



UNIVERSIDADE FEDERAL DO PARÁ  
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA  
CAMPUS UNIVERSITÁRIO DE BRAGANÇA  
FACULDADE DE MATEMÁTICA

**DOMINÓ DOS RESTOS: UM JOGO UTILIZADO COMO  
MÉTODO DE ENSINO E APRENDIZAGEM NA  
ARITMÉTICA MODULAR**

**EMILLY DE FÁTIMA SOUSA BARBOSA**

BRAGANÇA – PA

2022

**DOMINÓ DOS RESTOS: UM JOGO UTILIZADO COMO  
MÉTODO DE ENSINO E APRENDIZAGEM NA  
ARITMÉTICA MODULAR**

**EMILLY DE FÁTIMA SOUSA BARBOSA**

Trabalho de Conclusão de Curso apresentado à  
Universidade Federal do Pará, como parte dos  
requisitos necessários para obtenção do Título de  
Licenciada Plena em Matemática.

Orientadora: Profa. Dra. Marly dos Anjos  
Nunes.

Co-Orientador: Prof. Me. Oséas Guimarães  
Ferreira Neto.

BRAGANÇA – PA

2022

**DOMINÓ DOS RESTOS: UM JOGO UTILIZADO COMO  
MÉTODO DE ENSINO E APRENDIZAGEM NA  
ARITMÉTICA MODULAR**

**EMILLY DE FÁTIMA SOUSA BARBOSA**

Trabalho de Conclusão de Curso apresentado à  
Universidade Federal do Pará, como parte dos  
requisitos necessários para obtenção do Título de  
Licenciada Plena em Matemática.

Bragança, 11 de Julho de 2022

**BANCA EXAMINADORA**

---

Profa. Dra. Marly dos Anjos Nunes  
Orientadora – UFPA

---

Prof. Me. Oséas Guimarães Ferreira Neto  
Co-orientador – SEDUC-PA

---

Profa. Dra. Edilene Farias Rozal  
Examinadora Interna – UFPA

# Agradecimentos

Em primeiro lugar a Deus, autor principal, que fez com meus objetivos fossem alcançados, durante minha vida acadêmica e por me permitir ultrapassar todos os obstáculos encontrados ao longo da realização deste trabalho.

Aos meus pais, Alailson Barbosa e Edilce Maia, a minha irmã Evellyn Barbosa, que juntos me incentivaram a continuar meus estudos e compreenderam a minha ausência enquanto eu me dedicava à realização deste trabalho

Agradeço ao meu noivo André Costa, que jamais me negou apoio, carinho e incentivo, e também por sempre ter se mostrado compreensivo nos momentos de ausência durante os finais de semana para estudos.

Agradeço à minha orientadora querida Profa. Dra. Marly dos Anjos Nunes, por sempre estar presente para indicar a direção correta que o trabalho deveria tomar. Também agradeço o meu co-orientador Prof. Me. Oséas Guimarães Ferreira Neto que com sua vasta experiência me auxiliou na construção desse trabalho.

Gostaria de agradecer também aos membros da banca examinadora, na pessoa dos professores, Dra. Edilene Farias Rozal e o Prof. Me. Oséas Guimarães Ferreira Neto.

À grande amiga Glenda Amorim que foi uma das autoras na confecção do jogo Dominó dos Restos apresentado neste trabalho. Por ter se dedicado para que esse jogo promovesse grandes resultados no ensino de Matemática.

Agradeço à Universidade Federal do Pará (UFPA), por me proporcionar um ambiente confortável para os estudos. Gratidão a todo corpo docente da Faculdade de Matemática, a direção e a administração dessa instituição.

Aos amigos que a universidade me presenteou, Kamila Brito, Gabriela Ferreira, Rosely Alves, Joas Mota, Glenda Amorim, Júlia Barbosa, Ray Siqueira, Mateus Amorim e Klivea Martins, por todos os momentos de descontração e por me ajudarem nas ocasiões de dúvidas nos estudos matemáticos.

À todos que foram meus professores no ensino básico, de modo especial o Professor Pedro da Cruz, que foi quem me inspirou e sempre me motivou a ingressar na Faculdade de Matemática.

Por fim, agradeço a todos que contribuíram diretamente ou indiretamente para a construção desse trabalho.

“A matemática é a rainha das Ciências e a Teoria dos Números é a rainha da Matemática.” (Gauss)

# Resumo

O presente trabalho tem como objetivo mostrar o uso do jogo matemático Dominó dos Restos como uma metodologia diferenciada para o ensino e aprendizagem da Aritmética Modular, sendo um método e possibilidade de ensino, que pode contribuir de modo significativo para o desenvolvimento cognitivo e social do aluno, enfatizando a importância do jogo como ferramenta integrante ao processo do ensino e aprendizagem em sala de aula. É importante ressaltar que o conteúdo matemático base que está atrelado ao jogo é a disciplina Teoria dos Números, especificamente, o conteúdo de Aritmética Modular, permitindo o aperfeiçoamento e desenvolvimento de habilidades e competências dos discentes na resolução de problemas aritméticos, como a agilidade e o raciocínio lógico rápido. Servindo como um meio para o docente ensinar, de modo que colabore para a aprendizagem dos discentes sobre o assunto citado acima, associando toda teoria estudada com a praticidade obtida através do jogo. Dessa forma, apresentamos o jogo como instrumento de ensino, que foi testado por um grupo de discentes que fazem parte do Laboratório Pedagógico de Informática e Matemática (LA $\pi$ NMAT) e também foi aplicado através de oficina no evento nacional X Bienal de Matemática. Onde em ambas aplicações promoveu aos discentes envolvidos no jogo, interação social, concentração, raciocínio lógico, prazer e motivação. Trazendo resultados positivos, tais como uma maior contemplação do conteúdo de Aritmética Modular, para quem ainda não tinha cursado a componente Teoria dos Números causou grande motivação e expectativa em cursar a disciplina, além de provocar interesse no Professor mediador da oficina em utilizar o jogo em uma turma do Doutorado. Assim, notamos a grande relevância do jogo para o ensino de Aritmética Modular, acarretando em uma aprendizagem satisfatória, dinâmica e diferenciada.

**Palavras-chave:** Teoria dos Números; Aritmética Modular; Jogo Matemático; Dominó dos Restos.

## Lista de Figuras

1	Resultados das congruências para o jogo Dominó dos Restos . . . . .	32
2	Registro da Confeção do Protótipo do jogo Dominó dos Restos . . . . .	38
3	Peças do jogo Dominó dos Restos envolvendo congruência modular . . . . .	39
4	Peças carrões do Dominó dos Restos relacionando os restos . . . . .	39
5	Aplicação do jogo Dominó dos Restos com alguns colaboradores do Λαπματ	40
6	Aplicação do jogo Dominó dos Restos em oficina no evento nacional X Bienal de Matemática . . . . .	40

# Sumário

<b>1</b>	<b>Introdução</b>	<b>10</b>
<b>2</b>	<b>Divisibilidade no Conjunto dos <math>\mathbb{Z}</math></b>	<b>14</b>
2.1	Divisor de um Inteiro . . . . .	14
<b>3</b>	<b>Algoritmo de Euclides e Números Primos</b>	<b>19</b>
3.1	Máximo Divisor Comum . . . . .	19
3.2	Números Primos . . . . .	19
<b>4</b>	<b>Aritmética Modular</b>	<b>21</b>
4.1	Propriedades Elementares de Congruência . . . . .	21
4.2	Congruência no Conjunto dos Restos . . . . .	22
4.3	Propriedades da Congruência . . . . .	23
4.4	Teorema de Euler . . . . .	26
<b>5</b>	<b>Dominó dos Restos</b>	<b>29</b>
5.1	A importância dos Jogos para o ensino da Matemática . . . . .	29
5.2	Uma metodologia diferenciada no ensino da Aritmética Modular . . . . .	30
5.2.1	Procedimentos Metodológicos . . . . .	31
5.2.2	Regras do Jogo (Dominó dos Restos) . . . . .	32
<b>6</b>	<b>Aplicação do jogo Dominó dos Restos com Discentes e Docentes da Faculdade de Matemática</b>	<b>34</b>
6.1	Aplicação do Jogo com os Colaboradores do LA $\pi$ NMAT . . . . .	34
6.2	Aplicação do Jogo Dominó dos Restos em Oficina no Evento da X Bienal de Matemática . . . . .	35
6.3	Resultados e Discussões . . . . .	36
<b>7</b>	<b>Considerações Finais</b>	<b>37</b>
<b>A</b>	<b>Registro da Criação do Protótipo do Jogo Dominó dos Restos</b>	<b>38</b>
<b>B</b>	<b>Protótipo no aplicativo Canva do jogo Dominó dos Restos</b>	<b>39</b>
<b>C</b>	<b>Aplicação do jogo Dominó dos Restos</b>	<b>40</b>

# 1 Introdução

Segundo relatos históricos sobre a História da Matemática, disponível no site Toda Matéria, a Matemática que conhecemos hoje teria surgido no Antigo Egito e no Império Babilônico a partir de interesses de ambos impérios em cobrar impostos dos seus súditos, bem como organizar o plantio e a colheita, construir edificações, entre outras demandas. Ou seja, foram essas necessidades que incentivaram os governantes a desenvolverem um sistema de contagem e medição. Porém, é importante ressaltar que na pré-história os primeiros seres humanos já utilizavam conceitos básicos da Matemática, como contar e medir. A partir desse contexto histórico sobre a Matemática, notamos o quanto desde o princípio ela se mostrou como instrumento importante na vida do ser humano.

