-feira. Considerando apenas dias úteis (sem contar sábados e domingos), em que dia da semana ocorrerá a 4ª manutenção?

Solução: Seja x o dia da semana da 4ª manutenção, considerando segunda-feira como 0. Como a manutenção ocorre a cada 4 dias úteis, podemos escrever a congruência linear:

$$x \equiv 0 + 4 \cdot (4 - 1) \pmod{5}.$$

Calculando o deslocamento total:

$$4 \cdot 3 = 12.$$

Agora, reduzimos módulo 5 (considerando apenas os 5 dias úteis da semana):

$$12 \div 5 = 2 \text{ com resto } 2 \implies 12 \equiv 2 \pmod{5}.$$

Numerando os dias úteis como:

$$0 = \text{segunda-feira}, \quad 1 = \text{terça-feira}, \quad 2 = \text{quarta-feira}, \quad 3 = \text{quinta-feira}, \quad 4 = \text{sexta-feira},$$

o resto 2 corresponde à quarta-feira.

7. Um número x deixa resto 2 na divisão por 3, resto 3 na divisão por 5, e resto 2 na divisão por 7. Qual é o menor número maior que 100 que satisfaz essas condições?

Para essa questão temos duas soluções esperadas:

Solução 1: O problema pode ser escrito como um sistema de congruências:

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}. \end{cases}$$

Primeiro, resolvemos as duas primeiras congruências:

$$x \equiv 2 \pmod{3} \implies x = 3k + 2$$

Substituindo na segunda congruência:

$$3k + 2 \equiv 3 \pmod{5} \implies 3k \equiv 1 \pmod{5}.$$

O inverso de 3 módulo 5 é 2, pois $3 \cdot 2 \equiv 1 \pmod{5}$. Assim:

$$k \equiv 2 \cdot 1 \equiv 2 \pmod{5} \implies k = 5m + 2.$$

Substituindo de volta em x:

$$x = 3k + 2 = 3(5m + 2) + 2 = 15m + 8.$$

Agora usamos a terceira congruência:

$$15m + 8 \equiv 2 \pmod{7} \implies 15m \equiv -6 \equiv 1 \pmod{7}.$$

Como $15 \equiv 1 \pmod{7}$, temos:

$$m \equiv 1 \pmod{7} \implies m = 7n + 1.$$

Substituindo de volta:

$$x = 15m + 8 = 15(7n + 1) + 8 = 105n + 23.$$

O menor $x > 100$ ocorre para $n = 1$:

$$x = 105 \cdot 1 + 23 = 128.$$

Solução 2:(Usando o teorema chinês do resto) O problema é:

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$$

Pelo Teorema Chinês do Resto, como os módulos são coprimos dois a dois, existe uma solução única módulo $M = 3 \cdot 5 \cdot 7 = 105$.

Definimos:

$$M_1 = \frac{M}{3} = 35, \quad M_2 = \frac{M}{5} = 21, \quad M_3 = \frac{M}{7} = 15.$$

Agora, precisamos dos inversos:

$$y_1 \equiv M_1^{-1} \pmod 3 \implies 35y_1 \equiv 1 \pmod 3.$$

Como $35 \equiv 2 \pmod 3$, temos $2y_1 \equiv 1 \pmod 3 \implies y_1 \equiv 2 \pmod 3$.

$$y_2 \equiv M_2^{-1} \pmod 5 \implies 21y_2 \equiv 1 \pmod 5.$$

Como $21 \equiv 1 \pmod 5$, então $y_2 \equiv 1 \pmod 5$.

$$y_3 \equiv M_3^{-1} \pmod 7 \implies 15y_3 \equiv 1 \pmod 7.$$

Como $15 \equiv 1 \pmod 7$, então $y_3 \equiv 1 \pmod 7$.

