Universidade Regional do Cariri - URCA

UNIVERSIDADE REGIONAL DO CARIRI - URCA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

PROFMAT

PABLO YAGO DE OLIVEIRA PEREIRA

CHRYZODES E SUA CONEXÃO COM CURVAS EPICICLOIDAIS: uma abordagem teórica e uma experiência didática com *gallery walk*

(Juazeiro do Norte-CE)

2026

PABLO YAGO DE OLIVEIRA PEREIRA

CHRYZODES E SUA CONEXÃO COM CURVAS EPICICLOIDAIS: uma abordagem teórica e uma experiência didática com *gallery walk*

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Regional do Cariri como requisito parcial para a obtenção do título de Mestre - Área de Concentração: Matemática na Educação Básica.
Orientador: Prof. Dr. Flávio França Cruz.

(Juazeiro do Norte-CE)

2026

Ficha Catalográfica elaborada pelo autor através do sistema
de geração automático da Biblioteca Central da Universidade Regional do Cariri - URCA

Pereira, Pablo Yago De Oliveira

P436c CHRYZODES E SUA CONEXÃO COM CURVAS EPICICLOIDAIS uma abordagem teórica e uma experiência didática com gallery walk / Pablo Yago De Oliveira Pereira. Juazeiro do Norte -CE , 2026.

122p. il.

Dissertação. Mestrado Profissional em Matemática em Rede Nacional da Universidade Regional do Cariri - URCA.

Orientador(a): Prof. Dr. Flávio França Cruz

1.Chryzodes, 2.Curvas epicicloidais , 3.Sequência Didática , 4.Criação de mandalas; I.Título.

CDD: 510

PABLO YAGO DE OLIVEIRA PEREIRA

CHRYZODES E SUA CONEXÃO COM CURVAS EPICICLOIDAIS: uma abordagem teórica e uma experiência didática com *gallery walk*

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Centro de Ciências e Tecnologia da Universidade Regional do Cariri, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Aprovada em: 11 05 2026

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br FLAVIO FRANCA CRUZ
Data: 27/05/2026 19:55:42-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Flavio França Cruz – Orientador (URCA)

Documento assinado digitalmente
gov.br JOYCE SARAIVA SINDEAUX
Data: 25/05/2026 11:18:08-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Joyce Saraiva Sindeaux (URCA)

Documento assinado digitalmente
gov.br DANILO FERREIRA DA SILVA
Data: 25/05/2026 20:58:59-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Danilo Ferreira da Silva (URCA)

Documento assinado digitalmente
gov.br FRANCISCO PEREIRA CHAVES
Data: 26/05/2026 12:45:14-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Francisco Pereira Chaves (UFCA)

Dedico este trabalho à minha filha Merlyn, que já guia meus passos antes de dar os seus.

AGRADECIMENTOS

Ao meu orientador, Professor Doutor Flávio França Cruz, dedico meu primeiro agradecimento. Suas críticas construtivas e seu rigor acadêmico foram de extrema importância para este trabalho.

Agradeço a todos os professores que passaram pela minha vida até aqui, pois todos contribuíram para minha formação, com seus conhecimentos e ensinamentos.

Agradeço especialmente aos docentes do Programa PROFMAT da Universidade Regional do Cariri, cujas aulas e conversas extrapolaram o conteúdo formal, moldando meu pensamento crítico e minha visão.

Aos colegas que se tornaram companheiros de viagem. Nos seminários, nos grupos de estudo e nos intervalos, construímos juntos um espaço de aprendizado mútuo que foi essencial.

"O universo não é como uma tragédia de Shakespeare, onde você pode ser ou não ser. Aqui, você é e não é assim como todo resto".

(Baka Gaijin)

RESUMO

Esta dissertação investiga os padrões geométricos conhecidos como chryzodes, explorando sua fundamentação geométrica, suas propriedades matemáticas e suas potencialidades como ferramenta de ensino. O estudo centra-se em três eixos principais. Primeiramente, analisa-se a natureza epicicloidal dos chryzodes. Em segundo lugar, estabelece-se uma ponte formal entre a noção de chryzode e a teoria dos grafos. Demonstra-se que os chryzodes, sob certas condições, podem ser representados como ciclos hamiltonianos. Essa modelagem permite reinterpretar propriedades geométricas das curvas (como simetria e periodicidade) em termos gráficos, oferecendo uma perspectiva combinatória para um objeto tradicionalmente analisado pela geometria dinâmica. Por fim, o cerne aplicado do trabalho reside na aplicação e avaliação de uma sequência didática inovadora. Destinada prioritariamente a estudantes do 9º ano, embora adaptável a outras turmas, a sequência visa facilitar a compreensão integrada de conceitos de curvas paramétricas, divisão euclidiana e noções introdutórias de teoria dos grafos. Ela é composta por atividades que vão da construção manual de chryzodes à criação de mandalas com a técnica artística do string art. Os resultados da aplicação indicam que os chryzodes funcionam como um contexto rico e motivador para a aprendizagem, promovendo a interconexão entre diferentes domínios matemáticos e desenvolvendo o pensamento visual, algorítmico e abstrato

Palavras-chave: chryzodes; natureza epicicloidal; geometria dinâmica; teoria dos grafos; sequência didática.

ABSTRACT

This dissertation investigates the geometric patterns known as chryzodes, exploring their geometric foundation, their mathematical properties, and their potential as teaching tools. The study focuses on three main axes. Firstly, the epicicloidal nature of chryzodes is analyzed. Secondly, a formal bridge is established between the notion of chryzodes and graph theory. It is demonstrated that chryzodes, under certain conditions, can be represented as Hamiltonian cycles. This modeling allows for the reinterpretation of geometric properties of curves (such as symmetry and periodicity) in graph-theoretic terms, offering a combinatorial perspective on an object traditionally analyzed through dynamic geometry. Finally, the applied core of the work lies in the implementation and evaluation of an innovative didactic sequence. Aimed primarily at 9th-grade students, although adaptable to other classes, the sequence seeks to facilitate an integrated understanding of concepts related to parametric curves, Euclidean division, and introductory notions of graph theory. It consists of activities ranging from the manual construction of chryzodes to the creation of mandalas using the artistic technique of string art. The results of the application indicate that chryzodes function as a rich and motivating context for learning, promoting the interconnection between different mathematical domains and developing visual, algorithmic, and abstract thinking.

Keywords: chryzodes; epicyloidal nature; dynamic geometry; graph theory; didactic sequence.

LISTA DE ILUSTRAÇÕES

Figura 1 – Euclides de Alexandria. 21
Figura 2 – Étienne Bézout. 25
Figura 3 – Carl Friedrich Gauss. 26
Figura 4 – Pierre de Fermat. 30
Figura 5 – Diofanto de Alexandria. 32
Figura 6 – Leonhard Paul Euler. 37
Figura 7 – Chryzode $C_2(45)$. 45
Figura 8 – Chryzode $C_{12}(30)$. 45
Figura 9 – Construção do Chryzode $C_9(12)$ 47
Figura 10 – Construção do Chryzode $C_2(11)$. 48
Figura 11 – Outros exemplos de chryzodes. 49
Figura 12 – Chryzodes $C_2(29)$ e $C_{15}(29)$. 52
Figura 13 – Chryzode $C_2(7)$: sem e com transposição $P_3 \longleftrightarrow P_5$. 52
Figura 14 – Chryzodes $C_4(23)$ e $C_6(23)$. 53
Figura 15 – Chryzodes $C_4(99)$ e $C_{25}(99)$. 53
Figura 16 – Chryzodes $C_2(5)$ e $C_3(5)$. 54
Figura 17 – Chryzodes que satisfazem a Proposição 3.1.9. 56
Figura 18 – Chryzodes que satisfazem a Proposição 3.1.10. 57
Figura 19 – Exemplos de grafos. 58
Figura 20 – Exemplos de grafos completos. 58
Figura 21 – Trilha $(P_0,\ e_1,\ P_1,\ e_2,\ P_2,\ e_3,\ P_0,\ e_4,\ P_3)$. 59
Figura 22 – Exemplo de caminho e circuito. 60
Figura 23 – Chryzode $C_6(14)$ ou grafo $G(14,14)$ 60
Figura 24 – William R. Hamilton e dodecaedro com nomes de 20 cidades. 61
Figura 25 – Chryzode $C_{11}(15)$. 62
Figura 26 – Chryzode $C(3,7)$. 63
Figura 27 – Chryzode $C_6(11)$ feito na ordem de conexão. 65
Figura 28 – Epicicloide Simples, Encurtada e Alongada. 67
Figura 29 – Chryzode $C_2(m)$ com a circunferência ocultada, para $m = 10, 15, 20, 25, 30, 40, 50, 60$. 68

Figura 30 – Chryzode $C_3(m)$, com a circunferência ocultada, para $m = 20, 40, 60, 80, 100, 120$. 69
Figura 31 – Chryzode $C_4(m)$,com a circunferência ocultada, para $m = 20, 40, 60, 80, 100, 120$. 70
Figura 32 – Chryzode $C_{78}(84)$ 72
Figura 33 – Mandala feita com cordas e pregos 72
Figura 34 – Chryzode $C_{161}(340)$ 72
Figura 35 – Mandala inspirada no Chryzode $C_{161}(340)$ 72
Figura 36 – Chryzode $C_2(100)$ 73
Figura 37 – Mandala inspirada no Chryzode $C_2(100)$ 73
Figura 38 – Padrão polar cardiode 2D e 3D 73
Figura 39 – Exemplos de conjuntos de Mandelbrot. 74
Figura 40 – Tipos de materiais para criação das mandalas. 81
Figura 41 – Chryzode $C_{11}(16)$. 85
Figura 42 – Circuitos dentro do chryzode $C_{11}(16)$ 85
Figura 43 – Representação do grafo feito pelos alunos. 86
Figura 44 – Realização das operações 87
Figura 45 – Registro das construções 88
Figura 46 – Figuras produzidas pelos alunos durante a atividade. 89
Figura 47 – Construção das mandalas. 90
Figura 48 – Mandalas feitas pelos alunos. 91
Figura 49 – Alguns dos Chryzodes produzidos pelos alunos. 106
Figura 50 – Mandalas produzidas pelos alunos. 109
Figura 51 – Circunferência geradora e diretora antes do início do rolamento. 115
Figura 52 – Circunferência diretora com um rolamento de θ graus da circunferência geradora .116
Figura 53 – Representação dos pontos P_t 118

LISTA DE TABELAS

Tabela 1 – Algoritmo de Euclides Estendido 24
Tabela 2 – Exemplo de uso do Algoritmo 24
Tabela 3 – Números de 0 a $lm-1$ 38

LISTA DE GRÁFICOS

Gráfico 1 – Resultado da avaliação diagnóstica. 83
Gráfico 2 – Resultados da avaliação diagnóstica em taxa percentual. 83
Gráfico 3 – Resultado da avaliação somativa. 92
Gráfico 4 – Resultados da avaliação somativa em taxa percentual. 92

SUMÁRIO

1 INTRODUÇÃO 15
2 CONCEITOS PRELIMINARES 18
2.1 Conceitos de divisibilidade 18
2.2 Divisão Euclidiana 20
2.3 Máximo Divisor Comum 22
2.4 Algoritmo de Euclides 23
2.5 Propriedades do Maior Divisor Comum 24
2.6 Teorema Fundamental da Aritmética 27
2.7 Equações Diofantinas Lineares com duas variáveis 31
2.8 Congruências 34
2.9 Função Totiente de Euler 37
2.10 Congruência Linear 41
3 CHRYZODES 44
3.1 Construção e resultados sobre os chryzodes 44
3.2 Chryzodes em Teoria dos Grafos 57
3.3 A Natureza Epicicloidal dos Chryzodes 66
3.4 A presença dos Chryzodes na arte e na vida 72
4 ASPECTOS METODOLÓGICOS 76
4.1 Metodologia da pesquisa 76
4.1.1 Contexto e sujeitos 76
4.2 Propostas de atividades 77
4.2.1 Atividade 1 - Chryzode com papel, lápis e régua 77
4.2.2 Atividade 2 - Construção de mandalas 79
5 ANÁLISE E DISCUSSÃO DOS RESULTADOS 82
5.1 Avaliação diagnóstica 82
5.2 Conceitos Fundamentais 84
5.3 Chryzodes com papel, lápis e régua 87
5.4 Construção de mandalas no formato de chryzodes por meio da técnica de String Art 89

5.5 Avaliação somativa 91
6 CONSIDERAÇÕES FINAIS 95
REFERÊNCIAS 96
APÊNDICE A – AVALIAÇÃO DIAGNÓSTICA 98
APÊNDICE B – IMPRESSÕES PARA A ATIVIDADE 1 101
APÊNDICE C – CHRYZODES FEITOS DURANTE A ATIVIDADE DA ETAPA 3 106
APÊNDICE D – CONSTRUÇÕES DE MANDALAS REALIZADA NA ATIVIDADE DA ETAPA 4 109
APÊNDICE E – AVALIAÇÃO SOMATIVA 112
APÊNDICE F – DEMONSTRAÇÃO DO TEOREMA 3.3.3. 115

1 INTRODUÇÃO

Ensinar Matemática de forma inovadora pressupõe sair do modelo no qual o professor é o centro do conhecimento. Ao acolher as experiências e saberes prévios dos alunos, é possível construir um ensino que alia formalidade matemática e aplicação no cotidiano, promovendo engajamento genuíno. É nesse contexto que se inserem os Chryzodes, que são representações geométricas das congruências $i \cdot a \equiv b_i \pmod{m}$, para $i = 0, 1, ..., m-1$, com $a, m \in \mathbb{N}$, construídas a partir de um círculo dividido em m pontos equidistantes, numerados de 0 a $m-1$, com conexões visuais traçadas de cada i ao respectivo b_i. A investigação teórica dos chryzodes nos permite atravessar as fronteiras entre matemática, arte e simbolismo. Paralelamente, na dimensão prática, oferece ferramentas para transformar operações básicas abstratas em padrões visuais que facilitam compreensão e aprendizagem, conectando a intuição do aluno à linguagem precisa da matemática através da beleza e lógica dos padrões.

Os chryzodes oferecem um caminho para contextualizar operações matemáticas dentro de atividades lúdicas, facilitando a assimilação de conteúdos fundamentais como multiplicação e divisão. O documento que norteia as habilidades a serem trabalhados no Ensino Fundamental sobre esse tema é a Base Nacional Comum Curricular (Brasil, 2018). Ela apresenta habilidades diretamente relacionadas à utilização desses materiais, conforme a descrição a seguir:

i. **(EF07MA01)** Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos.

ii. **(EF07MA04)** Resolver e elaborar problemas que envolvam operações com números inteiros.

iii. **(EF07MA06)** Reconhecer que as resoluções de um grupo de problemas que têm a mesma estrutura podem ser obtidas utilizando os mesmos procedimentos.

iv. **(EF07MA16)** Reconhecer se duas expressões algébricas obtidas para descrever a regularidade de uma mesma sequência numérica são ou não equivalentes.

v. **(EF07MA21)** Reconhecer e construir figuras obtidas por simetrias de translação, rotação e reflexão, usando instrumentos de desenho ou softwares de geometria dinâmica e vincular esse estudo a representações planas de obras de arte, elementos arquitetônicos, entre outros

vi. **(EF07MA22)** Construir circunferências, utilizando compasso, reconhecê-las como lugar geométrico e utilizá-las para fazer composições artísticas e resolver problemas que envolvam objetos equidistantes.

"A Matemática caracteriza-se como uma forma de compreender e atuar no mundo e o conhecimento gerado nessa área do saber como um fruto da construção humana na sua interação constante com o contexto natural, social e cultural" (Brasil, 1998, p. 24). Portanto, este trabalho tem como objetivo geral oferecer, por meio de uma sequência didática, instrumentos que auxiliem os estudantes na aprendizagem das operações básicas a partir da divisão euclidiana. Especificamente, busca-se apresentar alguns resultados sobre os chryzodes, entre eles sua natureza epicicloidal, permitindo a visualização de suas aplicações em diferentes contextos do cotidiano, incluindo a arte.

A opção de investigar os chryzodes e seu uso pedagógico, justifica-se pela intersecção de duas necessidades prementes no cenário educacional contemporâneo: a urgência em se encontrar metodologias inovadoras que capturem o interesse discente e a imperiosa tarefa de formar cidadãos críticos e eticamente reflexivos. Pois, conforme apontam os Parâmetros Curriculares Nacionais (Brasil, 2000), as aulas expositivas costumam ser adotadas como recurso exclusivo, gerando a percepção de que se tratam de uma estratégia tediosa e pouco engajadora.

> Para os professores, o cálculo e a manipulação simbólica tendem a ser vistos como a base de toda a aprendizagem, o que constitui reconhecidamente uma visão redutora da Matemática. A ideia básica é a de que quem não sabe calcular não pode fazer o mais pequeno raciocínio. (...) Ignora-se dum modo geral a importância da diversificação das representações, a necessidade de tomar os conhecimentos dos alunos como ponto de partida das aprendizagens e a importância da interacção social na criação dos novos saberes, persistindo-se numa tradição pedagógica que tende a perpetuar a imagem da Matemática como algo de misterioso e inacessível (Ponte, 1994).

A estrutura proposta neste trabalho busca estabelecer uma conexão coerente que possibilite a compreensão e a identificação das delicadas nuances presentes nessas construções. Ao longo dos capítulos, são abordados múltiplos temas, dentre os quais se evidenciam:

- Capítulo 1: São apresentados o objeto e a sequência que será adotada para a descrição do trabalho.

- Capítulo 2: Neste capítulo, são expostos os conceitos básicos da teoria dos números que fundamentam a análise subsequente do comportamento e dos resultados acerca dos chryzodes.
- Capítulo 3: São apresentados a definição e o método de construção dos chryzodes, bem como sua relação com a teoria dos grafos. Aborda-se também sua natureza epicicloidal e sua utilidade em áreas como engenharia, artes e sistemas naturais.
- Capítulo 4: Este capítulo descreve a abordagem metodológica que estrutura a pesquisa, com foco na Sequência Didática desenvolvida e aplicada, delineando as estratégias, procedimentos e ferramentas utilizados para atingir os objetivos propostos.
- Capítulo 5: Este capítulo tem por finalidade expor e examinar os achados decorrentes da execução da Sequência Didática envolvendo os chryzodes. Procede-se à análise dos dados, promovendo um diálogo entre as evidências coletadas e o quadro teórico-conceitual que fundamenta o estudo.
- Capítulo 6: São apresentadas as considerações finais no sentido de comprovar que é possível através de uma sequência didática envolvendo chryzodes, trabalhar com instrumentos que auxiliem os estudantes na aprendizagem das operações básicas a partir da divisão euclidiana.

2 CONCEITOS PRELIMINARES

Neste capítulo, são apresentados os fundamentos da Aritmética Modular, essenciais para a compreensão dos tópicos subsequentes. A exposição teórica tem como referência principal a obra *Aritmética* (Hefez, 2022), com ênfase especial nas congruências aritméticas e em suas conexões intrínsecas com as operações de multiplicação e divisão.

2.1 Conceitos de divisibilidade

Dados dois números inteiros a e b, diremos que *a divide b*, escrevendo $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = c \cdot a$. Nesse caso, diremos também que a é *divisor* ou um *fator* de b ou, ainda, que b é um *múltiplo* de a.

Por outro lado, quando não existir nenhum inteiro c tal que $b = c \cdot a$, diz-se que *a não divide b*. Neste caso utilizaremos a notação $a \nmid b$.

Exemplo 2.1.1. Observe os exemplos:

(a) $7 \mid 42$ pois $42 = 6 \cdot 7$

(b) $3 \nmid 22$ pois $\nexists\, c \in \mathbb{Z}$ tal que $22 = c \cdot 3$

Estabeleceremos a seguir algumas propriedades da divisibilidade.

Proposição 2.1.2. *Sejam $a, b, c \in \mathbb{Z}$. temos que:*

(1) $1 \mid a$, $a \mid a$ e $a \mid 0$;

(2) $0 \mid a \iff a = 0$;

(3) $a \mid b \iff |a| \mid |b|$;

(4) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Obs.: Os itens (1) e (3) da proposição acima nos dizem que todo número inteiro a é divisível por ± 1 e por $\pm a$. Note também que (1) inclui o caso $a \mid 0$ e, portanto, todo número inteiro divide 0. Assim, 0 tem infinitos divisores.

Demonstração:

(1) Decorre das igualdades $a = a \cdot 1$, $a = 1 \cdot a$ e $0 = 0 \cdot a$.

(2) Suponhamos que $0 \mid a$, logo $\exists\, c \in \mathbb{Z}$ tal que $a = c \cdot 0$. Como $c \cdot 0 = 0,\ \forall c \in \mathbb{Z}$, então $a = 0$. Reciprocamente, basta observar que $0 \mid 0$, o que foi provado no item anterior.

(3) Se $a \mid b$ então $b = c \cdot a$, para algum $c \in \mathbb{Z}$. Aplicando módulo a ambos os membros da igualdade, obtemos $|b| = |c \cdot a| = |c| \cdot |a|$. Como $|c| \in \mathbb{Z}$ temos que $|a| \mid |b|$.

Agora, assuma $|a| \mid |b|$. Então $\exists\ m \in \mathbb{Z}$ tal que $|b| = |a| \cdot m$. Note que:

$$|a| = \pm a \ \text{ e } \ |b| = \pm b \ \text{ (dependendo dos sinais de } a \text{ e } b\text{).}$$

De $|b| = |a| \cdot m$, podemos escrever:

$$\pm b = (\pm a) \cdot m \ \Rightarrow \ b = a \cdot (\pm m).$$

Portanto, concluímos que $a \mid b$.

(4) $a \mid b$ e $b \mid c$ então existem c_1 e c_2 inteiros, tais que $b = c_1 \cdot a$ e $c = c_2 \cdot b$. Substituindo o valor de b da primeira equação na outra, obtemos: $c = c_2 \cdot (c_1 \cdot a) = (c_2 \cdot c_1) \cdot a$. Logo $a \mid c$ pois $c_2 \cdot c_1 \in \mathbb{Z}$. □

Proposição 2.1.3. *Se $a, b, c, d \in \mathbb{Z}$ então $a \mid b$ e $c \mid d \Rightarrow ac \mid bd$.*

Demonstração: Se $a \mid b$ e $c \mid d$, então $\exists\ c_1, c_2 \in \mathbb{Z}$ tal que $b = c_1 \cdot a$ e $d = c_2 \cdot c$. Portanto

$$b \cdot d = (c_1 \cdot a) \cdot (c_2 \cdot c) = (c_1 \cdot c_2) \cdot (a \cdot c)$$

Logo, $ac \mid bd$. □

Exemplo 2.1.4. Sabemos que $3 \mid 9$ e $4 \mid 16$, logo $3 \cdot 4 \mid 9 \cdot 16$, isso é, $12 \mid 144$.

Proposição 2.1.5. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a \mid (b \pm c)$. Então $a \mid b \iff a \mid c$.*

Demonstração: Suponha que $a \mid (b + c)$. Logo, existe $c_1 \in \mathbb{Z}$ tal que $b + c = c_1 \cdot a$. Agora, se $a \mid b$, temos que existe $c_2 \in \mathbb{Z}$ tal que $b = c_2 \cdot a$. Juntando as duas igualdades, temos:

$$c_2 \cdot a + c = c_1 \cdot a \ \Rightarrow \ c = (c_1 - c_2) \cdot a$$

Logo $a \mid c$.

Reciprocamente, se $a \mid c$ então existe $c_3 \in \mathbb{Z}$ tal que $c = c_3 \cdot a$. Desta forma,

$$\begin{aligned} & b + c = c_1 \cdot a \\ \Rightarrow\ & b + (c_3 \cdot a) = c_1 \cdot a \\ \Rightarrow\ & b = (c_1 - c_3) \cdot a \end{aligned}$$

Logo $a \mid b$.

Se $a \mid (b - c)$, a demonstração é análoga. □

Exemplo 2.1.6. Sabemos que $4 \mid (12+16)$, como $4 \mid 12$ temos que $4 \mid 16$.

Proposição 2.1.7. *Sejam $a,b,c \in \mathbb{Z}$, com $c \neq 0$. Se $ac \mid bc$, então $a \mid b$.*

Demonstração: Como $ac \mid bc$, então existe $c_1 \in \mathbb{Z}$ tal que $bc = c_1 \cdot (ac) = (c_1 a) \cdot c$, como $c \neq 0$, pela lei do corte, segue que $b = c_1 \cdot a$. Daí $a \mid b$. □

Exemplo 2.1.8. Sabemos que $30 \mid 270$, isso é, $6 \cdot 5 \mid 54 \cdot 5$. Logo $6 \mid 54$.

Proposição 2.1.9. *Se $a,b,c \in \mathbb{Z}$ são tais que $a \mid b$ e $a \mid c$, então para todos $x,y \in \mathbb{Z}$, temos que $a \mid (xb+yc)$.*

Demonstração: Sejam $a \mid b$ e $a \mid c$. Então existem inteiros c_1 e c_2 tais que $b = c_1 \cdot a$ e $c = c_2 \cdot a$. Logo, $xb = x(c_1 \cdot a)$ e $yc = y(c_2 \cdot a)$. Somando as duas igualdades, obtemos $xb+yc = x(c_1 \cdot a)+y(c_2 \cdot a) = (xc_1+yc_2) \cdot a$. Logo $a \mid (xb+yc)$. □

Exemplo 2.1.10. Sejam os números $4, 8$, e 12, tais que $4 \mid 8$ e $4 \mid 12$. Então $4 \mid (8x+12y), \forall x,y \in \mathbb{Z}$. Se considerarmos $x = 5$ e $y = 2$, teremos $4 \mid (8 \cdot 5+12 \cdot 2)$, ou seja, $4 \mid 64$.