Todavia, ainda que se saiba de sua grande valia para o desenvolvimento da humanidade, por meio do raciocínio lógico, criatividade, socialização, elaboração de hipóteses e resolução de problemas. Há muitos que têm aversão a Matemática, por julgarem-na como muito abstrata e difícil de ser compreendida, razão pela qual escutamos com muita frequência as célebres frases: “Eu não gosto de Matemática”, “Em que eu vou usar a Matemática?” ou ainda “A Matemática não serve pra nada”. E esse conflito entre os alunos e a Matemática na grande maioria está vinculado ao modo de como ela é ensinada pelo professor, conforme ratificado em pesquisas, que discutiremos no capítulo 5. É importante ressaltar também que geralmente essa problemática inicia nas séries iniciais, e dependendo da situação segue até a vida acadêmica do discente, conforme defendido por Lara (2011, p. 22):

É importante reconhecermos que os problemas de ensino e aprendizagem em Matemática não surgem apenas nas séries finais do Ensino Fundamental ou no Ensino Médio. A maioria dos alunos que apresentam dificuldades no final do Ensino Fundamental já as possuem nas Séries Iniciais.

Por conseguinte, a partir do momento em que os discentes iniciam seus estudos na Faculdade de Matemática, no caso, os graduandos, e se deparam com as disciplinas específicas do curso, acabam se frustrando, pois na maioria das vezes o docente de tal disciplina dispõe de uma metodologia de ensino totalmente voltada para a teoria, e não aborda a sua aplicabilidade no diário do discente, acarretando em dificuldades na compreensão do conteúdo exposto pelo professor, baixo rendimento acadêmico, alto índice de reprovação

e até mesmo evasão do curso.

De acordo com D’Ambrósio (1991):

[...]há algo errado com a Matemática que estamos ensinando. O conteúdo que tentamos passar adiante através dos sistemas escolares é obsoleto, desinteressante e inútil.

Desta forma, é necessário buscar por novos mecanismos que auxiliem os alunos no entendimento dos assuntos, sendo uma ferramenta complementar ao conteúdo que pode ser utilizado pelo professor para ensinar Matemática e um desses meios são os jogos, que servem para motivar e instigar o pensamento crítico, além de atenuar dúvidas que podem aparecer no decorrer do aprendizado e fazer com que as aulas se tornem mais atraentes, lúdicas e interessantes.

Segundo Smole (1996, p. 138), “O jogo propicia situações que, podendo ser comparadas a problemas, exigem soluções vivas, originais, rápidas. Nesse processo, o planejamento, a busca por melhores jogadas e a utilização de conhecimentos adquiridos anteriormente propiciam a aquisição de novas ideias, novos conhecimentos [...]”. Levando em consideração essa fala de Smole, este trabalho equivale a compreender a relevância dos jogos como metodologia diferenciada voltada para o ensino e aprendizagem dos discentes no que concerne ao conteúdo ensinado pelo professor, pois por ser um jogo, há mais participação, interação e motivação, além de os alunos se tornarem mais ativos, tendo como consequências positivas, melhorias no desenvolvimento das competências e habilidades, criatividade e na aprendizagem.

Para culminar, o bom uso dos jogos promovem grandes benefícios, não somente ao nosso público alvo nesse trabalho, que são discentes e docentes da faculdade de Matemática, mas também para que as pessoas de modo geral possam interagir e se expressar, trocando ideias e conhecimentos, bem como proporcionar momentos de descontração, comunicação, entrosamento social, competição e sensação de prazer.

Posto isso, o Laboratório Pedagógico de Informática e Matemática(LA $\pi$ NMAT)<sup>1</sup> da Universidade Federal do Pará – UFPA, campus Bragança, pensando em sanar ou minimizar esta problemática e vendo a necessidade de utilizar novas metodologias, pensou,

---

<sup>1</sup>O LAPINMAT (Laboratório Pedagógico de Informática e Matemática) foi submetido e aprovado ao edital LABINFRA 2019, tendo como idealizadoras a coordenadora a Profa. Dra. Marly Anjos e colaboradora a Profa. Dra. Edilene Rozal. O objetivo do projeto, voltado para o lado pedagógico é estudar e produzir objetos matemáticos e experiências que materializem e explique certos fenômenos, respectivamente.

elaborou e criou como tática de ensino o jogo matemático intitulado “Dominó dos Restos”, que tem como base teórica o assunto de Aritmética Modular que é agregado a componente curricular Teoria dos Números, com o intuito de auxiliar para a sua formação de forma significativa por meio do lúdico, despertando a curiosidade nos discentes e docentes de que há outros meios que eles podem buscar para complementar seu processo de aprendizagem sobre determinado assunto.

É importante ressaltar que com a criação deste jogo, o professor poderá utilizá-lo como meio de proporcionar aos discentes uma aula diferenciada, interativa e dinâmica. Pois, segundo Smole (2008, p. 09), “o jogo possibilita uma situação de prazer e aprendizagem significativa nas aulas de matemática”, ou seja, através da utilização do jogo em sala, além dos discentes terem uma maior contemplação do conteúdo aritmético, decerto implicaria automaticamente em os mesmos terem outra concepção sobre a Matemática.

No entanto, no decorrer da pesquisa nos questionamos:

**Como e porque os jogos são importantes para o ensino e aprendizagem do conteúdo Matemático?**

**Será que o uso do jogo Matemático “Dominó dos Restos” atrelado ao assunto de Aritmética Modular traria algum benefício para a aprendizagem dos discentes?**

**De que forma o docente poderia estar utilizando esse jogo como uma metodologia diferenciada para o ensino de Aritmética Modular?**

Nessa perspectiva, este trabalho tem por objetivo, mostrar os estudos metodológicos sobre o ensino da Matemática, com enfoque no assunto de Aritmética Modular. Mesclando teoria e prática obtida através do jogo “Dominó dos Restos”, com o intuito de colaborar para a formação acadêmica, despertando o interesse do discente, a motivação, o raciocínio lógico e uma aprendizagem satisfatória. E aos docentes, como uma ferramenta a ser utilizada em sala, para então promover aos discentes uma aula dinâmica, salutar e diferenciada.

Este trabalho foi organizado estruturalmente em 7 (sete) capítulos, a começar pelo capítulo 1 (um) que é introdução até o capítulo 7 (sete) que são as considerações finais. No capítulo 2 (dois) nos dedicamos aos estudos de divisibilidade no conjunto dos inteiros, por meio de definições, proposições, exemplos, bem como um dos principais teoremas conhecido como Teorema da Divisão Euclidiana e corolário. No capítulo 3 (três) apre-

sentamos um breve estudo sobre Máximo Divisor Comum (MDC) e números primos, um dos conceitos mais importantes da Matemática que será essencial para compreensão do capítulo seguinte.

No capítulo 4 (quatro) definimos alguns conceitos principais da Aritmética Modular, como definições, proposições, exemplos, propriedades elementares de congruência, que será a base fundamental e que rege o jogo “Dominó dos Restos” e para finalizar este capítulo enunciaremos e provaremos o Teorema de Euler que é uma ferramenta importante caso queiram expandir o jogo. No capítulo 5 (cinco) discorreremos acerca da importância dos jogos no ensino da Matemática, além de mostrar o jogo Dominó dos Restos como uma metodologia diferenciada de ensinar Aritmética Modular, contendo os procedimentos metodológicos, os resultados das congruências necessárias para a confecção e regras do jogo (Dominó dos Restos). E por fim, no capítulo 6 (seis) vamos expor as aplicações do jogo que foram realizadas com os discentes colaboradores do LA $\pi$ NMAT e apresentamos também no evento nacional da X Bienal de Matemática que ocorreu no período de 20 à 24 de Junho de 2022 na UFPA - Campus Belém, que pela primeira vez foi sediado na região norte do Brasil pela SBM (Sociedade Brasileira de Matemática), onde traremos algumas discussões e resultados sobre o uso do jogo no capítulo 6 (seis).

## 2 Divisibilidade no Conjunto dos $\mathbb{Z}$

Neste capítulo discorreremos sobre os conceitos e definições das divisões entre os números inteiros, incluindo os tópicos de divisibilidade, Teorema da Divisão Euclidiana, exemplos e corolário. Para assim formarmos um alicerce sólido e fundamental no que se trata da compreensão dos algoritmos que servirão como base no jogo Dominó dos Restos.

### 2.1 Divisor de um Inteiro

**Definição 2.1.** *Dados dois números inteiros  $a$  e  $b$ , diremos que  $a$  divide  $b$ , escrevendo  $a|b$ , quando existir  $c \in \mathbb{Z}$  tal que  $b = ca$ . Neste caso diremos também que  $a$  é um divisor ou um fator de  $b$  ou ainda que  $b$  é um múltiplo de  $a$  ou que  $b$  é divisível por  $a$ .*

A notação  $a|b$  não representa nenhuma operação em  $\mathbb{Z}$ .

A negação dessa notação é representada por  $a \nmid b$ , significando que não existe nenhum inteiro  $c$  tal que  $b = ca$ .

**Proposição 2.1.** Sejam  $a, b, c \in \mathbb{Z}$ . Tem-se que:

- i)  $1|a$ ,  $a|a$  e  $a|0$ .
- ii)  $0|a \iff a = 0$ .
- iii)  $a$  divide  $b$  se, e somente se,  $|a|$  divide  $|b|$ .
- iv) se  $a|b$  e  $b|c$ , então  $a|c$ .

**Demonstração:**

(i) Isto decorre das igualdades  $a = a.1$ ,  $a = 1.a$  e  $0 = 0.a$

(ii) Suponha que  $0|a$ ; logo existe  $c \in \mathbb{Z}$  tal que  $a = c.0$ . Conclui-se que  $a = 0$ . Para a recíproca basta observar que  $0|0$ , o que foi provado no item anterior.

