UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO CIÊNCIA EXATA E DA TERRA
DEPARTAMENTO DE MATEMÁICA
MESTRADO PROFISSIONAL
EM MATEMÁICA EM REDE NACIONAL – PROFMAT

MATEUS FELIPE MENDES DOS SANTOS

Aritmética dos Restos: Jogos e Aplicações para o Ensino

Orientador: Dr. Fagner Lemos de Santana

Natal/RN – 2024

MATEUS FELIPE MENDES DOS SANTOS

Aritmética dos Restos: Jogos e Aplicações para o Ensino

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT -CCET - UFRN, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador:

Profº. Dr. Fagner L. de Santana

Natal/RN – 2024

Universidade Federal do Rio Grande do Norte - UFRN
Sistema de Bibliotecas - SISBI
Catalogação de Publicação na Fonte. UFRN - Biblioteca Setorial Prof. Ronaldo Xavier de Arruda - CCET

Santos, Mateus Felipe Mendes dos.
Aritmética dos restos: jogos e aplicações para o ensino / Mateus Felipe Mendes dos Santos. - 2024.
66 f.: il.

Dissertação (mestrado) - Universidade Federal do Rio Grande do Norte, Centro de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT). Natal, RN, 2024.
Orientação: Prof. Dr. Fagner Lemos de Santana.

1. Aritmética - Dissertação. 2. Divisão - Dissertação. 3. Aplicações - Dissertação. 4. Jogos - Dissertação. I. Santana, Fagner Lemos de. II. Título.

RN/UF/CCET CDU 511.1(043.3)

Elaborado por Joseneide Ferreira Dantas - CRB-15/324

Dissertação de Mestrado sob o título “Aritmética dos Restos: Jogos e Aplicações para o Ensino” apresentado por Mateus Felipe Mendes dos Santos e aceito pelo Programa de Pós-Graduação em Matemática em Rede Nacional – PROFMAT da Universidade Federal do Rio Grande do Norte, como requisito parcial para obtenção do grau de Mestre, sendo aprovado por todos os membros da banca examinadora abaixo especificada:

Prof°. Dr°. Fagner Lemos de Santana
Orientador
UFRN - Universidade Federal do Rio Grande do Norte

Prof°. Dra°. Viviane Simioli Medeiros Campos
Examinadora Interna
UFRN - Universidade Federal do Rio Grande do Norte

Prof°. Dr°. Annaxsuel Araujo de Lima
Examinador Externo
IFRN - Instituto Federal do Rio Grande do Norte

Natal/RN - 2024

Dedicatória

A Deus, por ter me capacitado, me dado forças e me abençoado a cada dia para que eu possa concluir mais esse grande objetivo e a minha família por todo suporte e apoio durante todo processo.

Agradecimentos

Primeiramente a Deus, pois sem ele eu nada seria e nada conseguiria.

A minha família, em especial aos meus pais Bernadete Monteiro e Raimundo Mendes por todo suporte e apoio não só nesse curso, mas em todo meu período acadêmico, meus irmãos Vinicius, Sabrina e Lais por sempre me incentivarem a nunca desistir e buscar a cada dia ser melhor.

A minha namorada Claudia e toda sua família por sempre estarem ao meu lado em todos os momentos, sempre me incentivando, aconselhando e em muitas vezes cuidando de mim em momentos de complicações.

Ao meu orientador, Fagner Lemos, por ser uma pessoa extremamente humana, empática, sempre entendendo situações complicadas perpassadas durante essa caminhada, pelas instruções e várias orientações não só para a elaboração desse trabalho, mas para toda minha vida acadêmica.

A todos meus colegas de curso, em especial a Richardson Lucas, Marco Lira, Carla Soliane e Adriano Marques por sempre estarem comigo, me ajudando a melhorar cada dia mais e a passar por todos os obstáculos. Sem eles, seria tudo muito mais complicado.

Aos meus amigos da vida Madson, Erick, Ricardo, Geilson, Pedro, Guilherme, Vinicius e Lucas pelo incentivo de sempre e por todos os momentos de descontração quando necessário.

E aos meus professores por toda a contribuição acadêmica e pessoal durante todo período do curso me proporcionando uma formação de muita qualidade.

Resumo

Este trabalho tem por objetivo apresentar, de forma introdutória, o conceito de Aritmética dos restos ou Aritmética modular, destacando a importância dessa área em nosso cotidiano. Para isso, vamos mostrar alguns conceitos fundamentais que embasam essa área. Ademais, vamos perpassar pela parte histórica destacando os principais povos e matemáticos que contribuíram para o desenvolvimento dessa área. Mostraremos como a aritmética dos restos aparece na nossa vida em várias aplicações e finalizaremos este trabalho com jogos que se baseiam na aritmética dos restos os quais podem ser utilizados no Ensino Básico.

PALAVRAS-CHAVE: Aritmética, Divisão, Aplicações, Jogos.

Abstract

This work aims to present, in an introductory manner, the concept of Arithmetic of Remainders, or Modular Arithmetic, highlighting the importance of this area in our daily lives. To achives this, we will discuss some fundamental concepts that underlie this field. Furthermore, we will explore the historical context highlighting the main civilizations and mathematicians who contributed to the development at this area. We will demonstrate how the arithmetic of remainders appears in our lives through various applications, and we will conclude this work with games that utilize and are based on the arithmetic of remainders, which can be used in the basic education.

KEYWORDS: Arithmetic, Division, Applications, Games.

Sumário

Introdução

A aritmética é uma das mais antigas áreas da matemática. Trata-se de um campo do conhecimento fundamental que perpassa inúmeras situações da nossa vida cotidiana, mesmo que nem sempre estejamos conscientes de sua presença, desde uma simples contagem de objetos até complexas atuações em diversas áreas, tais como cálculo, estatística, física, economia, etc.

A aritmética modular, ou aritmética dos restos, é uma ramificação importante e específica da aritmética que nos fornece insights densos e inúmeras aplicações práticas. Ao compreendermos os fundamentos e as implicações da aritmética modular, teremos a aptidão para solucionarmos um vasto leque de problemas complexos.

Nessa perspectiva, sabemos que o ensino da matemática é uma fascinante jornada, cheia de descobertas, desafios e conquistas. Porém, em várias situações, os estudantes encontram enormes dificuldades, sejam elas emocionais ou cognitivas ao tentar entender os conceitos complexos aos quais são apresentados. Nesse cenário, os jogos pedagógicos surgem como uma ferramenta extraordinária, sendo útil no rompimento dessas dificuldades e na transformação do processo de aprendizagem em uma aventura instigante e envolvente.

Nos últimos anos está em alta a ideia de se trabalhar com jogos dentro do ambiente educacional. Existem várias definições para jogos dentro da matemática com vários objetivos e funções diferentes por causa da vasta gama de materiais existentes.

Segundo Mota ([18]), Os “jogos matemáticos” ou as “matemáticas recreativas” são matemáticas – sem importar de que tipo – com uma grande componente lúdica.

Afirmado também por Kishimoto ([14]):

> “O que oferece dificuldade para o conceito de jogo é o emprego de vários termos como sinônimos. Jogo, brinquedo e brincadeira têm sido utilizados com o mesmo significado. (…) O sentido usual permite que a língua portuguesa referende os três

> termos como sinônimos. Esta situação reflete o pouco avanço dos estudos na área.” (citado por Moura ([17]))

Logo, podemos concluir que a ideia de que o jogo é apenas uma brincadeira ou uma diversão está cada vez mais sendo considerada errônea e limitada, pois cada vez mais vão surgindo novas definições e ideias sobre essa temática.

Independente do ano escolar em que os educandos se encontram, quando se fala em jogos e materiais lúdicos é instantânea a reação positiva deles, tendo em vista a grande aceitação desses materiais tão importantes e ricos no ensino e aprendizagem de qualquer componente curricular.

Esses materiais lúdicos exercem um importante papel no processo de educação, principalmente na educação básica, onde os jovens, sobretudo as crianças, estão em um nível fundamental para se desenvolver cognitivamente, socialmente e emocionalmente. Introduzir esse elemento em sala de aula nos proporciona uma importante e eficiente abordagem no ensino o tornando mais eficaz, além de trazer diversas contribuições sobre as quais discorreremos nesse capítulo.

É interessante entender as visões gerais que esses materiais proporcionam aos alunos e saber a melhor maneira de utilizá-los.

> O jogo atrai a atenção pelo fato de estar competindo, e como todos os jogos, ou se destrói o inimigo, ou considera o adversário como referência constante para o diálogo consigo mesmo. Quando os jogos são propostos para as crianças, a reação mais comum entre eles é da alegria e interesse pela atividade, pelo material e pelas regras, mas o interesse e alegria pelo jogo simplesmente não bastam, é preciso que haja uma intervenção pedagógica a fim de que esse jogo seja útil na aprendizagem de conceitos. É necessário também que essa atividade represente um desafio, que seja capaz

> de gerar “conflitos cognitivos”. Segundo Jean Piaget, os conflitos cognitivos são fundamentais para o desenvolvimento intelectual do sujeito ([20]).

Os jogos são inerentemente motivadores. Eles prendem a atenção das crianças por sua capacidade de divertir e desafiar simultaneamente, criando um ambiente de engajamento e participação dos educandos. Além de serem confeccionados de modo a promover o desenvolvimento do aluno, incluindo habilidades como raciocínio lógico, resolução de problemas, pensamento crítico e tomada de decisões.

Utilizar os jogos no ensino da matemática pode auxiliar os alunos nos mais diferentes níveis de ensino, sempre utilizando jogos de fácil compreensão, com regras claras e objetivas, trazendo o conteúdo abordado de forma mais divertida e dinâmica de forma a desafiar as expectativas dos educandos. Portanto, para justificar essa metodologia de ensino, é importante salientar seus benefícios pedagógicos.

A matemática para alguns alunos pode estar associada a desafios e complicações e os jogos ajudam a quebrar esse estigma modificando essa visão da matemática e mostrando que ela pode ser uma experiência positiva, divertida e desafiadora. Além de serem naturalmente atrativos e estimularem bastante o interesse dos alunos, os jogos criam uma atmosfera lúdica trazendo assim um ambiente propício para explorar a ensino da matemática que por muitas vezes é feito apenas de forma tradicional.

É importante salientar também que esses materiais ajudam na consolidação de habilidades fundamentais como o reconhecimento de números, operações aritméticas, geometria e resolução de problemas, praticando assim essas habilidades de forma repetitiva e contextualizada, incentivando o educando a pensar criticamente e estrategicamente, planejando suas ações e tentando antecipar consequências de suas escolhas.

A escolha do material utilizado é muito importante. É interessante que os jogos possam sofrer adaptações visando atender os diferentes níveis de habilidades. Com isso, os professores têm um papel crucial, podendo escolher jogos que desafiem seus alunos mais avançados e, simultaneamente, fornecer apoio para aqueles que precisam de um reforço em

alguns conceitos, não desistindo de incentivar a autonomia e a autorregulação do aprendizado. É interessante que o próprio educando assuma o controle de sua aprendizagem, experimentando estratégias e tomando suas decisões, o que torna o aprendizado mais autêntico.

Nessa perspectiva, para Moura ([17]), os jogos e resolução de problemas são trazidos como uma espécie de fabricadores de conhecimento, possibilitando a aquisição de conhecimentos matemáticos. Com isso, o educando é “obrigado” a criar processos pessoais para poder jogar e solucionar os problemas que surgem de acordo com cada jogo, inovando seus pensamentos e conhecimentos.

> Desse modo, o jogo, na Educação Matemática, passa a ter o caráter de material de ensino quando considerado promotor de aprendizagem. A criança, colocada diante de situações lúdicas, aprende a estrutura lógica da brincadeira e, deste modo, aprende também a estrutura matemática presente ([17]).

Com isso, é importante destacar que nessa perspectiva, ao utilizar essa abordagem, o educando é levado a pensar e traçar estratégias que irá utilizar em cada jogada, avaliando todo o processo e observando as habilidades que está trabalhando na resolução de cada problemática abordada.

Diante do que foi dito, é possível observar que faz uma grande diferença para o aprendizado do aluno ter um material lúdico e manipulável como instrumento de estudo dentro da sala de aula, e que esse material pode ser de grande ajuda para o professor no desenvolvimento do ensino-aprendizagem dos alunos. Importante também é conhecer o real significado de jogos, na perspectiva de trazer uma atividade pedagógica que estimule sempre os objetivos a serem alcançados.

Junto à aplicação de jogos em sala de aula, deve ser feito um trabalho de levantamento e observação de dados para se perceber o grau de qualidade que essa metodologia traz para o conhecimento dos alunos. Importante também trabalhar e levar em consideração os

diferenciais de cada aluno, intensificando o respeito entre eles e a ampla gama de aspectos que são desenvolvidas dentro da sala de aula.

No primeiro capítulo, vamos fazer uma breve introdução sobre a aritmética dos restos e mostrar resultados importantes que utilizaremos no decorrer desse trabalho.

No segundo capítulo, vamos perpassar pela história da aritmética modular mostrando os principais elementos que contribuíram significativamente para o desenvolvimento dessa vertente.

No terceiro capítulo, traremos aplicações da aritmética dos restos no nosso cotidiano e como podemos observá-la e aplicá-la.

Por fim, no quarto capítulo, mostraremos jogos aritméticos, suas metodologias e estratégias para que os jogadores, que aprenderem a aritmética dos restos, consigam obter vitórias de formas assertivas.

Capítulo 1

Fundamentação Teórica

Neste capítulo apresentaremos uma breve introdução da aritmética dos restos, também conhecida como aritmética modular, a qual foi introduzida por Euler ainda no século XVIII. Um pouco depois, Carl Friederich Gauss (1777-1855) no seu trabalho conhecido como *Disquisitiones Arithmeticae*, de 1801, apresentou a abordagem moderna que é usada até os dias atuais. Vamos abordar os primeiros conceitos de divisibilidade e divisão euclidiana, além das ideias e alguns resultados da congruência modular, usando como referências principais [12] e [22].

1.1 – Divisibilidade

Começamos essa seção com o conceito fundamental de divisibilidade.