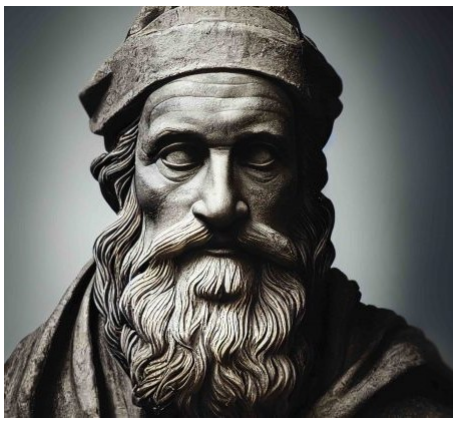
Proposição 2.1.11. *Dados $a,b \in \mathbb{Z}$, com $b \neq 0$, temos que se $a \mid b$, então $|a| \leq |b|$.*

Demonstração: Se $a \mid b$, existe $q \in \mathbb{Z}$ tal que $b = a \cdot q$. Levando módulo de ambos os lados da igualdade, temos que $|b| = |a \cdot q| = |a| \cdot |q|$. Como $b \neq 0$, resulta em $q \neq 0$, logo $1 \leq |q|$ e portanto, $|a| \leq |a| \cdot |q| = |b|$. □

2.2 Divisão Euclidiana

Euclides de Alexandria (c. 325–265 a.C.) foi um matemático grego cuja obra "Os Elementos" revolucionou o pensamento matemático ao introduzir um sistema axiomático rigoroso para a geometria e a aritmética. Seu método de organização do conhecimento com base em definições, postulados e teoremas tornou-se fundamento não apenas para a matemática, mas para as ciências exatas em geral. Euclides é particularmente relevante para esta dissertação devido à sua abordagem lógica e dedutiva, que influencia até hoje o ensino e a estruturação de teorias matemáticas, especialmente em temas como divisibilidade, algoritmos e propriedades dos números inteiros, conceitos centrais para o desenvolvimento deste trabalho.

Figura 1 – Euclides de Alexandria.



Fonte: (Selina; facts.net, 2024)

A *divisão euclidiana* é um processo que, dados dois números inteiros a (dividendo) e b (divisor), com $b \neq 0$, permite encontrar dois únicos inteiros q (quociente) e r (resto) tal que: $a = b \cdot q + r$ e $0 \leq r < |b|$.

Para demonstrar tal resultado, precisamos antes definir o Princípio da Boa Ordenação e a Propriedade Arquimediana.

Principio da Boa Ordenação (P.B.O.): Todo conjunto não vazio de números inteiros não negativos (ou seja, todo subconjunto não vazio de $\mathbb{N}$) possui um menor elemento.

Propriedade Arquimediana: Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $n \cdot b > a$.

Teorema 2.2.1. *Dado $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos inteiros q, r chamados, respectivamente, de quociente e resto, tais que:*

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

Demonstração:

Existência: Considere o conjunto $S = \{a - b \cdot k / k \in \mathbb{Z}\} \cap \mathbb{Z}_+$. Perceba que $S \neq \emptyset$, pois usando a propriedade arquimediana, existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$. Pelo *P.B.O.* existe $r = \textbf{min S}$ (menor elemento de S). Suponhamos então que $r = a - bq$ para algum $q \in \mathbb{Z}$. Resta mostrar que $r < |b|$. Por contradição, suponha que $r \geq |b|$, então $r' = r - |b| \geq 0$, resultando em $r' = a - bq - |b|$.

- Se $b > 0,\ r' = a - b(q+1) < r$, contradizendo o P.B.O.
- Se $b < 0,\ r' = a - b(q-1) < r$, mesma contradição.

Logo $r < |b|$.

Unicidade: Suponha duas representações:

$$a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2, \text{ onde } r_1, r_2, q_1, q_2 \in \mathbb{Z},\ 0 \leq r_1, r_2 < |b|$$

subtraindo:

$$b(q_1 - q_2) = r_2 - r_1.$$

Como $|r_2 - r_1| < |b|$, onde $|b| \cdot |q_1 - q_2| = |r_2 - r_1| < |b|$ só é possível se $q_1 = q_2$ e consequentemente $r_1 = r_2$. □

2.3 Máximo Divisor Comum

Sejam a e b dois números inteiros, não ambos nulos. Um *Máximo Divisor Comum* (MDC) de a e b é um inteiro d que satisfaz as duas seguintes propriedades:

1. d **divide ambos** a e b:

$$d \mid a \text{ e } d \mid b;$$

2. d **é maximal em relação a divisibilidade**: para todo inteiro c que divide ambos a e b, tem-se que c também divide d, ou seja,

$$\text{se } c \mid a \text{ e } c \mid b, \text{ então } c \mid d.$$

O inteiro d é denotado por $mdc(a,b)$.

Exemplo 2.3.1. Considere $D(a)$ o conjunto dos divisores de um número inteiro a, então temos que: $D(12) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$ e $D(20) = \{\pm1, \pm2, \pm4, \pm5, \pm10, \pm20\}$.

Observando tais conjuntos, verifica-se que esses apresentam números em comuns, que são: $\{\pm1, \pm2, \pm4\}$. Assim $mdc(12,20) = 4$.

Como o valor do $mdc(a,b)$ é independente da ordem dos elementos e do seu sinal, temos que:

(i) $mdc(a,b) = mdc(b,a)$;

(ii) $mdc(a,b) = mdc(-a,b) = mdc(a,b) = mdc(-a,-b)$.

O lema subsequente constitui um método eficaz para o cálculo do *mdc* e serve como base para o Algoritmo de Euclides, o qual possibilita a determinação eficiente do máximo divisor comum entre dois números naturais arbitrários.

Lema 2.3.2. *Seja $a,b,n \in \mathbb{Z}$. Se existir $mdc(a,b-na)$, então $mdc(a,b)$ existe e $mdc(a,b) = mdc(a,b-na)$.*

Demonstração: Tome $d = mdc(a,b-na)$. Logo $d \mid a$ e portanto $d \mid na$, segue ainda que $d \mid (b-na)$ e pela Proposição 2.1.5, concluímos que $d \mid b$. Logo, d é divisor comum de a e b. Suponha agora que d' seja um divisor comum de a e b. Dessa forma, a Proposição 2.1.9 assegura que d' é divisor comum de a e $b-na$, implicando $d' \mid d$. Isso prova que $d = mdc(a,b)$. □

2.4 Algoritmo de Euclides

O algoritmo de Euclides é um método eficiente para encontrar MDC entre dois números inteiros a e b, baseado no princípio da divisão euclidiana.

Dados $a,b \in \mathbb{Z}$, com $0 < b \leq a$. Se $b = 1$ ou $b = a$, ou ainda $b \mid a$, claramente teremos que $mdc(a,b) = b$. Portanto, suponhamos $0 < b < a$ e que $b \nmid a$. Assim, usando a divisão euclidiana, teremos:

$$a = b \cdot q_1 + r_1, \;\; 0 < r_1 < b$$

Temos duas possibilidades:

- $r_1 \mid b$. Nesse caso, $r_1 = mdc(b,r_1)$ e pelo Lema 2.3.2, temos que

$$r_1 = mdc(b,r_1) = mdc(b,a-b\cdot q_1) = mdc(b,a) = mdc(a,b),$$

e o algoritmo termina.

- $r_1 \nmid b$. Em tal caso, pela divisão euclidiana, obtemos

$$b = r_1 \cdot q_2 + r_2, \;\; \text{com } 0 < r_2 < r_1.$$

Novamente, temos duas possibilidades:

- Se $r_2 \mid r_1$, então $mdc(r_1,r_2) = r_2$ e outra vez, pelo Lema2.3.2,

$$r_2 = mdc(r_1,r_2) = mdc(r_1,b-r_1q_2) = mdc(r_1,b) = mdc(a-bq_1,b) = mdc(a,b),$$

e assim, se encerra o algoritmo.

- Se $r_2 \nmid r_1$. Pela divisão euclidiana, temos:

$$r_1 = r_2 q_3 + r_3, \text{ com } 0 < r_3 < r_2.$$

Este processo deve eventualmente terminar. A razão é que uma sequência estritamente decrescente $b > r_1 > r_2 > r_3 > ...$ de números naturais não pode existir, devido ao Princípio da Boa Ordenação (que diz que todo subconjunto não vazio dos naturais possui um elemento mínimo). Logo para algum n, temos que $r_n \mid r_{n-1}$, o que implica que $mdc(a,b) = r_n$.

A fim de ilustrar o resultado apresentado, constrói-se a seguinte tabela:

	q_1	q_2	q_3	q_4	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	r_3	$\cdots$	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	r_4		$\cdots$	$r_n = 0$	r_{n+1}	

Tabela 1 – Algoritmo de Euclides Estendido

Exemplo 2.4.1. Determine o $mdc(298,96)$, pelo algoritmo de Euclides.

Temos:

	3	9	1	1	2
298	96	10	6	4	2
10	6	4	2	0	

Tabela 2 – Exemplo de uso do Algoritmo

Logo $mdc(298,96) = 2$.

2.5 Propriedades do Maior Divisor Comum

Como já abordamos a definição do máximo divisor comum, é momento de aprofundar como suas propriedades impactam a teoria algébrica dos números. Nesta seção, demonstraremos como tais propriedades fundamentam conceitos importantes e exploraremos casos em que a generalização do MDC para contextos mais complexos revela aspectos cruciais para a resolução de problemas avançados.

Étienne Bézout (1730-1783) foi um matemático francês cujo trabalho se destaca no contexto do Iluminismo europeu, período de intenso desenvolvimento nas ciências exatas. Nascido em Nemours, França, Bézout tornou-se membro da Académie des Sciences e dedicou-se principalmente à álgebra e à teoria de equações. Suas contribuições foram fundamentais para a consolidação de conceitos que hoje são pilares da teoria dos números e da álgebra moderna. A seguir, veremos um importante resultado desse matemático.

Figura 2 – Étienne Bézout.

Fonte: (Wikipédia, 2024)

Teorema 2.5.1. *(IDENTIDADE DE BÉZOUT): Sejam a e b números inteiros não ambos nulos, e seja $mdc(a,b) = d$. Então existem inteiros x e y tais que:*

$$ax + by = d.$$

Demonstração: Considere o conjunto $S = \{ax + by;\ x, y \in \mathbb{Z},\ ax + by > 0\}$. Como a e b não são ambos nulos, $S \neq \emptyset$. Pelo Princípio da Boa Ordenação S possui um menor elemento, digamos $d = ax + by$, com $x, y \in \mathbb{Z}$. Temos que $d \mid a$ e $d \mid b$. De fato, pelo algoritmo da divisão,

$$a = qd + r,\ 0 \leq r < d.$$

Então,

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$

Se $r > 0$ então $r \in S$, mas $r < d$ contradizendo a minimalidade de d. Logo $r = 0$ e $d \mid a$. De modo análogo, $d \mid b$.

Agora, considere c um divisor comum de a e b. Então $a = ca'$ e $b = cb'$, portanto

$$d = ax + by = (ca')x + (cb')y = c(a'x + b'y),$$

logo $c \mid d$. Portanto, conclui-se que $mdc(a,b) = d = ax + by$. □

Sejam inteiros a e b com $mdc(a,b) = 1$, então diremos que a e b são *primos entre si*, ou *coprimos*.

Carl Friedrich Gauss nasceu em 1777 e viveu até 1855. É considerado um dos maiores matemáticos de todos os tempos. Gauss teve a estatura de Arquimedes e de Newton, e seus campos de interesse excederam os de ambos. Gauss contribuiu para todos os ramos da Matemática e para a Teoria dos Números (Amaral, 2023).

Figura 3 – Carl Friedrich Gauss.

Fonte: (Wikipédia, 2025)

Teorema 2.5.2. *(LEMA DE GAUSS): Sejam $a,b,c \in \mathbb{Z}$. Se $a \mid bc$ e $mdc(a,b) = 1$, então $a \mid c$.*

Demonstração: Dado $mdc(a,b) = 1$, o Teorema 2.5.1 garante que existem dois números $x,y \in \mathbb{Z}$, tais que $ax + by = 1$. Multiplicando essa equação por c, resulta:

$$(ac)x + (bc)y = c.$$

Como $a \mid ac$ e por hipótese $a \mid bc$, então pela Proposição 2.1.9, temos que $a \mid c$. □

Exemplo 2.5.3. Como $3 \mid 7 \cdot 6$ e $mdc(3,7) = 1$, temos pelo teorema 2.5.2 que $3 \mid 6$.

Teorema 2.5.4. *Se $a,b \in \mathbb{Z}$ e $a = q \cdot b + r$ onde $r,a \in \mathbb{Z}$, então $mdc(a,b) = mdc(b,r)$.*

Demonstração: Da igualdade $a = q \cdot b + r$, segue que $r = a - b \cdot q$. Assim, seja um $c \in \mathbb{Z}$ tal que $c \mid a$ e $c \mid b$. Sendo assim, da Proposição 2.1.9, concluímos que $c \mid r$. Portanto, c é um divisor comum de b e r. Reciprocamente, como $a = b \cdot q + r$, segue-se que todo divisor comum de b e r

também é divisor de a. Logo, o conjunto dos divisores comuns de a e de b é igual ao conjunto dos divisores comuns de b e de r. Portanto, $mdc(a,b) = mdc(b,r)$. □

Proposição 2.5.5. *Quaisquer que sejam $a,b \in \mathbb{Z}^*$, e $c \in \mathbb{N}$, tem-se que*

$$(ca,cb) = c(a,b).$$

Demonstração: Sejam a e b inteiros, não nulos, c um número natural e $mdc(a,b) = d$. Assim como $d \mid a$ e $d \mid b$, então $dc \mid ac$ e $dc \mid bc$. Portanto, $dc \mid (ac,bc)$. Agora vamos demonstrar que dc é divisível por todo divisor comum de ac e bc. De fato, seja k um número inteiro, tal que $k \mid ac$ e $k \mid bc$. Assim tomando os inteiros x e y, tais que $ax+by = d$, temos então que $cax+cby = cd$. E como $k \mid ac$ e $k \mid bc$, então $k \mid cd$. Logo, $(ac,bc) = dc$, e consequentemente $(ac,bc) = dc = c \cdot (a,b)$. □

Proposição 2.5.6. *Dados $a,b \in \mathbb{Z}^*$, tem-se que*

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

Demonstração: Se $mdc(a,b) = 1$, então a demostração segue diretamente. Suponha que $mdc(a,b) = d$, com $d \neq 1$. Suponha que $\left(\frac{a}{d}, \frac{b}{d}\right) = k$. Então pela Proposição 2.5.5, segue que $d = mdc(a,b) = mdc\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = d \cdot k$. Portanto, temos que $k = 1$. □

2.6 Teorema Fundamental da Aritmética

Define-se como número *primo* todo inteiro $n > 1$ cujos únicos divisores positivos são 1 e n. Um número natural maior que 1 que não é primo é denominado *composto*.

Proposição 2.6.1. *(Lema de Euclides) Sejam $a,b,p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração: Perceba que se $p \nmid a$, então $mdc(a,p) = 1$. De fato, se $mdc(p,a) = d$, temos que $d \mid p$ e $d \mid a$. Portanto $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $p = 1$. Logo, pela Teorema 2.5.2, temos que $p \mid b$. Analogamente, se $p \nmid b$, então $p \mid a$. □

Corolário 2.6.2. *Se $p,\ p_1,\ p_2, \ldots,\ p_n$ são números primos e se, $p \mid p_1 \cdots p_n$, então $p = p_i$, para algum $i = 1,2,\ldots,n$.*

Demonstração: Mostraremos usando indução sobre n.

Caso base: ($n = 1$) Se $p \mid p_1$, então como ambos são primos positivos, devemos ter $p = p_1$.

Hipótese de indução: Suponha que a afirmação seja verdadeira para um produto de n primos.
Passo indutivo: Mostraremos que o resultado será válido para o produto de $n+1$ primos.
Considere que $p \mid p_1 p_2 \cdots p_{n+1}$.

- Caso 1: Se $p \mid p_{n+1}$, então $p = p_{n+1}$ (pois ambos são primos), e o resultado está provado.
- Caso 2: Se $p \nmid p_{n+1}$, então o $mdc(p, p_{n+1}) = 1$. Logo pelo Lema 2.6.1, $p \mid p_1 \cdots p_n$. Pela hipótese de indução, existe $i \in \{1,2,...,n\}$ tal que $p = p_i$.

Portanto, em ambos os casos, $p = p_i$ para algum $i \in \{1,2,...,n\}$. □

Teorema 2.6.3. *(Teorema Fundamental da Aritmética) Todo número inteiro maior do que 1, ou é primo, ou é um número composto, e pode ser representado de maneira única (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração: Existência: Suponha por absurdo, que existe pelo menos um inteiro maior do que 1 que não possa ser representado por fatores primos. Seja A o conjunto de todos esses números. Como A é um subconjunto dos inteiros, A possui um elemento mínimo pelo Princípio da Boa Ordenação, chamamos de x esse elemento. Como x é maior do que 2 (pois 2 é primo, e tem fatoração em fatores primos), então existem a e b não primos, tais que $x = ab$, com $a < x$ e $b < x$, e como $a, b \notin A$, eles possuem fatoração em fatores primos e, portanto, $x = ab$, possui fatoração em fatores primos, logo um absurdo, pois $x \in A$. Portanto, A não pode ter elemento mínimo, logo $A = \emptyset$. O que prova a demostração da existência.
Unicidade: Da generalização da proposição 2.6.1, temos que se $p \mid a_1 a_2 a_3 ... a_n$, com p primo, então p divide pelo menos um fator a_i do produto, com $i \in \{1,2,...n\}$. Assim, sejam $y = p_1 p_2 ... p_k = q_1 q_2 ... q_n$ duas fatorações de y, tal que $k, n \in \mathbb{N}$ ($k > 1$ e $n > 1$). Da igualdade e da definição de divisibilidade, verificamos que $p_1 \mid q_1 q_2 ... q_n$ e, portanto, pela generalização da Proposição 2.6.1 acima, temos que existe r tal que, $p_1 \mid q_r$, portanto, $p_1 = q_r$, já que ambos são primos. Por extensão, para qualquer $j < k$, existe um $i < n$ tal que $p_j \mid q_i$, logo, $p_j = q_i$. Por último, basta provar que $n = k$, o que é trivial, já que, se $n > k$, teríamos que: $q_1 q_2 ... q_k ... q_n = p_1 p_2 ... p_k = q_1 q_2 ... q_k$, o que é um absurdo, já que os $q's$ são maiores que 1. Ou seja, o conjunto de q_i deve ser idêntico ao conjunto de p_j, o que prova a unicidade. □

Corolário 2.6.4. *Sejam $a, b, c \in \mathbb{Z}^+$, então $mdc(a, bc) = 1 \iff mdc(a,b) = mdc(a,c) = 1$.*

Demonstração: ($\Rightarrow$) Se $mdc(a, bc) = 1$, então a não tem fatores primos em comum com bc. Logo, a não tem fatores primos em comum com b nem com c. Portanto, $mdc(a,b) = mdc(a,c) = 1$.

($\Leftarrow$) Se $mdc(a,b) = mdc(a,c) = 1$, então a não compartilha fatores primos com b e nem com c. Como os fatores primos de bc são a união dos fatores primos de b e c (com multiplicidades), a não tem fator primo comum com bc. Logo, $mdc(a,bc) = 1$. □

Teorema 2.6.5. *Dado um número inteiro $n \neq 0, 1, -1$, existem primos $p_1 < \cdots < p_r$ e $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$, univocamente determinados, tais que $n = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.*

Demonstração: **Existência da fatoração:**

- Caso $n > 1$: Provamos por indução forte.

Caso base: Se $n = 2$, então n é primo e a fatoração é ele mesmo.
Hipótese de indução: Suponha que todo inteiro m com $1 < m < n$ possui uma fatoração em primos.
Passo indutivo: Se n é primo, então a fatoração é trivial. Se n é composto, então existem inteiros a, b com $1 < a, b < n$ tais que $n = ab$. Pela hipótese de indução, a e b possuem fatoração em primos:

$$a = q_1^{\beta_1} \cdots q_s^{\beta_s} \text{ e } b = r_1^{\gamma_1} \cdots r_t^{\gamma_t}.$$

Então:

$$n = ab = q_1^{\beta_1} \cdots q_s^{\beta_s} \cdot r_1^{\gamma_1} \cdots r_t^{\gamma_t}.$$

Reorganizando os primos em ordem crescente e agrupando potências iguais, obtemos a fatoração desejada.

- Caso $n < -1$:

  Se $n < -1$, então $-n > 1$. Pelo caso anterior, $-n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, logo:

  $$n = -p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

  Unicidade da fatoração:

  Suponha que n tenha duas fatorações em fatores primos:

  $$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = q_1^{\beta_1} \cdots q_s^{\beta_s}$$

com $p_1 < \cdots < p_r$ e $q_1 < \cdots < q_s$ primos, e $\alpha_i, \beta_i \in \mathbb{N}$.
Passo 1: Mostrar que $r = s$ e $p_i = q_i$ para todo i.

Como $p_1 \mid n = q_1^{\beta_1} \cdots q_s^{\beta_s}$, pelo Lema 2.6.1, p_1 deve dividir algum q_j com $j \in \{1,...,s\}$. Como q_j é primo, $p_1 = q_j$. Mas p_1 é o menor primo da primeira fatoração e q_1 é o menor da segunda, logo $p_1 = q_1$.

Cancelando p_1 de ambas as fatorações, obtemos:

$$p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r} = q_1^{\beta_1 - 1} \cdots q_s^{\beta_s}.$$

Repetindo o processo, concluímos que $r = s$ e $p_i = q_i$ para todo i.

Passo 2: Mostrar que $\alpha_i = \beta_i$, para todo i.

Após cancelar todos os fatores p_i, γ_i vezes, onde $\gamma_i = min(\alpha_i, \beta_i)$, obtemos:

$$p_1^{\alpha_1 - \gamma_1} \cdots p_r^{\alpha_r - \gamma_r} = p_1^{\beta_1 - \gamma_1} \cdots p_r^{\beta_r - \gamma_r}.$$

Se $\alpha_k > \beta_k$ para algum k, então o lado esquerdo seria divisível por p_k mas o direito não, uma contradição. Logo $\alpha_i = \beta_i$ para todo i. □

"Desde, pelo menos, 500 anos antes de Cristo, os chineses sabiam que, se p é um número primo, então, $p \mid 2^p - 2$. Coube a Pierre de Fermat, no século $XVII$, generalizar esse resultado "(Hefez, 2022, p. 131). Apresentaremos a prova desse resultado mais a frente. Antes, vejamos um lema auxiliar.

Figura 4 – Pierre de Fermat.

Fonte: (sciencephoto, 2025)

Lema 2.6.6. *Seja p um número primo. Os números* $\binom{p}{i}$*, onde* $0 < i < p$*, são todos divisíveis por p.*

Demonstração: Considere a fórmula do coeficiente binomial:

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

$$\Rightarrow \binom{p}{i} = \frac{p\cdot(p-1)\cdots(p-i+1)}{i!}.$$

Como p é primo e $0 < i < p$, então pelo Lema 2.6.1 sabemos que $p \nmid i!$ (pois caso contrário, $p \mid k$ tal que $0 < k \leq i < p$, resultando em um absurdo). Logo $mdc(i!, p) = 1$ e, portanto, pelo Lema 2.5.2, $i! \mid (p-1)\cdots(p-i+1)$. O resultado então segue, pois

$$\binom{p}{i} = p \cdot \frac{(p-1)\cdots(p-i+1)}{i!}.$$

□

Teorema 2.6.7. ***(Pequeno Teorema de Fermat)*** *Dado um número primo p, tem-se que* $p \mid a^p - a$, *para todo* $a \in \mathbb{Z}$.

Demonstração: Se $p = 2$, a verificação é direta, dado que $a^2 - a = a(a-1)$ é par. No caso em que p ímpar. a prova segue por indução em a.

Base: O resultado vale claramente para $a = 0$, pois $p \mid 0$.
Hipótese de indução: Supondo o resultado válido para a.
Passo Indutivo: Iremos prová-lo para $a+1$. Pela fórmula do Binômio de Newton,

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a.$$

Como, pelo Lema 2.6.6 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, segue-se o resultado. □

2.7 Equações Diofantinas Lineares com duas variáveis

Uma equação diofantina linear em duas variáveis é uma equação da forma:

$$aX + bY = c$$

com $a, b, c \in \mathbb{Z}$.

Tais equações são chamadas equações diofantinas lineares em homenagem a Diofanto de Alexandria (aproximadamente 300 d.C.). "Diofanto de Alexandria foi um importante matemático grego do século III a.C. e que atualmente é algumas vezes citado como 'o pai da álgebra'. Viveu em uma importante cidade que era centro de atividades matemáticas da Grécia antiga. Não se sabe muito sobre a vida desse matemático. Em seu túmulo foram encontrados versos com problemas enigmáticos, pelos quais deduz-se que ele viveu 84 anos"(Vieira, 2018).

Figura 5 – Diofanto de Alexandria.

Fonte: (Oduenyi, 2017)

Proposição 2.7.1. *Sejam $a,b,c \in \mathbb{Z}$. A equação $aX+bY=c$ admite solução em números inteiros se, e somente se, $mdc(a,b) \mid c$.*

Demonstração: Suponha que a equação $aX+bY=c$ admite solução em números inteiros, isto é, existem x_0, $y_0 \in \mathbb{Z}$ tais que $ax_0+by_0=c$. Como $mdc(a,b) \mid a$ e $mdc(a,b) \mid b$, pela Proposição 2.1.9 segue que $mdc(a,b) \mid c$.