(iii)

$(\Rightarrow) a|b \Rightarrow b = a.q \Rightarrow |b| = |a|.|q|, |q| \in \mathbb{Z} \Rightarrow |a||b|$

$(\Leftarrow) |a||b| \Rightarrow |b| = |a|.|q|$ , com 4 casos:

1)  $b > 0$  e  $a > 0 \Rightarrow b = a.q \Rightarrow a|b$

2)  $b > 0$  e  $a < 0 \Rightarrow b = (-a).q \Rightarrow a|b$

3)  $b < 0$  e  $a > 0 \Rightarrow -b = a.q \Rightarrow a|b$

4)  $b < 0$  e  $a < 0 \Rightarrow -b = (-a).q \Rightarrow a|b$

(iv)  $a|b$  e  $b|c$  implica que existem  $f, g \in \mathbb{Z}$ , tais que  $b = fa$  e  $c = gb$ . Substituindo o

valor de  $b$  da primeira equação na outra, obtemos

$$c = gb = g(fa) = (gf)a$$

o que nos mostra que  $a \mid c$ .

Suponha que  $a \mid b$  e que  $a \neq 0$ . Seja  $c \in \mathbb{Z}$  tal que  $b = ca$ . O número inteiro  $c$ , univocamente determinado, é chamado de **quociente** de  $b$  por  $a$  e denotado por  $c = \frac{b}{a}$ .

**Exemplo 2.1.**

(a)  $\frac{0}{1} = \frac{0}{2} = 0$ , sendo 0 o quociente de  $\frac{1}{0}$  e  $\frac{2}{0}$

(b)  $\frac{6}{2} = 3$ , sendo 3 o quociente de  $\frac{2}{6}$

**Observação:** Observe que  $a$  só divide  $b$  se estiver bem definida, isto é, se  $a \neq 0$ .

Enunciaremos e demonstraremos, agora, o teorema mais importante deste capítulo, chamado Teorema da Divisão Euclidiana.

**Teorema 2.1.** (*Teorema da Divisão Euclidiana*) *Sejam  $a$  e  $b$  dois números inteiros com  $b \neq 0$ . Existem dois únicos números inteiros  $q$  e  $r$  tais que*

$$a = bq + r, \text{ com } 0 \leq r < b$$

**Demonstração:**

Primeiro vamos definir um conjunto que denominaremos de  $S$

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

isto é,  $S$  é o conjunto de todos os inteiros não negativos da forma  $a - bx$ .

Agora mostraremos que  $S \neq \emptyset$ .

De fato, sendo  $b > 0$ , então  $b \geq 1$  e tomando  $x = -|a|$ , resulta que

$$a - bx = a - b(-|a|) = a + b|a| \geq a + 1 \cdot |a| \geq 0$$

Observe que  $S$  é limitado inferiormente por 0, assim pelo Princípio da Boa Ordenação,  $S$  possui um menor elemento. Seja  $r$  o elemento mínimo de  $S$  tal que,

$$r \geq 0$$

e

$$r = a - bq$$

Sendo  $q \in \mathbb{Z}$ . Assim,

$$a = bq + r$$

Até o presente momento, obtemos a existência de  $q$  e  $r$  com  $a = bq + r$  e  $r \geq 0$ .

Agora temos que assegurar que

$$r < b$$

Se  $r \geq b$ , teríamos  $r - b \geq 0$ . Sendo assim, como  $r = a - bq$ , tem-se

$$r - b = a - bq - b = a - b(q + 1) < a - bq = r,$$

o que contraria o fato de  $r$  ser o menor elemento de  $S$ .

O teorema garante a existência e unicidade dos inteiros  $q$  e  $r$ . Para provarmos a unicidade de  $q$  e  $r$ , suponha que existam dois pares diferentes de inteiros  $q$  e  $q_1$ ,  $r$  e  $r_1$  que satisfaçam

$$a = bq + r, \quad 0 \leq r < b$$

e

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

Desde que

$$a = a$$

$$bq + r = bq_1 + r_1$$

$$r - r_1 = b(q_1 - q), \tag{*}$$

o que implica

$$b \mid (r - r_1)$$

Por outro lado, temos

$$0 \leq r < b,$$

multiplicando por  $(-1)$ , tem-se

$$0 \geq -r > -b \implies -b < -r \leq 0$$

somando com

$$0 \leq r_1 < b,$$

obtemos

$$-b \leq -r \leq 0$$

$$0 \leq r_1 < b$$

$$-b < r_1 - r < b,$$

logo

$$|r_1 - r| < b$$

Por hipótese,  $b > 0$ , então

$$r_1 - r = 0$$

$$r_1 = r$$

E desde que  $b \neq 0$ , temos por (\*) que

$$r_1 - r = (q - q_1) \cdot b,$$

logo,

$$q - q_1 = 0$$

$$q = q_1 \quad \blacksquare$$

Os números  $q$  e  $r$  que aparecem no teorema acima são chamados respectivamente de **quociente** e **resto** da divisão de  $a$  por  $b$ .

Dessa forma, da divisão euclidiana, temos que o resto da divisão de  $a$  por  $b$  é zero se, e somente se,  $b$  divide  $a$ . Além do mais, quando o resto da divisão for zero dizemos que a divisão é exata.

**Exemplo 2.2.** *O quociente e o resto da divisão de 19 por 5 são  $q = 3$  e  $r = 4$ . O quociente e o resto da divisão de  $-19$  por 5 são  $q = -4$  e  $r = 1$ .*

Dado um número natural  $b$ , a unicidade do quociente e do resto na divisão euclidiana por  $b$  nos permitem definir duas importantes funções que descreveremos a seguir.

Denotando por  $q_b(a)$  o quociente da divisão do número  $a$  por  $b$ , definimos a função quociente por  $b$  como segue:

$$\begin{aligned} q_b: \mathbb{Z} &\longrightarrow \mathbb{Z} \\ a &\longmapsto q_b(a) \end{aligned}$$

**Corolário 2.1.** *Dados dois números inteiros  $a$  e  $b$  com  $b > 0$ , existe um único número inteiro  $n (= q_b(a))$  tal que*

$$nb \leq a < (n + 1)b$$

A afirmação contida no corolário acima (para  $a > 0$ ) foi feita, sem demonstração, por Euclides na sua obra os *Elementos*, que a utilizavam para justificar a sua divisão.

O inteiro  $q_b(a)$  pode ser também interpretado como o maior inteiro menor ou igual do que o número racional  $\frac{a}{b}$ .

De fato, pelo corolário 1, temos que, se  $r$  é o resto da divisão de  $a$  por  $b$ , então

$$q_b(a)b \leq a = q_b(a)b + r < (q_b(a) + 1)b,$$

daí,

$$q_b(a) \leq \frac{a}{b} < q_b(a) + 1.$$

Desse modo, o inteiro  $q_b(a)$  será denotado pelo símbolo  $[\frac{a}{b}]$  e será chamado de *parte inteira* do número racional  $\frac{a}{b}$ .

A segunda função importante determinada pela divisão euclidiana é a *função resto*, definida a seguir.

$$r_b : \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$a \longmapsto r_b(a)$$

onde  $r_b(a)$  é o resto da divisão de  $a$  por  $b$ .

### 3 Algoritmo de Euclides e Números Primos

Neste capítulo apresentaremos um breve estudo sobre os números primos, um dos conceitos mais importantes da Matemática. Esses números desempenham papel fundamental e a eles estão associados muitos problemas famosos cujas soluções têm resistido aos esforços de várias gerações de matemáticos. Mas, antes veremos brevemente conceitos e definições dos Algoritmos de Euclides, que será complemento essencial no estudo dos números primos.

#### 3.1 Máximo Divisor Comum

**Definição 3.1.** *Sejam  $a$  e  $b$  inteiros, onde um deles é não nulo. O máximo divisor comum de  $a$  e  $b$ , representado por  $\text{mdc}(a, b)$ , é o maior dentre os divisores positivos comuns de  $a$  e  $b$*

**Exemplo 3.1.** *Sejam  $a = 18$  e  $b = 30$ , dizemos então o  $\text{mdc}(18, 30) = 6$*

**Definição 3.2.** *Diremos que dois números  $a$  e  $b$  são primos entre si, se o  $\text{mdc}(a, b) = 1$ , ou seja, se o máximo divisor comum de ambos for igual a 1.*

#### 3.2 Números Primos

Agora tendo como base as definições de Máximo Divisor Comum, entraremos no assunto principal, que são os números primos.

**Definição 3.3.** *Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado de número **primo**.*

**Proposição 3.1.** *Dados dois números primos  $p$  e  $q$  e um número inteiro  $a$  qualquer, decorrem da definição acima os seguintes fatos:*

- (i) Se  $p|q$ , então  $p = q$ .
- (ii) Se  $p \nmid a$ , então  $(p, a) = 1$ .

**Demonstração:**

- (i) De fato, como  $p|q$  e sendo  $q$  primo, temos que  $p = 1$  ou  $p = q$ . Sendo  $p$  primo, tem-se que  $p > 1$ , o que acarreta  $p = q$ .
- (ii) De fato, se  $(p, a) = d$ , temos que  $d|p$  e  $d|a$ . Portanto,  $d = p$  ou  $d = 1$ . Mas,  $d \neq p$ ,

pois  $p \nmid a$  e, conseqüentemente,  $d = 1$ . ■

Um número maior do que 1 e que não é primo será dito composto.

Portanto, se um número natural  $n > 1$  é composto, existirá um divisor natural  $n_1$  de  $n$  tal que  $1 < n_1 < n$ . Logo, existirá um número natural  $n_2$  tal que

$$n = n_1 n_2, \text{ com } 1 < n_1 < n \text{ e } 1 < n_2 < n$$

Por exemplo, 2, 3, 5, 7, 11 e 13 são primos, enquanto que 4, 6, 8, 9, 10 e 12 são compostos.