Definição 1.1.1. *Dados dois números inteiros a e b, diremos que a divide b, escrevendo a|b, quando existir k ∈ Z tal que b = k.a. Neste caso, diremos também que a é um divisor ou um fator de b ou, ainda, que b é um múltiplo de a.*

Exemplo 1.1.1. 2|10, pois 10 = 5.2

Se *a* não divide *b*, utilizamos a notação *a∤b*, significando que não existe $k \in Z$ tal que $b = k.a$.

Suponha que $a|b$, com $a \neq 0$ e seja $k \in Z$ tal que $b = k.a$. O número inteiro k é chamado de quociente de b por a e denotado por $k = \frac{b}{a}$.

Exemplo 1.1.2. *Para todo a ∈Z temos 1|a, a|a e a|0.*

Isto decorre das igualdades a = a.1, a = 1.a e 0 = 0.a.

A seguir, vamos apresentar alguns resultados básicos sobre divisibilidade.

Proposição 1.1.1. *Sejam a, b, c ∈ Z. Se a|b e b|c, então a|c.*

Demonstração: Se a|b e b|c então existem m, n ∈ Z tais que b = m.a e c = n.b. Substituindo o valor de b da primeira equação na outra, obtemos c = n.b = n.m.a = (m.n).a, com *m, n ∈ Z,* o que nos mostra que a|c.

Proposição 1.1.2. *Sejam a, b, c, d ∈ Z. Se a|b e c|d, então a.c|b.d.*

Demonstração: Se a|b e c|d, então existem m, n ∈ Z tais que b = m.a e d = n.c. Então, b.d = m.a.n.c = (m.n).a.c, o que nos mostra que a.c|b.d.

Proposição 1.1.3. *Sejam a, b, c ∈ Z, tais que a|(b ± c). Então, a|b se, e somente se, a|c.*

Demonstração: Suponhamos que a|(b + c). Logo, existe k ∈ Z tal que b + c = k.a. De fato de a|b, existe m ∈ Z, tal que b = m.a. Juntando as duas igualdades acima, temos m.a + c = k.a, portanto c = k.a − m.a = (k – m).a, com k – m ∈ Z, o que nos mostra que a|c. De maneira análoga, demonstra-se a implicação contrária.

Propoição 1.1.4. *Se a, b, c ∈ Z são tais que a|b e a|c, então a|(x.b+y.c), para todo x, y ∈ Z.*

Demonstração: Se a|b e a|c então existem m, n ∈ Z tais que b = m.a e c = n.a. Logo, x.b + y.c = x.m.a + y.n.a = (x.m + y.n).a, com x.m + y.n ∈ Z, ou seja, a|(x.b + y.c).

Proposição 1.1.5. *Se a, b ∈ N e a|b, então a ≤ b.*

Demonstração: Se a|b, existe k ∈ Z tal que b = k.a. Como a, b > 0, segue-se que k ∈ N. Como 1 ≤ k, segue-se que 1.a ≤ k.a ou seja a ≤ b.

1.2 – Divisão Euclidiana

Teorema 1. *Sejam a e b dois números inteiros com a ≠ 0. Existe um único par de números inteiros q e r, tais que:*

$$b = a.q + r, \text{ com } 0 \leq r < |a|.$$

Demonstração: Inicialmente, defina $S = \{x = b - ay;\ y \in Z\} \cap N$.

É imediato que $S \subset N$. Se provarmos que $S \neq Ø$ podemos usar o princípio da boa ordenação. Uma análise caso a caso ($a > 0$ e $b \geq 0$; $a > 0$ e $b < 0$; $a < 0$ e $b \geq 0$; $a < 0$ e $b < 0$) e a propriedade arquimediana mostram que existe $n_0 \in Z$ tal que $n_0.(-a) > -b$, logo $b - n_0.a > 0$ e assim $S \neq Ø$. Sendo assim, pelo princípio da boa ordenação, temos que S possui um menor elemento, digamos r. Seja $q \in Z$ tal que $r = b - aq$. Já temos $r \geq 0$. Vamos mostrar que $r < |a|$. Suponha $r \geq |a|$. Dessa forma, existe $s \in N$ tal que $r = |a| + s$, o que implica em $0 \leq s < r$ pois $|a| > 0$. Note que $s = r - |a| = b - aq \pm a = b - (q \pm 1).a$, ou seja, $s \in S$. Como $s < r$, isso contradiz o fato de r ser o menor elemento de S. Portanto, $r < |a|$ e a parte da existência está provada.

Agora, vamos provar a unicidade de r e q. Suponha que $b = a.q + r = a.q' + r'$, onde $q, q' , r , r' \in Z$, $0 \leq r < |a|$ e $0 \leq r' < |a|$. Note que $-|a| < -r \leq r - r' < |a|$. Do mesmo modo, prova-se que $r' - r < |a|$ e assim, $|r - r'| < |a|$. Como, $a.(q - q') = r - r'$, segue que $|a||q - q'| = |r - r'| < |a|$, o que só é possível se $q = q'$ e consequentemente, $r = r'$. ■

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

Da divisão euclidiana, temos que o resto da divisão de b por a é igual a zero se, e somente se, a|b.

Exemplo 1.2.1. Vamos achar o quociente e o resto da divisão de 23 por 4.

Considere as diferenças sucessivas:

$$23 - 4 = 19 \Rightarrow 23 - 4.5 = 3 < 4$$

Isto nos dá $q = 4$ e $r = 3$.

1.3 – Congruência Modular

Aqui apresentamos de forma resumida e introdutória a congruência modular.

Definição 1.3.1. *Seja m um número natural diferente de zero. Dois números naturais a e b são congruentes módulo m se os restos de sua divisão por m são iguais. Denota-se esta relação da seguinte forma: $a \equiv b \bmod m$ ou $b \equiv a \bmod m$ (lê-se a é congruente a b módulo m).*

Exemplo 1.3.1. O número 8 é congruente ao número 13, módulo 5, pois ambos deixam resto 3, ao serem divididos por 5. Representamos isso por $8 \equiv 13 \bmod 5$.

Note que todo número inteiro é congruente módulo *m* ao seu resto pela divisão euclidiana por *m* e, portanto, é congruente módulo *m* a um dos números *0, 1, 2, ..., m−1.*

Proposição 1.3.1. *Dados m, a, b* $\in$ Z, com $b \neq 0$ e $m > 1$, temos $a \equiv b \bmod m$, *se, e somente se* $m|(b - a)$, *ou seja, a diferença* $(b - a)$ *é um múltiplo de m.*

Demonstração: Sejam a, b, m $\in$ Z, com $m \geq 1$.

Suponha que $a \equiv b \bmod m$. Sejam $a = m.q + r$ e $b = m.q' + r$, com $0 \leq r < m$, Logo:

$$b - a = mq' + r - (mq + r) = mq' - mq = m.(q' - q) \Rightarrow m|(b - a).$$

Reciprocamente, suponha que $m|(b - a)$. Sejam $a = m.q + r$ com $0 \leq r < m$ e $b = m.q' + r'$ com $r' < m$, Logo:

$$b - a = mq' + r' - (mq + r) = m(q' - q) + r' - r.$$

Como $m|(b - a)$ e $|r' - r| < m$, temos: $r' - r = 0 \Rightarrow r' = r \Rightarrow a \equiv b \bmod m$.

Exemplo 1.3.2. $13 \equiv 40 \bmod 3$ pois $40 - 13 = 27$ e $3|27$.

Proposição 1.3.2. A congruência módulo $m \geq 1$ é uma relação de equivalência em Z, ou seja, para quaisquer *a, b, c* $\in Z$:

I. $a \equiv a \bmod m$ (Reflexiva).

II. Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$ (Simétrica).

III. Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$ (Transitiva).

Demonstração:

I. Esta afirmação é equivalente a dizer que $m|(a - a) \Rightarrow m|0$. De fato, zero é múltiplo de qualquer inteiro m , uma vez que $0.m = 0$.

II. Se $a \equiv b \bmod m$, temos que $m|(b - a)$, ou seja, existe $k \in Z$ tal que $b - a = k.m$. Multiplicando esta igualdade por (-1), obtemos:

$$a - b = (-k).m \Rightarrow m|(a - b) \Rightarrow b \equiv a \bmod m.$$

III. Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, temos que $m|(b - a)$ e $m|(c - b)$, ou seja, existem $k, p \in Z$ tais que $b - a = k.m$ e $c - b = p.m$.

Somando membro a membro as duas igualdades obtemos:

$$(b - a) + (c - b) = k.m + p.m \Rightarrow c - a = (k + p).m \Rightarrow m|(c - a) \Rightarrow a \equiv c \bmod m.$$

Proposição 1.3.3. Sejam $a, b, c, d, m \in Z$, com $m > 1$.

I. Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então, $a + c \equiv b + d \bmod m$.

II. Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então, $a.c \equiv b.d \bmod m$.

Demonstração: Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, temos que $m|(b - a)$ e $m|(d - c)$.

I. Note que $m|(b - a) + (d - c)$, e podemos escrever $(b - a) + (d - c) = (b + d) - (a + c)$, logo:

$$m|(b + d) - (a + c), \text{ ou seja, } a + c \equiv b + d \bmod m.$$

II. Note que $m|d(b - a) + a(d - c)$ e $d(b - a) + a(d - c) = db - ac$, logo:

$$m|db - ac \Rightarrow a.c \equiv b.d \bmod m.$$

Capítulo 2

História da Aritmética Modular

A história da aritmética modular remonta a séculos atrás e envolve contribuições significativas de matemáticos de diferentes culturas. Os matemáticos babilônios foram alguns dos primeiros a explorar conceitos que podem ser relacionados à aritmética modular. Por volta de 2000 A.C., eles desenvolveram técnicas para resolver problemas de divisão e restos, que podem ser considerados rudimentos da aritmética modular.

2.1 – Contribuições Gregas

Foi na Grécia antiga que foram observadas importantes contribuições para o desenvolvimento da matemática, em especial, conceitos relevantes para a aritmética modular. Tales de Mileto (640-546 AC) foi um dos primeiros gregos que a estudou e levou seus estudos matemáticos para Grécia, tornando o local um dos mais importantes para o estudo e desenvolvimento dessa ciência até os dias atuais.

Logo em seguida veio Pitágoras de Samos (580-500 AC), e sua escola que perdurou por séculos conhecida como escola Pitagórica, que se dedicou aos estudos da teoria dos números, incluindo as propriedades do conjunto dos números inteiros positivos. Eles produziram pensamentos e ideias fenomenais sobre os números primos, divisibilidade e as propriedades sobre o conjunto dos números inteiros que foram relevantes para o desenvolvimento da aritmética modular.

Com um aporte de toda essa herança científica e cultural, em meados de 300 AC, Euclides com sua obra *"Os Elementos"* desenvolveu uma abordagem axiomática à geometria, e ainda que a geometria e a aritmética modular sejam áreas diferentes da

matemática, essa abordagem axiomática de Euclides influenciou diretamente no desenvolvimento da teoria dos números. Seu livro, “Os elementos”, é um tratado composto pela junção de treze livros (dez de geometria e três de aritmética), onde podemos observar o desenvolvimento de teorias e ideias cruciais no crescimento do conhecimento aritmético. Por exemplo, ele define as ideias de divisibilidade, números primos, máximo divisor comum, mínimo múltiplo comum, traz seu algoritmo para cálculos de máximo divisor comum, apresenta uma prova da existência de infinitos números primos e também de que um número natural é escrito como produto de primos, conhecido atualmente por Teorema Fundamental da Aritmética. ([13]).

Embora os gregos tenham tido uma importância fundamental para o desenvolvimento de conceitos matemáticos importantes para a aritmética, a aritmética modular do modo que conhecemos hoje teve um incremento significativo e substancial na índia e na china no decorrer dos séculos.

2.2 – Contribuições Hindus

Sobre os indianos, segundo relatos dos historiadores, eles foram os pioneiros no sistema de numeração hindu-arábico, sistema esse utilizado até os dias de hoje. Eles também foram responsáveis pela formalização teórica do zero que ainda não tinha sido utilizado pelas civilizações ocidentais e árabes nesse período. Os matemáticos indianos mudaram a história da matemática por transformar o zero de um mero “espaço vazio” a um número conceitual para utilizar em cálculos sendo útil em investigações de várias áreas de ensino na matemática ([9]).

A Índia e seus matemáticos deixaram relevantes subsídios de conhecimento para a humanidade, podemos citar o matemático e astrônomo Aryabhata (476-550), cujo principal legado foi a escrita de um trabalho semelhante a *“Os Elementos”* de Euclides, que veio a ser intitulado de *“Aryabhatiya”* publicada em 499 (século V), que abordava astronomia e matemática. Em seu vasto acervo de obras podemos destacar que Aryabhata tratava sobre conhecimentos geométricos como área e semelhança de triângulos, formas de determinar

volumes, e até apresentou uma aproximação para o valor do número π. Dentro da aritmética, ele explorou extensivamente as propriedades dos números, incluindo as relacionados a aritmética modular, chegando a expressar um algoritmo para resolução de equações indeterminadas na forma ax – by = c, atualmente conhecidas como equações lineares congruentes ou equações diofantinas ([16]).

Quase um século depois de Aryabhata, surge na Índia central um dos mais importantes matemáticos indianos da história, Brahmagupta (598 – 668). Das suas várias contribuições para a matemática, destacamos as ligadas com álgebra e aritmética. Seus estudos foram apresentados principalmente em sua obra *"Brahmasphutasiddhanta"* que é uma das primeiras obras matemáticas indianas que chegaram até o ocidente. Entre seus principais estudos na álgebra está a busca por soluções de equações quadráticas com raízes negativas.

Já na área de aritmética, podemos citar congruências modulares, onde desenvolveu normas especificas para lidar com operações aritméticas em um conjunto de números congruentes, estabelecendo propriedades e incluindo regras para operações básicas. Brahmagupta, assim como Aryabhata, também teve uma importante contribuição nas equações diofantinas, tipo de equação que é fundamental na teoria dos números e tem aplicações diretas na aritmética modular ([8]).

Considerado o mais importante matemático indiano da história, Bháskara (1114- 1185) também faz parte da lista dos importantes matemáticos/astrônomos hindus. No século VII, destacou-se sua principal obra “Siddhanta Siromani”, que foi dividida em quatro partes, “Lilavati, Bijaganita, Goladhyaya e Grahaganita”. Nela, ele completou alguns dos estudos deixados por Brahmagupta. Dentro da área da aritmética, Bháskara desenvolveu um teorema específico para a resolução de equações diofantinas. Este teorema é útil na resolução de problemas envolvendo números inteiros ([8]).