Vamos agora provar a recíproca. Seja $mdc(a,b)=d$. Se $d \mid c$, então existe $k \in \mathbb{Z}$ tal que $dk=c$. Pelo Teorema 2.5.1, existem $x_0, y_0 \in \mathbb{Z}$, com $d=ax_0+by_0$. Disso segue que $c=a(k\cdot x_0)+b(k\cdot y_0)$, o que implica que $k\cdot x_0$ e $k\cdot y_0$ é uma solução particular de $aX+bY=c$. □

Proposição 2.7.2. *Seja $x_0, y_0 \in \mathbb{Z}$ uma solução da equação $aX+bY=c$, onde $mdc(a,b)=1$. Então, as soluções, $x,y \in \mathbb{Z}$ da equação são da forma*

$$x=x_0+tb, \quad y=y_0-ta; \text{ onde } t \in \mathbb{Z}.$$

Demonstração: Seja x,y uma solução para equação $aX+bY=c$, logo,

$$ax_0+by_0=ax+by=c.$$

Consequentemente,

$$a(x-x_0)=b(y_0-y). \tag{1}$$

Como $mdc(a,b)=1$, segue que $b \mid (x-x_0)$. Logo,

$$x-x_0=tb, \quad t \in \mathbb{Z},$$
$$x=x_0+tb.$$

Substituindo a expressão de $x - x_0$ acima em (1), segue-se que

$$y_0 - y = ta,$$
$$y = y_0 - ta$$

o que prova que as soluções são do tipo exibido.

Por outro lado, x, y, como enuciado, é solução, pois

$$ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + atb + by_0 - atb = ax_0 + by_0 = c.$$

□

Exemplo 2.7.3. Resolva em $\mathbb{Z}$ a equação $45X + 14Y = 11$.

Solução: Perceba que $mdc(45, 14) = 1$. Como $1 \mid 11$, há solução inteira.

Refazendo o Algoritmo de Euclides de forma a expressar 1 como combinação de 45 e 14, encontramos que:

$$45 \cdot 5 + 14 \cdot (-16) = 1.$$

Multiplicando por 11, obtemos:

$$45 \cdot 55 + 14 \cdot (-176) = 11.$$

Logo, uma solução particular é:

$$x_0 = 55, \qquad y_0 = -176$$

Portanto, a solução geral é:

$$X = 55 + 14t$$
$$Y = -176 - 45t$$

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

2.8 Congruências

Em Teoria dos Números, congruência é um conceito fundamental que expressa quando dois números inteiros têm o mesmo resto quando divididos por um determinado inteiro positivo.

Dados $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$, dizemos que a é *congruente* a b módulo m, e escrevemos

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

se a e b deixam o mesmo resto na divisão por m.

Quando a relação $a \equiv b \pmod{m}$ for falsa, diremos que a e b *não são congruentes*, ou que são *incongruentes*, módulo m. Escreveremos, nesse caso, $a \not\equiv b \pmod{m}$.

Proposição 2.8.1. *Sejam $a, b, m \in \mathbb{Z}$, com $m > 0$. Então, $a \equiv b \pmod{m}$ se, e somente se, $m \mid b - a$.*

Demonstração: Pelo algoritmo de divisão, podemos escrever

$$a = mq_1 + r_1 \quad \text{e} \quad b = mq_2 + r_2$$

onde $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Sem perda de generalidade, podemos supor que $r_1 \leq r_2$. Podemos escrever então

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

Logo, $m \mid b - a$ se, e somente se, $m \mid r_2 - r_1$. Por ser $0 \leq r_2 - r_1 < m$, segue que $m \mid b - a$ se, e somente se, $r_2 - r_1 = 0$, ou seja, $r_2 = r_1$. □

Definição 2.8.2. Um *sistema completo de resíduos módulo m* é qualquer conjunto de m números inteiros tais que seus restos na divisão por m correspondam exatamente aos números

$$0, 1, 2, ..., m - 1,$$

sem repetições, podendo estar em qualquer ordem.

Propriedade Característica: Se $a_1, ..., a_m$ são m números inteiros dois a dois não congruentes módulo m, então eles formam um sistema completo de resíduos módulo m. De fato, como os m números são não congruentes dois a dois, seus restos na divisão por m são todos distintos. Logo, esses restos devem ser exatamente os inteiros de 0 a $m - 1$, em alguma ordem.

Proposição 2.8.3. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a \pm c \equiv b \pm d \pmod{m}$.*

Demonstração: Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $m \mid (b-a)$ e $m \mid (d-c)$. Logo, m divide

$$(b-a) \pm (d-c) = (b \pm d) - (a \pm c)$$

mostrando que $(b \pm d) \equiv (a \pm c) \pmod{m}$.

Concluímos, então, que as congruências de mesmo módulo somam-se e se subtraem membro a membro tal qual as igualdades. □

Corolário 2.8.4. *Sejam a e b dois números inteiros tais que* $a \equiv b \pmod{m}$. *Então, sendo c outro número inteiro, tem-se que* $(a \pm c) \equiv (b \pm c) \pmod{m}$.

Demonstração: Como $c \equiv c \pmod{m}$, pela proposição anterior, temos o resultado.

Proposição 2.8.5. *Sejam* $a,b,c,d,m \in \mathbb{Z}$, *com* $m > 1$. *Se* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então* $a \cdot c \equiv b \cdot d \pmod{m}$.

Demonstração: Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, $m \mid (a-b)$ e $m \mid (c-d)$. Como

$$a \cdot c - b \cdot d = a(c-d) + d(a-b),$$

segue da Proposição 2.1.9 que $m \mid a \cdot c - b \cdot d$, então $a \cdot c \equiv b \cdot d \pmod{m}$. □

Corolário 2.8.6. *Sejam dois números inteiros tais que* $a \equiv b \pmod{m}$. *Logo, sendo c outro número inteiro, tem-se que* $(a \cdot c) \equiv (b \cdot c) \pmod{m}$.

Demonstração: Como $c \equiv c \pmod{m}$, pela proposição anterior, temos o resultado. □

Corolário 2.8.7. *Para todo* $n \in \mathbb{N}$, $a,b \in \mathbb{Z}$, *se* $a \equiv b \pmod{m}$, *então tem-se que* $a^n \equiv b^n \pmod{m}$.

Demonstração: Vamos provar esse corolário, usando Indução Finita sobre n.

Caso base: Para $n = 1$ o resultado é válido pela hipótese.
Hipótese de indução: Suponhamos que a propriedade seja válida para algum n natural.
Passo indutivo: Mostraremos que $a^{n+1} \equiv b^{n+1} \pmod{n}$

Usando a hipótese e a proposição 2.8.5, obtemos o resultado. □

Exemplo 2.8.8. Calcular o resto da divisão de $5^{131} + 7^{131} + 11^{131} + 13^{131}$ por 9.

Solução: Perceba que

$$5 \equiv -4 \pmod 9 \Rightarrow 5^{131} \equiv (-4)^{131} \pmod 9$$
$$7 \equiv -2 \pmod 9 \Rightarrow 7^{131} \equiv (-2)^{131} \pmod 9$$
$$11 \equiv 2 \pmod 9 \Rightarrow 11^{131} \equiv 2^{131} \pmod 9$$
$$13 \equiv 4 \pmod 9 \Rightarrow 13^{131} \equiv 4^{131} \pmod 9.$$

Logo, teremos

$$5^{131} + 7^{131} + 11^{131} + 13^{131} \equiv -4^{131} - 2^{131} + 2^{131} + 4^{131} \equiv 0 \pmod 9.$$

Portanto, o resto da divisão da expressão numérica por 9 será 0.

Proposição 2.8.9. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Tem-se que*

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

Demonstração: Observe que

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

como $\dfrac{m}{(c,m)}$ e $\dfrac{c}{(c,m)}$ são coprimos, temos que

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

□

Proposição 2.8.10. *Se $a \equiv b \pmod{m_1}$, ..., $a \equiv b \pmod{m_n}$, onde $a, b, m_1, ..., m_n \in \mathbb{Z}$, com $m_i > 1$ para $i = 1, ..., n$. Então*

$$a \equiv b \pmod{[m_1, ..., m_n]},$$

onde $[m_1, ..., m_n]$ é o mínimo múltiplo comum dos números $m_1, ..., m_n$.

Demonstração: Se $a \equiv b \pmod{m_i}$, então $m_i \mid (b-a)$ para todo $i \in \{1, 2, ..., n\}$. Sendo $b-a$ um múltiplo de cada m_i, segue-se que $[m_1, ..., m_n] \mid b-a$, o que prova que prova que $a \equiv b \pmod{[m_1, ..., m_n]}$. □

2.9 Função Totiente de Euler

Leonhard Paul Euler é universalmente reconhecido como um dos matemáticos mais prolíficos e influentes de todos os tempos. Nascido em Basel, Suíça, em 15 de abril de 1707, sua produção intelectual extraordinária moldou fundamentalmente o desenvolvimento da matemática pura e aplicada, estabelecendo alicerces que permanecem vitais até os dias atuais.

Figura 6 – Leonhard Paul Euler.

Fonte: (Wikipédia, 2020)

Na teoria dos números, Euler estabeleceu resultados monumentais como o Teorema de Euler, generalizando o Pequeno Teorema de Fermat através da função totiente $\phi(m)$, e desenvolveu métodos analíticos que abriram caminho para a demonstração futura do teorema dos números primos.

Definição 2.9.1. Dado $m \in \mathbb{N}$, denotamos por $\phi(m)$ (função totiente de Euler) a quantidade de inteiros positivos menores do que m que são coprimos com m.

Lema 2.9.2. *Se p é primo e k natural, então $\phi(p^k) = p^{k-1} \cdot (p-1)$.*

Demonstração: Os inteiros de 1 a p^k que não são coprimos com p^k são exatamente aqueles divisíveis por p, ou seja, os elementos do conjunto $\{1,\ 2,\ 3,\ ...,\ p^k\}$ que são não coprimos com p^k são os elementos do conjunto $\{p,\ 2p,\ 3p,\ ...,\ p^k\}$. Logo teremos p^{k-1} números não coprimos com p^k. Como o total de inteiros de 1 até p^k é p^k e o total de inteiros não coprimos com p^k nesse intervalo é p^{k-1}, teremos que $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. □

Lema 2.9.3. *Sejam m e l primos entre si e $r \in \mathbb{Z}$. Então $\{r,\ r+l,\ r+2l,\ ...,\ r+(m-1)l\}$ é um sistema completo de resíduos módulo m.*

Demonstração: Suponha por absurdo que existem $i, j \leq m-1,\ i \neq j$ tais que

$$r+i\cdot l \equiv r+j\cdot l \pmod{m} \Rightarrow l(i-j)\equiv 0 \pmod{m}.$$

Como l e m são primos entre si, então teremos $i-j\equiv 0 \pmod{m}$, absurdo, pois $i,j\leq m-1$, $i\neq j$. Logo, concluímos que $i=j$. Portanto, elementos distintos no conjunto são incongruentes módulo m. Temos m elementos, todos incongruentes dois a dois módulo m. Isso significa que seus restos na divisão por m são todos diferentes. Como só existem m restos possíveis $0,1,...,m-1$, esses m elementos cobrem exatamente cada resto possível uma única vez. Sendo assim, conjunto $\{r+i\cdot l \ ; \ i=0,1,2,...,m-1\}$ é um sistema completo de resíduos módulo m.

Teorema 2.9.4. *Se l e m são primos entre si, então $\phi(m\cdot l)=\phi(m)\cdot\phi(l)$.*

Demonstração: Sejam $l,m\in\mathbb{N}$ com $mdc(l,m)=1$. Considere os números de 0 a $lm-1$. Podemos organizá-los em uma tabela $l\times m$.

0	1	$\cdots$	$m-1$
m	$m+1$	$\cdots$	$2m-1$
$2m$	$2m+1$	$\cdots$	$3m-1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$(l-1)m$	$(l-1)m+1$	$\cdots$	$lm-1$

Tabela 3 – Números de 0 a $lm-1$

Cada elemento da tabela pode ser escrito como:

$$a=q\cdot m+r, \ \text{ com } 0\leq q\leq l-1 \ \text{ e } \ 0\leq r\leq m-1.$$

Pelo Teorema 2.5.4, um número $a=q\cdot m+r$ é coprimo com m se, e somente se, $mdc(r,m)=1$. Por definição, há exatamente $\phi(m)$ valores de r com $0\leq r\leq m-1$ tais que $mdc(r,m)=1$.

Para um r fixo com $mdc(r,m)=1$, considere a coluna correspondente:

$$r, \ m+r, \ 2m+r, \ \ldots \ , \ (l-1)m+r$$

Esta é uma progressão aritmética módulo l. Como $mdc(m,l)=1$, pelo lema 2.9.3 estes l números formam um sistema completo de resíduos módulo l. Portanto, exatamente $\phi(l)$ deles são coprimos com l.

Pelo Corolário 2.6.4,

$$mdc(a,lm)=1 \iff mdc(a,l)=mdc(a,m)=1.$$

Logo, para cada um dos $\phi(m)$ valores de r coprimos com m, temos $\phi(l)$ valores de q tais que $a = q \cdot m + r$ é coprimo com l. Portanto, o número total de inteiros a com $0 \leq a \leq lm-1$ e $mdc(a,lm) = 1$ é $\phi(lm) = \phi(l) \cdot \phi(m)$. □

Corolário 2.9.5. *Se* $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, *então* $\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$.

Demonstração: Como $\phi(m) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})$, pelo Teorema 2.9.4, teremos:

$$\phi(m) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k}).$$

E pelo Lema 2.9.2, podemos escrever a igualdade acima, da seguinte forma:

$$\phi(m) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1).$$

Multiplicando o lado direito da igualdade acima por $1 = \dfrac{p_1 p_2 \cdots p_k}{p_1 p_2 \cdots p_k}$ e organizando os termos, teremos:

$$\phi(m) = \left[\frac{p_1}{p_1} \cdot p_1^{\alpha_1 - 1}(p_1 - 1)\right] \cdot \left[\frac{p_2}{p_2} \cdot p_2^{\alpha_2 - 1}(p_2 - 1)\right] \cdots \left[\frac{p_k}{p_k} \cdot p_k^{\alpha_k - 1}(p_k - 1)\right]$$

$$\Rightarrow \phi(m) = p_1^{\alpha_1}\left(\frac{p_1 - 1}{p_1}\right) \cdot p_2^{\alpha_2}\left(\frac{p_2 - 1}{p_2}\right) \cdots p_k^{\alpha_k}\left(\frac{p_k - 1}{p_k}\right).$$

Como $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, segue o resultado,

$$\phi(m) = m \cdot \left(\frac{p_1 - 1}{p_1}\right) \cdot \left(\frac{p_2 - 1}{p_2}\right) \cdots \left(\frac{p_k - 1}{p_k}\right) = m \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

□

Teorema 2.9.6. ***(Teorema de Euler)*** *Se* $a, m \in \mathbb{Z}$ *com* $m > 1$ *e* $mdc(a,m) = 1$. *Então,*

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

Demonstração: Seja $\{r_1, r_2, ..., r_{\phi(m)}\}$ o conjunto dos restos primos com m. Então os elementos do conjunto $A = \{ar_1, ar_2, ..., ar_{\phi(m)}\}$ também são restos primos com m, pois, $mdc(a,m) = mdc(r_i,m) = 1$ e, portanto, $mdc(ar_i,m) = 1$. Se

$$ar_i \equiv ar_j \pmod{m},$$

como $mdc(a,m) = 1$, pela Proposição 2.8.9, temos que $r_i \equiv r_j \pmod{m}$. Logo, $i = j$. Com isso, podemos concluir que os elementos de A são distintos módulo m. Portanto, A é uma permutação de $\{r_1, r_2, ..., r_{\phi(m)}\}$ módulo m.

Multiplicando todos os elementos de cada conjunto:

$$r_1 \cdot r_2 \cdots r_{\phi(m)} \equiv ar_1 \cdot ar_2 \cdots ar_{\phi(m)} = a^{\phi(m)} \cdot r_1 \cdot r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Como $mdc(r_1 \cdot r_2 \cdots r_{\phi(m)}, m) = 1$, e usando novamente a Proposição 2.8.9, podemos cancelar este produto em ambos os lados. Resultando em:

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

□

Perceba que o Teorema 2.6.7 (Pequeno teorema de Fermat) é uma aplicação do Teorema 2.9.6 (Teorema de Euler). Basta notar que, sendo p primo, $\phi(p) = p - 1$. Portanto,

$$a^{\phi(p)} \equiv 1 \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}.$$

Exemplo 2.9.7. Ache os últimos 3 dígitos de 7^{9999}.

Solução: Como $1000 = 2^3 \cdot 5^3$, utilizando o Corolário 2.9.5, temos que

$$\phi(1000) = \phi(2^3 \cdot 5^3) = 1000 \cdot (1 - \tfrac{1}{2}) \cdot (1 - \tfrac{1}{5}) = 400.$$

Sendo $mdc(7, 1000) = 1$, pelo Teorema 2.9.6, teremos a seguinte congruência:

$$\begin{gathered} 7^{400} \equiv 1 \pmod{1000} \\ \Rightarrow (7^{400})^{25} \equiv 1^{25} \pmod{1000} \\ \Rightarrow 7^{10000} \equiv 1 \pmod{1000}. \end{gathered}$$

Da congruência acima, temos que

$$\begin{gathered} 7^{10000} = 1000k + 1 = 1000(k-1) + 1001 = 1000(k-1) + 7 \cdot 143, \text{ com } k \in \mathbb{Z} \\ \Rightarrow 7^{10000} \equiv 7 \cdot 143 \pmod{1000} \end{gathered}$$

Da Proposição 2.8.9, podemos cancelar um fator 7 de ambos os lados da congruência, resultando em

$$7^{9999} \equiv 143 \pmod{1000}.$$

E portanto, o valor dos últimos 3 digitos de 7^{9999} é 143.

Definição 2.9.8. Seja $m \in \mathbb{Z}$, tal que $m > 1$. Seja $\mathbb{Z}_m^*$ o conjunto que contém os números i tal que $1 \leq i \leq m-1$ e $mdc(i,m) = 1$. Dizemos que a *ordem* deste conjunto (o número de elementos) é dada pela função totiente de Euler, $\phi(m)$.

Definição 2.9.9. Um número g é uma *raiz primitiva módulo m* se para cada inteiro $b \in \mathbb{Z}_m^*$, existe um inteiro $1 \leq k \leq m-1$, tal que

$$g^k \equiv b \pmod{m}.$$

Em outras palavras, dizemos que g gera o grupo multiplicativo $\mathbb{Z}_m^*$. Ou seja, g é raiz primitiva se, e somente se, g é um gerador do grupo multiplicativo de inteiros módulo n.

Exemplo 2.9.10. Mostre que o número 2 é raiz primitiva módulo 5, ou seja, que $g = 2$ gera $\mathbb{Z}_5^*$.

Solução: Perceba que $\mathbb{Z}_5^* = \{1,2,3,4\}$, logo $\phi(5) = 4$. Então:

$$2^4 \equiv 1 \pmod{5};$$
$$2^1 \equiv 2 \pmod{5};$$
$$2^3 \equiv 3 \pmod{5};$$
$$2^2 \equiv 4 \pmod{5}.$$

Logo para quaisquer $b \in \mathbb{Z}_5^*$, temos que existe $1 \leq k \leq 4$ tal que $2^k \equiv b \pmod{5}$. Portanto, 2 é raiz primitiva módulo 5.

2.10 Congruência Linear

Nesta seção, buscaremos resolver congruências da forma $aX \equiv b \pmod{m}$.

Definição 2.10.1. Seja $m > 1$ um inteiro. Chamamos de *congruência linear* a toda equação da forma:

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

onde $a, b, X \in \mathbb{Z}$, onde X são as soluções procuradas.

Proposição 2.10.2. *A congruência linear* $aX \equiv b \pmod{m}$ *possui solução se, e somente se, o máximo divisor comum de a e m divide b, ou seja,*

$$aX \equiv b \pmod{m} \Longleftrightarrow (a,m) \mid b.$$

Demonstração: $\Rightarrow$ Se $ax \equiv b \pmod{m}$, então $x \in \mathbb{Z}$ é solução, isto é, $m \mid ax - b$. Então para um certo k inteiro, teremos $ax - mk = b$, oque implica que a equação $ax + m(-k) = b$ admite solução e, pela Proposição 2.7.1, temos que $mdc(a,m) \mid b$.

$\Leftarrow$ Se $mdc(a,m) \mid b$, utilizando novamente a proposição 2.7.1, a equação $aX + mK = b$ admite uma solução $\{x,k\}$. Portanto, $ax = b - mk$, ou seja, x é solução de $ax \equiv b \pmod{m}$. □

Exemplo 2.10.3. A congruência linear $6x \equiv 8 \pmod{20}$ tem solução, pois $mdc(6,20) = 2$ e $2 \mid 8$. Em particular, $x = 8$ é solução.

Exemplo 2.10.4. A congruência linear $5x \equiv 8 \pmod{20}$ não tem solução, pois $mdc(5,20) = 5$ e $5 \nmid 8$.

Teorema 2.10.5. *Seja $a, b \in \mathbb{Z}$, com $m > 1$ e $mdc(a,m) \mid b$. Se x_0 é uma solução da congruência $aX \equiv b \pmod{m}$, então*

$$x_0, x_0 + \tfrac{m}{d}, x_0 + \tfrac{2m}{d}, \cdots, x_0 + \tfrac{m(d-1)}{d},$$

onde $d = mdc(a,m)$, formam um sistema completo de soluções da mesma congruência.

Demonstração: Veja (Hefez, 2022, p. 209). □

Corolário 2.10.6. *Se $mdc(a,m) = 1$, então a congruência $aX \equiv b \pmod{m}$ possui uma única solução módulo m.*

Demonstração: Decorre diretamente do teorema anterior. □

A congruência $aX \equiv 1 \pmod{m}$, com $mdc(a,m) = 1$, admite uma única solução módulo m. Esta solução é chamada de inverso multiplicativo de a módulo m.

Corolário 2.10.7. *Toda congruência do tipo $aX \equiv b \pmod{m}$ que tem solução é equivalente a uma congruência do tipo*

$$X \equiv c \pmod{n}.$$

Demonstração: Perceba que se a congruência

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

admite solução, então o $d = mdc(a,m) | b$. Por definição, $d \mid a$ e $d \mid m$.

Tomando

$$a' = \frac{a}{d}, \qquad b' = \frac{b}{d}, \qquad n = \frac{m}{d},$$

temos pela Proposição 2.8.9 que a congruência acima é equivalente à

$$a'X \equiv b' \pmod{n}, \text{ com } mdc(a,n) = 1.$$

Como $mdc(a',n) = 1$, existe inverso multiplicativo a'' de a módulo n. Multiplicando a última congruência por a'' obtemos:

$$X \equiv c \pmod{n},$$

onde $c = a'' \cdot b'$.

□

3 CHRYZODES

A relação entre aritmética e um círculo e linhas, que representam suas intersecções, proporciona uma ferramenta surpreendente. Uma das novidades surge da aplicação de um círculo, onde são inscritas sequências numéricas empregadas operações como adição, multiplicação, etc. A fim de demonstrar a extraordinária criatividade dessa abordagem, deu a esses gráficos o nome de chryzode "deriva do grego chrysos (escrita em ouro) e zoide (círculo), ou seja, escrita de ouro em um círculo" (Bello, 2011, p. 41).

Os chryzodes vão muito além de uma definição fixa e fechada. Na verdade, eles se mostram como objetos matemáticos extremamente ricos, que criam conexões entre a geometria tradicional, áreas mais abstratas como a teoria dos grafos, e até mesmo manifestações que encontramos na arte e no dia a dia. Neste capítulo, vamos explorar exatamente essa diversidade, organizando a discussão em quatro seções.

A primeira seção, é dedicada as construções e aos resultados fundamentais relacionados aos chryzodes. São apresentados os métodos geométricos clássicos para a sua geração, bem como os principais resultados que delineiam as suas propriedades estruturais. A segunda seção investiga a presença e o significado dos chryzodes na teoria dos grafos, em particular sobre os grafos hamiltonianos. Na terceira seção, aprofunda-se a análise de sua natureza epicicloidal, examinando como os chryzodes podem ser compreendidos como generalizações ou composições desses movimentos cíclicos. Por fim, a quarta seção amplia o horizonte da investigação para além do domínio estritamente matemático, ao explorar a presença dos chryzodes na arte e na vida por meio da análise de manifestações artísticas, padrões ornamentais e estruturas arquitetônicas.

3.1 Construção e resultados sobre os chryzodes

Fixados $m, a \in \mathbb{N}$, seja $C_a : \{0,1,...,m-1\} \to \{0,1,...,m-1\}$ a função definida por $C_a(i) = b_i$, onde $i \cdot a \equiv b_i \pmod{m}$. A função C_a está bem definida, pois a congruência $i \cdot a \equiv b_i \pmod{m}$ associa, para cada i, um único resto b_i dentro do conjunto estipulado.

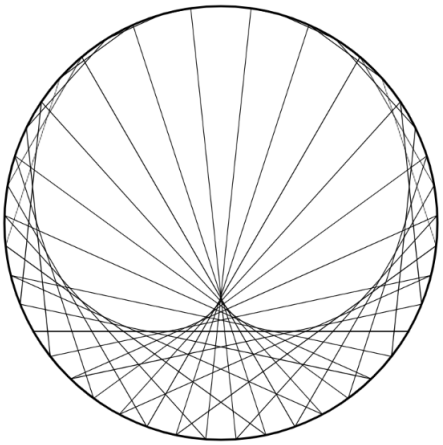
Definição 3.1.1. No plano, considere os pontos $P_i = \left(sen\ \frac{2\pi i}{m}, cos\ \frac{2\pi i}{m}\right)$, com $i = 0, 1, ..., m-1$, os quais estão sobre o círculo unitário. Um *chryzode* $C_a(m)$ de multiplicidade a e cardinalidade m, é a figura geométrica formada pela união do círculo com o conjunto de todas as cordas que ligam cada ponto P_i ao ponto P_{b_i}, isto é,

$$\bigcup_{i=0}^{m-1} \overline{P_i P_{b_i}},$$

onde $b_i \in \{0, 1, ..., m-1\}$, com $i \cdot a \equiv b_i \pmod{m}$.