Do ponto de vista da estrutura multiplicativa dos naturais, os números são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais, logo, todos os números inteiros não nulos, conforme veremos mais adiante no Teorema Fundamental da Aritmética.

**Teorema 3.1.** *(Teorema Fundamental da Aritmética) Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos*

### Demonstração:

Usando o Princípio de Indução, temos que;

Se  $n = 2$ , o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor do que  $n$  e vamos provar que vale para  $n$ .

Se o número  $n$  é primo, nada temos a demonstrar.

Suponhamos, então, que  $n$  seja composto. Logo, existem números naturais  $n_1$  e  $n_2$  tais que  $n = n_1 n_2$ , com  $1 < n_1 < n$  e  $1 < n_2 < n$ . Pela hipótese de Indução, temos que existem números primos  $p_1, \dots, p_r$  e  $q_1, \dots, q_s$ , tais que,

$$n_1 = p_1 \dots p_r \text{ e } n_2 = q_1 \dots q_s.$$

Portanto,  $n = p_1 \dots p_r q_1 \dots q_s$

Agora, vamos provar a unicidade da escrita.

Suponha que tenhamos  $n = p_1 \dots p_r = q_1 \dots q_s$ , onde os  $p_i$  e os  $q_j$  para algum  $j$ , que após reordenamento de  $q_1 \dots q_s$ , podemos supor que seja  $q_1$ . Portanto,

$$p_2 \dots p_r = q_2 \dots q_s.$$

Como  $p_2 \dots p_r < n$ , a hipótese de indução acarreta que  $r = s$  e os  $p_i$  e  $q_j$  são iguais aos pares ■

## 4 Aritmética Modular

Nesta seção delinearemos alguns conceitos de Aritmética Modular, como definições, proposições e suas propriedades elementares, e o Teorema de Euler, ou seja, a teoria base e essencial para o desenvolvimento desse trabalho.

**Definição 4.1.** *Dado um inteiro não nulo  $m$ , dizemos que os inteiros  $a$  e  $b$  são congruentes módulo  $m$ , se eles deixam mesmo resto na divisão euclidiana por  $m$ .*

Para indicar que  $a$  e  $b$  são congruentes módulo  $m$ , escreve-se:

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

A negação dessa notação é representada por  $a \not\equiv b \pmod{m}$ , ou seja, diremos que  $a$  e  $b$  não são congruentes (ou são incongruentes) módulo  $m$ .

**Exemplo 4.1.**

- (a)  $7 \equiv 4 \pmod{3}$ , pois deixam resto 1 na divisão por 3
- (b)  $8 \equiv -10 \pmod{-6}$  já que deixam resto 2 na divisão por -6
- (c)  $25 \not\equiv 9 \pmod{5}$  pois deixam restos distintos na divisão por 5.

### 4.1 Propriedades Elementares de Congruência

Da definição 4.1, segue de forma imediata que a congruência módulo  $m$  tem as seguintes propriedades para quaisquer inteiros  $a$ ,  $b$  e  $c$ .

- (i) **Reflexiva:**  $a \equiv a \pmod{m}$ ;
- (ii) **Simétrica:** Se  $a \equiv b \pmod{m}$ , então  $b \equiv a \pmod{m}$ ;
- (iii) **Transitiva:** Se  $a \equiv b \pmod{m}$  e  $b \equiv c \pmod{m}$ , então  $a \equiv c \pmod{m}$ .

Considere as observações abaixo:

**Observação - 1.** Como o resto da divisão de qualquer número inteiro por 1 é sempre zero, então para quaisquer inteiros  $a$  e  $b$ , tem-se

$$a \equiv b \pmod{1}.$$

**Observação - 2.** Se  $a \equiv b \pmod{m}$ , ambos deixam o mesmo resto na divisão por  $m$ , isto é, existem inteiros  $q_1$ ,  $q_2$  e  $r$ , com  $0 \leq r < |m|$ , tais que

$$a = mq_1 + r \quad \text{e} \quad b = mq_2 + r$$

Segue daí,

$$a = (-m)(-q_1) + r \quad \text{e} \quad b = (-m)(-q_2) + r$$

ou seja,  $a$  e  $b$  também deixam o mesmo resto na divisão por  $-m$ , portanto também temos  $a \equiv b \pmod{-m}$ .

$$a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{-m}$$

Em vista das observações 1 e 2 vamos nos restringir ao caso em que o inteiro  $m > 1$ . A proposição abaixo nos fornece uma forma equivalente de definir a congruência módulo  $m$ .

**Proposição 4.1.** *Seja  $m > 1$  um inteiro. Para quaisquer inteiros  $a, b$  tem-se que*

$$a \equiv b \pmod{m} \text{ se, e somente se, } m|(a - b).$$

**Demonstração:**

$$(\Rightarrow) a \equiv b \pmod{m} \Rightarrow m|(a - b):$$

$a \equiv b \pmod{m} \Rightarrow$  existem inteiros  $q_1, q_2$  e  $r$ , com  $0 \leq r < m$ , tais que:

$$a = mq_1 + r \text{ e } b = mq_2 + r \Rightarrow a - b = m(q_1 - q_2) \Rightarrow m|(a - b)$$

$$(\Leftarrow) m|(a - b) \Rightarrow a \equiv b \pmod{m} :$$

$$m|(a - b) \Rightarrow \exists k \in \mathbb{Z}, \text{ tal que } a - b = mk \Rightarrow a = b + mk.$$

Seja  $r$  o resto da divisão de  $a$  por  $m$ , então  $a = mq + r$ , com  $q \in \mathbb{Z}$ . Assim,

$$a = b + mk = mq + r \Rightarrow b = m(q - k) + r$$

Como  $0 \leq r < m$ , da unicidade do resto, segue que  $r$  é também o resto da divisão de  $b$  por  $m$ , logo  $a \equiv b \pmod{m}$

**Exemplo 4.2.**

(a)  $47 \equiv 11 \pmod{9}$ , pois  $9|(47 - 11)$ ;

(b)  $24 \equiv 314 \pmod{29}$ , pois  $29|(24 - 314)$ ;

(c)  $16 \not\equiv 5 \pmod{4}$ , pois  $4 \nmid (16 - 5)$

## 4.2 Congruência no Conjunto dos Restos

Já vimos que na divisão euclidiana por um inteiro  $m > 1$ , os possíveis restos pertencem ao conjunto

$$R = \{0, 1, 2, \dots, m - 1\}$$

Vejamos algumas conclusões relevantes, referentes à congruência, que podemos tirar sobre o conjunto  $R$ .

- Sabemos que para qualquer inteiro  $a$ , existem únicos inteiros  $q$  e  $r$ , com  $r \in R$ , tais que  $a = mq + r$ . Então,

$$a = mq + r \Rightarrow a - r = mq \Rightarrow m|(a - r) \Rightarrow a \equiv r \pmod{m}.$$

Com isso podemos afirmar

Todo inteiro é congruente módulo  $m$  ao seu resto  $r$  na divisão por  $m$ , e como esse resto é único, ele é congruente a um único elemento do conjunto  $R = \{0, 1, 2, \dots, m - 1\}$

**Exemplo 4.3.**  $23 = 5 \cdot 4 + 3 \Rightarrow 5|(23 - 3) \Rightarrow 23 \equiv 3 \pmod{5}$ .

- Existem elementos distintos  $b, c \in R = \{0, 1, 2, \dots, m - 1\}$ , tais que  $b \equiv c \pmod{m}$ ?

Para responder a essa pergunta, suponhamos que existam  $b, c \in R$ , distintos, tais que  $b \equiv c \pmod{m}$ . Sendo distintos, então  $b < c$  ou  $c < b$ . Vamos considerar  $b < c$ . Como

$$0 \leq b < c \leq m - 1 \Rightarrow 0 < c - b \leq m - 1$$

Porém, se

$$b \equiv c \pmod{m} \Rightarrow m|(c - b) \Rightarrow m \leq c - b \leq m - 1 \Rightarrow m \leq m - 1,$$

um absurdo. Portanto, podemos afirmar que

Quaisquer dois elementos distintos em  $R = \{0, 1, 2, \dots, m - 1\}$  são incongruentes módulo  $m$ . Portanto, se  $r_i, r_j \in R$ , são tais que

$$r_i \equiv r_j \pmod{m}$$

então,

$$r_i = r_j.$$

### 4.3 Propriedades da Congruência

No início desta seção vimos que a reflexividade, a simetria e a transitividade são propriedades elementares da congruência, e que caracteriza a congruência como relação de equivalência. Como a congruência está estritamente relacionada com a divisibilidade, podemos deduzir mais algumas propriedades que seguem diretamente das propriedades de divisibilidade vistas no item 4.1.