A solução é dada por:

$$x \equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \pmod M,$$

onde $a_1 = 2, a_2 = 3, a_3 = 2$. Substituindo:

$$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}$$

$$x \equiv 140 + 63 + 30 \equiv 233 \pmod{105}.$$

Reduzindo módulo 105:

$$233 \div 105 = 2 \text{ com resto } 23 \implies x \equiv 23 \pmod{105}.$$

Portanto, todos os números que satisfazem o sistema são da forma:

$$x = 23 + 105n, \quad n \in \mathbb{Z}.$$

O menor número maior que 100 é para $n = 1$:

$$x = 23 + 105 = 128.$$

8. Qual é o último dígito de 3^{2025}?

Solução: Procuramos o último dígito de 3^{2025}, ou seja, $3^{2025} \pmod{10}$.

Observa-se o ciclo das potências de 3 módulo 10:

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^3 \equiv 7, \quad 3^4 \equiv 1 \pmod{10},$$

e o ciclo se repete a cada 4 expoentes.

Calculamos o resto de 2025 na divisão por 4:

$$2025 \div 4 = 506 \text{ com resto } 1 \quad \Rightarrow \quad 2025 \equiv 1 \pmod{4}.$$

Como o expoente é congruente a 1 módulo 4, temos

$$3^{2025} \equiv 3^1 \equiv 3 \pmod{10}.$$

APÊNDICE B – Planejamento de Aulas da Intervenção Didática

Este apêndice apresenta os planejamentos detalhados das quatro aulas que compuseram a intervenção didática. O objetivo é registrar de forma sistematizada a organização de cada encontro, contemplando a distribuição do tempo, os conteúdos abordados, as estratégias didáticas empregadas e as atividades propostas aos estudantes.

A inclusão desses planejamentos possibilita uma visão mais clara do percurso metodológico adotado, servindo tanto como material de consulta quanto como registro complementar à descrição realizada no corpo da dissertação.

1ª Aula

Tabela 3 – Planejamento da 1ª aula da Intervenção Didática

Tempo	**Atividade**
5 min	Revisão da divisão euclidiana com exemplos iniciais.
10 min	Apresentação do conceito de números primos.
10 min	Definição de divisibilidade e critérios (2, 3, 5, 7, 9 e 11).
10 min	Introdução ao máximo divisor comum (MDC) e mínimo múltiplo comum (MMC).
15 min	Comentário e aplicação de exercícios.

Fonte: Autor (2025).

2ª aula

Tabela 4 – Planejamento da 2ª aula da Intervenção Didática

Tempo	**Atividade**
20 min	Introdução às congruências: definição formal, relação com os conteúdos da aula anterior, propriedades básicas e exercícios introdutórios.
20 min	Pequeno Teorema de Fermat: apresentação breve e acessível, acompanhada de exemplos básicos para facilitar a compreensão.
10 min	Exercícios comentados para consolidar os conceitos trabalhados.

Fonte: Autor (2025).

3ª aula

Tabela 5 – Planejamento da 3ª aula da Intervenção Didática

Tempo	Atividade
20 min	Retomada dos conteúdos das aulas anteriores (congruências e Pequeno Teorema de Fermat), com o objetivo de esclarecer dúvidas e reforçar conceitos.
30 min	Comentário detalhado e resolução de exercícios com a participação dos alunos, promovendo a consolidação prática dos conteúdos.

Fonte: Autor (2025).

4ª aula

Tabela 6 – Planejamento da 4ª aula da Intervenção Didática

Tempo	Atividade
40 min	Sistemas de congruências lineares: resolução de exercícios básicos, transformando múltiplas congruências em uma única e utilizando propriedades trabalhadas nas aulas anteriores.
40 min	Teorema Chinês do Resto: apresentação do algoritmo com exercícios de números pequenos, para facilitar a compreensão prática.
20 min	Discussão e comentários sobre os exercícios, promovendo a consolidação dos conceitos estudados.

Fonte: Autor (2025).