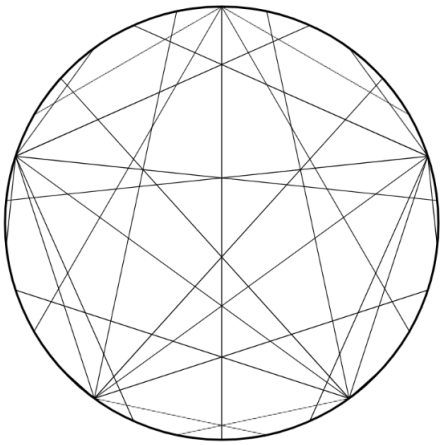
Na Figura 7 e na Figura 8 temos exemplos de chryzodes, gerados através do software Geogebra.

Figura 7 – Chryzode $C_2(45)$.



Fonte: Autor.

Figura 8 – Chryzode $C_{12}(30)$.



Fonte: Autor.

Para construir os chryzodes, distribuem-se m pontos igualmente espaçados em uma circunferência. Cada ponto P recebe um número sequencial de 0 a $(m-1)$. Posteriormente, calculam-se os valores dos restos b_i, os quais são utilizados para realizar o mapeamento das conexões $P_i \to P_{b_i}$, ou seja:

$$\begin{gathered} 0 \cdot a \equiv 0 \pmod{m}; \\ 1 \cdot a \equiv b_1 \pmod{m}; \\ 2 \cdot a \equiv b_2 \pmod{m}; \\ \vdots \\ (m-2) \cdot a \equiv b_{m-2} \pmod{m}; \\ (m-1) \cdot a \equiv b_{m-1} \pmod{m}. \end{gathered}$$

De maneira geral,

$$i \cdot a \equiv b_i \pmod{m}$$

para $i = 0, 1, ..., m-1$.

Em seguida, conecta-se cada ponto P_i por um segmento de reta ao ponto cuja posição é congruente a $i \cdot a \pmod{m}$, isso é, liga-se P_i aos pontos P_{b_i}, sendo a um número natural pré-definido. Portanto os chryzodes também são frequentemente apresentados, como uma visualização da operação de multiplicação por a, num módulo m.

Como um chryzode é definido a partir da função C_a, para cada elemento i do domínio existe exatamente um correspondente $b_i = C_a(i)$ no contradomínio. Em particular, temos $0 \cdot a \equiv 0 \pmod{m}$, ou seja, $C_a(0) = 0$. Dessa forma, o ponto P_0 dá origem a um segmento nulo, pois não produz nenhuma corda. Para qualquer outro ponto P_i, ou também se forma um segmento nulo (quando $C_a(i) = i$), ou se forma exatamente uma corda (quando $C_a(i) = b_i$, com $i \neq b_i$). Com base nisso, para $i = 0, 1, ..., m-1$, consideraremos qualquer segmento nulo $\overline{P_i P_i}$ como um elemento do conjunto formado pelas cordas do chryzode.

Exemplo 3.1.2. (Construção do chryzode de mutiplicidade 9 e cardinalidade 12). Para construirmos tal chryzode, distribuímos 12 pontos equidistantes e enumerados de 0 até 11 ao longo de uma circunferência. Em seguida construímos segmentos ligando o ponto P_i ao ponto congruente a $P_i \cdot 9 \pmod{12}$. Temos, portanto, a seguinte sequência de congruências:

$$0 \cdot 9 \equiv 0 \pmod{12} \qquad 4 \cdot 9 = 36 \equiv 0 \pmod{12} \qquad 8 \cdot 9 = 72 \equiv 0 \pmod{12}$$

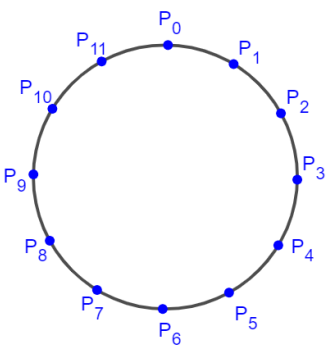
$$1 \cdot 9 \equiv 9 \pmod{12} \qquad 5 \cdot 9 = 45 \equiv 9 \pmod{12} \qquad 9 \cdot 9 = 81 \equiv 9 \pmod{12}$$

$$2 \cdot 9 = 18 \equiv 6 \pmod{12} \qquad 6 \cdot 9 = 54 \equiv 6 \pmod{12} \qquad 10 \cdot 9 = 90 \equiv 6 \pmod{12}$$

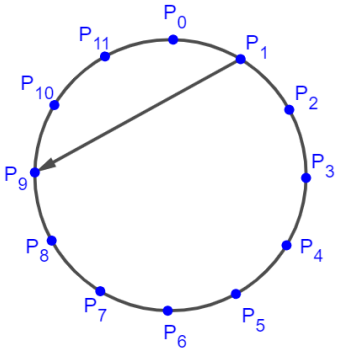
$$3 \cdot 9 = 27 \equiv 3 \pmod{12} \qquad 7 \cdot 9 = 63 \equiv 3 \pmod{12} \qquad 11 \cdot 9 = 99 \equiv 3 \pmod{12}$$

As figura a seguir, apresentam os passos de construção.

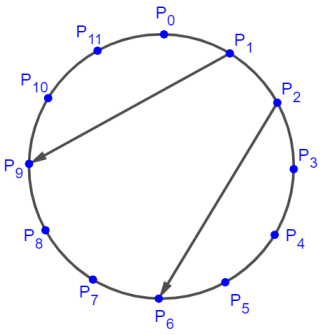
Figura 9 – Construção do Chryzode $C_9(12)$



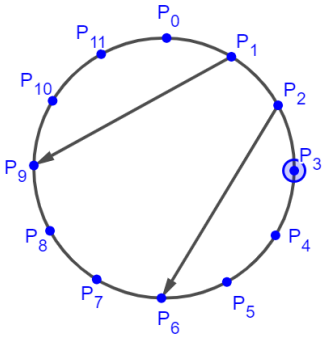
$0 \cdot 9 \equiv 0 \pmod{12}$



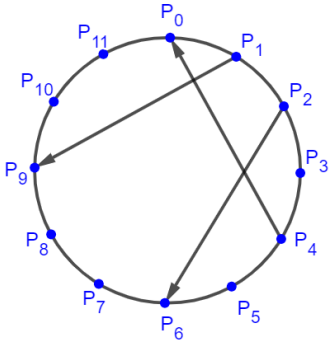
$1 \cdot 9 \equiv 9 \pmod{12}$



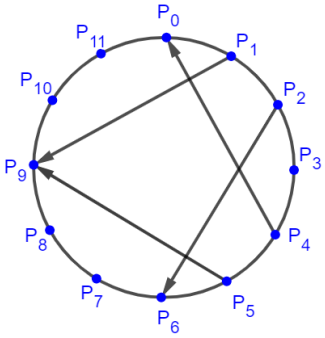
$2 \cdot 9 \equiv 6 \pmod{12}$



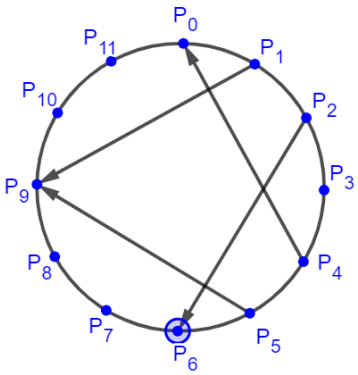
$3 \cdot 9 \equiv 3 \pmod{12}$



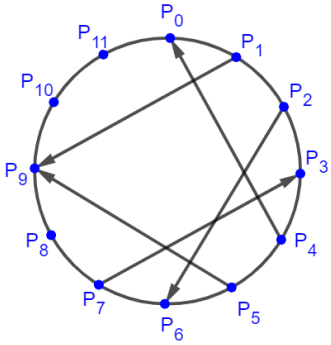
$4 \cdot 0 \equiv 9 \pmod{12}$



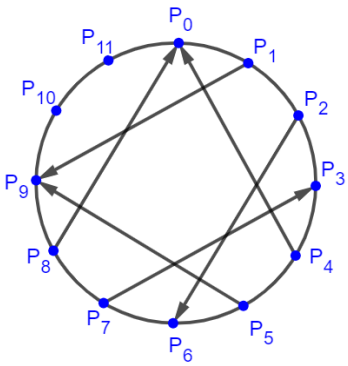
$5 \cdot 9 \equiv 9 \pmod{12}$



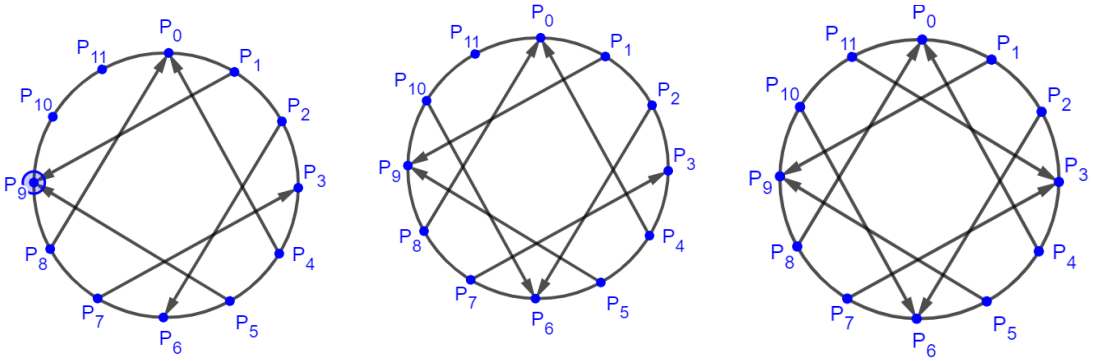
$6 \cdot 9 \equiv 6 \pmod{12}$



$7 \cdot 9 \equiv 3 \pmod{12}$



$8 \cdot 9 \equiv 0 \pmod{12}$



$9 \cdot 9 \equiv 9 \pmod{12}$ $10 \cdot 9 \equiv 6 \pmod{12}$ $11 \cdot 9 \equiv 3 \pmod{12}$

Fonte: Autor.

Exemplo 3.1.3. (Construção do Chryzode de multiplicidade 2 e cardinalidade 11). Para construirmos tal chryzode, distribuímos 11 pontos equidistantes e enumerados de 0 até 10 ao longo de uma circunferência. Em seguida construímos segmentos ligando cada ponto P_i ao ponto congruente a $P_i \cdot 2 \pmod{11}$. Temos, portanto, a seguinte sequência de congruências:

$$0 \cdot 2 \equiv 0 \pmod{11} \qquad 6 \cdot 2 = 12 \equiv 1 \pmod{11}$$

$$1 \cdot 2 \equiv 2 \pmod{11} \qquad 7 \cdot 2 = 14 \equiv 3 \pmod{11}$$

$$2 \cdot 2 = 4 \equiv 4 \pmod{11} \qquad 8 \cdot 2 = 16 \equiv 5 \pmod{11}$$

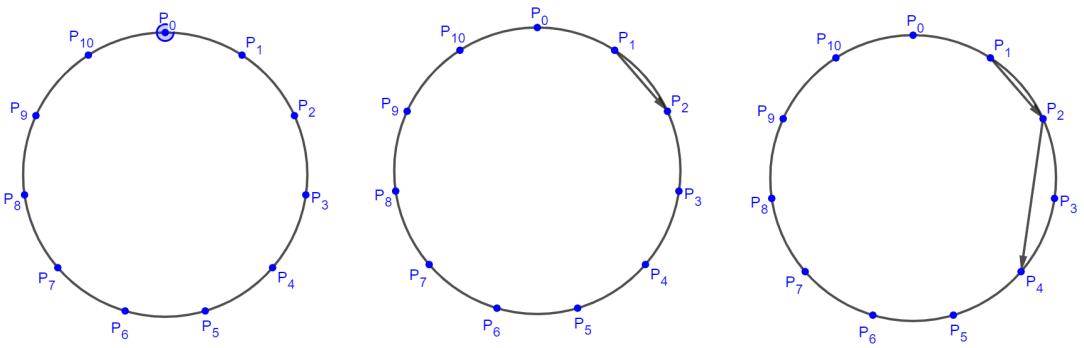
$$3 \cdot 2 = 6 \equiv 6 \pmod{11} \qquad 9 \cdot 2 = 18 \equiv 7 \pmod{11}$$

$$4 \cdot 2 = 8 \equiv 8 \pmod{11} \qquad 10 \cdot 2 = 20 \equiv 9 \pmod{11}$$

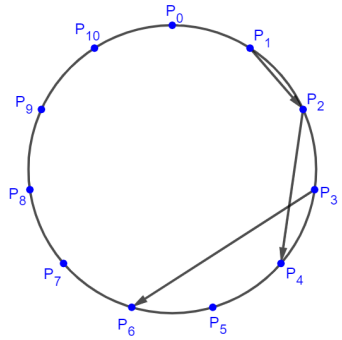
$$5 \cdot 2 = 10 \equiv 10 \pmod{11}$$

A Figura 10 a seguir, apresenta os passos de construção.

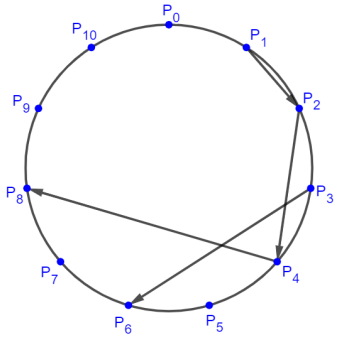
Figura 10 – Construção do Chryzode $C_2(11)$.



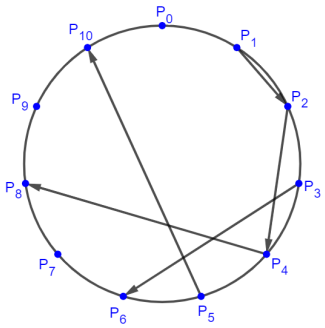
$0 \cdot 2 \equiv 0 \pmod{11}$ $1 \cdot 2 \equiv 2 \pmod{11}$ $2 \cdot 2 \equiv 4 \pmod{11}$



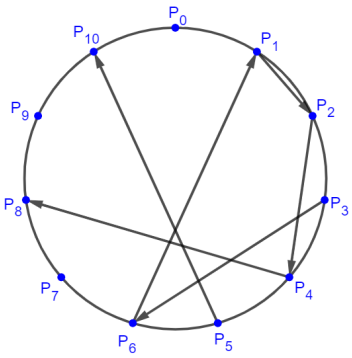
$3 \cdot 2 \equiv 6 \pmod{11}$



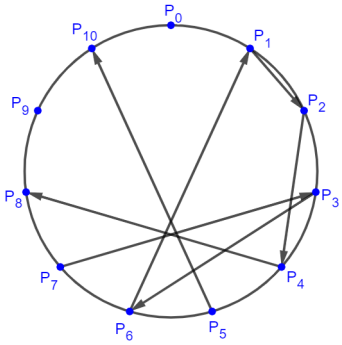
$4 \cdot 2 \equiv 8 \pmod{11}$



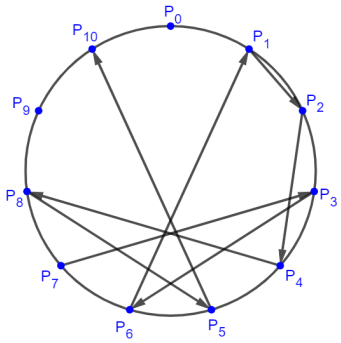
$5 \cdot 2 \equiv 10 \pmod{11}$



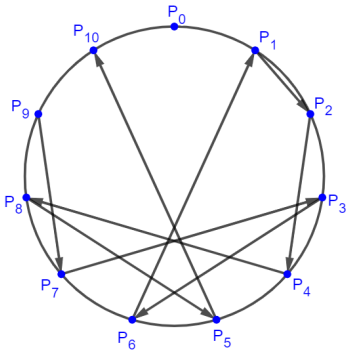
$6 \cdot 2 \equiv 1 \pmod{11}$



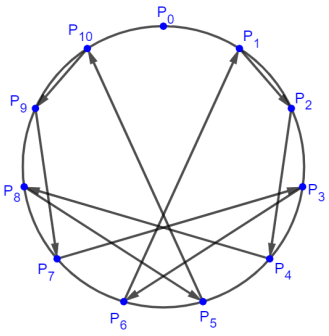
$7 \cdot 2 \equiv 3 \pmod{11}$



$8 \cdot 2 \equiv 5 \pmod{11}$



$9 \cdot 2 \equiv 7 \pmod{11}$

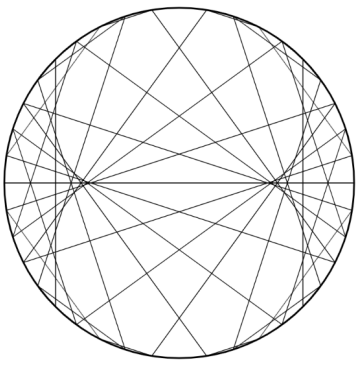


$10 \cdot 2 \equiv 9 \pmod{11}$

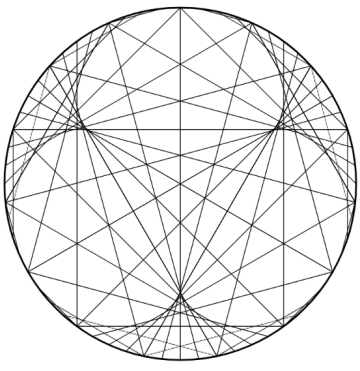
Fonte: Autor.

Segue adiante mais alguns exemplos de chryzodes.

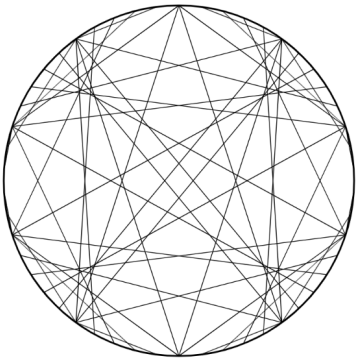
Figura 11 – Outros exemplos de chryzodes.



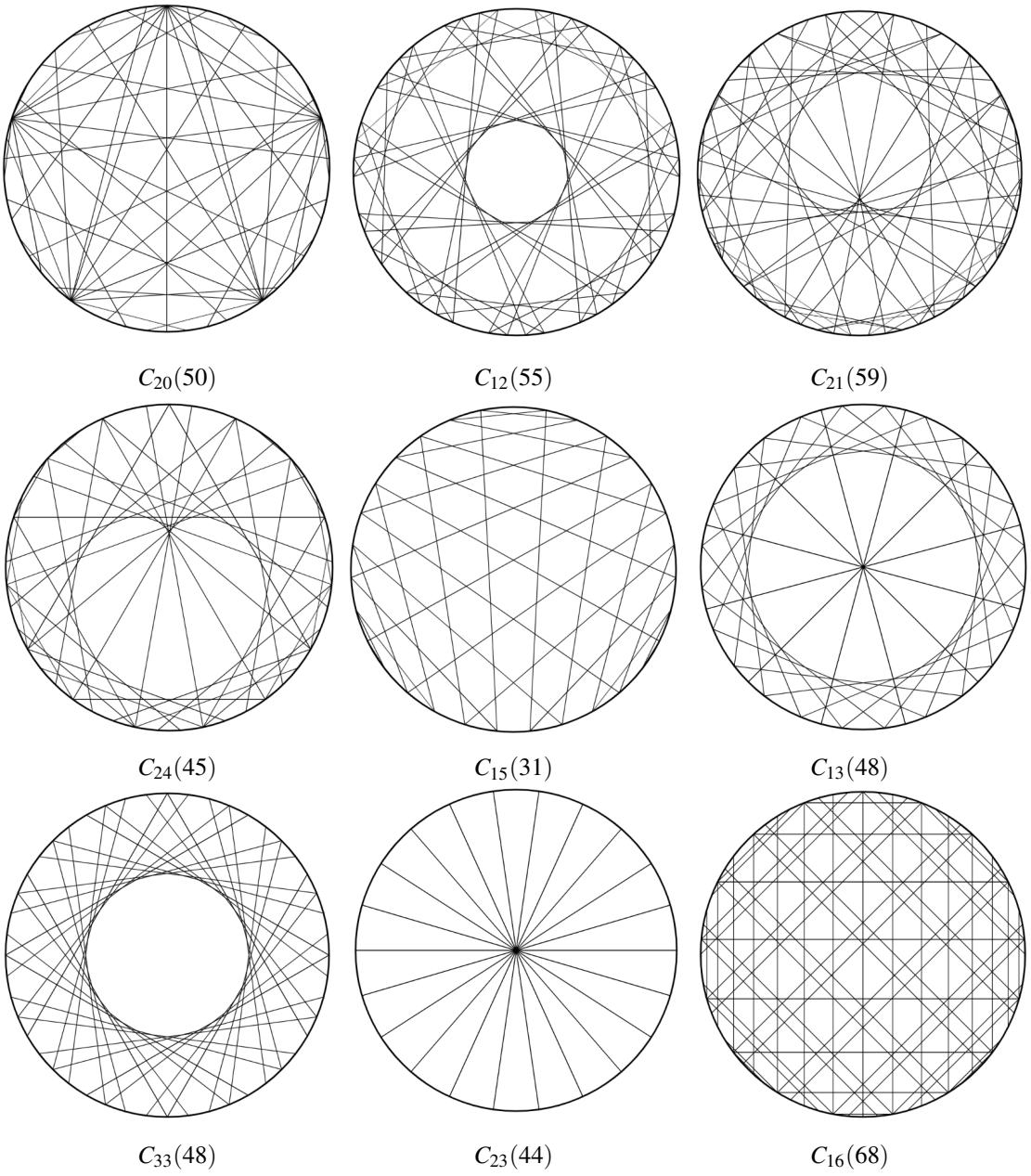
$C_3(40)$



$C_4(60)$



$C_5(50)$



$C_{20}(50)$ $C_{12}(55)$ $C_{21}(59)$

$C_{24}(45)$ $C_{15}(31)$ $C_{13}(48)$

$C_{33}(48)$ $C_{23}(44)$ $C_{16}(68)$

Fonte: Autor.

Proposição 3.1.4. *A função C_a é bijetiva se, e somente se, $mdc(a,m) = 1$.*

Demonstração: Vamos provar que a função $C_a : \{0,1,...,m-1\} \to \{0,1,...,m-1\}$ definida por $C_a(i) = i \cdot a \pmod{m}$, para $i = \{0,1,...,m-1\}$, é bijetiva se, e somente se, $mdc(a,m) = 1$.

Vamos provar a contrapositiva: se $mdc(a,m) = d > 1$, então C_a não é injetiva, logo não é bijetiva.

- Se $d > 1$, $C_a(i) = C_a(j)$ com $i \neq j$, então $i \cdot a \equiv j \cdot a \pmod{m}$ se, e somente se, $i \equiv j \pmod{\frac{m}{d}}$ mas $i \not\equiv j \pmod{m}$.
- Considere $i = 0$ e $j = \dfrac{m}{d}$. Temos:

$$C_a(0) = 0 \cdot a \equiv 0 \pmod{m};$$
$$C_a(\tfrac{m}{d}) = \frac{m}{d} \cdot a = \frac{m}{d} \cdot (d \cdot k) = m \cdot k \equiv 0 \pmod{m}$$

onde $a = d \cdot k$, pois d divide a. Assim $C_a(0) = C_a(\frac{m}{d})$, com $0 \neq \frac{m}{d}$, logo C_a não é injetiva. Portanto, não pode ser bijetiva. Com isso, concluímos que se C_a for bijetiva, devemos ter $mdc(a,m) = 1$.

Agora considere $mdc(a,m) = 1$, precisamos mostrar que C_a é injetiva e sobrejetiva.

(a) Injetividade.

Suponha $C_a(i) = C_a(j)$, ou seja:

$$i \cdot a \equiv j \cdot a \pmod{m} \Longleftrightarrow (i-j) \cdot a \equiv 0 \pmod{m}.$$

Como $mdc(a,m) = 1$, a é invertível módulo m. Portanto, teremos:

$$i - j \equiv 0 \pmod{m} \Longleftrightarrow i \equiv j \pmod{m}.$$

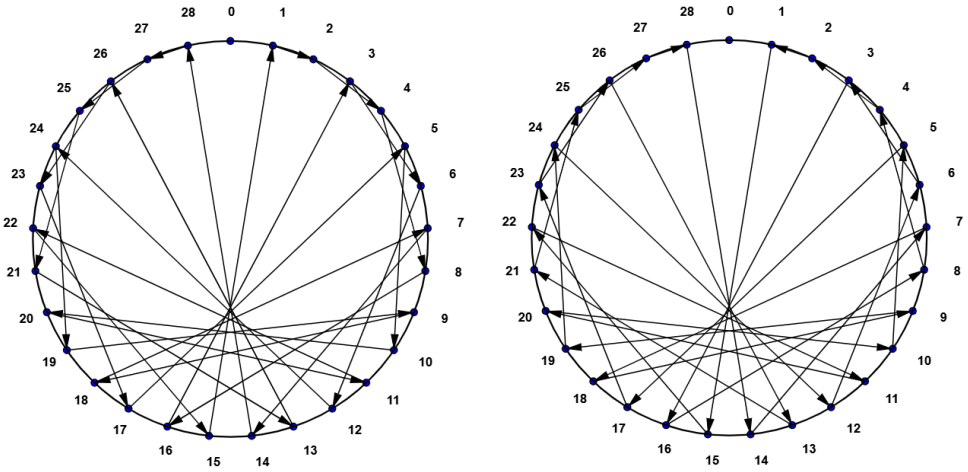
Como $i, j \in \{0, 1, ..., m-1\}$, a única possibilidade é $i = j$. Logo C_a é injetiva.

(b) Sobrejetividade.

Como o domínio e o contradomínio têm a mesma cardinalidade m (ambos são conjuntos finitos com m elementos), e a função é injetiva, segue-se imediatamente que ela é também sobrejetiva. □

Certos sistemas de congruências, embora distintos, resultam em um mesmo chryzode. Observe que, na figura abaixo, os chryzodes $C_2(29)$ e $C_{15}(29)$ produzem a mesma configuração final, mantendo inalterado o padrão geométrico resultante, ainda que modifique, no sentido oposto, a ordem de estabelecimento das conexões entre os pontos.