Dado um inteiro  $m > 1$ , a relação de congruência módulo  $m$ , definida em  $\mathbb{Z}$ , tem as seguintes propriedades, para quaisquer inteiros  $a, b, c$  e  $d$

(iv) Se  $a \equiv b \pmod{m}$ , então  $\begin{cases} a + c \equiv b + c \pmod{m} \\ ac \equiv bc \pmod{m}. \end{cases}$

**Demonstração:**

$a \equiv b \pmod{m} \Rightarrow m|(a - b)$ . Das propriedades de divisibilidade, segue que:

$$(1) m|[(a - b) + (c - c)] \Rightarrow m|[(a + c) - (b + c)] \Rightarrow a + c \equiv b + c \pmod{m}$$

$$(2) m|(a - b)c \Rightarrow m|(ac - bc) \Rightarrow ac \equiv bc \pmod{m}$$

■

(v) **Cancelamento da adição na congruência:**

Se

$$a + c \equiv b + c \pmod{m}$$

então,

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

**Demonstração:**

Por hipótese

$$a + c \equiv b + c \pmod{m}$$

usando a proposição 4.1, temos

$$m|[(a + c) - (b + c)],$$

como

$$a + c - (b + c)$$

$$a + c - b - c$$

$$a - b,$$

temos

$$m|a - b,$$

Portanto

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

■

(vi) **Cancelamento da Multiplicação na Congruência**

Se

$$ac \equiv bc \pmod{m} \text{ e } \text{mdc}(c, m) = 1,$$

então,

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

**Demonstração:**

$$ac \equiv bc \pmod{m} \Rightarrow m|(ac - bc) \Rightarrow m|(a - b)c.$$

Como por hipótese

$$mdc(m, c) = 1,$$

Logo, por definição

$$m|(a - b)$$

Portanto

$$a \equiv b \pmod{m} \quad \blacksquare$$

$$(vii) \text{ Se } \begin{cases} a \equiv b + c \pmod{m} \\ e \\ c \equiv d \pmod{m} \equiv bc \pmod{m} \end{cases} \text{ então, } \begin{cases} a + c \equiv b + c \pmod{m} \\ ac \equiv bc \pmod{m} \end{cases}$$

**Demonstração:**

$a \equiv b \pmod{m}$  e  $c \equiv d \pmod{m} \Rightarrow m|(a - b)$  e  $m|(c - d)$ . Segue das propriedades de divisibilidade que:

$$(1) m|[(a - b) + (c - d)] \Rightarrow m|[(a + c) - (b + d)] \Rightarrow a + c \equiv b + d \pmod{m};$$

$$(2) m|(a - b)c \text{ e } m|(c - d)b \Rightarrow m|[(ac - bc) + (bc - bd)] \Rightarrow m|(ac - bd) \Rightarrow ac \equiv bd \pmod{m} \quad \blacksquare$$

Apresentaremos a seguir uma das propriedades mais importantes desta seção, que foi utilizada para calcular e obtermos os resultados das congruências para a confecção do jogo Dominó dos Restos.

(viii) Se

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

então, para todo inteiro  $n \in \mathbb{N}$ , tem-se também

$$a^n \equiv b^n \pmod{m}$$

**Demonstração:**

Consideremos o menor elemento de  $\mathbb{N}$ , assim para  $n = 1$ , temos que se

$$a \equiv b \pmod{m}, \text{ então } a^1 \equiv b^1 \pmod{m}.$$

Suponha que a propriedade seja válida para  $n = k$ , o qual chamaremos de hipótese de indução

$$\text{Se } a \equiv b \pmod{m}, \text{ então } a^k \equiv b^k \pmod{m}.$$

Queremos mostrar que a propriedade é válida para  $n = k + 1$ , isto é, se  $a \equiv b \pmod{m}$ , então  $a^{k+1} \equiv b^{k+1} \pmod{m}$ .

Por hipótese da propriedade e pela hipótese de indução, temos respectivamente

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

$$a^k \equiv b^k \pmod{m}$$

multiplicando membro a membro as congruências acima, obtemos

$$a \cdot a^k \equiv b \cdot b^k \pmod{m}$$

$$a \cdot a^{k+1} \equiv b \cdot b^{k+1} \pmod{m} \quad \blacksquare$$

## 4.4 Teorema de Euler

Veremos agora um teorema que é um importante resultado em Teoria dos Números (Aritmética) que está ligado a um grande matemático chamado Leonhard Euler<sup>2</sup>. A importância desse resultado tem relevância tanto na história da Matemática, quanto na Aritmética.

Sabemos que o jogo Dominó dos Restos pode ser expandido, a começar pelos resultados das congruências, para isso necessitamos de ferramentas mais poderosas, uma delas é o Teorema de Euler que será enunciado a seguir.

Mas antes, falaremos brevemente sobre sistema reduzido de resíduos.

Um *sistema reduzido de resíduos* módulo  $m$  é um conjunto de números inteiros  $r_1, \dots, r_s$  tais que

- a)  $(r_i, m) = 1$ , para todo  $i = 1, \dots, s$ ;
- b)  $r_i \not\equiv r_j \pmod{m}$ , se  $i \neq j$ ;
- c) Para cada  $n \in \mathbb{Z}$  tal que  $(n, m) = 1$ , existe  $i$  tal que  $n \equiv r_i \pmod{m}$

Pode-se obter um sistema reduzido de resíduos  $r_1, \dots, r_s$ , módulo  $m$ , a partir de um sistema completo qualquer de resíduos  $a_1, \dots, a_m$ , módulo  $m$ , eliminando os elementos  $a_i$  que não são primos com  $m$ .

De fato, as propriedades (i) e (ii) da definição são claramente verificadas para  $r_1, \dots, r_s$ . Por outro lado, dado um número inteiro  $n$ , existe  $j$  tal que  $n \equiv a_j \pmod{m}$ . Se  $(n, m) = 1$ , então, logo, tendo como resultado que  $(a_j, m) = 1$ , e, portanto, para algum  $j$ , temos que  $a_j = r_i$  e, conseqüentemente,  $n \equiv r_i \pmod{m}$ .

Vamos agora verificar que dois sistemas reduzidos de resíduos módulo  $m$  têm o mesmo número de elementos.

---

<sup>2</sup>Leonhard Euler (1707-1783) foi um importante matemático e cientista suíço, foi considerado um dos maiores estudiosos da matemática, em sua época. Entre suas contribuições mais conhecidas na matemática moderna estão: a introdução da função gama, a analogia entre o cálculo infinitesimal e o cálculo das diferenças finitas, quando discutiu minuciosamente todos os aspectos formais do Cálculo Diferencial e Integral, da época. Euler foi considerado o mestre dos matemáticos do século XVIII.

Sejam  $r_1, \dots, r_s$  e  $r't$  dois sistemas reduzidos de resíduos módulo  $m$ . Vamos estabelecer uma bijeção entre esses dois conjuntos. Dados  $(r'_1, m) = 1$ . Como  $r_1, \dots, r_s$  formam um sistema reduzido módulo  $m$ , então existe um único  $j$  tal que  $r'_i \equiv r_j \pmod{m}$ . Isso define uma função  $f$  entre os dois sistemas. Reciprocamente, do mesmo modo, está bem definida uma função  $g$  de  $\{r'_1, \dots, r't\}$  em  $\{r_1, \dots, r_s\}$ . Suponha que  $g(r'_i) = r_k$ , então  $r'_i \equiv r_k \pmod{m}$ . Como também  $r'_i \equiv r_j \pmod{m}$ , segue que  $r_j \equiv r_k \pmod{m}$  e, conseqüentemente,  $r_j \equiv r_k \pmod{m}$ , mostrando que  $g$  é a função inversa de  $f$ .

Designaremos por  $\varphi(m)$  o número de elementos de um sistema reduzido de resíduos módulo  $m > 1$ , que corresponde à quantidade de números naturais entre 0 e  $m - 1$  que são primos com  $m$ . Pondo  $\varphi(1) = 1$ , isso define uma importante função.

$$\varphi: \mathbb{N} \longrightarrow \mathbb{N} \quad ,$$

chamada de *função fi de Euler*.

Pela definição, temos que

$$\varphi(m) \leq m - 1,$$

para todo  $m \geq 2$ , então  $\varphi(m) = m - 1$  se, e somente se,  $m$  é um número primo.

De fato,  $m$  é primo se, e somente se,  $1, 2, \dots, m - 1$  formam um sistema reduzido de resíduos módulo  $m$ , o que equivale a dizer que  $\varphi(m) = m - 1$ .

A seguir mostraremos a fórmula para calcular  $\varphi(m)$ .

$$\varphi(m) = (p - 1).(q - 1), \text{ onde } p \text{ e } q \text{ números primos distintos}$$

**Teorema 4.1.** *Sejam  $m, a \in \mathbb{Z}$  com  $m > 1$  e  $(a, m) = 1$ . Então,*

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

**Demonstração:**

Seja  $r_1, \dots, r_{\varphi(m)}$  um sistema reduzido de resíduos módulo  $m$ . Logo, pela proposição 5.1,  $ar_1, \dots, ar_{\varphi(m)}$  formam um sistema reduzido de resíduos módulo  $m$  e, portanto,

$$ar_1 \cdot ar_2 \dots ar_{\varphi(m)} \equiv r_1 \cdot r_2 \dots r_{\varphi(m)} \pmod{m} \quad .$$

Conseqüentemente,

$$a^{\varphi(m)} r_1 \cdot r_2 \dots r_{\varphi(m)} = ar_1 \cdot ar_2 \dots ar_{\varphi(m)} \equiv r_1 \cdot r_2 \dots r_{\varphi(m)} \pmod{m}$$

Como  $(r_1 \cdot r_2 \dots r_{\varphi(m)}, m) = 1$ , segue-se que

$$a^{\varphi(m)} \equiv 1 \pmod{m} \quad \blacksquare$$

**Proposição 4.2.** *Sejam  $m, m' \in \mathbb{N}$  tais que  $(m, m') = 1$ . Então*

$$\varphi(m, m') = \varphi(m)\varphi(m')$$

**Demonstração:** Ver [2], pág.199

**Proposição 4.3.** *Se  $p$  é um primo e  $r$ , um número natural, então tem-se que*

$$\varphi(p^r) = p^r - p^{r-1} = p^r(1 - \frac{1}{p})$$

**Demonstração:** Ver [2], pág. 200

Finalmente, podemos obter a expressão de  $\varphi(m)$  para qualquer  $m \in \mathbb{N}$

**Teorema 4.2.** *Seja  $m > 1$  e seja  $m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$  a decomposição de  $m$  em fatores primos.*

*Então,*

$$\varphi(m) = p_1^{\alpha_1} \dots p_n^{\alpha_n} (1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_n}).$$

**Demonstração:**

O resultado decorre imediatamente das Proposições 4.2 e 4.3.