2.3 – Contribuições Chinesas

Os chineses desempenharam um papel importantíssimo na evolução da matemática em diversas áreas, desde a aritmética básica até a geometria. Em especial, podemos destacar

desenvolvimentos substanciais na aritmética modular.

Depois da queda de produção da matemática grega, foi a matemática chinesa que conseguiu obter relevantes resultados em todas as áreas de estudos, superando até os matemáticos europeus. Segundo Eves ([7]), os chineses foram responsáveis pela criação de um sistema numérico posicional decimal, por apresentar um chamado triângulo aritmético que viria a ser conhecido como de Pascal, descobrindo algumas propriedades interessantes várias centenas de anos antes de Blaise Pascal na Europa, e também pela utilização de métodos matriciais na resolução de equações lineares, que fornece uma formulação inicial do Teorema dos Restos Chineses, a mais notória contribuição desse povo dentro dos estudos da aritmética modular, que é um teorema que fornece uma solução para um sistema de equações lineares congruentes simultâneas.

2.4 – Contribuições a partir do século XVII

O estudo da matemática remete a muitos séculos antes de cristo, mas é valido salientar que especificamente a Teoria dos Números, ficou um pouco esquecida até meados do século XVII. Nesse século podemos destacar importantes matemáticos que impulsionaram o crescimento dos estudos da Teoria dos números como Pierre de Fermat, Leonard Euler e Friedrich Gauss.

2.4.1 – Pierre de Fermat

Pierre de Fermat (1601 – 1665) é frequentemente considerando o “pai” da Teoria dos Números. Embora suas contribuições não tenham sido muito bem formalizadas, ele desempenhou um papel importante no desenvolvimento da concepção inicial da Teoria dos Números.

Segundo Coutinho ([4]), Pierre de Fermat era um matemático amador, pois não tinha a matemática como sua profissão, já que era um magistrado que nas horas vagas lia e estudava sobre matemática. Foi por volta de 1621 quando houve a publicação do texto *Aritmética* de

Diofanto que Pierre de Fermat ao ler tal documento começou suas anotações com ideias sobre essa temática. Um dos maiores matemáticos da época, Marin Mersenne, era amigo de Fermat com quem sempre conversou sobre essa temática. Depois da morte de Pierre de Fermat, coube ao seu filho, Samuel Fermat, reunir todas suas anotações e publicar para a comunidade.

Fermat não estudava apenas a Teoria dos Números, tendo contribuições também na área de cálculo, geometria e teoria da probabilidade. Mas dentre suas contribuições no que diz respeito a Teoria dos Números, podemos destacar uma afirmação conhecida como Pequeno Teorema de Fermat que relata o seguinte:

Dados $a \in Z$ e p primo, se p não divide a, então p divide $a^{p-1} - 1$.

Fermat também trabalhou em equações diofantinas, linha a qual pertence "Último Teorema de Fermat", uma conjectura que ele escreveu sem prova em uma das margens do livro (onde costumava fazer anotações) o seguinte:

Não existem inteiros positivos x, y, z, n, com $n > 2$, de modo que $x^n + y^n = z^n$.

Esse Teorema foi um dos responsáveis pela fama de Pierre de Fermat dentro da Teoria dos Números, embora tenha afirmado ter uma prova, ele nunca a apresentou, sendo este resultado provado quase 300 anos depois, já no século XX, pelo matemático britânico Andrew Wiles. ([13]).

2.4.2 – Leonhard Euler

Leonhard Euler (1707 – 1783) é considerado o sucessor de Fermat nos estudos matemáticos relacionados ao ramo da Teoria dos Números. Segundo Coutinho ([4]), Euler tinha a matemática como sua profissão e ele publicou obras em quase todas as áreas do conhecimento matemático puro e aplicado no século XVIII.

Chegaram ao conhecimento de Euler os estudos de Fermat sobre a Teoria dos Números e seu verdadeiro interesse no tema começou em meados de 1730.

Euler fez contribuições substanciais para a Teoria dos Números e a aritmética modular. Ele introduziu a notação moderna para a aritmética modular, usando o símbolo de congruência (≡), onde a notação $a \equiv b \, mod \, m$ significa que a e b têm o mesmo resto quando divididos por m, dados a e b inteiros.

Euler desenvolveu também uma generalização do Pequeno Teorema de Fermat, conhecido como Teorema de Euler estabelecendo que:

Dados a e m inteiros, se a é coprimo de m, então $a^{\varphi(m)} \equiv 1 \, (mod \, m)$*, onde* $\varphi(m)$ *é a função totiente de Euler, que representa o número de inteiros positivos menores que m e coprimos com m.*

Euler também trabalhou em problemas práticos relacionados à aritmética modular, como o problema da congruência linear e a resolução de equações diofantinas.

2.4.3 - Carl Friedrich Gauss

Carl Friederich Gauss (1777-1855) é considerado um dos maiores matemáticos de todos os tempos, sendo conhecido até como o "príncipe da matemática". Aos dezessete anos Gauss decide adentrar nos estudos sobre Aritmética, onde em 1801, "produz uma das obras primas de toda matemática, o livro *Disquisitiones Aríthmeticae*" ([13]).

No livro, Gauss aborda diversas das suas contribuições para a aritmética, tais como a noção de congruência, na qual simbologias, definições e conceitos foram construídos, a Lei da Reciprocidade, dentre outras.

Gauss também foi o responsável por demonstrar o Teorema Fundamental da Álgebra, algo que ninguém antes na história havia conseguido. Também fez contribuições significativas na Teoria das Probabilidades e em de Geometria Diferencial ([13]).

Capítulo 3

Aplicações da Aritmética Modular

Na atualidade, a aritmética modular se tornou uma ferramenta cujas aplicações trazem enormes facilidades para nosso cotidiano. São aplicações com os mais variados níveis de complexidade, que envolvem desde situações simples até as mais avançadas, todas com o intuito de resolver problemas onde a ideia de divisibilidade é determinante.

Muito tem se escrito sobre essa temática, em sua maioria no universo da Teoria dos Números, a qual está ligada diretamente ao conceito de resto de divisão de números inteiros. É um tema bastante contemporâneo e que pode ser desenvolvido em trabalhos em turmas do Ensino Fundamental II e de Ensino Médio, trazendo uma excelente oportunidade de sua contextualização na metodologia do ensino de matemática.

Dentre as aplicações da aritmética modular no cotidiano podemos citar o sistema de identificação de publicações através do ISBN, controle de lotes de produtos através de códigos de barras, a identificação de pessoas através do Cadastro de pessoas Físicas (CPF), carteiras de identidade (RG), passaporte, título de eleitor, dentre outros.

Além desses, também temos a criptografia que consiste em métodos de alterar informações fornecendo mais seguridade, principalmente em informações sigilosas, representando outra forma de aplicações de congruência modular. A criptografia tem sido abordada e utilizada nas linguagens de programação de computadores, sistemas bancários, aplicativos de uso individual e nos sistemas de informações de uso tanto em empresas como no uso doméstico.

Vamos destacar no decorrer desse capítulo algumas dessas aplicações de Aritmética Modular que podem ser abordadas por professores de matemática na Educação Básica, como forma de contextualização da matemática.

3.1 – Cadastro de Pessoa Física – CPF

O Cadastro de Pessoa Física (CPF) é o documento que identifica o contribuinte perante a Receita Federal. Cada contribuinte pessoa física possui um Cartão CPF, ou simplesmente CPF, que comprova o cadastro. Ele contém um número identificador que não muda. Não é obrigatório portar o cartão, mas o número do CPF é exigido em várias situações, principalmente em operações financeiras, como abertura de contas em bancos.

O número do CPF de uma pessoa no Brasil possui 11 (onze) dígitos, onde o primeiro bloco tem 9 dígitos e o segundo bloco tem 2 dígitos, que são os dígitos de verificação. É na obtenção desses 2 dígitos de verificação da segunda parte que a congruência modular é usada ([21] e [3]).

FIGURA 1 – Cédula de CPF
FONTE: Google Imagens

Para determinarmos o décimo digito (primeiro digito verificador), devemos resolver uma congruência de módulo 11, em uma operação com os nove dígitos iniciais, como descrito a seguir:

I. Considere os nove dígitos iniciais do CPF organizados em sequência:

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\}$$

II. Agora consideremos os naturais entre 1 e 9:

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

III. Multiplique cada digito do CPF pelos fatores da sequência, respectivamente, e depois some os nove números obtidos. Denote por S essa soma:

$$S = a_1.1 + a_2.2 + a_3.3 + a_4.4 + a_5.5 + a_6.6 + a_7.7 + a_8.8 + a_9.9$$

IV. O décimo digito do CPF (a_{10}), é o número que ao ser subtraído da soma obtida, gere um múltiplo de 11, de forma que $\mathbf{S - a_{10} \equiv 0\ mod\ 11}$. Ou seja, é o resto da divisão de S por 11.

Para determinarmos o décimo primeiro digito do CPF (o segundo digito verificador), o método é bem parecido o que vimos anterior, agora acrescentamos o décimo digito encontrado. Além disso, acrescentamos o zero ao início da base de multiplicação, já que agora temos um número a mais:

I. Observe os dez dígitos iniciais do CPF:

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}\}$$

II. Os números que serão usados:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

III. Procedemos da mesma forma já feita: multiplica-se cada digito do CPF pelos números acima, respectivamente, e depois somamos os dez números, obtendo um número S:

$$S = a_1.0 + a_2.1 + a_3.2 + a_4.3 + a_5.4 + a_6.5 + a_7.6 + a_8.7 + a_9.8 + a_{10}.9$$

IV. O décimo primeiro digito do CPF (a_{11}), é o número que ao ser subtraído da soma obtida, gere um múltiplo de 11, de forma que **S - $a_{11} \equiv 0\ mod\ 11$.** Ou seja, é o resto da divisão de S por 11.

Exemplo 3.1.1. Vamos usar o CPF fictício 054.894.927 como exemplo para encontrarmos os dígitos verificadores.

Determinando o a_{10}:
S = 0.1 + 5.2 + 4.3 + 8.4 + 9.5 + 4.6 + 9.7 + 2.8 + 7.9
S = 0 + 10 + 12 + 32 + 45 + 24 + 63 + 16 + 63 = 265
265 - $a_{10} \equiv 0\ mod\ 11 \Rightarrow a_{10} = 1$

Determinando o a_{11}:
S = 0.0 + 5.1 + 4.2 + 8.3 + 9.4 + 4.5 + 9.6 + 2.7 + 7.8 + 1.9
S = 0 + 5 + 8 + 24 + 36 + 20 + 54 + 14 + 56 + 9 = 226
226 - $a_{11} \equiv 0\ mod\ 11\ \Rightarrow\ a_{11} = 6$

Com os resultados obtidos, podemos afirmar que o CPF completo é 054.894.927-16.

Caso o resto da divisão fosse 10, ou seja, o número encontrado na soma fosse congruente a 10 modulo 11, usaríamos o dígito zero ([21]).

Observação: Vale ressaltar que o nono digito do CPF representa o estado onde ele foi emitido. No exemplo utilizado anteriormente, pode-se observar que o nono digito é o número 7, isso significa que o CPF foi emitido no estado do Espírito Santo ou no Rio de Janeiro. Alguns estados brasileiros compartilham o mesmo código, pois eles variam de zero a nove e como sabemos o Brasil possui 26 estados e um Distrito Federal. O número que representa cada estado pode ser visto na tabela a seguir:

9º dígito	Estados emissor
0	RS
1	DF, GO, MS, MT, TO
2	AC, AM, AP, PA, RO, RR
3	CE, PI, MA
4	AL, PB, PE, RN
5	BA, SE
6	MG
7	ES, RJ
8	SP
9	PR, SC

3.2 – Cartão de Crédito

Os cartões de crédito surgiram de forma ainda rudimentar e bastante limitada nos anos 1920 em lojas de departamento e companhias de petróleo ([23]).

A ideia original foi aprimorada pelo Diners Club que em 1953 já era aceito internacionalmente. Com o passar dos anos vários outros cartões foram surgindo e hoje temos uma boa variedade deles (Visa, MasterCard, American Express, etc.).

No Brasil, os cartões de crédito atuais possuem dezesseis dígitos, os primeiros quinze são de informações da bandeira do cartão e dados do cliente. Apenas o último digito é de verificação, para encontrá-lo, usa-se o algoritmo de Luhn criado por Hans Peter Luhn em 1954. ([15]).

Considere um cartão de crédito qualquer, cujos 15 primeiros dígitos são conhecidos e estão representados abaixo:

$$a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}a_{14}a_{15}a_{16}$$

Vamos descrever o método para encontrarmos o digito verificador (a_{16}):

I. Soma-se todos os dígitos de posição par:

$$S1 = a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12} + a_{14}$$

II. Quanto aos dígitos de posição ímpar, faz-se o seguinte:

Para cada índice i ímpar entre 0 e 16, defina $b_i = 2.a_i$, se $2.a_i \leq 9$ e $b_i = 2.a_i - 9$, se $2.a_i > 9$.

$$S2 = b_1 + b_3 + b_5 + b_7 + b_9 + b_{11} + b_{13} + b_{15}$$

III. Fazendo S = S1 + S2, o décimo sexto digito (a_{16}), é o número cuja soma S + a_{16} resulte em um múltiplo de 10, ou seja, tal que $\mathbf{S + a_{16} \equiv 0\ mod\ 10}$.

Exemplo 3.2.1. Vamos determinar o digito verificador, de um cartão de crédito hipotético, onde os primeiros quinze dígitos são dados por: 2134.5678.9012.345.