Figura 12 – Chryzodes $C_2(29)$ e $C_{15}(29)$.



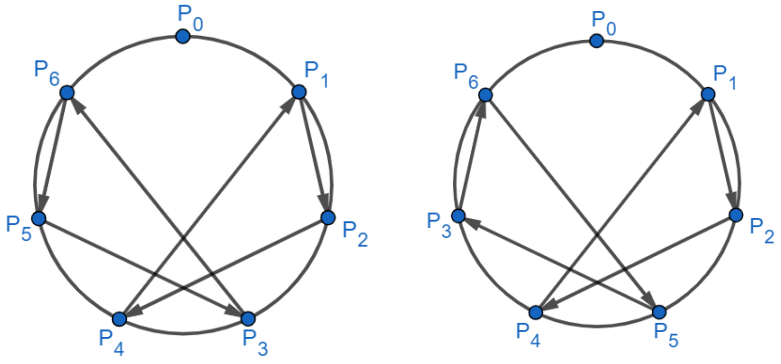
$C_2(29)$ $C_{15}(29)$

Fonte: Autor.

Definição 3.1.5. Dois chryzodes são considerados *equivalentes* quando suas estruturas de conexões são idênticas, admitindo-se como únicas diferenças possíveis transformações geométricas simples como rotação e reflexão, ordem das conexões, ou até mesmo, renumerações dos pontos.

Exemplo 3.1.6. A permutação dos pontos P_3 e P_5 em um Chryzode $C_2(7)$ não altera a configuração final da figura, mantendo inalterado o padrão geométrico resultante, ainda que modifique a ordem de estabelecimento das conexões entre esses pontos.

Figura 13 – Chryzode $C_2(7)$: sem e com transposição $P_3 \longleftrightarrow P_5$.

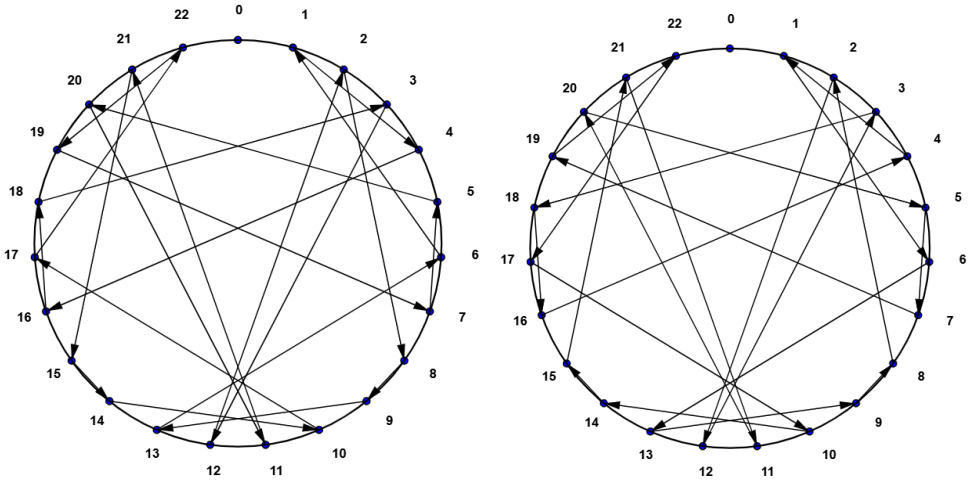


Sem permurtar Permutando

Fonte: Autor.

A seguir ilustramos mais alguns exemplos de chryzodes equivalentes.

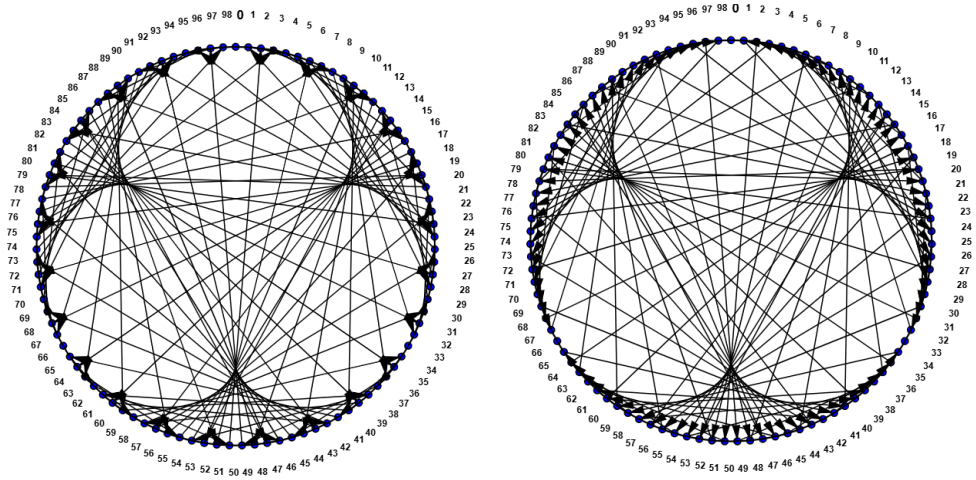
Figura 14 – Chryzodes $C_4(23)$ e $C_6(23)$.



$C_4(23)$ $C_6(23)$

Fonte: Autor.

Figura 15 – Chryzodes $C_4(99)$ e $C_{25}(99)$.



$i \cdot 4 \pmod{99}$ $i \cdot 25 \pmod{99}$

Fonte: Autor.

Proposição 3.1.7. *Os chryzodes $C_a(m)$ e $C_k(m)$, são equivalentes se $ak \equiv 1 \pmod{m}$.*

Demonstração: Seja o chryzode $C_a(m)$ formado pelo seguinte sistema:

$$i \cdot a \equiv b_i \pmod{m} \iff (i \cdot a)k \equiv b_i \cdot k \pmod{m} \iff i(a \cdot k) \equiv b_i \cdot k \pmod{m}.$$

Pela hipótese que $ak \equiv 1 \pmod{m}$, teremos

$$i \equiv b_i \cdot k \pmod{m} \iff b_i \cdot k \equiv i \pmod{m}.$$

Note que o chryzode $C_k(m)$, formado pelo sistema de congruência $b_i \cdot k \equiv i \pmod{m}$ da proposição, possui as conexões $b_i \to i$, ou seja, trata-se das conexões em sentido oposto às do

chryzode $C_a(m)$, uma vez que $i, b_i \in \{0,1,...,m-1\}$ e $a,k \in \mathbb{N}$. Dessa forma, $C_a(m)$ e $C_k(m)$ apresentam estruturas de conexões idênticas, sendo, portanto, equivalentes. □

Perceba que um chryzode $C_a(m)$ só terá um chryzode $C_k(m)$ como seu equivalente se a função C_a for bijetiva, isto é, C_a admitirá a inversa C_k, onde k no conjunto $\{0,1,...,m-1\}$ é único. Note que k realmente é único, pois, caso contrário, suponha k_1 e k_2, tais que

$$a \cdot k_1 \equiv 1 \pmod{m} \text{ e } a \cdot k_2 \equiv 1 \pmod{m}$$

subtraindo as congruências, temos:

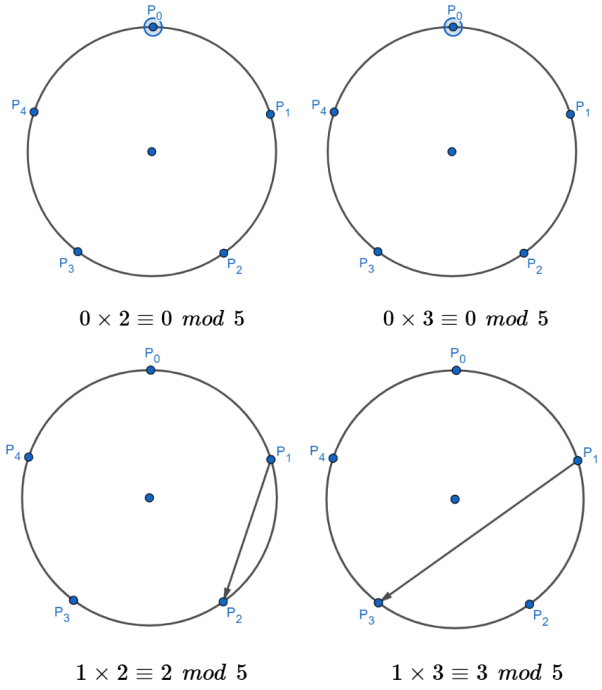
$$a \cdot (k_1 - k_2) \equiv 0 \pmod{m} \iff m \mid a \cdot (k_1 - k_2).$$

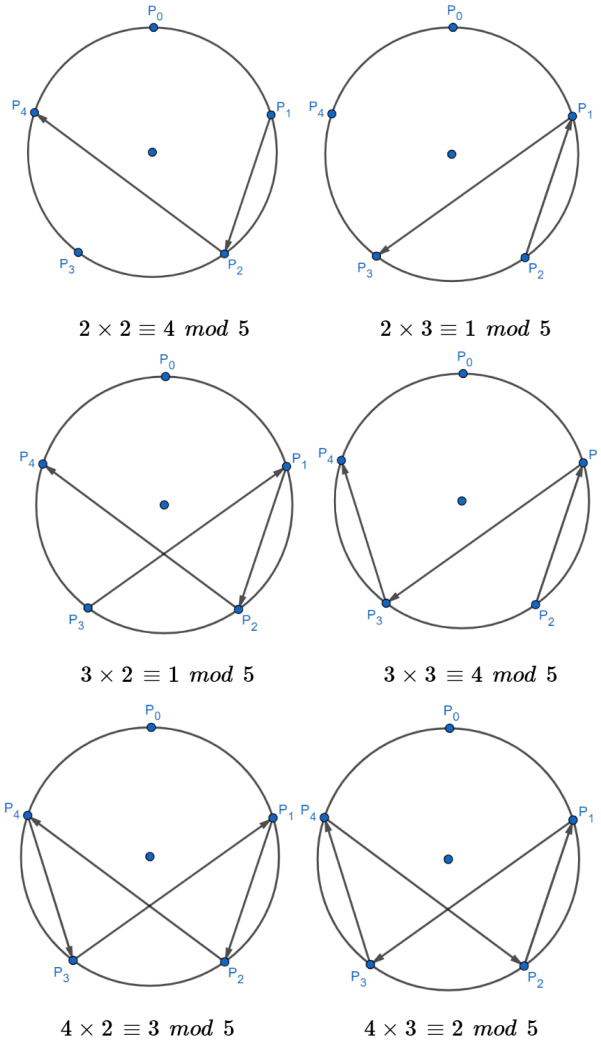
Como $mdc(a,m) = 1$, teremos que $m \mid (k_1 - k_2)$, ou seja, $k_1 \equiv k_2 \pmod{m}$. Logo, existe um único k no conjunto $\{0,1,...,m-1\}$ que satisfaz a congruência.

Na equivalência de Chryzodes, essa proposição é usada para inverter conexões (transformar as conexões $i \to b_i$ em $b_i \to i$), garantindo que estruturas de grafos seja preservada sob inversão modular.

Exemplo 3.1.8. Os chryzodes $C_2(5)$ e $C_3(5)$ são equivalentes, pois $2 \cdot 3 \equiv 1 \pmod{5}$. Perceba que tal equivalência leva as conexões dos chryzodes já formados em sentido oposto.

Figura 16 – Chryzodes $C_2(5)$ e $C_3(5)$.





Fonte: Autor.

Proposição 3.1.9. *Para quaisquer chryzodes $C_{\frac{m}{2}}(m)$, quando m é par, temos o seguinte comportamento:*

1. *Se i for ímpar, então $i \cdot \frac{m}{2} \equiv \frac{m}{2} \pmod{m}$;*
2. *Se i for par, então $i \cdot \frac{m}{2} \equiv 0 \pmod{m}$.*

Em outros termos, as cordas $\overline{P_{2k+1}P_{\frac{m}{2}}}$ e $\overline{P_{2k}P_0}$, com $k \cup \{0\} \in \mathbb{N}$, pertencem ao chryzode $C_{\frac{m}{2}}(m)$.

Demonstração:

1. Caso i ímpar: Seja $i = 2k+1$, onde $k \in \mathbb{N} \cup \{0\}$. Então:

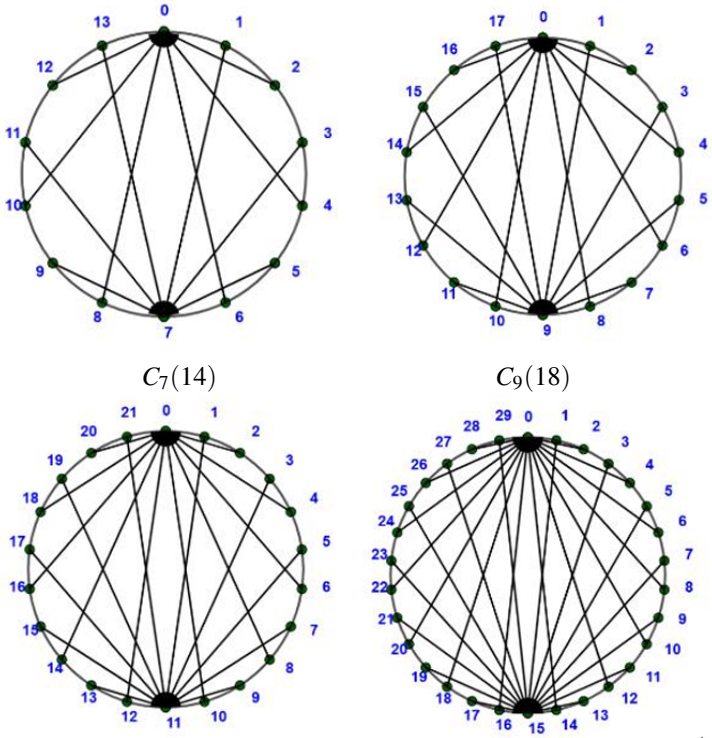
$$i \cdot \frac{m}{2} = (2k+1) \cdot \frac{m}{2} = km + \frac{m}{2} \equiv \frac{m}{2} \pmod{m}.$$

2. Caso i par: Seja $i = 2k$, onde $k \in \mathbb{N} \cup \{0\}$. Então:

$$i \cdot \frac{m}{2} = 2k \cdot \frac{m}{2} = km \equiv 0 \pmod{m}.$$

□

Figura 17 – Chryzodes que satisfazem a Proposição 3.1.9.



$C_7(14)$ $C_9(18)$

$C_{11}(22)$ $C_{15}(30)$

Fonte: Autor.

Proposição 3.1.10. *Para quaisquer chryzodes $C_{\frac{m}{2}+1}(m)$, quando m é par, temos o seguinte comportamento:*

1. *Se i for ímpar, então $i \cdot (\frac{m}{2}+1) \equiv \frac{m}{2}+i \pmod{m}$;*

2. *Se i for par, então $i \cdot (\frac{m}{2}+1) \equiv i \pmod{m}$.*

Em outros termos, quando i é ímpar, as cordas $\overline{P_iP_{(\frac{m}{2}+i)}}$ pertencem ao chryzode $C_{\frac{m}{2}+1}(m)$. Observe que tal corda é, na verdade, um diâmetro, pois o ângulo central entre dois pontos consecutivos P_i e P_{i+1} é dado por $\theta = \frac{360^\circ}{m}$. Logo, a corda $\overline{P_iP_{(\frac{m}{2}+i)}}$ corresponde a um ângulo central de $\frac{360^\circ}{m} \cdot \frac{m}{2} = 180^\circ$.

Demonstração:

1. Se $i = 2k+1$, com $k \in \mathbb{N} \cup \{0\}$, então:

$$i \cdot (\tfrac{m}{2}+1) = (2k+1)(\tfrac{m}{2}+1) = km + \tfrac{m}{2} + (2k+1) \equiv \tfrac{m}{2} + (2k+1) \pmod{m}$$
$$\Rightarrow i \cdot (\tfrac{m}{2}+1) \equiv \tfrac{m}{2} + i \pmod{m}.$$

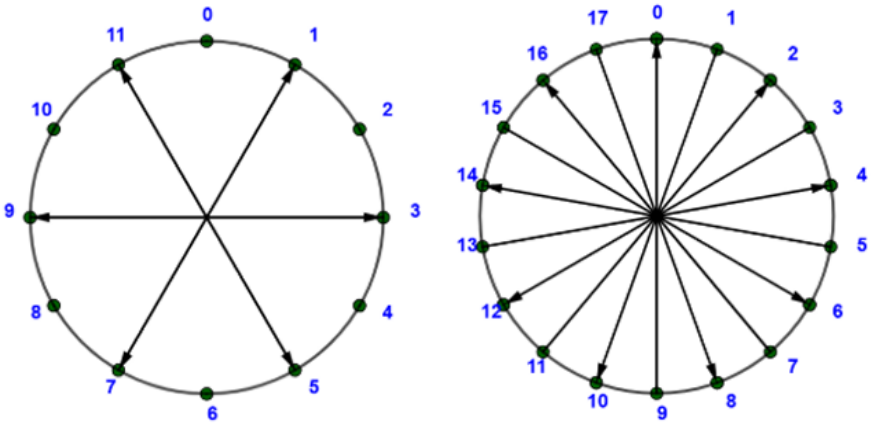
2. Se $i = 2k$, com $k \in \mathbb{N} \cup \{0\}$, então:

$$i \cdot (\tfrac{m}{2}+1) = 2k \cdot (\tfrac{m}{2}+1) = km + 2k \equiv 2k \pmod{m}$$
$$\Rightarrow i \cdot (\tfrac{m}{2}+1) \equiv i \pmod{m}.$$

□

A figura a seguir mostra exemplos de chryzodes desse tipo.

Figura 18 – Chryzodes que satisfazem a Proposição 3.1.10.



$C_7(12)$ $C_{10}(18)$

Fonte: Autor.

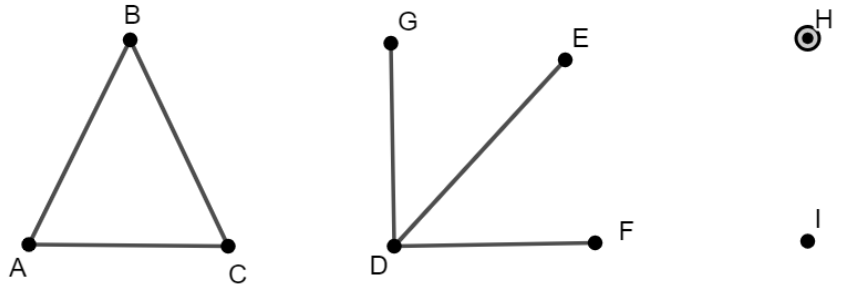
3.2 Chryzodes em Teoria dos Grafos

Adotaremos para os grafos a mesma notação utilizada por (Souza, 2013) no trabalho "*Teoria dos Grafos e Aplicações*".

Definição 3.2.1. Um *grafo* $G = (V, E)$ é caracterizado por seu conjunto de vértices V (um conjunto não vazio de pontos) e seu conjunto de arestas E, onde cada aresta estabelece uma relação entre dois vértices de V.

Uma aresta $e \in E(G)$ é representada por $e = \{u, v\}$ sempre que interliga dois vértices (pontos) u e v de $V(G)$. Dois vértices ligados por uma mesma aresta são denominados adjacentes e pode-se dizer que uma aresta e é incidente em u, se u for extremidade de e. Veja alguns exemplos de grafos na Figura 19.

Figura 19 – Exemplos de grafos.



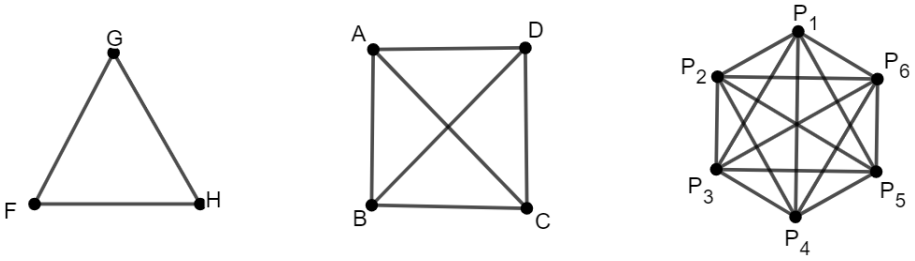
(a) (b) (c)

Fonte: Autor.

Um grafo de aresta do tipo $e = \{u, u\}$, ou seja, com extremidades iguais as da aresta, é denominado *laço*.

Definição 3.2.2. Um grafo G é *completo* se a conectividade entre vértices é máxima, ou seja, se cada vértice está ligado a todos os demais.

Figura 20 – Exemplos de grafos completos.



(a) (b) (c)

Fonte: Autor.

Dado um grafo $G(V, E)$, o *grau de um vértice* $v \in V$, denotado por $g(v)$, é igual ao número de arestas que incidem nele. Na Figura 20 (b), o grau de cada vértice é 3. Considerando que em cada vértice $v \in V$ incidem $g(v)$ arestas e que cada aresta incide em 2 vértices, tem-se:

Lema 3.2.3. ***(Lema do Aperto de Mão)*** *Para todo grafo* $G = (V, E)$

$$\sum_{v \in V(G)} g(v) = 2 \cdot |E|,$$

onde $|E|$ representa o número de arestas do conjunto E.

Demonstração: Basta observar que ao somar os graus dos vértices, cada aresta é contada duas vezes, pois incide em dois vértices. □

Corolário 3.2.4. *Todo grafo G possui um número par de vértices de grau ímpar.*

Demonstração: Suponha que exista um número ímpar de vértices de grau ímpar. Nesse caso, a soma total dos graus seria ímpar. Mas, pelo lema 3.2.3, essa soma é $2 \cdot |E|$, que é par, resultando numa contradição. □

Definição 3.2.5. Quando todos os vértices de um grafo possuem o mesmo grau, ele é chamado de *grafo regular* de grau r.

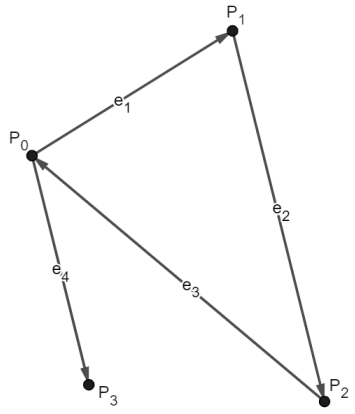
Exemplo 3.2.6. Todos os grafos da Figura 20 são exemplos de grafos regulares.

Definição 3.2.7. Um *passeio* P de v_0 a v_n, é uma sequência finita e não vazia $(v_0, e_1, v_1, e_2, v_2, ..., e_n, v_n)$, cujos elementos são alternadamente vértices e arestas de um grafo G, e tal que $e_i = (v_{i-1}, v_i)$ para $1 \leq i \leq n$.

Definição 3.2.8. Uma *trilha* é um passeio em que as arestas são duas a duas distintas. (vértices podem ser repetidos).

A figura 21 a seguir, retrata um exemplo de trilha.

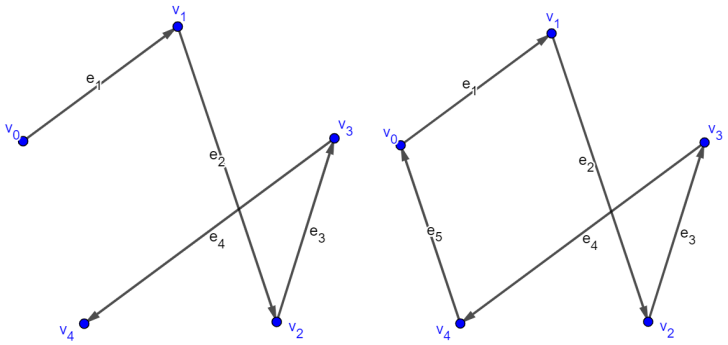
Figura 21 – Trilha $(P_0,\ e_1,\ P_1,\ e_2,\ P_2,\ e_3,\ P_0,\ e_4,\ P_3)$.



Fonte: Autor.

Definição 3.2.9. Um *caminho* é uma trilha em que os vértices são dois a dois distintos (não repete arestas nem vértices, exceto possivelmente o primeiro e o último). Quando um caminho possui seu vértice inicial e final coincidentes, dizemos que ele constitui um *circuito*.

Figura 22 – Exemplo de caminho e circuito.

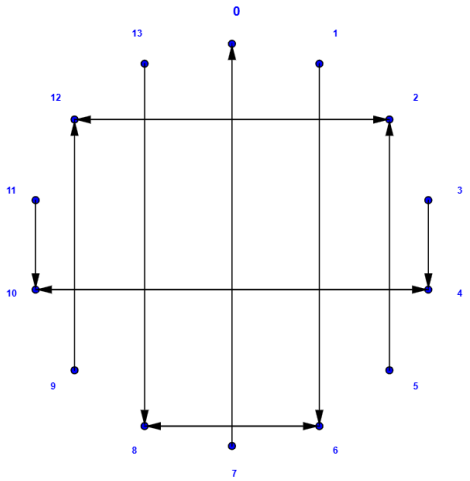


(a) Caminho $(V_0, V_1, V_2, V_3, V_4)$ (b) Circuito $(V_0, V_1, V_2, V_3, V_4, V_0)$

Fonte: Autor.

Um chryzode $C_a(m)$ pode ser interpretado, sob a ótica da teoria dos grafos, como um grafo $G(m, E)$, onde m representa o número de vértices do grafo e E é o conjunto de arestas (cordas). Quando tratarmos chryzodes como grafos, iremos considerar as ordens de conexão importantes,isto é, que as arestas $\{P_i, P_{b_i}\}$ e $\{P_{b_i}, P_i\}$, formadas pelas conexões $i \to b_i$ e $b_i \to i$, são distintas (ou seja, o grafo será orientado ou as arestas serão consideradas ordenadas). Vamos considerar também que um segmento nulo (um laço $e = \{P_i, P_i\}$), pertence ao conjunto de arestas (cordas). Portanto a estrutura do chryzode quando tratadas como grafos impõe que o número de arestas seja igual do número de vértices, ou seja, $|E| = m$. Portanto, todo chryzode pode ser interpretado como um grafo, mas nem todo grafo pode ser interpretado como um chryzode.