Para calcular o resto da divisão de uma potência  $a^n$  por um número natural  $m > 1$ , é conveniente achar um expoente  $h \in \mathbb{N}$  de modo que  $a^h \equiv 1 \pmod{m}$ , pois, se  $n = hq + r$  é a divisão euclidiana de  $n$  por  $h$ , teremos  $a^n \equiv a^{hq+r} \equiv a^r \pmod{m}$ . Portanto, é clara a utilidade do Teorema de Euler para a resolução desse tipo de questão.

A seguir veremos um exemplo, onde se aplica a divisão euclidiana e o teorema anterior para encontrar o resto de uma potência com expoente grande.

**Exemplo 4.4.** *Vamos achar o resto da divisão de  $3^{100}$  por 34.*

Solução:

Note que

$$\varphi(34) = \varphi(2 \cdot 17) = 2^0 \cdot 17^0 (2 - 1)(17 - 1) = 16.$$

Pelo Teorema de Euler, temos que  $3^{16} \equiv 1 \pmod{34}$ , logo,

$$3^{100} = 3^{16 \cdot 6 + 4} \equiv 3^4 \equiv 13 \pmod{34}.$$

Portanto, 13 é o resto da divisão de  $3^{100}$  por 34.

## 5 Dominó dos Restos

### 5.1 A importância dos Jogos para o ensino da Matemática

Não há dúvidas de que a Matemática é uma das bases fundamentais para o processo do desenvolvimento intelectual do ser humano, visto que, por meio dela o indivíduo tem a aptidão de estimular seu raciocínio lógico, bem como despertar sua criatividade e sua capacidade de investigação e solução de problemas.

Porém, apesar de sua grande importância na história da humanidade, uma grande parte desta população não são adeptos a essa área da ciência, por julgarem como algo muito abstrato e esotérico, ou seja, impossível de ser compreendido. Segundo pesquisas realizadas pelo professor David Kollosche, da Universidade de Klagenfurt, na Áustria, o desinteresse das pessoas pela Matemática está diretamente relacionado ao método de como a mesma é ensinada.

Por esse motivo, se faz necessário novas metodologias para o ensino da Matemática que valorize a importância desta ciência no diário do discente. Ou seja, formas que auxiliem os alunos no entendimento do conteúdo matemático, e uma dessas formas é a utilização de jogos no contexto de sala de aula, para motivar e instigar o pensamento crítico do aluno e o raciocínio lógico, bem como tornar o processo de aprendizagem matemática mais prazeroso, motivador, lúdico e menos maçoso.

De acordo com Smole (2008):

Ao jogar, os alunos tem a oportunidade de resolver problemas, investigar e descobrir a melhor jogada; refletir e analisar as regras, estabelecendo relações entre os elementos do jogo e os conceitos de aprendizagem (SMOLE, 2008, p 11).

A BNCC (Base Nacional Comum Curricular) ressaltam que “Como ferramenta de ensino, o lúdico proporciona maior integração interpessoal, além de estimular a imaginação, a concentração e o raciocínio lógico, gerando dinamismo na abordagem dos conceitos matemáticos e uma forma mais ampliada de avaliação do aprendizado”. De fato, quando agregamos o uso dos jogos nas aulas de matemática, percebemos claramente que até mesmo os alunos que depreciam essa disciplina, tendem a olhá-la por outro ângulo, percebendo o quão bela é esta área da ciência e o quanto ela está inteiramente aplicada a algo que pode nos promover prazer, em especial, o jogo.

No entanto, apesar de sua grande relevância no ensino da matemática, muitos professores ainda resistem em considerar o uso de jogos nas aulas de matemática como algo irrelevante e sem importância. Segundo Cândido (2007), o lúdico sofre muito preconceito e é considerado por muitos professores como uma perda de tempo.

Em contrapartida, Smolle diz que "O trabalho com jogos nas aulas de Matemática, quando bem planejado e orientado, auxilia o desenvolvimento de habilidades como observação, análise, levantamento de hipóteses, busca de suposições, reflexão, tomada de decisão, argumentação e organização, que estão estreitamente relacionadas ao chamado raciocínio lógico."

Segundo Borin (1996, p. 09)

Outro motivo para a introdução de jogos nas aulas de Matemática é a possibilidade de diminuir bloqueios apresentados por muitos de nossos alunos que temem a Matemática e sentem-se incapacitados para aprendê-la.

Com efeito, notamos a grande relevância dos jogos como metodologia de ensino e aprendizagem dos alunos no que se refere ao conteúdo matemático, pois por meio do lúdico, há mais participação e o aluno se torna ativo, tendo como consequência melhorias no desenvolvimento das competências e na criatividade. Dessa forma proporcionando aos alunos mais apropriação do conhecimento abordado.

Nessa conjuntura, ressaltamos a importância dos jogos no ensino da matemática, tendo em vista o objetivo principal que é de colaborar com a aprendizagem dos discentes e mostrar para o professor formas de ministrar uma aula mais atrativa, dinâmica e motivadora. Além de, desmitificar a ideia que muitos estudantes têm, de que a matemática é um "bicho de sete cabeças", e de que não serve para nada, mostrando aos discentes um método divertido de estudar matemática e o quanto ela é essencial no nosso dia-a-dia.

## **5.2 Uma metodologia diferenciada no ensino da Aritmética Modular**

No início desta seção discorreremos a cerca da importância do uso dos jogos no ensino da Matemática. Relacionado a isso mostraremos à seguir o jogo matemático intitulado "Dominó dos Restos", como uma metodologia diferenciada para o ensino-aprendizagem da Aritmética Modular.

O jogo "Dominó dos Restos" foi pensado, elaborado e confeccionado a partir da necessidade que se tinha de promover aos docentes e discentes da Faculdade de Matemática - Campus Bragança, métodos diferenciados para ensinar o assunto de Aritmética Modular, e trazendo uma perspectiva inovadora enquanto ao fato de ser um recurso a mais que pode ser utilizado pelo docente, de forma a possibilitar uma aprendizagem prazerosa aos discentes.

É importante mencionar também, que um dos fatores que colaborou e incentivou a construção do jogo mencionado anteriormente, foi o evento nacional X Bienal de Matemática, organizado pela SBM (Sociedade Brasileira de Matemática) em parceria com a UFPA (Universidade Federal do Pará), que ocorreu no período de 20 à 24 de Junho de 2022, onde pela primeira vez foi sediado na região norte do Brasil, precisávamos elaborar um trabalho com uma temática que fosse relevante e atrativa.

Ressalto também outro fator essencial, o Laboratório recém conquistado chamado LA $\pi$ NMAT, do qual fazemos parte, cujo objetivo é produzir jogos matemáticos a serem estudados e confeccionados a fim de materializar a matemática por meio do lúdico, tornando-a mais acessível ao conhecimento do aluno.

### 5.2.1 Procedimentos Metodológicos

Para a execução deste trabalho, foi elaborado um planejamento de materiais referidos ao laboratório de matemática, dentre eles o jogo que será o eixo principal desse trabalho, chamado "Dominó dos Restos", tendo como conhecimento matemático base a disciplina de Teoria dos Números com enfoque no conteúdo de Aritmética Modular, tendo em vista não somente ser uma ferramenta pedagógica para o ensino de Matemática, mas também fornecer habilidades variadas, como atenção, interação, memória, raciocínio lógico, planejamento, tomadas de decisão de forma que contribua para minimização do deficit de aprendizagem em matemática.

Segue abaixo as etapas utilizadas para a construção do jogo Dominó dos Restos:

**1<sup>a</sup> Etapa** – Discutimos acerca do assunto colocado em pauta por um grupo de discentes colaboradores do Laboratório Pedagógico de Informática e Matemática (LA $\pi$ NMAT), ou seja, a Aritmética Modular com a finalidade de criar um material concreto que pudesse ser utilizado em aulas por docentes e para os discentes como forma de aprendizado diferenciado.

**2ª Etapa** – Pensamos em um jogo de fácil acesso e que a maioria tivesse conhecimento sobre, assim escolhemos o dominó, onde foram feitas as modificações necessárias para o conteúdo que queríamos esclarecer.

**3ª Etapa** – De posse do conhecimento base sobre a Aritmética Modular e da ideia de abordarmos congruências que deixassem restos de 0 a 7, utilizamos a definição 4.1 aplicando alguns algoritmos para então utilizar esses resultados na confecção do jogo. Abaixo temos uma tabela ilustrando como se deu esse processo.