Determinando S1:

$$S1 = 1 + 4 + 6 + 8 + 0 + 2 + 4 = 25$$

Determinando S2:

$$b_1 = 2.a_1 = 2.2 = 4 \leq 9 \Rightarrow b_1 = 4$$
$$b_3 = 2.a_3 = 2.3 = 6 \leq 9 \Rightarrow b_3 = 6$$
$$b_5 = 2.a_5 = 2.5 = 10 > 9 \Rightarrow b_5 = 10 - 9 = 1$$
$$b_7 = 2.a_7 = 2.7 = 14 > 9 \Rightarrow b_7 = 14 - 9 = 5$$
$$b_9 = 2.a_9 = 2.9 = 18 > 9 \Rightarrow b_9 = 18 - 9 = 9$$
$$b_{11} = 2.a_{11} = 2.1 = 2 \leq 9 \Rightarrow b_{11} = 2$$
$$b_{13} = 2.a_{13} = 2.3 = 6 \leq 9 \Rightarrow b_{13} = 6$$
$$b_{15} = 2.a_{15} = 2.5 = 10 > 9 \Rightarrow b_{15} = 10 - 9 = 1$$

$$S2 = 4 + 6 + 1 + 5 + 9 + 2 + 6 + 1 = 34$$

Determinando S:

$$S = S1 + S2 = 25 + 34 = 59$$

Determinando a_{16}:

S + $a_{16} \equiv 0\ mod\ 10$

59 + $a_{16} \equiv 0\ mod\ 10$

a_{16} = 1

Logo, temos que o dígito verificador, a_{16}, é 1, portanto o cartão de crédito tem a seguinte numeração 2134.5678.9012.3451.

3.3 - ISBN

O ISBN (International Standart Book Number) é um sistema de catalogação de livros criado em 1967. Trata-se de um número criado com o objetivo de identificar uma produção bibliográfica (livro, artigo, etc.), a qual é amplamente usada até os dias atuais.

FIGURA 2 – Código ISBN com 10 dígitos

FONTE: Google Imagens

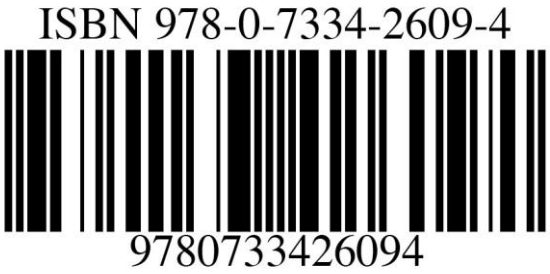


FIGURA 3 – Código ISBN com 13 dígitos

FONTE: Google Imagens

> "Graças a essa combinação, é possível individualizar e catalogar as informações particulares e específicas de cada uma das diversas publicações produzidas ao redor do planeta. Essa série numérica reconhecida em mais de 200 países permite o compartilhamento de **metadados** das obras em diferentes sistemas. Não é à toa que criação deste padrão representou um marco no mercado editorial, melhorando os processos de produção, distribuição, análise de vendas e armazenamento dos dados bibliográficos." ([5]).

No ISBN o último algarismo é o dígito de verificação, o qual é calculado utilizando a aritmética modular e operações matemáticas com os demais dígitos que são sempre separados por hífen, os quais carregam informações sobre o país da publicação, editora e o livro em questão ([21]).

Mostraremos a forma de se obter o dígito de controle para o ISBN que utiliza dez dígitos.

I. Considere um ISBN qualquer cujos dígitos estão representados abaixo:

$$a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10}$$

II. Estabelecemos a sequência de base para multiplicação:

$$\{10, 9, 8, 7, 6, 5, 4, 3, 2\}$$

III. Multiplicam-se os nove dígitos iniciais do código ISBN pelos fatores da sequência, respectivamente, e depois soma-os obtendo como resultado um valor S:

$$S = a_1.10 + a_2.9 + a_3.8 + a_4.7 + a_5.6 + a_6.5 + a_7.4 + a_8.3 + a_9.2$$

IV. O décimo digito do código ISBN (a_{10}), é o número que ao ser somado com S, resulta em um múltiplo de 11, ou seja,

$$S + a_{10} \equiv 0 \; mod \; 11.$$

Exemplo 3.3.1. Tomando o livro Temas e Problemas Elementares, da coleção Professor de Matemática, da SBM, o qual tem o código de ISBN 85-85818-29-8 vamos confirmar que seu dígito de verificação é realmente o 8.

Determinando o a_{10}:

$$S = 8.10 + 5.9 + 8.8 + 5.7 + 8.6 + 1.5 + 8.4 + 2.3 + 9.2$$

$$S = 80 + 45 + 64 + 35 + 48 + 5 + 32 + 6 + 18 = 333$$

$$333 + a_{10} \equiv 0 \; mod \; 11 \Rightarrow \; a_{10} = 8$$

Exemplo 3.3.2. Utilizando o livro Matemática Aplicada a Administração, Economia e Contabilidade, da editora Thompson, que tem o código ISBN 85-221-0399, vamos determinar seu dígito de verificação.

Determinando o a_{10}:

$$S = 8.10 + 5.9 + 2.8 + 2.7 + 1.6 + 0.5 + 3.4 + 9.3 + 9.2$$

$$S = 80 + 45 + 16 + 14 + 6 + 0 + 12 + 27 + 18 = 218$$

$$218 + a_{10} \equiv 0 \; mod \; 11 \Rightarrow \; a_{10} = 2$$

Assim, podemos garantir que o código ISBN do livro citado é 85-221-0399-2.

Observa-se nos exemplos que ambos possuem o prefixo 85, indicando o dígitos que são utilizados por publicações feitas no Brasil.

No ISBN, se o dígito de verificação for 10, é usada a representação do número 10 utilizando os algarismos romanos, no caso o X ([21]), como na figura 2 no início dessa seção.

3.4 – Código de Barras

A criação do código de barras foi um marco importante para o mundo, tendo em vista sua importância na organização de estoques e produtos no comércio. Os primeiros esforços para a sua criação foram feitos em 1952 por Joseph Woodland e Bernard Silver. Os códigos da forma que conhecemos hoje foram criados por George J. Laurer na década de 1970. Esse código continha 12 dígitos e foi aceito em 1973 quando recebeu o nome de Código Universal de Produtos “UPC” (*Universal Product Code*).

FIGURA 4 – Código Universal de Produtos “UPC”
FONTE: Esquinca ([6])

Em 1976 Laurer acrescentou um dígito ao código para que fosse possível identificar também o país de origem dos produtos, e esse novo código com 13 dígitos recebeu o nome de EAN-13 (*European Numbering System*).

FIGURA 5 – Código EAN-13 (*European Numbering System*).
FONTE: Esquinca ([6])

Segundo Sá ([21]) o código EAN-13 é um dos mais utilizados no mundo. O dígito de verificação tem essa utilidade em todas as aplicações. Para encontrar o 13°dígito, é utilizada a congruência módulo 10.

Mostraremos a seguir, como obter o digito de verificação do código de barras EAN-13.

I. Representamos os dígitos do código de barras EAN-13 pelos seguintes símbolos:

$$a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}\,a_{11}a_{12}a_{13}$$

II. A sequência de base para multiplicação:

$$\{1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3\}$$

III. Multiplicam-se os doze dígitos iniciais do código de barras EAN-13 pelos fatores da sequência, respectivamente, e depois somam-se os resultados obtendo como resultado um valor S:

$$S = a_1.1 + a_2.3 + a_3.1 + a_4.3 + a_5.1 + a_6.3 + a_7.1 + a_8.3 + a_9.1 + a_{10}.3 + a_{11}.1 + a_{12}.3$$

Ou

$$S = (a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + 3(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12})$$

IV. O décimo terceiro digito (a_{13}) do código de barras, é o número que ao ser somado com S resulta em um múltiplo de 10, ou seja,

$$S + a_{13} \equiv 0\ mod\ 10.$$

Exemplo 3.4.1. Vamos determinar o dígito de verificação do código de barras EAN-13, a seguir:

FIGURA 6 – Código real EAN-13 sem o último algarismo

FONTE: Google imagens (Editada para exemplificação)

Determinando o a_{13}:

S = (9 + 5 + 1 + 5 + 5 + 4) + 3*(7 + 1 + 1 + 5 + 4 + 4)

S = 29 + 66 = 95

S + $a_{13} \equiv 0\ mod\ 10$

95 + $a_{13} \equiv 0\ mod\ 10$

a_{13} = 5

Portanto, como pode ser verificado, o dígito de verificação do código de barras acima é o digito 5.

FIGURA 7 – Código real EAN-13 completo

FONTE: Google imagens

Para calcular o digito de verificação de um código de barras no sistema UPC, a única diferença seria na base de multiplicação, onde seriam utilizados os valores {3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1}.

3.5 - Criptografia

Criptografia é a prática de proteger informações por meio da conversão de dados em uma forma ilegível para quem não tem a informação correta, ela desempenha um papel vital na segurança da comunicação. Essa técnica tem suas raízes na antiguidade, mas sua importância aumenta cada dia mais com o avanço da tecnologia digital e com o uso de dispositivos conectados.

> "A criptografia é uma técnica de escrita tão antiga quanto a própria escrita convencional. Os egípcios, os gregos e, especialmente os romanos,

> faziam uso da criptografia para evitar que suas mensagens fossem lidas por quem não deveria, caso interceptadas. Seu uso na Segunda Guerra mundial foi de tamanha grandeza. Nesta época os britânicos criaram um grupo de trabalho especialmente dedicado a interceptar e decodificar as mensagens trocadas entre os alemães, italianos e japoneses e, desde então, as técnicas criptográficas tornaram-se cada vez mais evoluídas." ([15])

Atualmente, é imprescindível o uso da criptografia, pois ela é responsável por "esconder" várias informações, principalmente no mundo virtual onde a segurança de dados se tornou algo primordial, tanto para pessoas como para empresas, mantendo sua segurança e sua confiabilidade.

Para Leopold ([15]) a criptografia pode ser considerada a base para a computação moderna, onde suas técnicas avançadas são constantemente aprimoradas, levando os algoritmos matemáticos a ficarem cada vez mais complexos, garantindo a segurança e a inviolabilidade de informações.

Segundo Oliveira ([19]) a criptografia teve seu início e aplicabilidade pelo governo do imperador romano Júlio Cesar com o propósito de se comunicar com seus generais e tropas em períodos de conflitos, de modo que se algum indivíduo que intercepte sua mensagem não conseguisse decifrá-las. Com uma simples regra chamada de "Cifra de César" onde o emissor da mensagem substituía cada letra do alfabeto pela letra três posições após ela (chave 3) e o receptor da mensagem, sabendo dessa chave, aplicava a operação inversa, de modo a substituir cada letra da mensagem pela letras três posições antes dela, assim obtendo a mensagem verdadeira.

Observe como funcionava a famosa chave 3 de Júlio César:

A	B	C	D	E	F	G	H	I	J	K	L	M
d	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
q	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*	*a*	*b*	*c*

FIGURA 8 – Criptografia de Júlio César (Chave 3)
FONTE: Oliveira ([19])

Assim, podemos observar por exemplo que a palavra MATEMATICA, seria escrita como PDWHPDWLFD ou que a palavra MESTRE seria escrita como PHVWUH utilizando a ideia da chave 3 de Júlio César.

Segundo Oliveira ([19]) a pré codificação transforma a mensagem em números e a codificação o transforma em outros números. Portanto, para codificarmos uma mensagem usando a ideia de criptografia de César, primeiro pré codificamos e depois codificamos utilizando um número natural *k*, o qual chamamos de chave, fazendo assim a modificação.

Observe como funcionava a pré codificação na criptografia de Júlio César:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	*01*	*02*	*03*	*04*	*05*	*06*	*07*	*08*	*09*	*10*	*11*	*12*
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*

FIGURA 9 – Criptografia de Júlio César (Pré codificação)
FONTE: Oliveira ([19])

Exemplo 3.5.1. Utilizando a chave 3 de Júlio César, vamos codificar a palavra MATEMÁTICA usando a pré codificação observada acima:

Pré codificando a mensagem a ser enviada:

12 – 00 – 19 – 04 – 12 – 00 – 19 – 08 – 02 – 00

Usando a chave 3 para codificar, ou seja, vamos somar 3 em cada número:

$$15 – 03 – 22 – 07 – 15 – 03 – 22 – 11 – 05 – 03$$

Agora, usando a correspondência observada acima, podemos visualizar a mensagem enviada:

"PDWHPDWLFD"

Podemos observar que a criptografia, como observado na "Cifra de César", é baseada nos conceitos da aritmética modular, de modo que:

"Seja Y o equivalente numérico de uma letra do texto e X o equivalente numérico do texto cifrado correspondente, sendo assim, $X \equiv Y + k \pmod{26}$, onde $0 \leq X \leq 26$ e k é a chave de criptografia de modo que $k \in Z^*$".

Exemplo 3.5.2. Dada a palavra MESTRE, codifique-a usando a chave k = 11.

Pré codificação de MESTRE: 12 – 04 – 18 – 19 – 17 – 04

Vamos codificar usando a expressão $X \equiv Y + 11 \pmod{26}$

$$X \equiv 12 + 11 \equiv 23 \pmod{26}$$

$$X \equiv 04 + 11 \equiv 15 \pmod{26}$$

$$X \equiv 18 + 11 \equiv 29 \equiv 03 \pmod{26}$$

$$X \equiv 19 + 11 \equiv 30 \equiv 04 \pmod{26}$$

$$X \equiv 17 + 11 \equiv 28 \equiv 02 \pmod{26}$$

$$X \equiv 04 + 11 \equiv 15 \pmod{26}$$

Logo, a mensagem codificada a ser emitida é 23 – 15 – 03 – 04 – 02 – 15.

Para decodificar a mensagem, podemos utilizar a expressão $X \equiv Y - 11 \pmod{26}$ onde Y são

os números da mensagem codificada.

Segundo Sá ([21]) atualmente a criptografia não sofreu muitas alterações na sua função principal. O que houve foi a modernização na sua complexidade visando melhorar a segurança de informações. Essa melhoria se deu pela ascendência da Internet, pois a comunicação existente entre os computadores e outros dispositivos não podem ser acessada por terceiros.

Por causa desse crescimento, sabe-se que a criptografia é muito mais complexa do que foi mostrado nesse capítulo, pois apenas foram mostradas as ideias iniciais que são simples de modo a mostrar sua relação com a aritmética modular. Por exemplo, a criptografia RSA que segundo Coutinho ([4]) é o mais conhecido dos métodos de criptografia, foi inventado em 1977 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.), onde é bastante utilizada atualmente e seu método (algoritmo) também utiliza aritmética modular, porém de forma bem mais complexa.