Figura 23 – Chryzode $C_6(14)$ ou grafo $G(14, 14)$

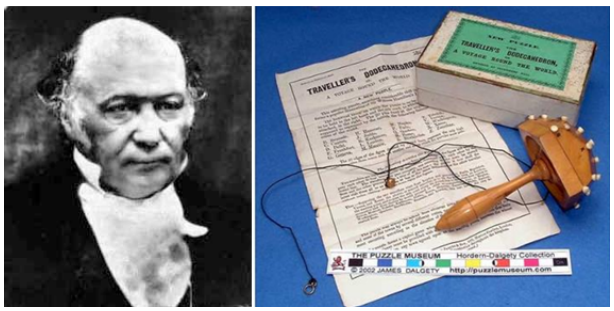


fonte: Autor.

Um dos problemas clássicos da teoria dos grafos consiste em determinar se é possível percorrer um grafo visitando cada um de seus vértices exatamente uma vez e retornando ao ponto de partida. "Em 1856, William Hamilton inventou o seguinte brinquedo: dado um dodecaedro em cujos vértices estão indicados nomes de 20 cidades distintas, usando uma cordinha que pode passar

apenas ao longo das arestas do dodecaedro, o brinquedo consiste em visitar cada uma das 20 cidades exatamente uma vez e terminar na cidade de partida" (Yoshiko, 2020). A definição desse tipo de problema é apresentada logo após a Figura 24.

Figura 24 – William R. Hamilton e dodecaedro com nomes de 20 cidades.



Fonte: (Yoshiko, 2020).

Definição 3.2.10. Um *caminho hamiltoniano* ou *caminho rastreável* é um caminho que permite passar por todos os vértices de um grafo G, não repetindo nenhum, ou seja, passar por todos uma e uma só vez. Caso esse caminho seja possível descrever um ciclo, este é denominado *ciclo hamiltoniano* (ou *circuito hamiltoniano*) em G. Um grafo que possua tal circuito é chamado de *grafo hamiltoniano*.

Desse modo, surge a seguinte questão acerca dos chryzodes: é possível que algum chryzode constitua um ciclo hamiltoniano?

Para mostrar que um chryzode $C_a(m)$ gerado pelo sistema de congrência $i \cdot a \equiv b_i \pmod{m}$ pode gerar um ciclo hamiltoniano, precisamos entender as condições sob as quais isso ocorre. Considere o conjunto de números inteiros $\{0,1,2,...,m-1\}$. Queremos saber se a função $C_a(i) = i \cdot a \pmod{m}$ gera um caminho que visita todos os elementos desse conjunto (apenas uma vez) quando iterada a partir de um ponto inicial.

Note que:

$$0 \cdot a \equiv 0 \pmod{m}.$$

Portanto, se começarmos em 0, ficamos presos no 0. Além disso para qualquer i tal que $mdc(i,m) \neq 1$, pode haver comportamentos problemáticos. Para evitar isso, geralmente é restringido o conjunto aos elementos invertíveis módulo m. Esse conjunto é denotado por $\mathbb{Z}_m^*$ e contém os números i com $1 \leq i \leq m-1$ e $mdc(i,m) = 1$ (Definição 2.9.8).

Suponha que $mdc(a,m) = 1$, isso significa que a é invertível módulo m (isso decorre do Teorema 2.5.1). No entanto, isso não é suficiente para garantir que a multiplicação por a gere um

ciclo hamiltoniano em $\mathbb{Z}_m^*$. Por exemplo, tome $m = 15$ e $a = 11$, logo $mdc(11,15) = 1$. Agora perceba que o Chryzode $C_{11}(15)$ não forma um ciclo hamiltoniano.

$$C_{11}(1) = 1 \cdot 11 \pmod{15} = 11 \qquad C_{11}(8) = 8 \cdot 11 \pmod{15} = 13$$

$$C_{11}(2) = 2 \cdot 11 \pmod{15} = 7 \qquad C_{11}(9) = 9 \cdot 11 \pmod{15} = 9$$

$$C_{11}(3) = 3 \cdot 11 \pmod{15} = 3 \qquad C_{11}(10) = 10 \cdot 11 \pmod{15} = 5$$

$$C_{11}(4) = 4 \cdot 11 \pmod{15} = 14 \qquad C_{11}(11) = 11 \cdot 11 \pmod{15} = 1$$

$$C_{11}(5) = 5 \cdot 11 \pmod{15} = 10 \qquad C_{11}(12) = 12 \cdot 11 \pmod{15} = 12$$

$$C_{11}(6) = 6 \cdot 11 \pmod{15} = 6 \qquad C_{11}(13) = 13 \cdot 11 \pmod{15} = 8$$

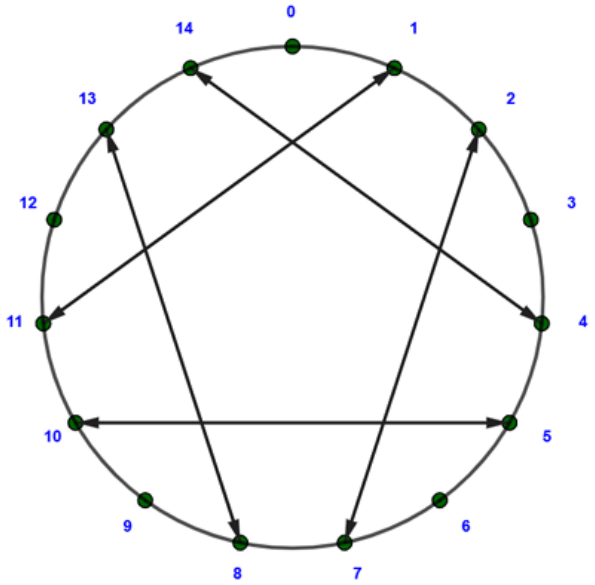
$$C_{11}(7) = 7 \cdot 11 \pmod{15} = 2 \qquad C_{11}(14) = 14 \cdot 11 \pmod{15} = 4$$

Perceba que $C_{11}(i) = i$ quando i é múltiplo de 3. De fato, se $i = 3q$ com $q \in \mathbb{Z}$, temos:

$$i \cdot 11 = 3q \cdot 11 = 3q \cdot (10+1) = 30q + 3q \equiv 3q = i \pmod{15}.$$

E ainda não gera um ciclo único que visite todos os elementos de $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$.

Figura 25 – Chryzode $C_{11}(15)$.



Fonte: Autor.

Para termos uma condição correta, precisamos da Definição 2.9.9, sobre raízes primitivas módulo m.

Dessa maneira, para que a multiplicação por a gere um ciclo que visite todos os elementos de $\mathbb{Z}_m^*$, é necessário que a seja um gerador de $\mathbb{Z}_m^*$. Isso significa que a ordem de a módulo m deve

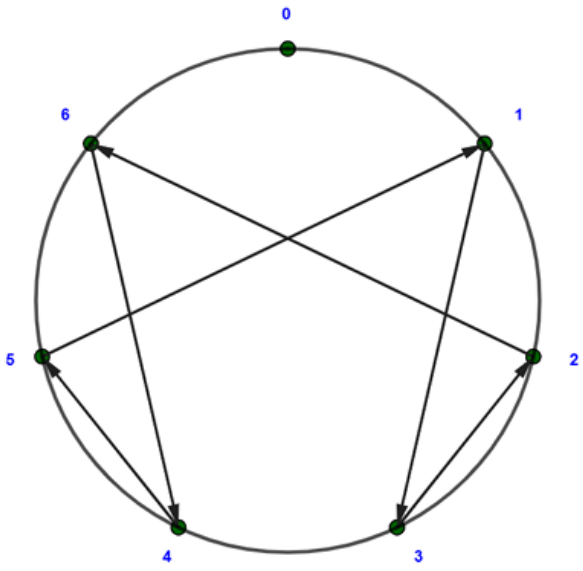
ser igual a $\phi(m)$, onde ϕ é a função totiente de Euler (Definição 2.9.1). Nesse caso, a é dito raiz primitiva módulo m .

Exemplo 3.2.11. Para $m = 7$, temos $\phi(7) = 6$ pois $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$. Tome $a = 3$, verifique:

$$3^1 \equiv 3 \pmod 7$$
$$3^2 \equiv 2 \pmod 7$$
$$3^3 \equiv 6 \pmod 7$$
$$3^4 \equiv 4 \pmod 7$$
$$3^5 \equiv 5 \pmod 7$$
$$3^6 \equiv 1 \pmod 7.$$

Portanto, $a = 3$ gera $\mathbb{Z}_7^*$. A sequência $1,3,2,6,4,5$ é um caminho hamiltoniano e consequentemente $1,3,2,6,4,5,1$ é um ciclo. Sendo assim, o chryzode $C_3(7)$ é considerado como um chryzode hamiltoniano.

Figura 26 – Chryzode $C(3,7)$.



Fonte: Autor.

Se insistirmos em incluir o zero, o problema se torna mais complexo. Para $m, a \in \mathbb{N}$, note que se $C_a : \{0,1,...,m-1\} \to \{0,1,...,m-1\}$ é uma função tal que $i \cdot a \equiv C_a(i) \pmod m$, isso é, $C_a(i) = i \cdot a - mq$, para certos $a, q \in \mathbb{N}$, teremos:

1. $C_a(0) = 0$;

2. Para $i \neq 0$, se $mdc(i,m) = d > 1$, então $mdc(i \cdot a, m) \geq d \Rightarrow mdc(mq + C_a(i), m) \geq d$.

Logo pelo Lema 2.3.2, obtemos que $mdc(C_a(i), m) \geq d$. Portanto, nunca sairemos do subconjunto de números não invertíveis se começarmos de um deles. Assim, o subconjunto total $\{0, 1, 2, ..., m-1\}$ não é fechado sob a operação de multiplicação por a no sentido de formar um único ciclo. Na verdade, ele se divide em:

1. Um ciclo trivial em $\{0\}$;
2. Vários ciclos dentro do conjunto de números não invertíveis (se existirem);
3. Ciclos dentro do grupo $\mathbb{Z}_m^*$.

Portanto, não é possível obter um ciclo hamiltoniano que inclua o zero usando multiplicação modular. Para organizar melhor as ideias, colocaremos tal informação como uma proposição.

Proposição 3.2.12. *O chryzode $C_a(m)$ gera um ciclo hamiltoniano no grupo $\mathbb{Z}_m^*$ se, e somente se, a for uma raiz primitiva módulo m.*

Demonstração: Suponha que a operação $i \to i \cdot a \pmod{m}$ gera um ciclo hamiltoniano em $\mathbb{Z}_m^*$. Isso significa que, a partir de qualquer $i \in \mathbb{Z}_m^*$, a sequência $i,\ i \cdot a,\ i \cdot a^2,\ ...$ eventualmente percorre todos os elementos de $\mathbb{Z}_m^*$ antes de retornar a i. Seja ϕ a função Totiente, em particular, começamos de $i = 1$ a sequência $1,\ a,\ a^2,\ ...,\ a^{\phi(m)-1} \pmod{m}$ deve conter todos os elementos de $\mathbb{Z}_m^*$. Portanto, a é um gerador de $\mathbb{Z}_m^*$, o que significa, pela Proposição 2.9.9, que a é uma raiz primitiva módulo m.

Agora, suponha que a seja uma raiz primitiva módulo m. Então, a gera $\mathbb{Z}_m^*$, isto é, $\mathbb{Z}_m^* = \{a^k \pmod{m};\ k = 1, 2, ..., \phi(m)\}$. A seguir, considere um ciclo começando em 1:

$$1 \to 1 \cdot a \to 1 \cdot a^2 \to \cdots \to 1 \cdot a^{\phi(m)-1} \to 1 \cdot a^{\phi(m)} = 1 \cdot 1 = 1$$

(já sabemos pelo Teorema 2.9.6 que $a^{\phi(m)} \equiv 1 \pmod{m}$).

Como a é raiz primitiva , os valores $1 \cdot a^k \pmod{m}$ para $k = 1, 2, ..., \phi(m) - 1$ são todos distinto e cobrem $\mathbb{Z}_m^*$. Portanto, esse ciclo é um ciclo hamiltoniano em $\mathbb{Z}_m^*$. □

Observe que se m for primo, o ciclo conterá todos os vértices do chryzode, exceto P_0, pois teremos $\phi(m) = m - 1$.

Exemplo 3.2.13. O Chryzode $C_5(7)$ gera um ciclo hamiltoniano em $\mathbb{Z}_7^*$.

Perceba que 5 é uma raiz primitiva módulo 7, pois $a = 5$ gera $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.

$$5^1 \equiv 5 \pmod 7 \qquad 5^4 = (5^2)^2 \equiv 4^2 = 16 \equiv 2 \pmod 7$$

$$5^2 = 25 \equiv 4 \pmod 7 \qquad 5^5 = 5^4 \cdot 5 \equiv 2 \cdot 5 = 10 \equiv 3 \pmod 7$$

$$5^3 = 5^2 \cdot 5 \equiv 4 \cdot 5 = 20 \equiv 6 \pmod 7 \qquad 5^6 = (5^3)^2 \equiv 6^2 = 36 \equiv 1 \pmod{11}$$

Portanto, pela Proposição 3.2.12 o Chryzode $C_5(7)$ gera um ciclo hamiltoniano. Perceba ainda que $3 \cdot 5 \equiv 1 \pmod 7$, logo pela Proposição 3.1.7 os Chryzode $C_5(7)$ e $C_3(7)$ da Figura 26 são equivalentes.

Exemplo 3.2.14. O Chryzode $C_6(11)$ gera um ciclo hamiltoniano em $\mathbb{Z}_{11}^*$.

Perceba que 6 é uma raiz primitiva módulo 11, pois $a = 6$ gera $\mathbb{Z}_{11}^* = \{1, 2, 3, ..., 10\}$.

$$6^1 \equiv 6 \pmod{11} \qquad 6^6 = (6^3)^2 \equiv 7^2 = 49 \equiv 5 \pmod{11}$$

$$6^2 = 36 \equiv 3 \pmod{11} \qquad 6^7 = 6^6 \cdot 6 \equiv 5 \cdot 6 = 30 \equiv 8 \pmod{11}$$

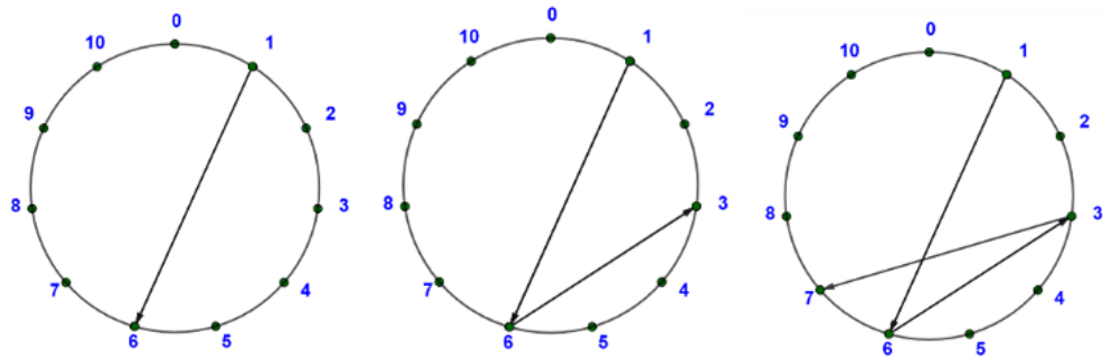
$$6^3 = 6^2 \cdot 6 \equiv 3 \cdot 6 = 18 \equiv 7 \pmod{11} \qquad 6^8 = (6^4)^2 \equiv 9^2 = 81 \equiv 4 \pmod{11}$$

$$6^4 = (6^2)^2 \equiv 3^2 = 9 \pmod{11} \qquad 6^9 = 6^8 \cdot 6 \equiv 4 \cdot 6 \equiv 2 \pmod{11}$$

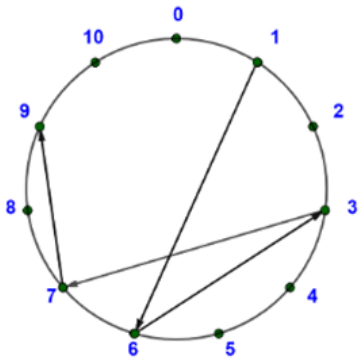
$$6^5 = 6^4 \cdot 6 \equiv 9 \cdot 6 = 54 \equiv 10 \pmod{11} \qquad 6^{10} = (6^5)^2 \equiv 10^2 = 100 \equiv 1 \pmod{11}$$

Observe a construção desse Chryzode feito na ordem de conexão na figura a seguir.

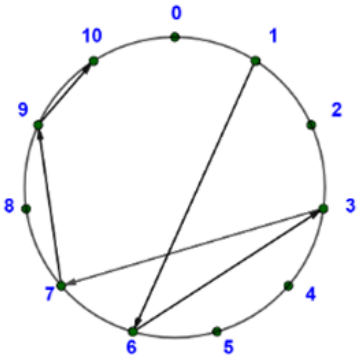
Figura 27 – Chryzode $C_6(11)$ feito na ordem de conexão.



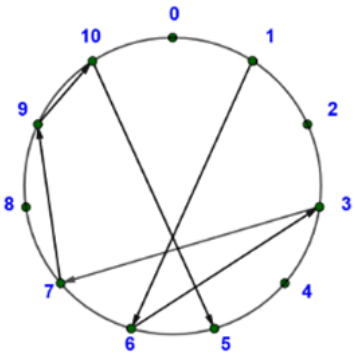
$1 \cdot 6 \equiv 6 \pmod{11}$ $\quad$ $6 \cdot 6 \equiv 3 \pmod{11}$ $\quad$ $3 \cdot 6 \equiv 7 \pmod{11}$



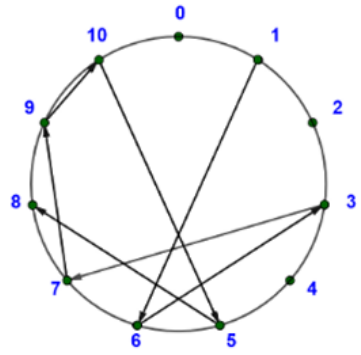
$7 \cdot 6 = 42 \equiv 9 \pmod{11}$



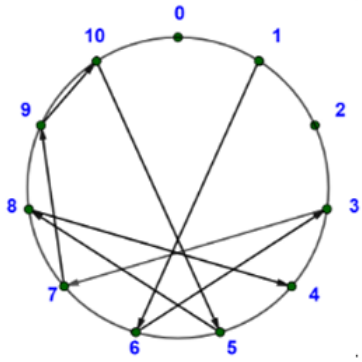
$9 \cdot 6 = 54 \equiv 10 \pmod{11}$



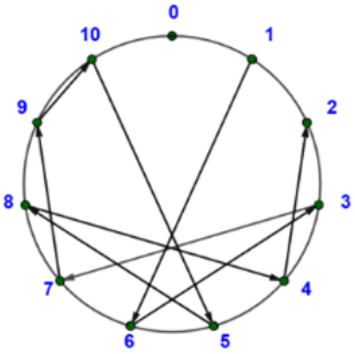
$10 \cdot 6 \equiv 5 \pmod{11}$



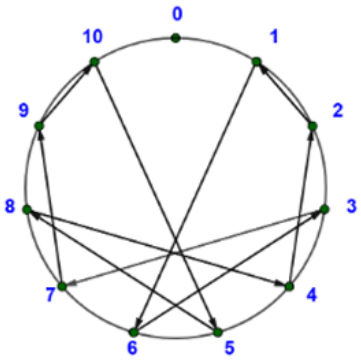
$5 \cdot 6 = 30 \equiv 8 \pmod{11}$



$8 \cdot 6 = 48 \equiv 4 \pmod{11}$



$4 \cdot 6 \equiv 2 \pmod{11}$



$2 \cdot 6 = 12 \equiv 1 \pmod{11}$

Fonte: Autor.

3.3 A Natureza Epicicloidal dos Chryzodes

Desde os esforços da astronomia antiga para modelar os céus até as formulações modernas da teoria dos sistemas dinâmicos, a composição de movimentos circulares revela-se uma ferramenta fundamental para a compreensão de padrões complexos. Uma *Epicicloide* é uma curva que surge a partir do movimento de um ponto em um círculo que rola sem deslizar ao longo do perímetro de outro círculo fixo maior. É nesse contexto histórico e conceptual que os chryzodes, encontram sua mais profunda e surpreendente ressonância.

Esta seção investiga a hipótese central de que os chryzodes podem ser compreendidos como as manifestações discretas de epicicloides. Enquanto uma epicicloide clássico é uma curva

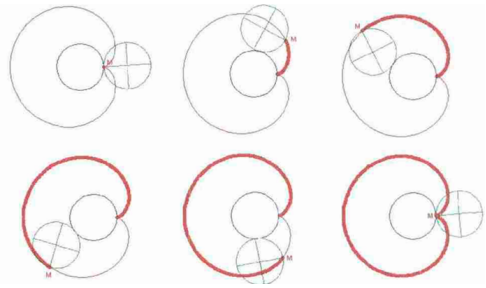
contínua, definida parametricamente no plano real ou complexo, um chryzode emerge de um processo aritmético discreto: a iteração da transformação $i \to i \cdot a \pmod{m}$, onde $a, m \in \mathbb{N}$ com $i = 0, 1, ..., m-1$. Apesar da disparidade inicial entre o domínio contínuo e o discreto, verificaremos que tais estruturas tendem a ser isomórficas. Para uma melhor compreensão, vamos adotar as difinições a seguir conforme (Putnoki, 1990).

Definição 3.3.1. Chama-se *epicicloide* a curva descrita por um ponto de um raio (ou do prolongamento de um raio) de uma circunferência que rola externamente, sem escorregamento, sobre a outra circunferência fixa.

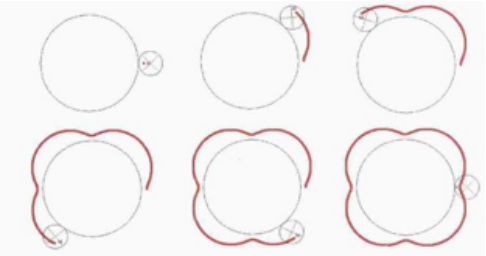
A circunferência móvel é denominada *circunferência geradora*, o ponto que descreve a epicicloide é chamado *ponto gerador* e a circunferência fixa é denominada *circunferência diretora*. Desde que o ponto gerador pertença à circunferência geradora, esteja no seu interior ou no seu exterior, a epicicloide é chamada, respectivamente de simples, encurtada ou alongada.

A Figura 28 apresenta exemplos dessas epicicloides, enquanto a Figura 29 mostra o comportamento do chryzode $C_2(m)$ com valores cada vez maiores de m.

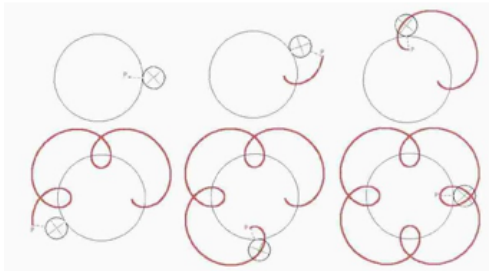
Figura 28 – Epicicloide Simples, Encurtada e Alongada.



Epicicloide Simples (Cardióide).

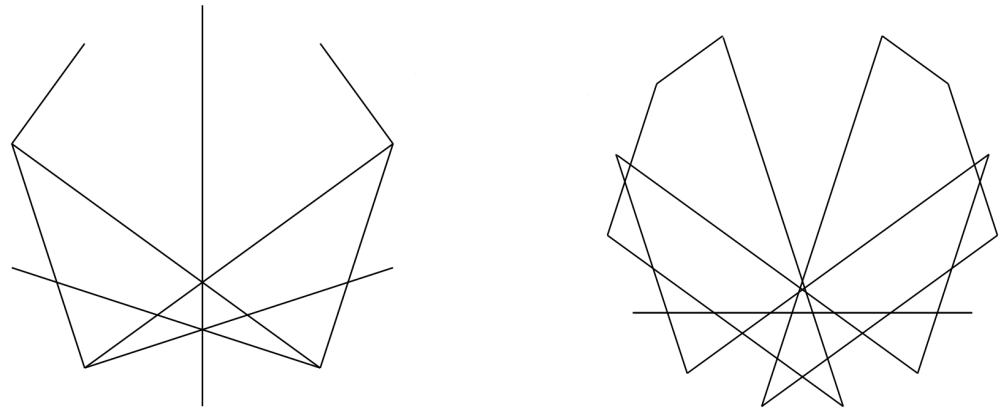


Epicicloide Alongada.

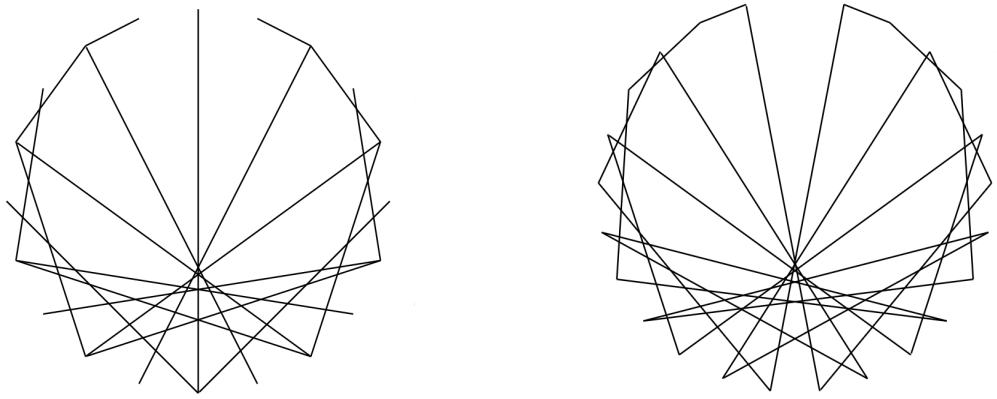


Epicicloide Encurtada.
Fonte: (Ferretto, 2003, p. 52).