APÊNDICE C – Atividades e soluções da segunda aplicação

Neste apêndice estão reunidas as atividades propostas na segunda aplicação, acompanhadas das soluções esperadas. As resoluções servem como referência para a análise do desempenho e para a identificação das principais estratégias de resolução utilizadas.

Atividades

1. Qual é o menor número natural maior que 20 que deixa resto 3 quando dividido por 5 e por 8 ao mesmo tempo?

   Solução: O problema pode ser escrito como o seguinte sistema de congruências:

$$\begin{cases} x \equiv 3 \pmod{5}, \\ x \equiv 3 \pmod{8}. \end{cases}$$

   Como ambos os restos são iguais, podemos reescrever: (2.6.5)

$$x \equiv 3 \pmod{\text{mmc}(5,8)}.$$

   Sabemos que $\text{mmc}(5,8) = 40$. Assim:

$$x \equiv 3 \pmod{40}.$$

   Logo, as soluções são da forma:

$$x = 40k + 3, \quad k \in \mathbb{Z}.$$

   Procuramos o menor número maior que 20:

$$40 \cdot 0 + 3 = 3 \quad (\text{menor que } 20),$$
$$40 \cdot 1 + 3 = 43 \quad (\text{maior que } 20).$$

2. Se hoje é dia 13 do mês, que dia do mês será daqui a 279 dias?

Solução: Um mês é considerado com 30 dias. Assim, devemos calcular o resto da divisão de 279 por 30:

$$279 \equiv 9 \pmod{30}.$$

Portanto, após 279 dias, será 9 dias após o dia 13:

$$13 + 9 \equiv 22 \pmod{30}$$

Logo, a data será o dia 22 do mês.

3. Um professor marcou uma prova para uma terça-feira. Ele disse que a segunda prova acontecerá exatamente 50 dias depois. Em que dia da semana cairá a segunda prova?

Solução: A semana se repete a cada 7 dias. Assim, basta reduzir 50 módulo 7:

$$50 \equiv 1 \pmod{7}.$$

Logo, 50 dias correspondem a um avanço de 1 dia na semana. Partindo de terça-feira,

$$\text{terça} + 1 \text{ dia} = \text{quarta-feira}.$$

4. (OBMEP, 2011) O pendrive de Jonas tem 400 músicas, todas com 4 minutos de duração, organizadas na sequência: samba, rock, pagode, pop, sertanejo, samba, rock, pagode, pop, sertanejo, samba, rock, pagode, pop, sertanejo, e assim por diante. Ele ouviu, desde o início, duas horas de música. Qual o estilo da última música tocada?

Solução: Duas horas correspondem a 120 minutos. Como cada música tem 4 minutos, o número de músicas ouvidas é

$$\frac{120}{4} = 30.$$

Portanto a última música tocada foi a 30-ésima da sequência.

A sequência de estilos tem período 5. Numerando as posições no ciclo como

$$1 = \text{samba}, \; 2 = \text{rock}, \; 3 = \text{pagode}, \; 4 = \text{pop}, \; 5 = \text{sertanejo},$$

devemos determinar a posição de 30 módulo 5. Usando congruências:

$$30 \equiv 0 \pmod{5}.$$

O resto 0 corresponde à quinta posição do ciclo, isto é, *sertanejo*.

5. (OBMEP, 2010) 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?

Solução: Os treinos ocorrem a cada 3 dias (um de treino + dois de descanso). Assim, o n-ésimo treino acontecerá no dia

$$\text{segunda-feira} + (n-1)\cdot 3 \text{ dias.}$$

Para o 100° treino:

$$(100-1)\cdot 3 = 99\cdot 3 = 297 \text{ dias após a segunda-feira inicial.}$$

Agora, reduzimos módulo 7 (número de dias da semana):

$$297 \equiv 3 \pmod 7.$$

Logo, o 100° treino ocorre 3 dias após uma segunda-feira:

$$\text{segunda} + 3 \text{ dias} = \text{quinta-feira.}$$

6. Qual é o menor número natural que deixa restos 5, 4, 3 e 2 quando dividido, respectivamente, por 6, 5, 4 e 3?

Solução: Seja x o número procurado. As condições dadas podem ser escritas em forma de congruências:

$$\begin{cases} x \equiv 5 \pmod 6, \\ x \equiv 4 \pmod 5, \\ x \equiv 3 \pmod 4, \\ x \equiv 2 \pmod 3. \end{cases}$$