Capítulo 4

Jogos Combinatórios

Os jogos combinatórios são um nicho encantador quando falamos da Teoria dos Jogos e da Matemática Discreta. Esses tipos de jogos envolvem dois jogadores que se alternam em fazer uma quantidade finita de movimentações, onde elementos como sorte (cartas ou dados, por exemplo) são inexistentes, e, com informações completas, ou seja, onde todos os jogadores conhecem completamente a configuração do jogo, e o objetivo é alcançar uma determinada condição de vitória.

Segundo Gomes ([10]) os jogos combinatórios são tipos de jogos que satisfazem algumas condições, tais como número de jogadores (2), jogadas alternadas e regras e critérios de vitória bem definidas e conhecidos entre os jogadores.

Segundo Almeida e Carvalho ([2]) é importante salientar que, quando existe uma estratégia vencedora para um dos jogadores, o jogo “deixa de existir”, uma vez que a competição em jogos combinatórios é uma disputa entre oponentes com a mesma possibilidade de vitória. Se um dos jogadores domina a estratégia vencedora do jogo e a aplica, deixa de existir competição.

Nesse trabalho focaremos em mostrar a ideia de alguns jogos combinatórios e como suas formas de vencer se relacionam com a aritmética, mais precisamente com aritmética dos restos.

4.1 – Jogo de Kayles

Kayles é um jogo matemático de estratégia que pertence à categoria dos jogos de remoção de objetos, inventado por Henry Dudeney em 1908. É jogado por duas pessoas, e

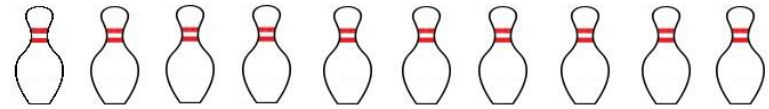
sua simplicidade nas regras esconde uma interessante estratégia a qual revelaremos a diante ([25]).

Dada uma fileira de pinos de boliche imaginários, os jogadores se revezam para derrubar um pino ou dois pinos adjacentes, até que todos os pinos desapareçam.

O jogo começa com um número de pinos (ou palitos) dispostos em uma linha reta. O número de pinos pode variar, mas para fins ilustrativos, podemos imaginar começando com 10 pinos e o objetivo é ser o jogador a remover o último pino ou par de pinos. O jogo termina quando todos os pinos são removidos e o jogador que remove o último pino ou conjunto de pinos ganha o jogo.

Existe uma estratégia simples que garante a vitória de quem inicia o jogo desde que no início tenhamos ao menos 3 pinos. Comece com uma remoção central que divida os pinos em duas filas com o mesmo número de pinos em cada. Isso pode ser feito não importa quantos pinos tenhamos no jogo. Sendo N a quantidade total de pinos, se N for par, remova os pinos $\frac{N}{2}$ e $\frac{N}{2}$ + 1. Dessa forma, restam $\frac{N}{2}$ – 1 pinos à esquerda e $\frac{N}{2}$ – 1 a direita. Se N for ímpar, remova o pino $\frac{N+1}{2}$. Assim, restam $\frac{N-1}{2}$ pinos de cada lado.

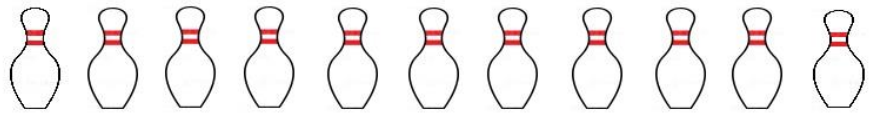
Por exemplo, se N = 10, remova os pinos 5 $\left(\frac{N}{2}\right)$ e 6 $\left(\frac{N+1}{2}\right)$.



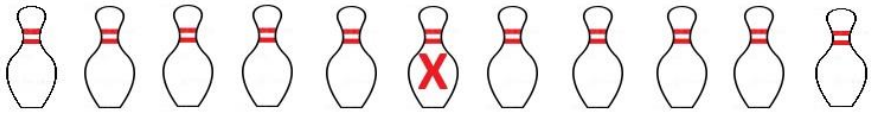
10 PINOS

Retirando os pinos 5 e 6 restam 4 $\left(\frac{N}{2} - 1\right)$.pinos de cada lado.

Se N = 11, remova o pino 6 $\left(\frac{N}{2} + 1\right)$.



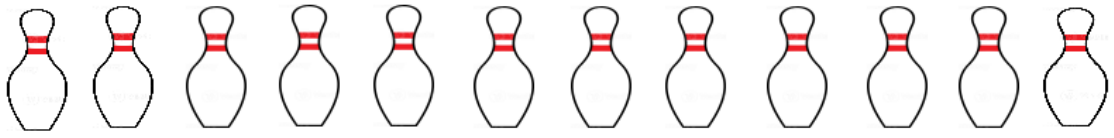
11 PINOS



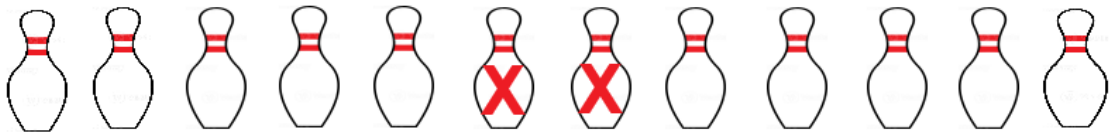
Retirando o pino 6 restam 5 $\left(\frac{N}{2}-1\right)$ pinos de cada lado.

Depois disso, é a vez do seu oponente jogar. Ele só poderá remover pinos de uma das filas formadas depois da primeira retirada. Depois da jogada dele, remova exatamente os mesmos pinos na outra fila. Dessa forma, sempre depois da sua jogada haverá exatamente a mesma quantidade de pinos em cada fila formada após a primeira retirada. Sendo assim, em alguns momentos, depois da sua jogada haverá um ou dois pinos (adjacentes) em cada fila. No caso de serem dois, seu adversário pode remover os dois e você ganha na sua próxima jogada. Se ele retirar apenas 1, você também retira apenas 1 e restam um pino de cada lado. Agora, ele só pode remover um (os dois pinos não são adjacentes) e na sua jogada você remove o último e vence.

Exemplo 4.1.1. Considere N = 12.



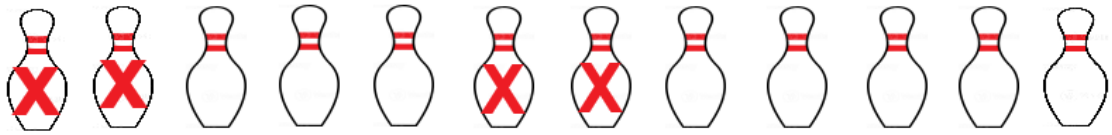
12 PINOS



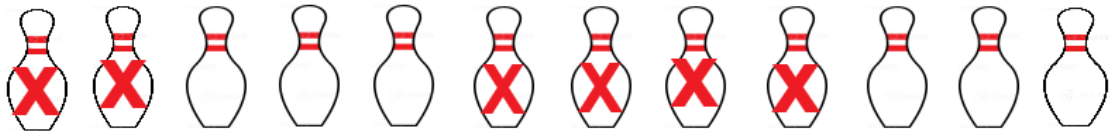
Jogada do jogador 1

De acordo com o que foi descrito acima como estratégia vencedora, com essa jogada o

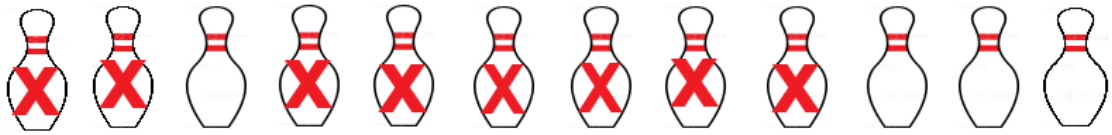
jogador 1 garantiu sua vitória dividindo a fila de pinos em duas filas de mesma quantidade. Agora, basta ele retirar a mesma quantidade de pinos que o jogador 2 tirar de uma fila na outra fila que foi formada.



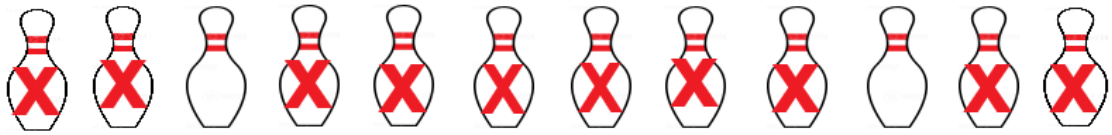
Jogada do jogador 2



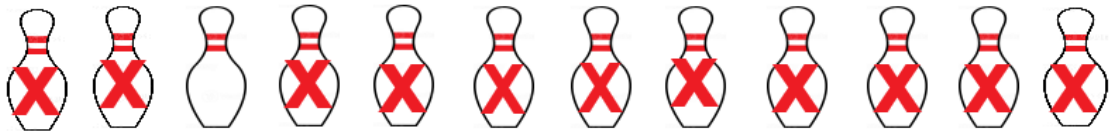
Jogada do jogador 1



Jogada do jogador 2



Jogada do jogador 1



Jogada do jogador 2

O jogador 1 retira o último pino e vence a partida.

4.2 – Jogo de Nim

O jogo do Nim é um clássico exemplo de jogo matemático de estratégia, amplamente estudado na teoria dos jogos. A beleza do Nim está em sua simplicidade e nas estratégias

matemáticas que podem ser aplicadas para garantir a vitória.

Segundo Almeida e Carvalho ([2]), Nim é um dos jogos mais antigos que se conhece. Existem relatos de que na China da Idade Média esse jogo já era jogado pelos soldados, porém, sua origem real ainda é desconhecida. Os primeiros relatos de trabalhos relacionados ao jogo Nim foram formalizados por Charles Leonard Bouton no início do século XX. Para Buton, Nim tem uma "teoria matemática extremamente simples e completa". Outra curiosidade, a qual foi observada pelos autores em [2], é que se percebe que a palavra nim espelhada forma a palavra "win", que em inglês significa ganhar.

Segundo Grando ([11]) o Jogo de Nim deve sua popularidade à investigação da estratégia que garante a um jogador sempre vencer, e por ser de fácil programação computacional.

O jogo começa com uma certa quantidade de objetos (pedras, palitos, etc). Os jogadores se alternam para realizar suas jogadas e em cada turno, um jogador pode escolher no mínimo um e no máximo uma quantidade já pré-estabelecida para remover dessa pilha. O jogo termina quando todos os objetos são removidos. Deve ser definido se o jogador que retira o último palito ganha ou perde o jogo.

No que segue, vamos apresentar as estratégias que garantem vitórias, as quais utilizam aritmética dos restos e divisão euclidiana ([11]).

Vamos denotar por N o número total de palitos e por n o número máximo de palitos a serem retirados por jogada.

4.2.1 - Caso 1: Quem tira o último palito perde.

Comecemos com um exemplo.

Exemplo 4.2.1.1. Considere N = 27 e n = 4.

Nesse exemplo, N = 27 e n+1 = 5, e o resto da divisão de 27 por 5 é 2, pois, 27 = 5.5+2.

A estratégia para vencer deve ser feita de forma que, depois de alguma jogada sua, reste apenas 1 palito. Podemos fazer a seguinte separação: 1 palito no início, 5 grupos de 5 palitos

e 1 palito no final.

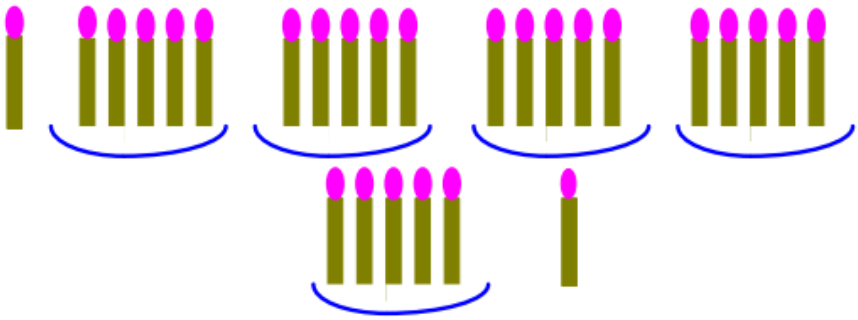


FIGURA 1 – Palitos divididos seguindo a estratégia vencedora

FONTE: Grando ([11])

Na sua primeira jogada, retire apenas o 1°palito. Como a cada jogada pode-se retirar no mínimo 1 e no máximo 4 palitos então não importa quantos palitos o seu adversário retira, você sempre pode completar 5 na sua vez. Com isso, na sua jogada você sempre completa a retirada de um dos 5 grupos de 5 palitos e, portanto, na sua sexta jogada você terá completado a retirada do último grupo de 5 palitos, deixando apenas 1 palito para seu adversário retirar e assim perder o jogo.

A estratégia vencedora está totalmente baseada no resto da divisão de N por $n+1$. O teorema da divisão de Euclides garante a existência de números naturais q (quociente) e r (resto) tais que $N = q.(n+1) + r$, sendo $0 \leq r \leq n$.

Vamos agora generalizar a estratégia vencedora, separando em 3 possibilidades:

- Vamos começar com o caso em que r >1.

Para esse caso, existe uma estratégia vencedora para quem joga primeiro (jogador 1). Como $r > 1$ e $N = q.(n+1) + r$, podemos escrever $N = r-1 + q.(n+1) + 1$. Note que $r - 1 > 0$ já que $r > 1$. Com isso, podemos dividir os N palitos em um grupo inicial com $r-1$ palitos depois q grupos com $n+1$ palitos e mais "um grupo" com apenas 1 palito. Essa é a situação do exemplo introdutório com $N = 27$ e $n = 4$. Vamos descrever a estratégia vista no exemplo agora no caso geral.

O jogador 1 retira $r-1$ palitos na sua primeira jogada (lembre-se que $0 < r-1 < n$, logo essa primeira jogada é possível). Com isso, o primeiro grupo de $r-1$ palitos já foi retirado. Em sua

primeira jogada, o jogador 2 retira k palitos. Como $1 \leq k \leq n$, temos que $1 \leq n+1 - k \leq n$, logo na próxima jogada, o jogador 1 tira $n+1-k$ palitos e assim o primeiro dos q grupos com $n+1$ foi retirado. O jogador 1 deverá seguir fazendo isso: na sua jogada ele retira $n+1-k$, onde k foi a quantidade retirada pelo jogador 2 na jogada anterior. Seguindo assim, sempre que o jogador 1 fizer sua jogada um dos q grupos de $n+1$ palitos será retirado. Na jogada de número $q+1$ do jogador 1 o último grupo de $n+1$ palitos será retirado, restando assim apenas 1 palito a ser retirado pelo jogador 2 o que dá a vitória ao jogador 1.