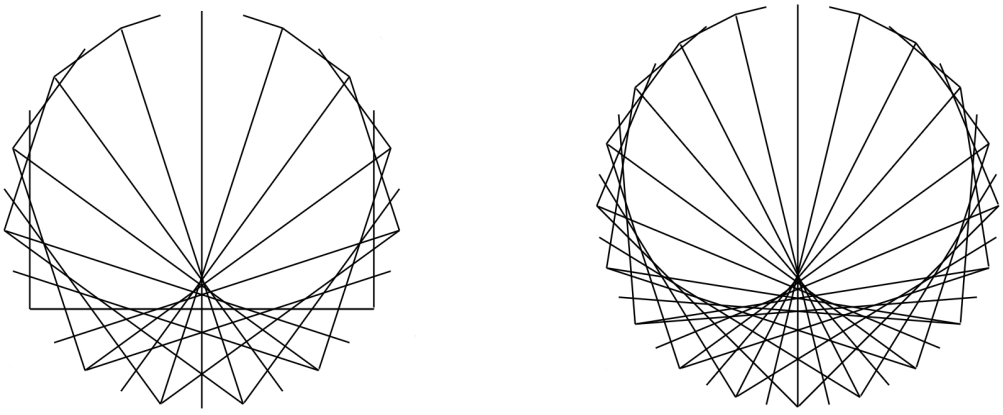
Figura 29 – Chryzode $C_2(m)$ com a circunferência ocultada, para $m = 10, 15, 20, 25, 30, 40, 50, 60$.



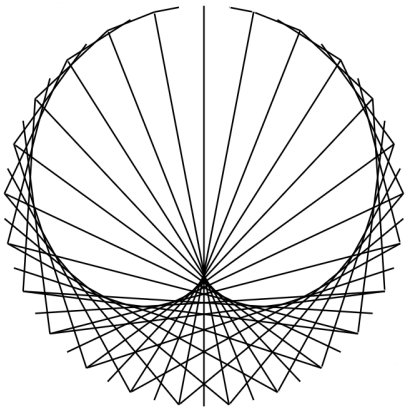
$C_2(10)$ $C_2(15)$



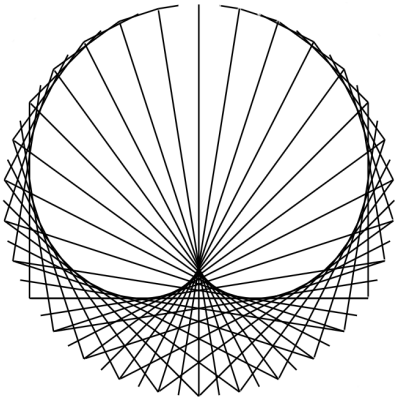
$C_2(20)$ $C_2(25)$



$C_2(30)$ $C_2(40)$



$C_2(50)$



$C_2(60)$

Fonte: Autor.

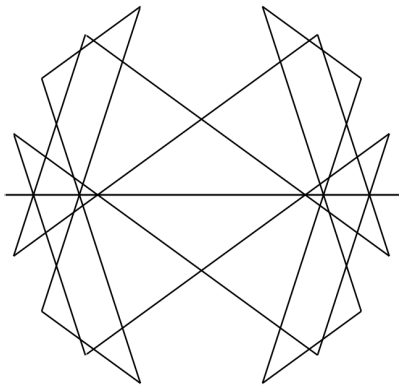
Nota-se que valores crescentes de m produzem curvas que se assemelham progressivamente a um coração. Assim, no limite $m \to +\infty$, o padrão resultante tende a se tornar uma epicicloide denominado *cardioide*.

Definição 3.3.2. Sejam R e r, respectivamente, os raios das circunferências diretora e geradora de uma epicicloide. Então $n = \dfrac{2\pi R}{2\pi r} = \dfrac{R}{r}$ é o número de ciclos da epicicloide, isto é, o número de voltas em que a circunferência geradora percorre a volta inteira da circunferência diretora. Em particular, são denominadas *epicicloides notáveis* e para os casos em que $n \geq 3$, a figura constituída pela reunião dos n ciclos é chamada *polígono epicicloidal*.

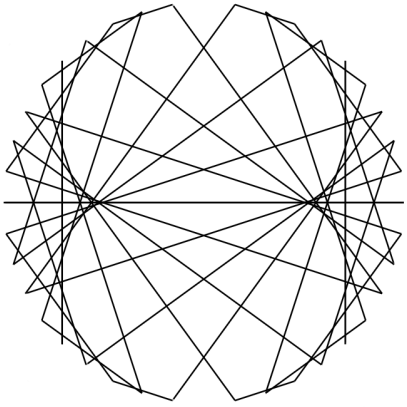
Vale ressaltar que cada ciclo de uma epicicloide notável de n ciclos corresponde a um ângulo de $\dfrac{360}{n}$ graus na circunferência diretora.

Como já vimos, o chryzode $C_2(m)$ quando $m \to +\infty$, tende a ser um cardioide. Agora observe a figura seguir, quando $a = 3$ e o m assume valores cada vez maiores.

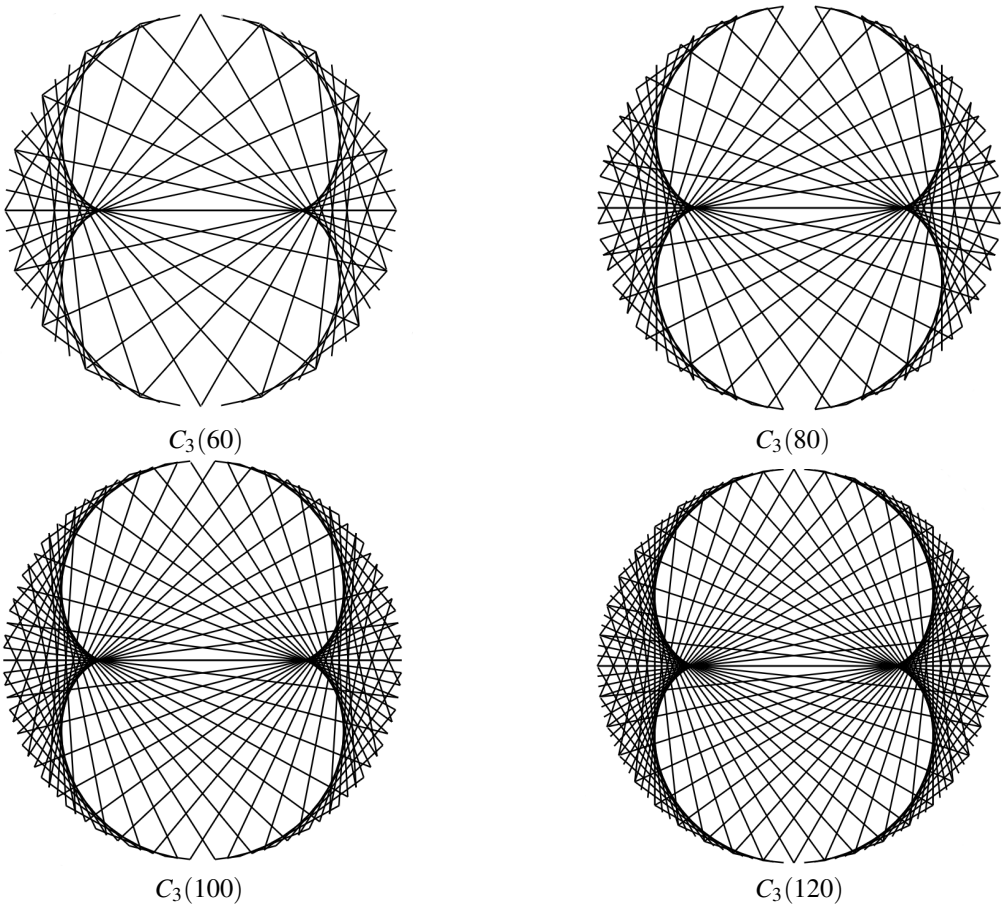
Figura 30 – Chryzode $C_3(m)$, com a circunferência ocultada, para $m = 20, 40, 60, 80, 100, 120$.



$C_3(20)$



$C_3(40)$



$C_3(60)$ $C_3(80)$

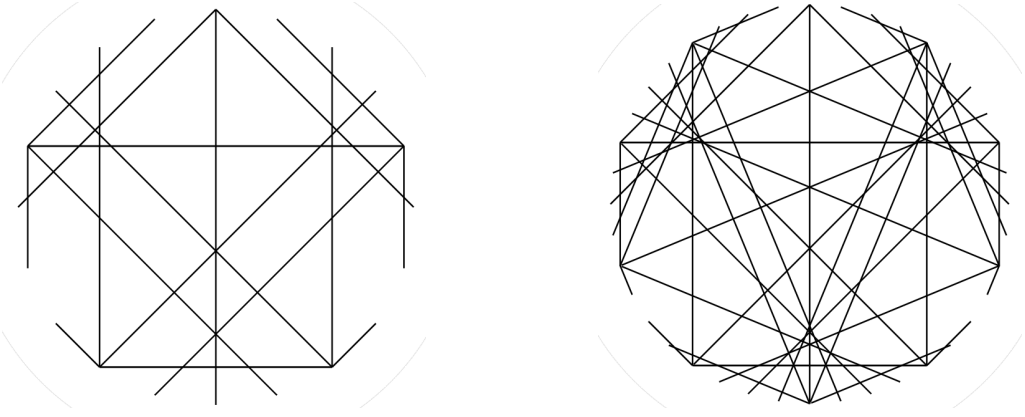
$C_3(100)$ $C_3(120)$

Fonte: Autor.

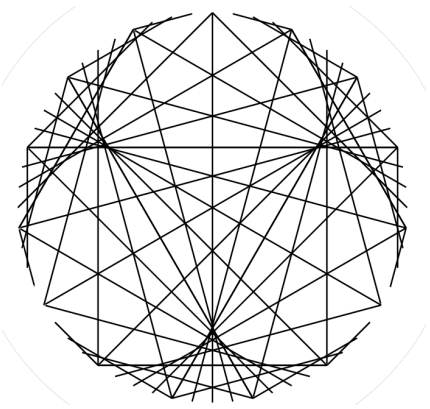
Nota-se que valores crescentes de m produzem uma curva que se assemelham progressivamente a um rim. Assim, no limite $m \to +\infty$, o padrão resultante tende a se tornar uma epicicloide denominado *nefroide*.

Observa-se que, com o aumento de m, o chryzode definido por $i \cdot 4 \pmod{m}$ converge para uma epicicloide de 3 ciclos.

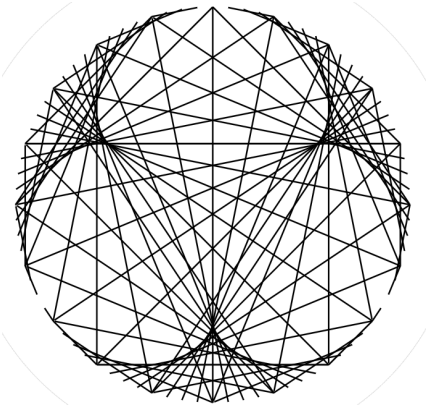
Figura 31 – Chryzode $C_4(m)$,com a circunferência ocultada, para $m = 20, 40, 60, 80, 100, 120$.



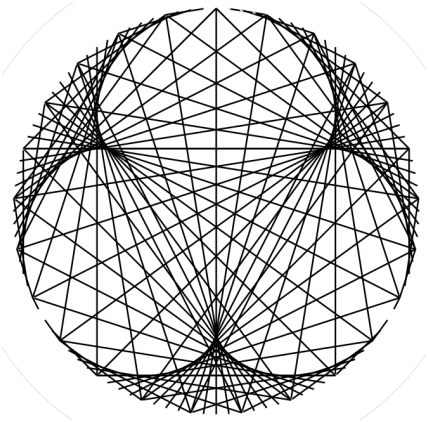
$C_4(20)$ $C_4(40)$



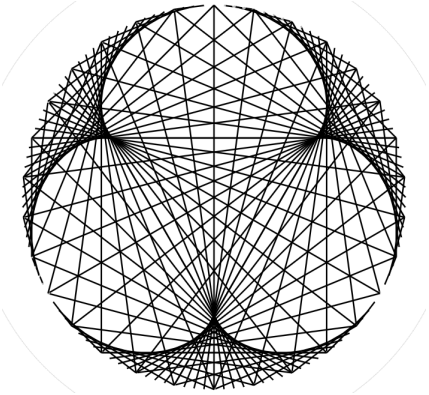
$C_4(60)$



$C_4(80)$



$C_4(100)$



$C_4(120)$

Fonte: Autor.

Portanto, inicialmente podemos supor que o número n de ciclos de uma epicicloide tem relação com a multiplicidade a de um chryzode quando $m \to +\infty$. Já que,

$$a = 2 \Rightarrow n = 1,$$
$$a = 3 \Rightarrow n = 2,$$
$$a = 4 \Rightarrow n = 3,$$

o que nos faz acreditar que

$$n = a - 1.$$

Teorema 3.3.3. *Dado um chryzode $C_a(m)$ onde $a, m \in \mathbb{N}$ e $2 \leq a \leq m-1$, este converge para uma epicicloide simples de $n = a-1$ ciclos quando $m \to +\infty$.*

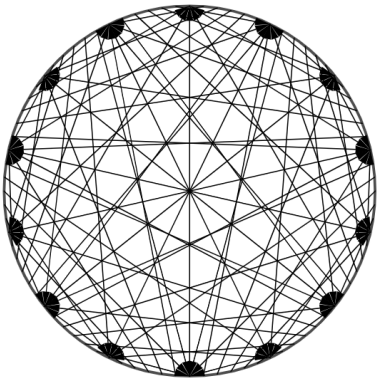
A demonstração deste teorema, se encontra no Apêndice F, uma vez que seu desenvolvimento completo demanda de conceitos de cálculo que ultrapassam o escopo e os objetivos propostos para esta dissertação.

3.4 A presença dos Chryzodes na arte e na vida

Há milénios que a humanidade expressa na linguagem universal da geometria a sua busca por padrão, ordem e significado. Dos círculos sagrados dos povos nativos aos rosetões das catedrais góticas, onde a luz se desmaterializa em cor, os padrões geométricos consagram-se como arquétipos de centricidade, totalidade e a busca pelo sagrado. De forma similar, o "*String Art*" ou "arte das cordas" (técnica construtiva que, através de cordas esticadas, transfere medidas e gera formas) personifica o conhecimento matemático, unindo a abstração numérica ao mundo físico.

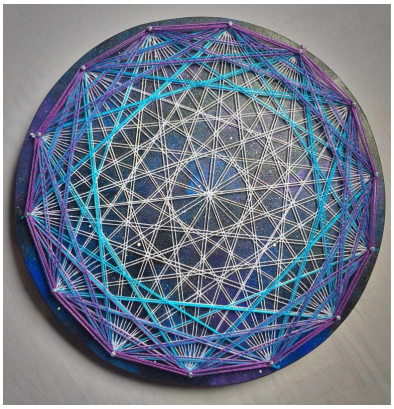
O uso do string art para criação de mandalas[1], por exemplo, pode ser análogo à construção de um chryzode. As figuras alinhadas à esqueda e á direita apresentam, respectivamente, chryzodes construídos no software GeoGebra e mandalas desenvolvidas com base nesses padrões.

Figura 32 – Chryzode $C_{78}(84)$



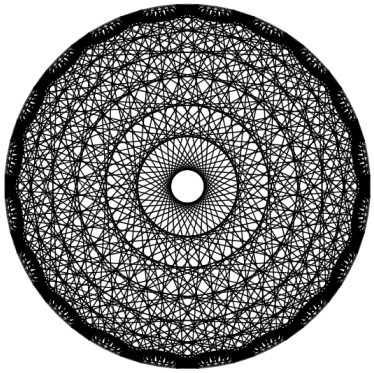
Fonte: Autor.

Figura 33 – Mandala feita com cordas e pregos



Fonte: (Decor, 2024).

Figura 34 – Chryzode $C_{161}(340)$



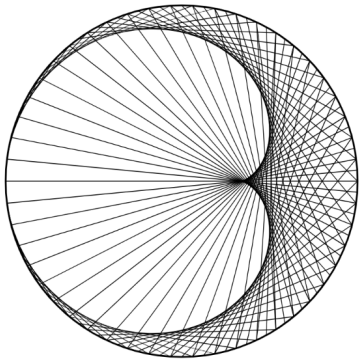
Fonte: Autor.

Figura 35 – Mandala inspirada no Chryzode $C_{161}(340)$

Fonte: (Yoon, 2017).

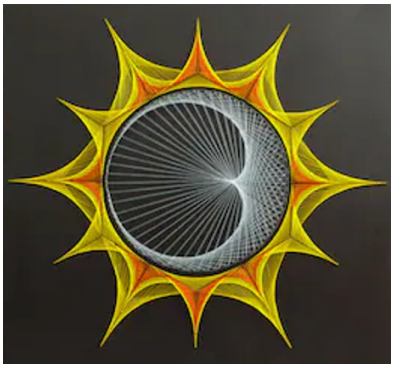
[1] "A mandala é, originalmente, um círculo que contém em seu interior desenhos de formas geométricas, figuras humanas e cores variadas. São encontradas em religiões como o budismo e o hinduísmo, bem como na cultura de tribos indígenas norte-americanas como os Sioux"(Bezerra, s.d.).

Figura 36 – Chryzode $C_2(100)$



Fonte: Autor.

Figura 37 – Mandala inspirada no Chryzode $C_2(100)$



Fonte: (Pankova, 2025).

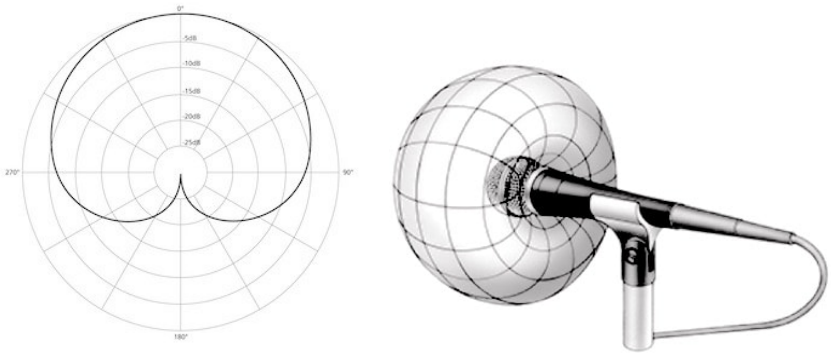
Além da arte, os chryzodes como padrões epicicloidais transcendem a estética pura, manifestando-se como uma linguagem geométrica universal que modela fenômenos surpreendentemente diversos.

O formato e o funcionamento de certos microfones são exemplos disso. Entre as dezenas de milhares de designs de microfones existentes, o padrão polar cardioide é o mais popular.

Segundo Stegmayer (s.d.) "um microfone cardioide tem um padrão de captação/polar cardióide unidirecional. É mais sensível a sons no eixo (onde o microfone “aponta”), geralmente 6 decibéis[2] menos sensível às laterais, e possui um ponto nulo na parte traseira". Microfones cardioides são reverenciados por sua direcionalidade e rejeição de sons traseiros.

A Figura 38 mostra várias linhas que representam ângulos ao redor da cápsula do microfone em 2D (em incrementos de 30°). Também mostra círculos de sensibilidade (em incrementos de 5 dB).

Figura 38 – Padrão polar cardiode 2D e 3D



Fonte: (Stegmayer, s.d.).

A escolha do padrão polar cardioide em transdutores acústicos traz consigo vantagens operacionais tão significativas que o tornaram um dos diagramas mais universais e adaptáveis na engenharia de áudio. Alguns desses benefícios são:

[2] Unidade de medida que expressa a intensidade do som (dB).

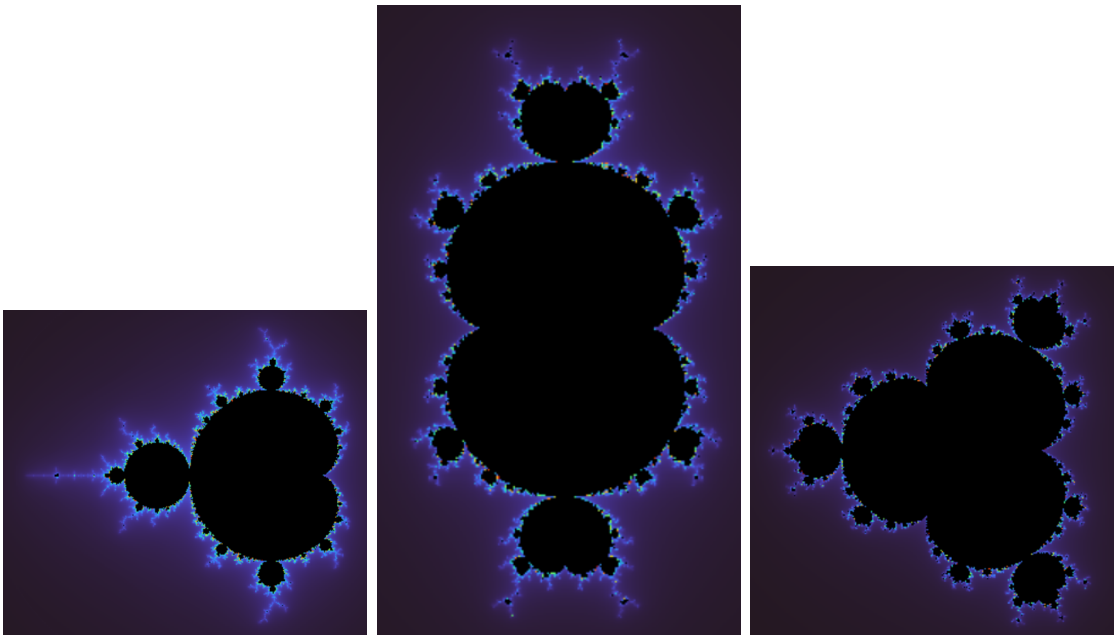
1. **Captação Frontal Preferencial**, tendo rejeição de ruídos de fundo.
2. **Maior Ganho antes do Feedback**, permitindo maiores níveis de volume em sistemas de sonorização sem causar o característico "apito"de realimentação.
3. **Versatilidade de Aplicação**.
4. **Controle Criativo**: Oferece possibilidades artísticas através do ajuste da distância entre a fonte e o microfone.

Esses padrões também estão presentes no estudo de fractais[3], particularmente em conjuntos como o de Mandelbrot. Conjunto de Mandelbrot é um fractal definido como o conjunto de pontos c no plano complexo para o qual a sequência definida recursivamente:

$$z_0 = 0$$
$$z_{n+1} = z_n^k + c,$$

onde $k \in \mathbb{N}$.

Figura 39 – Exemplos de conjuntos de Mandelbrot.



z^2+c z^3+c z^4+c

Fonte: Autor (feito em "mandelbrot.site").

[3] *Fractais* são estruturas geométricas complexas que exibem auto-similaridade, ou seja, partes menores da figura possuem a mesma aparência ou padrão que a figura maior. Diferente das formas geométricas tradicionais, que possuem dimensões inteiras, os fractais frequentemente possuem dimensões fracionárias que descrevem melhor a sua complexidade.

Para um estudo mais aprofundado sobre fractais e o conjunto de Mandelbrot, recomenda-se a consulta a (Reis, 2016).

Em síntese, os chryzodes transcendem o interesse puramente matemático, constituindo-se como modelos de organização implícita capazes de interpretar e reproduzir padrões complexos em domínios diversos como arte, engenharia e sistemas naturais. Sua relevância estende-se para além da teoria, consolidando-os como ferramentas conceptuais com aplicabilidade direta na interpretação e criação de estruturas no mundo real.

4 ASPECTOS METODOLÓGICOS

Neste capítulo, descrevemos uma sequência didática elaborada para enfrentar um desafio recorrente em nossa educação: o fato de muitos estudantes finalizarem o Ensino Fundamental sem o domínio das operações básicas, particularmente da multiplicação e da divisão. Nosso objetivo, portanto, é fornecer um caminho estruturado para sanar essa defasagem.

Zabala (2010, p. 18 apud Jesuita, 2022, p.39), define sequência didática como sendo "um conjunto de atividades ordenadas, estruturadas e articuladas para a realização de certos objetivos educacionais, que têm um princípio e um fim conhecidos tanto pelos professores como pelos alunos". Ao empregar estratégias variadas (como leituras, experimentos, jogos), essas atividades visam aprofundar o tema de estudo. A abordagem prolongada ao longo de várias aulas oferece ao aluno a oportunidade de assimilar e se apropriar do conteúdo de forma significativa.

Este produto propõe a utilização do tema Chryzodes como uma estratégia lúdica para evidenciar a presença das operações matemáticas elementares no dia a dia. Objetiva-se, com isso, que os alunos reconheçam a multiplicação e a divisão como bases para a compreensão de fenômenos variados, como a criação artística de mandalas através do estudo desses padrões geométricos.

4.1 Metodologia da pesquisa

Esta pesquisa caracteriza-se como uma sequência didática de abordagem mista, combinando métodos quantitativos e qualitativos. Na dimensão quantitativa, serão coletados e analisados dados numéricos referentes ao desempenho e à frequência de padrões de compreensão dos estudantes em atividades envolvendo chryzodes e aritmética básica. Paralelamente, na vertente qualitativa, serão investigadas as percepções, as estratégias e os processos de raciocínio desenvolvidos pelos participantes, por meio de observações e análise de produções. Essa integração metodológica visa obter uma compreensão abrangente tanto dos resultados mensuráveis quanto das experiências subjetivas associadas ao uso didático dos chryzodes.