Observamos que:

$$x \equiv 5 \pmod 6 \quad \Rightarrow \quad x+1 \equiv 0 \pmod 6,$$

$$x \equiv 4 \pmod 5 \quad \Rightarrow \quad x+1 \equiv 0 \pmod 5,$$

$$x \equiv 3 \pmod 4 \quad \Rightarrow \quad x+1 \equiv 0 \pmod 4,$$

$$x \equiv 2 \pmod 3 \quad \Rightarrow \quad x+1 \equiv 0 \pmod 3.$$

Portanto, $x+1$ deve ser múltiplo comum de $6, 5, 4, 3$ (2.6.5).

O mínimo múltiplo comum é

$$\text{mmc}(6, 5, 4, 3) = 60.$$

Logo,

$$x + 1 = 60 \quad \Rightarrow \quad x = 59.$$

7. Um número x deixa resto 2 na divisão por 3, resto 3 na divisão por 5 e resto 2 na divisão por 7. Qual é o menor número *maior que* 100 que satisfaz essas condições?

Solução: Escrevemos o sistema de congruências

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}. \end{cases}$$

Os módulos são coprimos dois a dois, portanto aplicamos o Teorema Chinês do Resto. Calcule $M = 3 \cdot 5 \cdot 7 = 105$ e

$$M_1 = \frac{M}{3} = 35, \quad M_2 = \frac{M}{5} = 21, \quad M_3 = \frac{M}{7} = 15.$$

Determinamos os inversos y_i tais que $M_i y_i \equiv 1 \pmod{m_i}$:

$$35y_1 \equiv 1 \pmod{3} \quad \Rightarrow \quad 35 \equiv 2 \pmod{3} \Rightarrow 2y_1 \equiv 1 \pmod{3} \Rightarrow y_1 \equiv 2;$$

$$21y_2 \equiv 1 \pmod{5} \quad \Rightarrow \quad 21 \equiv 1 \pmod{5} \Rightarrow y_2 \equiv 1;$$

$$15y_3 \equiv 1 \pmod{7} \quad \Rightarrow \quad 15 \equiv 1 \pmod{7} \Rightarrow y_3 \equiv 1.$$

A solução geral é

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{M},$$

com $a_1 = 2,\ a_2 = 3,\ a_3 = 2$. Assim

$$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}$$

$$x \equiv 140 + 63 + 30 \equiv 233 \pmod{105}.$$

Reduzindo módulo 105:

$$233 \equiv 23 \pmod{105},$$

portanto todas as soluções são $x = 23 + 105k,\ k \in \mathbb{Z}$.

Procuramos o menor $x > 100$. Para $k = 0$ temos $x = 23$ (menor que 100); para $k = 1$:

$$x = 23 + 105 = 128 > 100.$$

8. (ENQ, 1998) O resto da divisão de 12^{12} por 5 é?.

Solução: Primeiro, observamos que:

$$12 \equiv 2 \pmod 5.$$

Portanto:

$$12^{12} \equiv 2^{12} \pmod 5.$$

Agora, usamos o fato de que $2^4 \equiv 1 \pmod 5$ (2.7.1):

$$2^1 \equiv 2 \pmod 5, \quad 2^2 \equiv 4 \pmod 5, \quad 2^3 \equiv 3 \pmod 5, \quad 2^4 \equiv 1 \pmod 5.$$

Como $2^{12} = (2^4)^3 \equiv 1^3 \equiv 1 \pmod 5$, temos:

$$12^{12} \equiv 1 \pmod 5.$$