- Agora vamos tratar o caso r = 1.

Aqui, existe uma estratégia vencedora para o jogador 2. Temos $N = q.(n+1) + 1$ e a divisão dos N palitos já está feita: q grupos com $n+1$ palitos e "um grupo" de 1 palito. O jogador 1 já está em uma posição perdedora pois ao retirar k palitos na primeira jogada com $1 \leq k \leq n$ ele permite que o jogador 2 retire $n+1-k$ o que completa a retirada do primeiro grupo de $n+1$ palitos. Imagine o caso anterior ($r > 1$) sem os $r-1$ palitos do grupo inicial. O jogador 1 aqui passa para a situação do jogador 2 de lá. Assim, seguindo a mesma ideia, o jogador 2 (daqui) sempre completa $n+1$ palitos retirados junto com a jogada anterior do jogador 1. Depois da jogada de número q do jogador 2 restará 1 único palito a ser retirado pelo jogador 1 o que dá a vitória ao jogador 2.

Exemplo 4.2.1.2. Considere N = 13 e n = 2.
Nesse exemplo, N = 13 e n+1 = 3, logo o resto da divisão de 13 por 3 é 1, pois, 13 = 3.4+1. Aqui a estratégia vencedora deve ter seguinte separação: 4 grupos de 3 palitos e 1 palito no final.

Para o jogador 2 vencer, ele deve seguir a ideia da estratégia vencedora explicada anteriormente. A cada jogada ele retira uma quantidade de palitos que completa a retirada de um grupo de 3 palitos. Depois da sua 4ªjogada restará um palito.

- Finalmente, vamos ao caso r = 0.

Nesse último caso há uma estratégia vencedora para o jogador 1. Aqui temos $N = q.(n+1)$, ou seja, q grupos de $n+1$ palitos. O jogador 1 deve retirar n palitos em sua primeira jogada. Com isso, restarão $N-n$ palitos. É claro que se $N = n+1$, o jogador 1 já ganhou. Vamos considerar $N > n+1$ o que implica em $q > 1$.

Assim,

$$\begin{aligned} N-n &= q.(n+1) - n \\ &= qn + q - n = (q-1).n + q - n \\ &= (q-1).n + q - 1 + 1 - n = (q-1)(n+1) + 1, \end{aligned}$$

Ou seja, temos $N-n$ palitos e o resto da divisão de $N-n$ por $n+1$ é 1. Estamos no caso anterior ($r = 1$) e a estratégia de lá faz com que quem começa lá, ou seja, o segundo a jogar aqui, perca. Com isso o jogador 1 vence.

Exemplo 4.2.1.3. Considere N = 16 e n = 4.

Nesse exemplo, N = 16 e n+1 = 5, logo o resto da divisão de 16 por 4 é 0, pois, 16 = 4.4. Aqui a estratégia vencedora deve ter seguinte separação: 4 grupos de 4 palitos.

Para o jogador 1 vencer, ele deve seguir a ideia da estratégia vencedora explicada anteriormente. A cada jogada ele retira uma quantidade de palitos que completa a retirada de um grupo de 5 palitos. Depois de sua 5ª jogada restará apenas um palito.

4.2.2 - Caso 2: Quem tira o último palito ganha

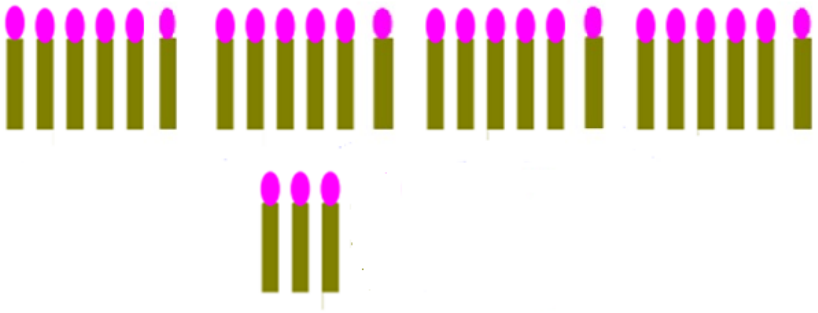
De forma análoga ao primeiro caso, temos uma quantidade N de palitos. Por regra já determinada, cada jogador na sua oportunidade, deve retirar pelo menos 1 palito e no máximo n palitos, com n > 1. Dessa vez, ganha o jogo o jogador que retirar o último palito.

Aqui, a estratégia também começa pelo conhecimento do resto e do quociente da divisão de N por $n+1$. Sejam q o quociente r e o resto dessa divisão, então, temos $N = q(n+1) + r$, com $0 \leq r \leq n$. Deve-se dividir mentalmente os palitos em q grupos de n+1 palitos mais um grupo de r palitos. Analisemos as duas situações para r.

- Vamos começar com o caso em que r ≥ 1.

Para esse caso existe uma estratégia vencedora para quem joga primeiro (jogador 1). Como r ≥ 1 e $N = q(n+1) + r$ podemos dividir os N palitos em um grupo inicial com r palitos e mais q grupos com n+1 palitos. A estratégia consiste no jogador 1 tirar os r palitos do primeiro grupo na 1ª jogada e depois de cada jogada do seu adversário retirando k palitos o jogador 1 retira n+1-k palitos e completa a retirada de um dos q grupos de n+1 palitos. Depois da q-ésima jogada do jogador 1 restarão exatamente n+1 palitos (último dos q grupos). Mais uma vez o jogador 2 faz sua retirada de k palitos deixando n+1-k palitos, e como $1 \leq n+1 - k \leq n$, o jogador pode retirar todos os palitos restantes e vencer o jogo.

Exemplo 4.2.2.1. Considere N = 27 e n = 5



Nesse exemplo queremos que no final do jogo não reste nenhum palito. Assim, temos que 27 = 4.6 + 3, assim, o jogador 1 terá que retirar inicialmente 3 palitos para vencer o jogo, nas próximas jogadas ele deve retirar a quantidade de palitos complementar a 6, de acordo com cada jogada do jogador 2. Logo, o jogador 1 vencerá seguindo essa estratégia.

- Agora, vamos tratar do caso r = 0.

Nesse caso, temos que N é múltiplo de $n+1$, ou seja, $N = q(n+1)$. Aqui já deve estar claro que a estratégia vencedora é para o jogador 2 e consiste em simplesmente a cada jogada

completar a retirada de um dos *q* grupos de *n+1* palitos.

Exemplo 4.2.2.2. Considere N = 16 e n = 3.

Nesse exemplo, também queremos que final do jogo não reste nenhum palito. Como temos que 16 = 4.4, logo, o jogador 1 iniciará retirando uma quantidade $1 \leq k \leq 3$ de palitos, e nas próximas jogadas o jogador 2 deve retirar a quantidade de palitos para completar 4 (quantidade de palitos que forma cada grupo), de acordo com cada jogada do jogador 1. Logo, o jogador 2 vencerá seguindo essa estratégia.

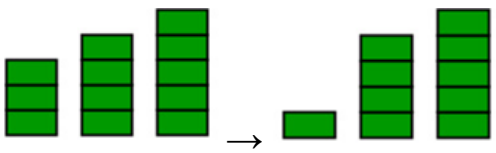
4.2.3 – Variação do Jogo de Nim: Grupos

Vamos agora analisar uma variação do jogo de Nim. Colocamos sobre uma mesa uma quantidade N de palitos separados em m grupos. Por regra, cada jogador na sua oportunidade, deve retirar uma quantidade qualquer de palitos de apenas um dos grupos. Alternadamente, os jogadores vão retirando os palitos e ganha o jogo o jogador que retirar o último palito.

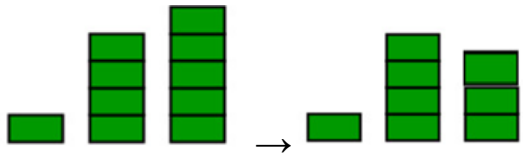
Exemplo 4.2.3.1. Vamos fazer um exemplo utilizando N = 12 separados em 3 grupos com 3, 4 e 5 palitos, respectivamente.

Vamos representar a quantidade de palitos em cada grupo por um tripla ordenada. No início do jogo a situação é (3, 4, 5).

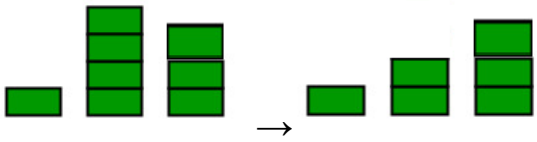
Na primeira jogada o jogador 1 tira dois palitos do primeiro grupo alterando o jogo da situação (3, 4, 5) para (1, 4, 5).



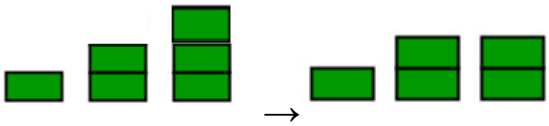
Na segunda jogada o jogador 2 tira dois palitos do terceiro grupo alterando o jogo da situação (1, 4, 5) para (1, 4, 3).



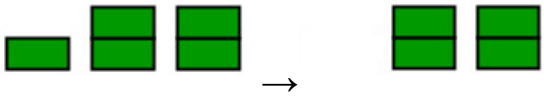
Na terceira jogada o jogador 1 retira dois palitos do segundo grupo, alterando o jogo da situação (1, 4, 3) para (1, 2, 3).



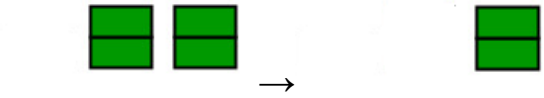
Na quarta jogada, o jogador 2 retira um palito do terceiro grupo, alterando o jogo da situação (1, 2, 3) para (1, 2, 2).



Na quinta jogada, o jogador 1 retira um palito do primeiro grupo, alterando o jogo da situação (1, 2, 2) para (0, 2, 2).



Assim, agora o jogador 2 retira dois palitos do segundo grupo, alterando o jogo da situação (0, 2, 2) para (0, 0, 2).



Logo, o jogador 1 retira os dois últimos palitos do terceiro grupo, tornando- se assim vencedor do jogo.

Vamos agora apresentar a estratégia vencedora no caso do jogo com apenas dois grupos.

Nesse caso, qualquer situação do tipo (0, x) ou (x, 0) faz com que o próximo a jogar

vença, pois ele pode remover todos os x palitos do segundo grupo.

Se em alguns momentos do jogo tivermos a mesma quantidade de palitos nos dois grupos, o próximo a jogar será o perdedor. Vamos chamá-lo de jogador A. A estratégia é a mesma do jogo Kayles: a cada jogada do jogador A basta o outro jogador (vamos chamá-lo de jogador B) retirar a mesma quantidade de palitos no outro grupo. Em algum momento o jogador A terá que "zerar" a quantidade de palitos em um grupo, chegando em uma situação (0, k) ou (k, 0), com $k > 0$, e então basta o jogador B tirar os k palitos e vencer.

Sendo assim, vamos separar a estratégia em dois casos:

- No primeiro caso o jogo inicia com dois grupos com o mesmo número de palitos, digamos x. Assim, a situação inicial é exatamente a descrita acima, logo a estratégia descrita acima garante a vitória do segundo a jogar.
- No caso de grupos com quantidades diferentes de palitos, digamos x e y, com x > y, basta o primeiro jogador retirar x-y palitos do grupo com x palitos, chegando a situação (y, y) e com a estratégia acima fica garantida a vitória do 1°jogador.

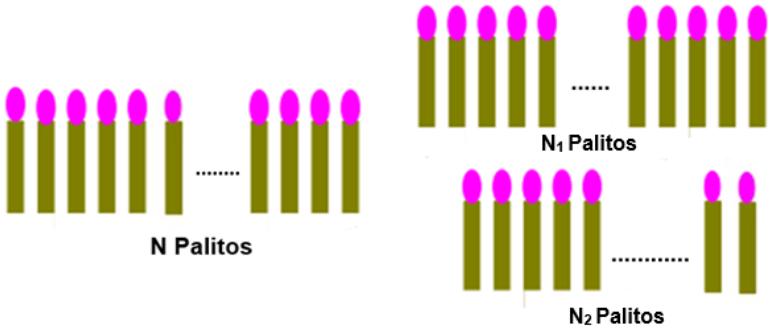
Exemplo 4.2.3.2. Considere N = 10, x = 6 e y = 4.

Nesse exemplo, temos 2 grupos um com 6 palitos e o outro com 4 palitos, e queremos que final do jogo não reste nenhum palito. Assim, seguindo a estratégia descrita acima, o jogador 1 terá que retirar inicialmente 6 – 4, ou seja, 2 palitos do grupo com 6 para vencer o jogo, em nas próximas jogadas ele deve retirar a quantidade de palitos igual a que o jogador 2 retirar só que no outro grupo de palitos. Portanto, o jogador 1 vencerá seguindo essa estratégia.

No caso de três ou mais grupos de palitos, para determinar a estratégia vencedora é bem mais complexo. Para um estudo desse caso recomendamos a leitura de ([1]).

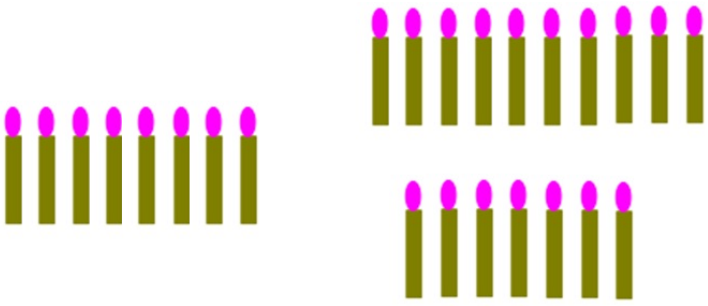
4.2.4 – Nim Bifurcado

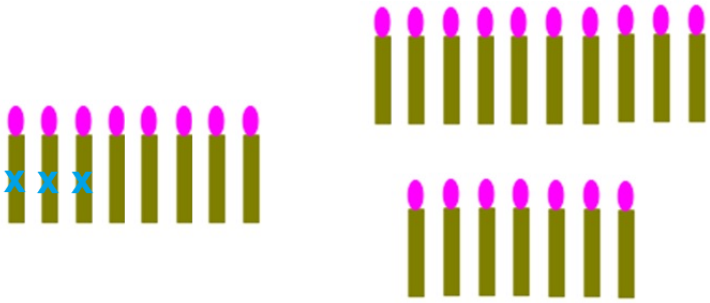
Aqui vamos introduzir uma variação do jogo de Nim que batizamos de "Nim bifurcado". Para quem já viu o jogo de Nim clássico a ideia é bastante simples:
Temos N palitos formando uma fila a qual se bifurca formando outras duas filas, uma com N_1 e a outra com N_2 palitos, sendo $N_1 \neq N_2$.