Figura 1: Resultados das congruências para o jogo Dominó dos Restos

	0	1	2	3	4	5	6	7
0	0	$10^2 \equiv ? \pmod{5}$ $43 \equiv ? \pmod{2}$	$144 \equiv ? \pmod{4}$ $2^4 \equiv ? \pmod{3}$	$15^2 \equiv ? \pmod{25}$ $59 \equiv ? \pmod{8}$	$289 \equiv ? \pmod{17}$ $58 \equiv ? \pmod{9}$	$8^2 \equiv ? \pmod{4}$ $25 \equiv ? \pmod{4}$	$343 \equiv ? \pmod{7}$ $87 \equiv ? \pmod{9}$	$6^0 \equiv ? \pmod{1}$ $77 \equiv ? \pmod{10}$
1		1	$4^2 \equiv ? \pmod{3}$ $14 \equiv ? \pmod{4}$	$82 \equiv ? \pmod{9}$ $25 \equiv ? \pmod{7}$	$6^2 \equiv ? \pmod{5}$ $34 \equiv ? \pmod{6}$	$101 \equiv ? \pmod{10}$ $5^4 \equiv ? \pmod{10}$	$5^4 \equiv ? \pmod{6}$ $39 \equiv ? \pmod{11}$	$11 \equiv ? \pmod{5}$ $97 \equiv ? \pmod{6}$
2			2	$3^2 \equiv ? \pmod{5}$ $3^3 \equiv ? \pmod{6}$	$32 \equiv ? \pmod{6}$ $2^5 \equiv ? \pmod{14}$	$4^2 \equiv ? \pmod{7}$ $68 \equiv ? \pmod{7}$	$47 \equiv ? \pmod{9}$ $69 \equiv ? \pmod{7}$	$2^7 \equiv ? \pmod{6}$ $3^4 \equiv ? \pmod{9}$
3				3	$19 \equiv ? \pmod{8}$ $44 \equiv ? \pmod{8}$	$5^2 \equiv ? \pmod{11}$ $15^2 \equiv ? \pmod{10}$	$84 \equiv ? \pmod{9}$ $66 \equiv ? \pmod{10}$	$7^2 \equiv ? \pmod{4}$ $5^3 \equiv ? \pmod{2}$
4					4	$3^2 \equiv ? \pmod{5}$ $5^2 \equiv ? \pmod{15}$	$7^2 \equiv ? \pmod{5}$ $6^2 \equiv ? \pmod{10}$	$8^2 \equiv ? \pmod{5}$ $59 \equiv ? \pmod{7}$
5						5	$7^2 \equiv ? \pmod{11}$ $9^2 \equiv ? \pmod{3}$	$77 \equiv ? \pmod{8}$ $127 \equiv ? \pmod{12}$
6							6	$2^5 \equiv ? \pmod{25}$ $4^4 \equiv ? \pmod{10}$
7								7

Fonte: Própria da Autora

**4ª Etapa** - Confeccionamos um protótipo do “Dominó dos Restos” (Apêndice A), usando papel A4 e papelão com formato retangular em tamanho x por y, onde as peças dos carrões são escrita os restos e as demais peças continham as congruências modulares. Além disso, foi feito no site Canva disponível em: <https://www.canva.com> as peças na forma digital (Apêndice B).

**5ª Etapa** – Testamos o jogo para verificar se, de fato, alcançava nossas expectativas e se conseguiríamos assimilar os conceitos ministrados pelo docente relacionado a esse assunto. (Apêndice C)

### 5.2.2 Regras do Jogo (Dominó dos Restos)

**Objetivo:** De posse do assunto, o objetivo é baixar na mesa as peças primeiro, jogando ao longo da partida as peças que se encaixam corretamente de acordo com as equivalências das congruências. Há a possibilidade do jogo fechar, isto é, quando as duas pontas têm o mesmo número e não existe mais peças com este número na mão dos jogadores, neste caso vence quem tiver a menor quantidade de peças.

**Descrição:** O jogo dispõe de 36 peças, no formato similar ao do dominó tradicional, contendo nas peças carrões os restos que variam de 0 a 7, nas peças restantes contendo a divisibilidade e as congruências modulares.

**Público-Alvo:** Discentes e docentes do curso de Matemática ou que tenham a disciplina Teoria dos Números na sua grade curricular.

**Composição:** 36 peças.

**Instruções:**

1. Para iniciar o jogo, deverá ter até 6 participantes;
2. As peças são embaralhadas por um jogador, com a face voltada para baixo;
3. Cada participante receberá 6 peças, caso haja um quantitativo inferior de jogadores as peças que sobraem ficam disponíveis para serem compradas;
4. Determina-se qual é a peça de saída, no caso, o participante que tiver a peça  $7 \times 7$ ;
5. O próximo a jogar será o participante a direita daquele que inicia a partida, caso ele não tenha a peça, o próximo participante poderá jogar, e assim, por diante;
6. O jogador que ficar sem peças na mão, vence o jogo;
7. Caso haja o fechamento do jogo, ou seja, quando os jogadores não possuem a peça em mãos e nem para ser comprada o prosseguimento para o jogo, vence quem tiver a menor quantidade de peças;
8. Quem deverá fazer a confirmação do vencedor são os próprios jogadores, no caso os adversários.

## 6 Aplicação do jogo Dominó dos Restos com Discentes e Docentes da Faculdade de Matemática

Neste capítulo iremos apresentar a aplicação do jogo Dominó dos Restos contextualizando o conteúdo matemático, no caso a Aritmética Modular com a prática obtida através do jogo, criando um ambiente significativo de aprendizagem. Além disso, traremos algumas discussões acerca do jogo, assim como resultados relevantes sobre as aplicações que foram realizadas no laboratório e em oficina no evento nacional X Bienal de Matemática.

### 6.1 Aplicação do Jogo com os Colaboradores do LA $\pi$ NMAT

Não há dúvidas de que, o processo metodológico para confeccionar um jogo não é tão simples assim, pois requer, tempo, dedicação e paciência. No entanto, um dos principais problemas que os designers de jogos enfrentam, é com a incerteza se de fato aquele jogo atenderá as expectativas pelos quais eles foram construídos. E com o jogo Dominó dos Restos não foi diferente, ou seja, criamos o jogo, mas precisávamos ter certeza que de fato ele daria certo, se seria relevante.

Por esse motivo, resolvemos aplicar o jogo no Laboratório Pedagógico de Informática e Matemática (LA $\pi$ NMAT), onde os jogadores foram os próprios colaboradores. É importante ressaltar que apesar do jogo ter sido elaborado para atender até 6 jogadores, nesse episódio contamos com quatro participantes.

No entanto, antes de iniciar o momento de testagem foi apresentado a eles a definição 4.1 acompanhada de alguns exemplos para que relembassem a teoria estudada na componente curricular Teoria dos Números, especificamente o conteúdo de Aritmética Modular para então utilizarem como subsídio no momento em que estivessem jogando. Uma vez, que para jogar alguma peça do dominó o aluno tinha que descobrir o resto deixado em cada congruência para então saber como fazer uma jogada estratégica.

Partindo desse pressuposto iniciamos o jogo, sendo o primeiro a jogar o jogador que tinha em mãos a peça carrão de resto 7, e após demos continuidade a partida, levando em consideração as regras do jogo e seguindo a risca as instruções colocadas como forma de manual para eles.

É importante ressaltar que no decorrer da partida, notamos a grande motivação e entusiasmo que os jogadores estavam. Além disso, percebemos o quanto o ato de jogar es-

estimulou o raciocínio lógico deles, bem como promoveu a sensação de prazer, descontração e socialização.

Portanto, percebemos em relação ao conteúdo matemático, no caso, a Aritmética Modular, que atrelado o lúdico os discentes conseguiram compreender melhor o assunto vinculado ao jogo, no caso a Aritmética, acarretando grandes benefícios como, motivação, interação e raciocínio lógico rápido.

## **6.2 Aplicação do Jogo Dominó dos Restos em Oficina no Evento da X Bienal de Matemática**

Além de ter sido aplicado com discentes colaboradores do Laboratório de Matemática, como já mencionado na seção anterior, o jogo Dominó dos Restos foi apresentado e aplicado no evento nacional X Bienal de Matemática, organizado pela SBM em parceria com a UFPA. Onde a comissão organizadora disponibilizou por meio de plataforma virtual as inscrições tanto para participar do evento, quanto para submeter trabalhos, de forma que se enquadrassem em um dos eixos temáticos postos por eles.

Diante disso, submetemos o jogo Dominó dos restos que se enquadrava no eixo temático (T3 - Laboratório de Ensino de Matemática), tanto para atividade em oficina quanto para apresentação oral (palestras curtas), onde em ambas as modalidades foi aprovado pela comissão do evento.

Posteriormente, na ocasião do evento, aplicamos o referido jogo em oficina chamada “Uma aplicação lógica entre jogos de mesa, divisibilidade e congruência modular”, onde além do dominó teve também o jogo do carteadado da divisibilidade. Para jogar o Dominó dos Restos, aplicamos seguindo instruções, a participação de 6 jogadores, que eram discentes de Matemática de outras instituições.

Porém, antes de iniciar a partida, apresentamos através de slides a definição de congruência modular **4.1**, afim de que soubessem como de que forma eles teriam que calcular o resto das congruências para então decidirem de forma coerente qual seria a peça correta a ser jogada

Após explicação da teoria de Aritmética Modular e das regras do jogo, demos inicio a partida, que por ventura foi bem disputada entre os jogadores. Na primeira rodada do jogo foi dado a cada jogador um tempo de 2 minutos e na próxima rodada esse tempo foi reduzido para 1 minuto para que eles decidissem qual peça era conveniente jogar. Além

disso, motivá-los ainda mais teria um prêmio para quem vencesse a partida.

### 6.3 Resultados e Discussões

Tendo em vista que este trabalho se enquadra na modalidade de pesquisa qualitativa, discorreremos a seguir sobre os resultados e discussões para saber se de fato houve engajamento e se atendeu às nossas expectativas enquanto autores do jogo Dominó dos Restos.

É importante ressaltar os resultados apresentados posteriormente serão baseados na forma em que o referido jogo foi abordado em ambas aplicações. Visto que só a partir disso pudemos ter resultados concretos sobre esse recurso lúdico criado como metodologia diferenciada no ensino de Aritmética.

No momento em que os colaboradores do laboratório jogavam a partida, notamos uma grande interação e competição entre os mesmos, além disso após a primeira rodada o raciocínio lógico deles para efetuarem as jogadas estava bem mais rápido. Percebemos também que por meio da praticidade do jogo, eles fixaram melhor o conteúdo de Aritmética Modular e sentiram-se super motivados.