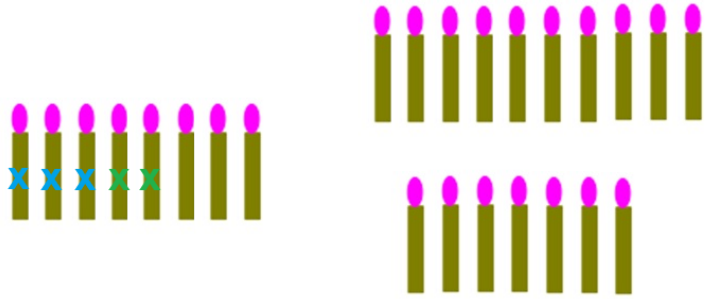
Novamente, a cada jogada um dos dois jogadores deve tirar entre 1 e n palitos, sendo o número n fixado no início do jogo. Aqui os palitos devem ser retirados em ordem e da esquerda para a direita. Ao chegar no último palito da primeira fila de N palitos o jogador deve escolher se prossegue pela fila com N_1 ou pela fila com N_2. Uma vez escolhida a fila, o jogo continua por ela sem possibilidade de mudar para a outra. No início do jogo deve ser estabelecido se quem tira o último palito ganha ou perde.

Exemplo 4.2.4.1. N = 8, N_1 = 10, N_2 = 7, n = 3 e quem tirar o último vence.

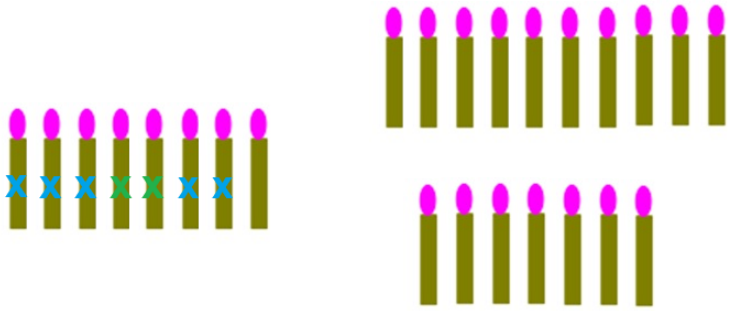




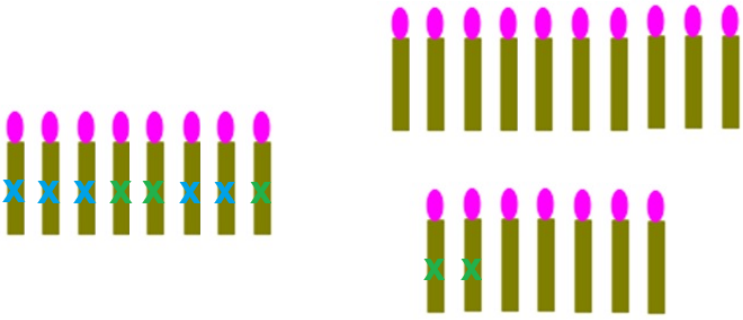
Jogada do Jogador 1



Jogada do jogador 2

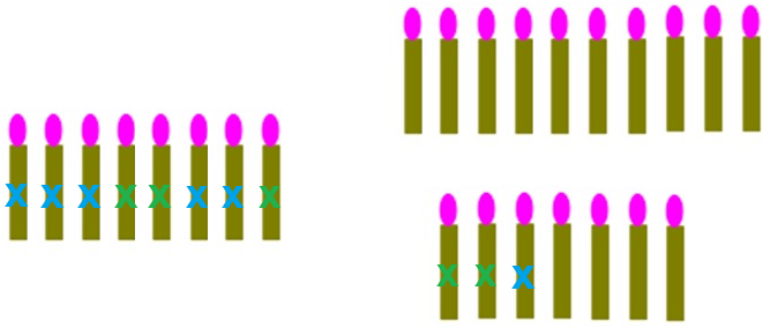


Jogada do jogador 1



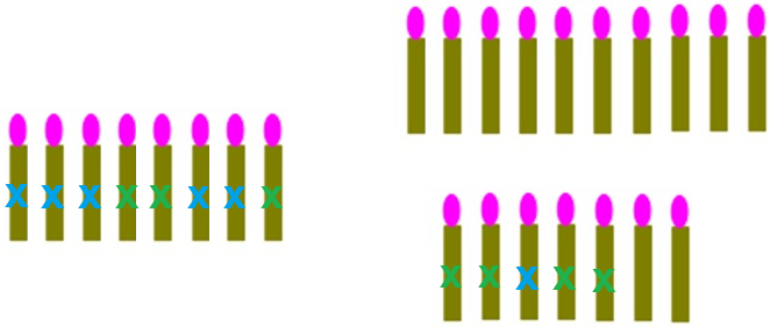
Jogada do jogador 2

Nessa última jogada o jogador 2 resolveu tirar 3 palitos e como chegou ao final da 1ªfila teve que optar por uma das duas filas para seguir.

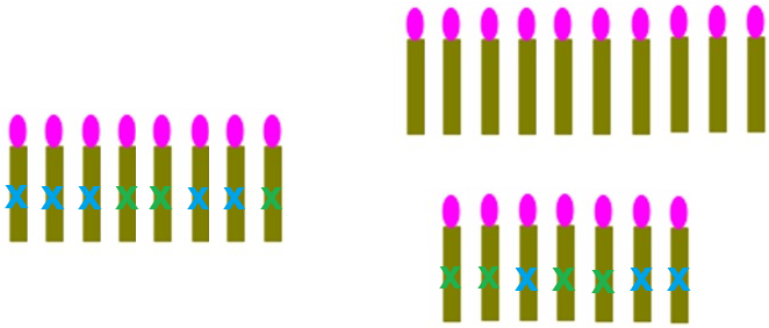


Jogada do jogador 1

Aqui o jogador 1 tirou um palito, deixando 4 e com isso garantiu a sua vitória.



Jogada do jogador 2



Jogada do jogador 1

Fim de jogo.

As várias possibilidades para N, N_1 *e* N_2 *e* n nos mostram que não existe uma estratégia vencedora para todos os casos. No exemplo acima, N deixa resto maior ou igual a 1 na divisão por $n+1$ (8 = 2.3 + 2). Nesse caso, existe uma estratégia que permite ao jogador 1 tirar o último palito da primeira fila. Daí o jogador 2 deverá escolher por qual das duas filas o jogo vai seguir e começar sua retirada. Assim, estamos em um jogo de Nim clássico com N_1 ou N_2 palitos e o jogador 2 nesse novo jogo é o primeiro a jogar.

Se quisermos uma estratégia vencedora para um jogador específico, não podemos

contar com a garantia de que o seu adversário irá retirar o último palito da primeira fila, pois não há como garantir isso (a menos que n = 1, mas esse é o caso mais desinteressante do jogo de Nim). Para termos algum controle, devemos garantir que o jogador para o qual estamos desenvolvendo a estratégia vencedora retire o último palito da primeira fila.

Vamos começar considerando que quem retira o último palito perde o jogo.

- Jogador 1 ganha.

Aqui, o resto da divisão de N por $n+1$ deve ser $r \geq 1$ e o resto da divisão tanto de N_1, como de N_2 por $n+1$ deve ser 1. Já vimos uma estratégia que garante que o jogador 1 retira o último palito da 1ªfila. Assim, o jogador 2 irá "começar um novo jogo Nim" com N_1 ou N_2 palitos e nesse caso já temos uma estratégia vencedora para o segundo a jogar, que seria o jogador 1.

Exemplo 4.2.4.2. Considere N = 13, N_1 = 11, N_2 = 6, n = 4 e quem tirar o último perde.
Nessa configuração inicial do jogo e pela estratégias descritas acima, o jogador 1 conseguirá retirar o último palito da 1ªfila e assim o jogador 2 irá iniciar a retirada da próxima fila. O jogador 2 retirará o último palito dando a vitória ao jogador 1.

- Jogador 2 ganha.

O resto da divisão de N por $n+1$ deve ser 0 e usamos a estratégia que garante ao jogador 2 retirar o último palito da 1ªfila. Depois, N_1 e N_2 devem novamente deixar ambos resto 1 na divisão por $n+1$. Com isso basta seguir exatamente a mesma estratégia do caso anterior.

Exemplo 4.2.4.3. Considere N = 8, N_1 = 13, N_2 = 5, n = 3 e quem tirar o último perde.
Nessa configuração inicial do jogo e pela estratégias descritas acima, o jogador 2 conseguirá retirar o último palito da 1ªfila e assim o jogador 1 irá iniciar a retirada da próxima fila. Seguindo a mesma estratégia do exemplo anterior, o jogador 1 retirará o último palito dando a vitória ao jogador 2.

Agora, vamos considerar que quem tirar o último palito vence. Seremos breves apenas

indicando como devem ser N, N_1 *e* N_2.

- Jogador 1 ganha.

O resto de N por $n+1$ deve ser $r \geq 1$ *e* N_1 *e* N_2 devem ser múltiplos de $n+1$.

Exemplo 4.2.4.4. N = 10, N_1 = 12, N_2 = 8, n = 3

- Jogador 2 ganha.

Aqui N, N_1 *e* N_2 devem ser todos múltiplos de $n+1$

Exemplo 4.2.4.5. N = 15, N_1 = 10, N_2 = 5, n = 4

As estratégias acima deixam as coisas muito amarradas. Devemos escolher N, N_1, N_2, n quem começa e se quem tira o último ganha ou perde. A seguir vamos ver uma situação em que precisamos escolher apenas um dos números N_1 ou N_2 para termos uma estratégia vencedora para o jogador 2 (quem tira o último palito vence). O resto da divisão de N por $n+1$ deve ser n, ou seja, $N = q.(n+1) + n$ e o resto da divisão de pelo menos um dos números N_1 ou N_2 por $n+1$ deve ser 1. A cada jogada do jogador 2 ele deve completar a retirada de um grupo de $n+1$ palitos. Assim, depois de sua q-ésima jogada restarão exatamente n palitos da mesma fila. O jogador 1 então retira k palitos com $1 \leq k \leq n$. Depois, o jogador 2 retira $n-k+1$ palitos. Com isso, ele retira o último palito da 1ª fila, caso ainda haja algum palito aí, e o mais importante, ele tira mais 1 palito da fila cuja quantidade de palitos deixa resto 1 na divisão por $n+1$. Digamos que essa quantidade é N' ($N' = N_1$ *ou* $N' = N_2$). Assim, o jogo seguirá por essa fila ainda tendo q' grupos de $n+1$ palitos ($N= q'(n+1)+1$) e será a vez do jogador 2 seguir a já conhecida estratégia de completar sempre a retirada de um grupo de $n+1$ palitos na sua vez. Isso lhe garante a retirada do último palito e a vitória.

Se quem tira o último palito perde, então basta que N seja como acima e um dos números N_1 ou N_2 deixe resto 2 na divisão por $n+1$ e basta seguir exatamente a mesma estratégia do caso anterior.

Exemplo 4.2.4.6. N = 15, N_1 = 9, N_2 = k (tanto faz), n = 3 e quem tirar o último vence.

Nessa configuração, e seguindo a estratégia descrita acima, o jogador 1 iniciará retirando k palitos do primeiro grupo, e assim basta o segundo jogador retirar 4-k palitos que ao final restará 3 palitos a serem retirados pelo jogador 2. Agora, o jogador irá retirando palitos da próxima fila escolhida e o jogador 2 vai retirando uma quantidade complementar como foi descrita na estratégia. Assim, o jogador 2 irá retirar o último palito e vencer o jogo.
Se fosse combinado que quem tirasse o último palito perdesse o jogo, bastava tomar uma configuração com N_1 = 10 e seguir a mesma estratégia para vencer.

4.3 – Jogo dos Restos

O Jogo dos Restos consiste em tentar descobrir um número dentro de um intervalo (neste caso, de 1 a 100) conhecendo apenas o resto das divisões desse número por números entre 1 e 10. Esse jogo está intimamente relacionado ao conceito de congruência da teoria dos números. “O computador pensará em um número entre 1 e 100. Você consegue descobrir qual é? Escolha um divisor e o computador lhe dará algumas informações sobre o número. Quanto menos divisões você precisar, mais pontos você ganha.” ([24])

Inicialmente, tem-se um número N no intervalo de 1 a 100 e para tentar descobrir esse número, o jogador recebe o resto da divisão de N por diferentes números de 1 a 10, os quais são escolhidos pelo jogador. O objetivo é descobrir N com o menor número possível de informações (sobre os restos).

Vamos mostrar que com duas ou três informações é possível descobrir N. Deve ser claro para todos que com uma única informação não é possível descobrir N.

Em seu primeiro movimento, o jogador deve pedir o resto da divisão de N por 10. Isso restringe bastante as possibilidades, sobrando exatamente dez números. Por exemplo, se o resto da divisão por 10, $r_{10} = 3$, então $N \in \{3, 13, 23, 33, 43, 53, 63, 73, 83, 93\}$. De modo geral, vamos denotar o resto e o quociente da divisão de N por k como r_k e q_k respectivamente. Assim, temos $N = 10q_{10} + r_{10}$.

O próximo movimento é pedir o resto da divisão de N por 9. Com isso, temos:

$$N = 10q_9 + r_9.$$

O resto da divisão de $N = 10q_{10} + r_{10}$ por 9 é igual ao resto da divisão de $q_{10} + r_{10}$ por 9. De fato,

$10q_{10} + r_{10} = 9q_9 + r_9$

$9q_{10} + q_{10} + r_{10} = 9q_9 + r_9$

$q_{10} + r_{10} = 9\,(q_9 - q_{10}) + r_9$

Note que, se $q_9 < q_{10}$ então $q_9 - q_{10} < -1$, logo $9(q_9 - q_{10}) < -9 \Rightarrow 9(q_9 - q_{10}) + r_9 < 0$, já que $r_9 \leq 8$ e assim teríamos $q_{10} + r_{10} < 0$, um absurdo!

Assim, $k = q_9 - q_{10} \geq 0$, logo $q_{10} + r_{10} = 9k + r_9$ e r_9 também é o resto da divisão de $q_{10} + r_{10}$ por 9, como queríamos demonstrar.

Vamos analisar as possibilidades.

- Se $r_{10} = 0$, então temos 10 possibilidades: 10, 20, ..., 90, 100, ou seja, $N = 10q_{10,}$ com $1 \leq q \leq 10$ e os restos das divisões desses números por 9 são: 1, 2, 3, ..., 7, 8, 0, 1, respectivamente. Se $r_9 \neq 1$, então $N = 10r_{9.}$ Se $r_9 = 1$, então $N = 10$ ou $N = 100$. Nesse caso, precisamos de mais uma informação: o resto da divisão por 8. Se $r_8 = 2$, então $N = 10$ e se $r_8 = 4$, então $N = 100$.
- Se $r_{10} > 0$, então $1 \leq r_{10} \leq 9$ e assim teremos também 10 possibilidades: $r_{10,}$ $10 + r_{10}$, $20 + r_{10}$, ..., $90 + r_{10.}$

  Se $r_9 = r_{10}$, então

  $N = 10q_{10} + r_{10} = 9q_9 + r_9$

  $\Rightarrow 10q_{10} = 9q_9$

  $\Rightarrow 9q_{10} + q_{10} = 9q_9$

  $\Rightarrow q_{10} = 9\,(q_9 - q_{10})$

  $\Rightarrow q_9 \geq q_{10,}$

  já que $q_{10} \geq 0$, e assim q_{10} é múltiplo de 9. Como $1 \leq N \leq 100$, então $q_{10} = 0$ ou $q_{10} = 9$. Desse modo, $N = r_{10}$ (caso $q_{10} = 0$) ou $N = 90 + r_{10}$ (caso $q_{10} = 9$). Como q_{10} é desconhecido, precisamos de mais uma informação, o resto da divisão por 8, por exemplo:

r_{10}	r_8	$90 + r_{10}$	r_8
1	1	91	3
2	2	92	4
3	3	93	5
4	4	94	6
5	5	94	7
6	6	96	0
7	7	97	1
8	0	98	2
9	1	99	3

Por sabermos o r_{10}, sabemos em qual linha da tabela acima estamos e como r_{10} e $90 + r_{10}$ tem restos diferentes na divisão por 8, essa nova informação (r_8) é suficiente para descobrir o N.

- Agora, vamos considerar o caso de $r_{10} \neq r_9$. Aqui, devemos ter o $10 \leq N \leq 90$. Como também estamos no caso $r_{10} > 0$, então $N \neq 10q$ para qualquer q, logo $N = 10q_{10} + r_{10}$ com $1 \leq q_{10} \leq 8$ e $1 \leq r_{10} \leq 9$.

  Se descobrirmos q_{10}, temos N. Pela observação acima, basta testar qual dos números $k + r_{10}$ com $1 \leq k \leq 8$ deixa resto r_9 na divisão por 9. Como temos 8 números consecutivos para testar e 9 possíveis restos, não há repetição, assim vamos encontrar um único valor para q_{10} e teremos $N = 10q_{10} + r_{10}$.

Exemplo 4.3.1. Descobrir N, tal que $r_{10} = 2$ e $r_9 = 2$.

Temos que $r_{10} > 0$ e $r_{10} = r_9$, então N = 2 ou N = 92. Nesse caso, precisamos dividir N por 8. Se $r_8 = 2$ então N = 2, e se $r_8 = 4$ então N = 92.

Exemplo 4.3.2. Descobrir N, tal que $r_{10} = 3$ e $r_9 = 3$.

r_{10}	r_9	r_{10} ou 90 + r_{10}	r_8	N
3	3	3	3	3
3	3	93	5	93

Novamente, temos que $r_{10} > 0$ *e* $r_{10} = r_9$, então N = 3 ou N = 93. Nesse caso, precisamos dividir N por 8. Se $r_8 = 3$ então N = 3, e se $r_8 = 5$ então N = 93.

Exemplo 4.3.3. Descobrir N, tal que $r_{10} = 2$ e $r_9 = 1$.

Temos que $r_{10} > 0$ *e* $r_{10} \neq r_9$, logo $N = 10q_{10} + r_{10}$ com $1 \leq q_{10} \leq 8$ e $1 \leq r_{10} \leq 9$. Vamos observar qual dos números $k + r_{10} = k + 2$, com $1 \leq k \leq 8$ e deixa resto 1 na divisão por 9.

k	k + 2	r_9
1	3	3
2	4	4
3	5	5
4	6	6
5	7	7
6	8	8
7	9	0
8	10	1

Logo, temos que $q_{10} = 8$, assim $N = 10.8 + 2 = 82$.

O leitor mais experiente deve perceber que conhecendo r_{10}, r_8 e r_9 temos $N \equiv r_{10} \pmod{10}$, $N \equiv r_9 \pmod{9}$ e $N \equiv r_8 \pmod{8}$, ou seja, um sistema de congruências e o estudo das soluções desse tipo de sistema pode ser feito por meio do Teorema chinês dos restos ([13]), o qual não é visto na educação básica e por isso optamos por não fazê-lo aqui.

Capítulo 5

Considerações Finais

O presente trabalho explorou o tema da Aritmética dos Restos, com foco no desenvolvimento e análise de aplicações dessa área no cotidiano e jogos para o ensino. A pesquisa teve como objetivo evidenciar como conceitos abstratos da Teoria dos Números podem ser exibidos de maneira lúdica e interativa, promovendo a compreensão dos educandos e um ambiente mais engajador.

Ao longo do estudo, foi possível notar que a aplicação dos jogos que foram citados como Kayles, Jogo dos Restos, Nim, que são baseados no conceito de Aritmética dos Restos, oferece uma ferramenta poderosa para o ensino, principalmente no ensino básico. Esses materiais permitem que os educandos desenvolvam habilidades importantes como resolução de problemas, raciocínio lógico e trabalho colaborativo, além de ajudar na assimilação de conteúdos que são considerados difíceis.

Ao desenvolver uma nova variação do jogo Nim, o Nim Bifurcado, observamos que é possível trazer uma nova metodologia e nova experiência para o ensino da aritmética criando mais um espaço onde a matemática é vista como uma atividade prazerosa e desafiadora, buscando sempre tornar a base teórica mais sólida para o desenvolvimento do pensamento matemático.

Portanto, vemos que a aritmética dos restos, através das aplicações que podemos observar na sociedade e através de jogos educativos, pode ser integrada ao currículo escolar de forma eficiente, servindo como uma ferramenta de apoio aos docentes e potencializando a aprendizagem dos alunos nessa área tão importante. Além disso, este trabalho abre caminho para futuras pesquisas visando investigar o impacto dos jogos abordados quando trabalhados em sala.

Referências

[1] ALI, Alonso. Jogos combinatórios imparciais. **Resumo UNICAMP**, Universidade Estadual de Campinas - UNICAMP, p. 1-4, 29 jun. 2018. Disponível em: https://ic.unicamp.br/~rafael/cursos/1s2018/mc758/resumos/resumo_alonso.pdf. Acesso em: 7 ago. 2024.

[2] ALMEIDA, B. I; CARVALHO, R. B. de. **A MATEMÁTICA DO JOGO DE NIM EM UMA ABORDAGEM INVESTIAGTIVA.** 2016. 79 f. Monografia (Licenciatura em Matemática)- Licenciatura em Matemática, Instituto Federal de Educação, Ciência e Tecnologia Fluminense. Campos dos Goytacazes, RJ, 2016.

[3] BANCO CENTRAL (Brasil). Caixa Econômica Federal. **CPF: CADASTRO DE PESSOAS FÍSICAS.** *In*: CPF - Cadastro de Pessoas Físicas. [*S. l.*], 2024. Disponível em: https://www.caixa.gov.br/servicos/cpf/Paginas/default.aspx. Acesso em: 25 jul. 2024.

[4] COUTINHO, Severino Collier. **CRIPTOGRAFIA,** Rio de Janeiro: Ed OBMEP, 2009.

[5] DUDZIAK, Elisabeth Adriana. **O QUE É ISBN E COMO OBTER?** Notícias, 27 Jul. 2021. Disponível em: https://www.abcd.usp.br/noticias/o-que-e-isbn-e-como-obter/ Acesso em: 18/03/2024

[6] ESQUINCA, Josiane. **ARITMÉTICA: CÓDIGOS DE BARRAS E OUTRAS APLICAÇÕES DE CONGRUÊNCIAS.** 2013. Dissertação (Mestrado) - Universidade Federal do Mato Grosso do Sul - UFMS, Mato Grosso do Sul, 2013.

[7] EVES, Howard. **INTRODUÇÃO A HISTÓRIA DA MATEMÁTICA**. 5. ed. Universidade Estadual de Campinas - UNICAMP: UNICAMP, 2011.

[8] FRAZ, Joeanne Neves. **MIL E UMA CENAS DO PROCESSO DE ENSINO E APRENDIZAGEM DA MATEMÁTICA NA MODALIDADE A DISTÂNCIA:**: REPRESENTAÇÕES SOCIAIS DE PROFESSORES DE MATEMÁTICA ENVOLVIDOS NA TRAMA DA FORMAÇÃO INICIAL. 2022. Tese (Doutorado - PPGE) - Universidade de Brasília - UnB, Brasília, 2022.

[9] GUIMARÃES, Fabiane. **O SENTIDO DO ZERO**. 112f. Dissertação de Mestrado em Educação Matemática. São Paulo: Pontifícia Universidade Católica de São Paulo – PUCSP, 2008.

[10] GOMES, Ygor Franzotti. **UMA PROPOSTA DE SEQUÊNCIA DIDÁTICA PARA JOGOS COMBINATÓRIOS**. 2015. Dissertação (Mestrado - PROFMAT) - Universidade Federal do Espirito Santo - UFES, [*S. l.*], 2015.

[11] GRANDO, Regina Célia. **O CONHECIMENTO MATEMÁTICO E O USO DE JOGOS NA SALA DE AULA.** 2000. Tese (doutorado) - Faculdade de Educação, Universidade Estadual de Campinas, Campinas, SP, 2000.

[12] HEFEZ, Abramo. **INICIAÇÃO A ARITMÉTICA** / Abramo Hefez. – Rio de Janeiro, RJ : IMPA/OBMEP, 2015.

[13] HEFEZ, Abramo. **ELEMENTOS DE ARITMÉTICA**. Textos Universítários. – Rio de Janeiro, RJ : Sociedade Brasileira de Matemática, 2005.

[14] KISHIMOTO, Tizuko Morchida. **JOGO, BRINQUEDO, BRINCADEIRA E A EDUCAÇÃO**. São Paulo: Editora cortez,1998.

[15] LEOPOLD, Guilherme Liegel – **CONGRUÊNCIA E APLICAÇÕES**. Dissertação (Mestrado em Profissional em Matemática em Rede Nacional) - Universidade Estadual de

Maringá, 2015.

[16] MAIA, Beatriz Maria. **O ENSINO DE POLÍGONOS DE BRAHMAGUPTA COM O AMPARO DO SOFTWARE GEOGEBRA**: UM CONTRIBUTO DA ENGENHARIA DIDÁTICA. 2021. Dissertação (Mestrado) - Universidade Federal do Ceará, Ceará, 2021.

[17]MOURA, M.O. de. **A CONSTRUÇÃO DO SIGNO NUMÉRICO EM SITUAÇÃO D ENSINO**. São Paulo:USP,1996.

[18]MOTA, Paula Cristina. **JOGOS NO ENSINO DA MATEMÁTICA**. 2009. Dissertação (Mestrado) - Universidade Portucalense Infante D. Henrique, Porto, 2009. Disponível em: https://repositorio.upt.pt/server/api/core/bitstreams/057680be-390d-4dd2-b379-876c72d57117/content. Acesso em: 12 ago. 2024.

[19]OLIVEIRA, Maykon. **ARITMÉTICA: CRIPTOGRAFIA E OUTRAS APLICAÇÕES DE CONGRUÊNCIA**. 2013. Dissertação (Mestrado) - Universidade Federal do Mato Grosso do Sul - UFMS, [*S. l.*], 2013.

[20] RIZZI, Leonor, HAYDT, Regina Célia C. **ATIVIDADES LÚDICAS NA EDUCAÇÃO DA CRIANÇA**. São Paulo: Editora ética, 2001.

[21]SÁ, I.P. **ARITMÉTICA MODULAR E ALGUMAS DE SUAS APLICAÇÕES**. Minicurso. IX ENEM (Encontro Nacional de Educação Matemática). 18 a 21 de julho de 2007. (Disponível em : (99+) ARITMÉTICA MODULAR E ALGUMAS DE SUAS APLICAÇÕES | Valentim Júnior - Academia.edu)

[22] SANTOS, José Plínio. **INTRODUÇÃO A TEORIA DOS NÚMEROS** – Rio de Janeiro, RJ : IMPA, 2009.

[23]SERVICOOP (Brasil). **UMA BREVE HISTÓRIA SOBRE A CRIAÇÃO DOS CARTÕES DE CRÉDITO**. [*S. l.*], 17 maio 2018. Disponível em: https://servicoop.com.br/uma-breve-historia-sobre-a-criacao-dos-cartoes-de-credito/. Acesso em: 9 abr. 2024.

[24] UNIVERSIDADE DE CAMBRIDGE (Reino Unido). The Remainders Game. *In*: **THE REMAINDERS GAME.** Reino Unido: Projeto NRICH, 2024. Disponível em: https://nrich.maths.org/6402. Acesso em: 7 ago. 2024.

[25] WIKIPEDIA. *In*: **JOGO DE KAYLES**. [*S. l.*], 6 abr. 2024. Disponível em: https://en.wikipedia.org/wiki/Kayles. Acesso em: 19 jun. 2024.