De forma análoga os participantes da oficina, que jogaram o Dominó dos Restos relataram que apreciaram muito o jogo, e que sentiram-se interessados em adquirir o jogo para auxiliar em seus estudos sobre Aritmética. É importante ressaltar que dois desses alunos ainda não tinham estudado a disciplina Teoria dos Números, mas através do momento de descontração, aprendizagem e prazer obtido através do jogo sentiram curiosidade em estudar, aprender e ter um contato mais preciso com esse ramo da matemática.

Em paralelo a isso, o Professor que estava como mediador na sala onde estava sendo realizada a oficina, mostrou grande interesse em aplicar o jogo Dominó dos Restos em uma turma de Doutorado, onde ele leciona a disciplina de Aritmética (Teoria dos Números). Pois, o mesmo percebeu que o jogo proporcionou interação social entre os alunos (jogadores), e que esses discentes assimilarem de forma rápida o conteúdo matemático de Aritmética através da praticidade obtida por meio do jogo.

De modo geral, notamos que o jogo Dominó dos Restos, atendeu as nossas expectativas enquanto ao fato de ser um novo método de ensinar e aprender Aritmética de uma forma diferente ao método tradicional de ensino. Enfim, podemos observar como o número de possibilidades de aprendizagem é ampla quando se usa o jogo como auxílio.

## 7 Considerações Finais

Esse trabalho pretendeu mostrar o uso do jogo matemático Dominó dos Restos, como uma metodologia diferenciada para ensino e aprendizagem de Aritmética Modular, um recurso que poderá ser utilizado tanto pelos discentes quanto por docentes de Matemática. Nesse sentido enfatizamos a importância de se utilizar objetos concretos em sala de aula, para que o abstrato se torne mais fácil de ser compreendido, tornando as aulas atrativas, dinâmicas e lúdicas.

Nessa conjunção, o jogo Dominó dos Restos proporcionou durante a confecção, um entendimento mais preciso para se ter um olhar crítico sobre a construção e o processo de regras do jogo, com o intuito de ratificar sua eficiência quanto a aprendizagem dos jogadores e o estímulo do raciocínio lógico. O contato com o jogo esclareceu definições e sanou dúvidas, favorecendo a motivação durante o ato de jogar.

Em paralelo a eficiência da aplicação do jogo com os alunos da Graduação em Matemática, também contribuiu de forma significativa para o meu processo de aprendizagem e estimulou minha percepção sobre a importância de se pensar, elaborar e criar meios diferenciados de ensinar para promover uma Educação Matemática de qualidade aos meus futuros alunos.

É importante ressaltar que apesar, do público alvo neste trabalho serem os discentes e docentes da graduação em Matemática, o mesmo pode ser adaptado para ser utilizado no ensino básico, bem como também pode ser expandido para servir como recurso na pós graduação de Matemática. As peças do dominó podem ser escritas na notação da divisão euclidiana, envolvendo divisões simples e para a confecção do dominó a ser aplicado na pós graduação, pois utilizam expoentes de valores bem elevados e assim utilizam a seção 4.4 para encontrar suas relações. Ademais, pode-se readaptar o dominó para outros conteúdos matemáticos, como propriedades de potenciação e radiciação, geometria, funções e outros.

Enquanto um dos autores, percebi o quanto esse trabalho foi relevante para os sujeitos envolvidos, pois além de ter alcançado nossas expectativas, provocamos neles a curiosidade em saber que há outros métodos que eles podem procurar para aprender um determinado conteúdo matemático.

## A Registro da Criação do Protótipo do Jogo Dominó dos Restos

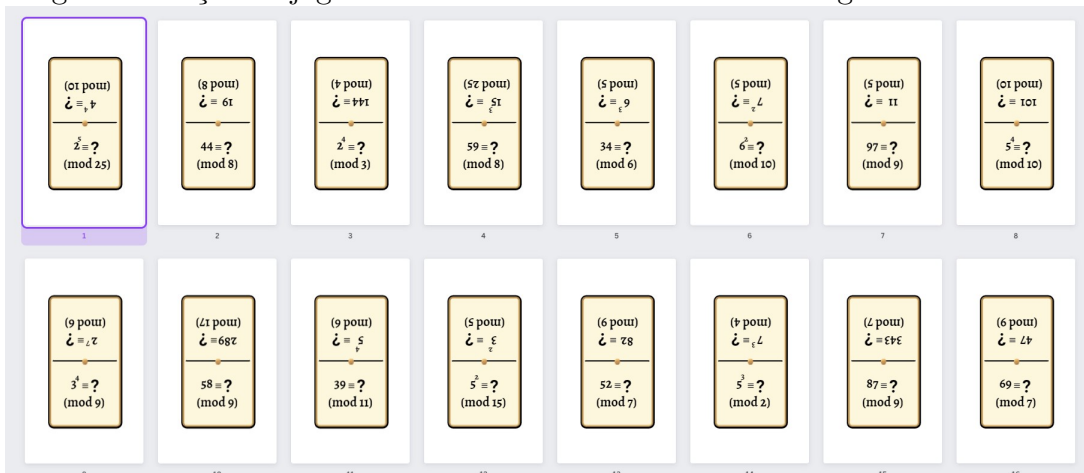
Figura 2: Registro da Confeção do Protótipo do jogo Dominó dos Restos



Fonte: Própria da Autora

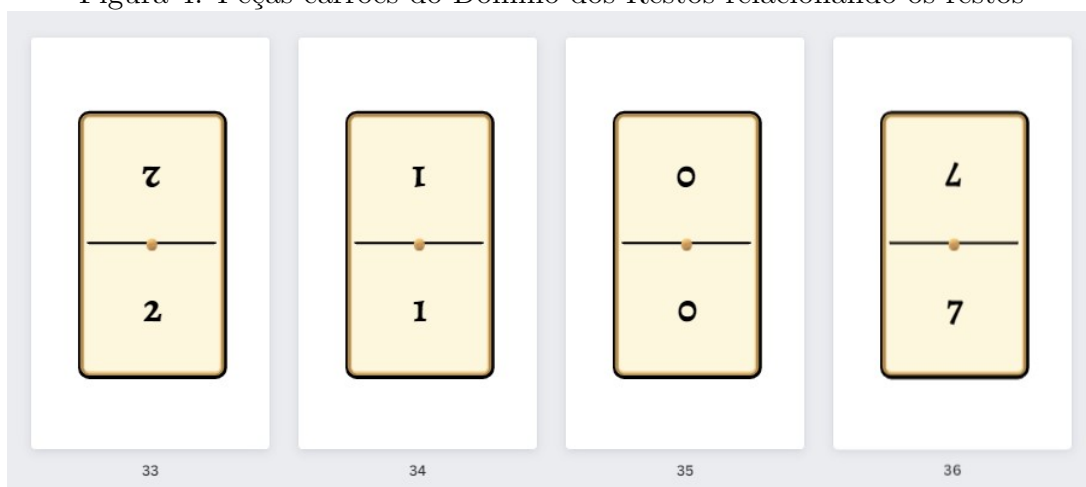
## B Protótipo no aplicativo Canva do jogo Dominó dos Restos

Figura 3: Peças do jogo Dominó dos Restos envolvendo congruência modular



Fonte: Própria da Autora

Figura 4: Peças carrões do Dominó dos Restos relacionando os restos



Fonte: Própria da Autora

## C Aplicação do jogo Dominó dos Restos

Figura 5: Aplicação do jogo Dominó dos Restos com alguns colaboradores do Laπmat



Fonte: Própria da Autora

Figura 6: Aplicação do jogo Dominó dos Restos em oficina no evento nacional X Bienal de Matemática



Fonte: Própria da Autora

## Referências

- [1] BEZERRA, N. **Teoria dos Números: Um Curso Introdutório**. 1ª ed. Belém: editAed, 2018.
- [2] HEFEZ, A. **Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2016.
- [3] LARA, I. C. M, **Jogando com a Matemática na Educação Infantil e Anos Iniciais**. 2ª ed. Catanduva,SP: Editora Rêspel, 2011.
- [4] CARNEIRO, F. **Criptografia e Teoria dos Números**. 1ª ed. Rio de Janeiro, Ciência Moderna Ltda, 2017.
- [5] C.C.P. “**Resumo - a Matemática Na Educação Infantil: A Teoria Das Inteligências Múltiplas Na Prática Escolar -.**” Curso Completo de Pedagogia, 12 Feb. 2021, [cursocompletodepedagogia.com/resumo-a-matematica-na-educacao-infantil-a-teoria-das-inteligencias-multiplas-na-pratica-escolar/](https://cursocompletodepedagogia.com/resumo-a-matematica-na-educacao-infantil-a-teoria-das-inteligencias-multiplas-na-pratica-escolar/). Acessado em 03 de Março de 2022.
- [6] MELO, S. A.; SARDINHA, M. O. B.: **Jogos no Ensino e Aprendizagem de Matemática: uma estratégia para aulas mais dinâmicas**. Revista F@pciência, Apucarana – PR, 2009
- [7] SELVA. K. R.; CAMARGO. M.: **O Jogo Matemático como Recurso para a Construção do Conhecimento**. X EGEM - RS, 2009.
- [8] SMOLE, Kátia Cristina Stocco. **A matemática na educação infantil: a teoria das inteligências múltiplas na prática escolar**. Porto Alegre: Artes Médicas, 1996.
- [9] GUIMARÃES, O. **Aplicações de Divisibilidade e Congruência Modular: do Ensino Básico ao Superior**. Dissertação (Mestrado/ PROFMAT) - Originalmente apresentada como dissertação de Mestrado – Universidade Federal do Pará – Faculdade de Matemática. Bragança. 2021.