4.1.1 Contexto e sujeitos

Esta sequência didática foi desenvolvida para ser aplicada em turmas de 9º ano, podendo ser adaptada a outras séries. Ela está organizada em cinco etapas, distribuídas ao longo de nove aulas, conforme a seguinte distribuição:

Etapa 1: Aplicação de uma avaliação diagnóstica com o objetivo de investigar e quantificar o conhecimento dos alunos em relação a aritmética básica. Esta etapa é desenvolvida durante a primeira aula e o questionário utilizado está disponível no apêndice A.

Etapa 2: Serão explicadas as definições necessárias e os procedimentos de construção dos chryzodes, assim como a definição de circuitos hamiltonianos, para que os alunos possam analisar e compreender os diferentes "caminhos" gerativos presentes na estrutura desses objetos matemáticos. No momento de explicar a criação dos chryzodes, é importante que o docente parta da operação $i \cdot a = mq + b_i$ em vez da notação formal de congruência, abordando os elementos dessa operação (dividendo, divisor, quociente e resto). Esta etapa é desenvolvida durante a segunda e terceira aulas.

Etapa 3: Uma atividade tratando da construção de um chryzode com papel, lápis e régua, seguida de uma análise dos caminhos formados pelas conexões dos pontos. Nessa fase, torna-se crucial o acompanhamento pelo professor dos procedimentos adotados pelos alunos na execução das operações, permitindo compreender as conexões estabelecidas em seu raciocínio. Esta etapa é desenvolvida durante a quarta e quinta aulas.

Etapa 4: Propõe-se a realização de uma atividade artística empregando a técnica *String Art* (arte com cordas) para a confecção de mandalas inspiradas nos chryzodes. Este processo desenvolve-se ao longo da sexta, sétima e oitava aulas.

Etapa 5: Na nona aula, é aplicada uma avaliação somativa para verificar o desempenho e a evolução dos estudantes ao final da sequência didática. Tal avaliação está disponível no apêndice E.

4.2 Propostas de atividades

Nesta seção, trazemos as propostas de atividades realizadas nas etapas três e quatro da sequência didática proposta. Todas as atividades são detalhadas mediante descrição, listagem de materiais e roteiro de aplicação. Materiais impressos complementares para atividades selecionadas encontram-se nos apêndices.

4.2.1 Atividade 1 - Chryzode com papel, lápis e régua

Nesta atividade, é disponibilizado um círculo com pontos equidistantes em sua circunferência. O aluno deve enumerá-los de 0 a $m-1$, onde m representa o número total de pontos, e subsequentemente executar as operações matemáticas necessárias para a construção do chryzode, com ênfase no conceito de "resto" da divisão.

A decisão de utilizar o círculo com pontos previamente demarcados ou de desenvolver a construção geométrica completa (incluindo o uso do compasso e a marcação de pontos equidistantes) fica a critério do docente. Para orientações sobre a construção do círculo e a demarcação de pontos com o auxílio de um transferidor, recomenda-se a consulta ao trabalho de (Oliveira, 2015).

- **Habilidades**:

  (EF07MA01) Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos.

  (EF07MA04) Resolver e elaborar problemas que envolvam operações com números inteiros.

  (EF07MA06) Reconhecer que as resoluções de um grupo de problemas que têm a mesma estrutura podem ser obtidas utilizando os mesmos procedimentos.

  (EF07MA16) Reconhecer se duas expressões algébricas obtidas para descrever a regularidade de uma mesma sequência numérica são ou não equivalentes.

- **Objetivo geral**: Capacitar o aluno a construir chryzodes, integrando conceitos de aritmética e geometria para reforçar o aprendizado de operações fundamentais e estimular a criatividade.

- **Materiais necessários**: Papel A4 (contendo o círculo com os pontos já demarcados), régua, lápis, borracha, caneta, lápis de cor (opcional).

  Observação: Caso se opte pela construção completa da figura geométrica, será necessário utilizar compasso e transferidor para traçar o círculo e marcar os pontos equidistantes.

- **Metodologia**: Cada aluno ou grupo receberá a definição do padrão a ser construído, correspondente à multiplicação por um valor a em módulo m. Para a execução, devem ser observadas as seguintes etapas:

  1. (Opcional) Sobre uma folha de papel A4, construir geometricamente um círculo utilizando um compasso e, posteriormente, demarcar pontos equidistantes em sua circunferência com o uso de um transferidor;
  2. Atribuir valores numéricos sequenciais aos pontos, no sentido horário, iniciando em 0 e finalizando em $m-1$, de acordo com o módulo m definido;
  3. Determinar e realizar as conexões $i \to b_i$ do chryzode $i \cdot a \equiv b_i \pmod{m}$ dado, encontrando os valores de b_i nas equações $i \cdot a = mq + b_i$ para cada ponto i;

4. Analisar os padrões de conexão formados, verificando se o chryzode resultante constitui um circuito hamiltoniano ou, alternativamente, se apresenta circuitos menores em subconjuntos de pontos;
5. (Opcional) Colorir o chryzode.

É fundamental que o professor supervisione a execução das operações pelos alunos, permitindo-lhes desenvolver suas próprias estratégias de resolução. É comum que alguns discentes identifiquem primeiro os múltiplos de a como método auxiliar para determinar os restos b_i.

4.2.2 Atividade 2 - Construção de mandalas

A presente atividade concentra-se na construção de mandalas por meio da técnica de *String Art*, prevendo, ao término do processo, a apresentação e discussão das produções pelos alunos.

Para a realização desta atividade, recomenda-se que os discentes sejam organizados em equipes de três ou quatro integrantes. Após a divisão dos grupos e antes da atividade prática, cabe ao professor apresentar uma breve explanação sobre o conceito de mandala, abordando sua origem, significado e contexto histórico e religioso em diferentes culturas. O estudo de (Ramos, 2006) oferece uma base teórica sólida para a compreensão das mandalas em seus aspectos históricos e simbólicos.

Utilizaram-se *sousplats*[1] de MDF (painel de fibras de madeira de média densidade) com o formato circular de 20 *cm* de raio, que serviram como suporte para a construção das mandalas.

Visando à segurança dos alunos, orienta-se que o docente realize previamente a marcação dos pontos nessas bases utilizando pregos, evitando assim o manuseio de objetos pontiagudos pelos discentes.

- **Habilidades**:

  (EF07MA01) Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos.

  (EF07MA04) Resolver e elaborar problemas que envolvam operações com números inteiros.

  (EF07MA06) Reconhecer que as resoluções de um grupo de problemas que têm a mesma estrutura podem ser obtidas utilizando os mesmos procedimentos.

[1] *Sousplat* é um item de mesa de origem francesa que significa "sob o prato". Ele serve como um suporte redondo maior que o prato principal, criando uma moldura elegante e funcional. Além de proteger a toalha de mesa de respingos, o sousplat também ajuda a organizar os espaços na mesa e a marcar os lugares dos convidados.

(EF07MA16) Reconhecer se duas expressões algébricas obtidas para descrever a regularidade de uma mesma sequência numérica são ou não equivalentes.

(EF07MA21) Reconhecer e construir figuras obtidas por simetrias de translação, rotação e reflexão, usando instrumentos de desenho ou softwares de geometria dinâmica e vincular esse estudo a representações planas de obras de arte, elementos arquitetônicos, entre outros.

(EF07MA22) Construir circunferências, utilizando compasso, reconhecê-las como lugar geométrico e utilizá-las para fazer composições artísticas e resolver problemas que envolvam objetos equidistantes.

- **Objetivo geral**: Consolidar a aprendizagem dos conceitos por meio da integração entre matemática, arte e cultura.
- **Objetivos específicos**:

  1. Promover a interdisciplinaridade;
  2. Fortalecer competências socioemocionais;
  3. Facilitar a abstração e a generalização de padrões;
  4. Aplicar e compreender a operação de resto da divisão;
  5. Desenvolver a atenção e o pensamento lógico;
  6. Trabalhar o espírito competitivo.

- **Materiais necessários**: Sousplats de MDF, pregos, martelo, barbante, cola, papel A4 (para fazer os cálculos), lápis, borracha, régua, tesoura, compasso e transferidor.
- **Metodologia**: Esta atividade foi feita para ser desenvolvida em três aulas, onde foram realizadas as seguintes etapas:

  1. Organizar os discentes em equipes de três ou quatro integrantes;
  2. Apresentar uma explicação concisa sobre a mandala, incluindo sua definição, origem, significado e a importância cultural e religiosa que assume em diversas sociedades;
  3. Distribuir os materiais necessários para a atividade: cola, barbante e os sousplats com os pregos já fixados;
  4. Atuar como mediador no processo de cada grupo, intervindo de forma orientativa sempre que se fizer necessário;

5. Encerrar a atividade promovendo um momento de *gallery walk*[2], onde todos podem apreciar e debater as mandalas criadas por cada equipe.

Segundo Rocha; Cardoso; Moura (2019, p. 4) a "*gallery walk* é uma metodologia ativa colaborativa, muito utilizada na Finlândia, na qual os alunos deixam de ser sujeitos estáticos, transformando-se em agentes ativos, construindo juntos um conhecimento determinado pelo professor ou por eles mesmos. O docente é meramente observador desse processo, no qual ele pode e deve mediar oferecendo suporte aos alunos, e quando necessário intervir".

Tal abordagem pode demonstrar vantagens significativas, especialmente no estímulo ao trabalho colaborativo e no desenvolvimento da criatividade e interatividade em sala de aula. No entanto, é crucial que sua implementação seja cuidadosamente planejada e estruturada, uma vez que parte dos alunos podem ter dificuldades em assimilar os objetivos da proposta, e alguns podem encontrar resistência na adaptação ao método. Essa situação evidencia, portanto, a importância do professor como mediador essencial nesse processo.

Os modelos de sousplats e a especificação do barbante empregados na atividade encontram-se representados abaixo.

Figura 40 – Tipos de materiais para criação das mandalas.

Sousplat circular (20*cm* de raio) Barbante de ordem 6

Fonte: autor.

[2] A "*gallery walk*"significa "caminhada na galeria". É uma metodologia educacional onde os alunos percorrem diferentes estações para discutir e aprender sobre temas específicos, promovendo a colaboração e o debate entre os participantes.

5 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Este capítulo apresenta a análise e discussão dos resultados obtidos da sequência didática apresentada do capítulo 4. A aplicação foi conduzida com alunos do 9º ano do ensino fundamental da Escola E.M.T.I. Antônio Paes de Andrade, localizada no município de Farias Brito-CE. A população do estudo compreende todos os 45 estudantes matriculados no 9º ano, distribuídos em duas turmas: a turma A, com 23 alunos, e a turma B, com 22 alunos, ambas em modalidade de ensino presencial. O estudo foi conduzido separadamente com cada turma, mantendo-se idênticos o número de aulas (nove aulas) e a metodologia empregada.

Apesar de este trabalho focar em habilidades da BNCC destinadas ao 7º ano, a aplicação das atividades foi realizada com turmas do 9º ano. A justificativa para essa decisão reside na defasagem de aprendizagem em Matemática apresentada por muitos alunos ao final do Ensino Fundamental.

Cabe ao professor de Matemática criar situações que instiguem os alunos a investigar, analisar e resolver diferentes problemas, assegurando um maior amadurecimento intelectual e a formação de um pensamento crítico.

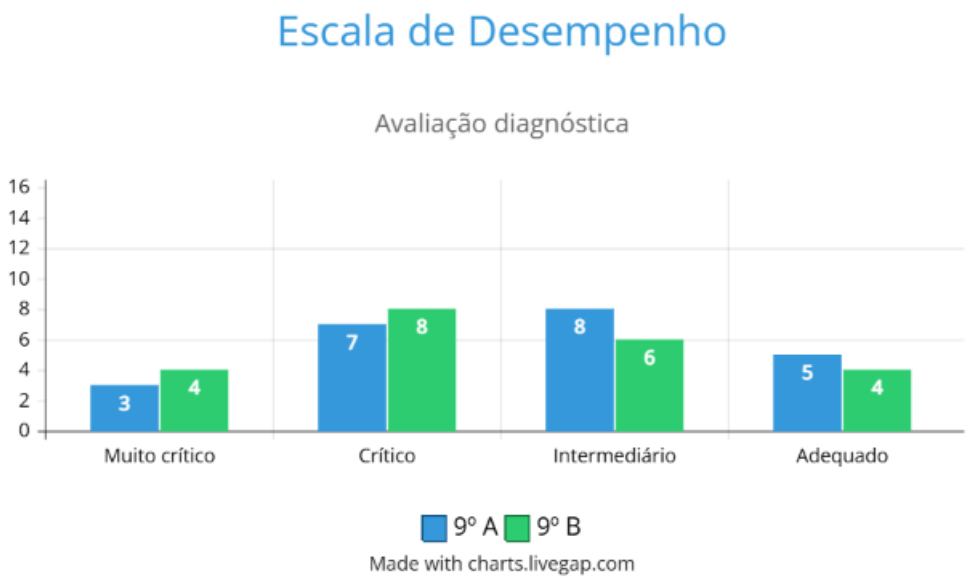
A seguir temos os registros, resultados e fotos da aplicação do plano de aula.

5.1 Avaliação diagnóstica

A primeira etapa consistiu na aplicação do questionário diagnóstico, com o objetivo de investigar e mensurar a compreensão dos alunos acerca dos conhecimentos prévios essenciais ao tema. O gráfico a seguir exibe os resultados conforme a seguinte escala de desempenho:

- **Muito crítico**: até 25% de acertos ($\leq 25\%$);
- **Crítico**: mais de 25% e até 50% acertos ($> 25\%$ e $\leq 50\%$);
- **Intermediário**: mais de 50% e até 75% acertos ($> 50\%$ e $\leq 75\%$);
- **Adequado**: mais de 75% de acertos ($> 75\%$).

Gráfico 1 – Resultado da avaliação diagnóstica.

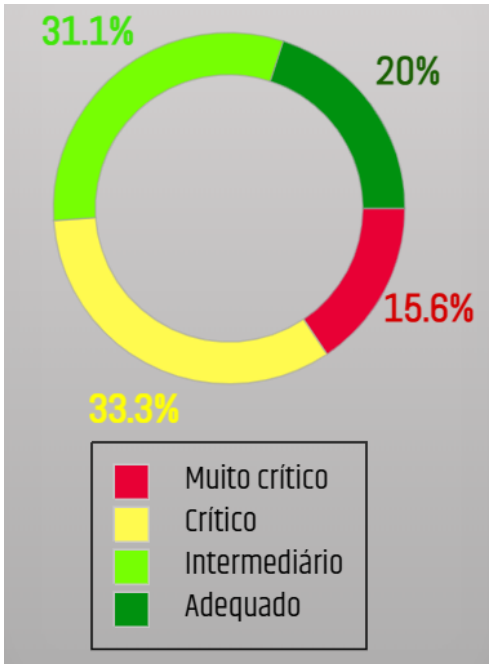


Fonte : Feito pelo autor no site "charts.livegap.com".

Os dados revelaram que 48,9% dos alunos (22 de 45) encontram-se em patamares considerados críticos ou muito críticos, isto é, abaixo do nível intermediário. Tal fato ressalta uma realidade preocupante: verifica-se que uma proporção significativa de estudantes finaliza o Ensino Fundamental sem dominar os conteúdos básicos de Matemática.

O Gráfico 2 exibe a distribuição percentual consolidada dos resultados das duas turmas.

Gráfico 2 – Resultados da avaliação diagnóstica em taxa percentual.



Fonte : Feito pelo autor no site "charts.livegap.com".

A realidade desses dados é pelos dados corroborada pelos resultados do Programa Internacional de Avaliação de Estudantes (PISA). Conforme o relatório da Organisation for Economic Co-operation and Development (2022), 73% dos estudantes avaliados situaram-se abaixo do nível 2 de proficiência em matemática, o que indica que os adolescentes não dominam competências elementares ou não conseguem realizar operações matemáticas básicas.

5.2 Conceitos Fundamentais

Nesta seção, serão apresentado os conceitos utilizados na segunda e terceira aulas, correspondente à etapa 2 da sequência didática.

Para introduzir o conteúdo, parte-se de uma situação-problema: "Uma escola precisa distribuir 47 alunos em grupos de 6. Determine quantos grupos completos serão formados e quantos alunos permanecerão sem grupo". Após um período de reflexão individual e discussão em duplas, introduz-se a relação fundamental da divisão, expressa por $a = m \cdot q + b$, onde $0 \leq b < m$, que, aplicada ao contexto, resultou em $47 = 6 \cdot 7 + 5$. Evidenciou-se que esse resultado é proveniente da estrutura algorítmica da divisão, sendo 47 o dividendo, 6 o divisor, 7 o quociente e 5 o resto.

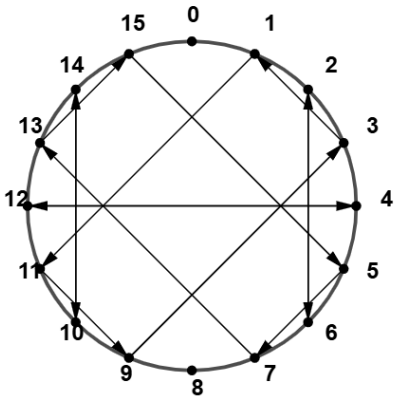
Em seguida, apresenta-se aos alunos que as estruturas geométricas geradas pela relação $i \cdot a = mq + b_i$, onde $i, b_i \in \mathbb{N} \cup \{0\}$ com $0 \leq b_i < m$, são denominadas Chryzodes. Foram mostradas as aparências e as particularidades dessas figuras quando os parâmetros a e m assumem determinados valores.

A partir desse ponto, detalhou-se o método de construção. Para um dado $m \in \mathbb{N}$, resolve-se o sistema de congruências

$$a \cdot i \equiv b_i \pmod{m} \longrightarrow i \cdot a = mq + b_i,$$

para cada ponto i no intervalo $0 \leq i < m$, determinando assim os restos b_i. Em seguida, cada ponto i é conectado ao seu respectivo b_i. O chryzode utilizado como exemplo de construção está representado abaixo na Figura 41.

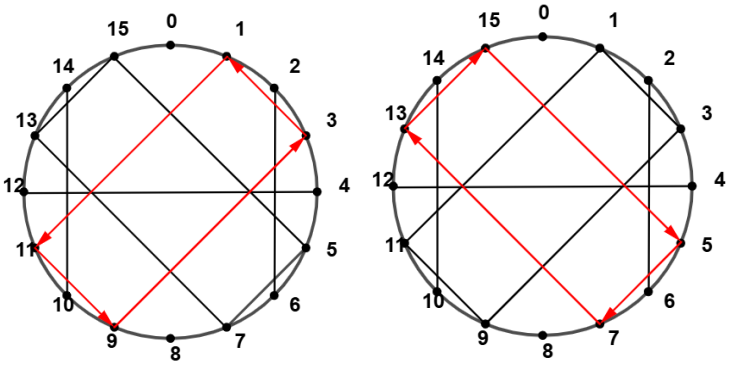
Figura 41 – Chryzode $C_{11}(16)$.



Fonte: autor.

Em seguida, introduziu-se os conceitos de caminhos e circuitos (ou ciclos) da teoria dos grafos, utilizando o chryzode da Figura 41 como referência. A análise conduzida com os alunos permitiu que identificassem a presença de dois circuitos distintos na figura: o primeiro, dado pela sequência $(1 \to 11 \to 9 \to 3 \to 1)$, e o segundo, por $(5 \to 7 \to 13 \to 15 \to 5)$.

Figura 42 – Circuitos dentro do chryzode $C_{11}(16)$



$(1 \to 11 \to 9 \to 3 \to 1)$ $(5 \to 7 \to 13 \to 15 \to 5)$

Fonte: autor.

Durante a discussão, surgiu a questão: "Existe um chryzode que forme um circuito passando por todos os pontos?". Esse questionamento introduziu naturalmente a Definição 3.2.10 de grafo hamiltoniano. Explicou-se que um circuito envolvendo todos os vértices (ciclo hamiltoniano) é impossível na configuração padrão de um chryzode. A justificativa reside no ponto 0: como $0 = 0 + 0$, iniciar o percurso neste vértice resulta em um loop estacionário, impedindo a visita aos outros. No entanto, tais ciclos tornam-se possíveis se o ponto 0 for excluído da análise.

Diante da ausência de conhecimento prévio sobre o tema, o conceito de grafo foi abordado de forma intuitiva. O resultado foi satisfatório: todos os discentes assimilaram o conceito e suas formas de representação, e muitos inclusive estabeleceram conexões com experiências do seu dia a dia. Para maior compreensão, foi apresentado o seguinte exemplo:

Na turma do 9º ano, alguns alunos são melhores amigos:

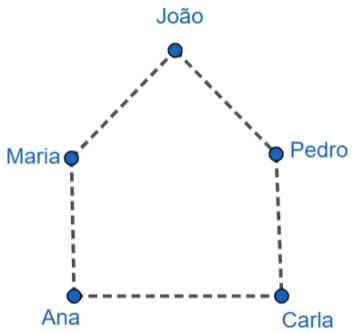
- João é amigo de Maria e Pedro;
- Maria é amiga de João e Ana;
- Pedro é amigo de João e Carla;
- Ana é amiga de Maria e Carla;
- Carla é amiga de Ana e Pedro.

Tarefa: Desenhe o diagrama que representa essas amizades, onde cada aluno é um ponto (vértice) e cada amizade é uma linha (aresta) conectando dois pontos. Responda:

- Quantas amizades existem no total?
- Quem tem mais amigos? Quantos?
- Quem tem apenas um amigo?
- João e Carla são amigos? Como podemos saber olhando o diagrama?

A maioria dos alunos conseguiu nrealizar o desafio, desenhando grafos similares a figura a seguir.

Figura 43 – Representação do grafo feito pelos alunos.



Fonte: autor.

Onde as respostas foram:

- Total de amizades: 5;
- Quem tem mais amigos: João, Maria, Ana, Carla e Pedro (todos têm 2 amigos);
- Ninguém tem apenas 1 amigo;
- João e Carla não são amigos diretos (não há linha conectando-os).

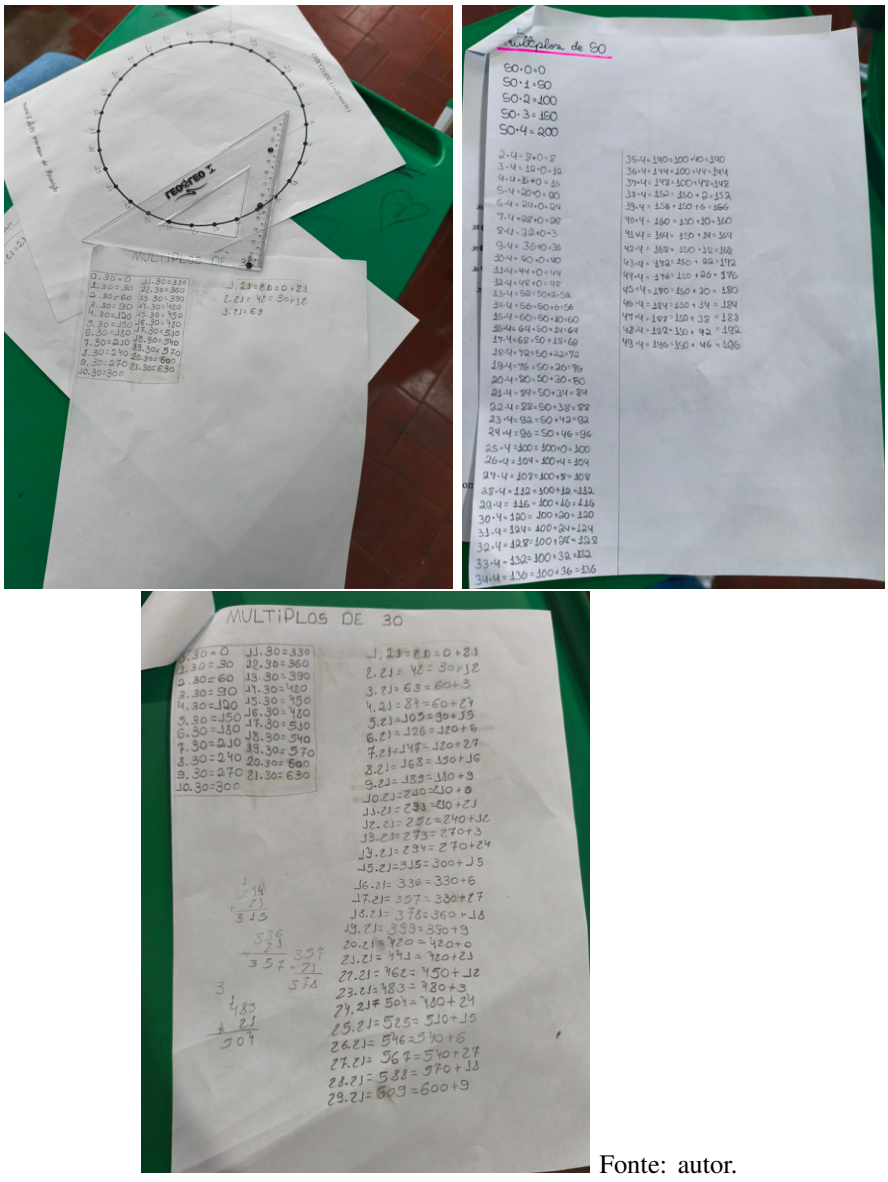
5.3 Chryzodes com papel, lápis e régua

Para a realização desta atividade, referente a etapa 3 da sequência didática, foram entregues a cada aluno os materiais necessários e um tipo de padrão para construção, disponibilizado para impressão no Apêndice B.

No inicio, os estudantes realizaram a enumeração dos pontos de acordo com o padrão recebido. Em seguida, foi solicitado que realizassem as operações $i \cdot a = mq + b_i$ para cada ponto i, a fim de determinar suas respectivas conexões.

A atividade foi concluída com sucesso pela maioria dos estudantes, os quais, em sua maior parte, utilizaram a listagem dos múltiplos de m (termos mq) como ferramenta de apoio. A Figura 44 registra a realização desse procedimento por alguns alunos.

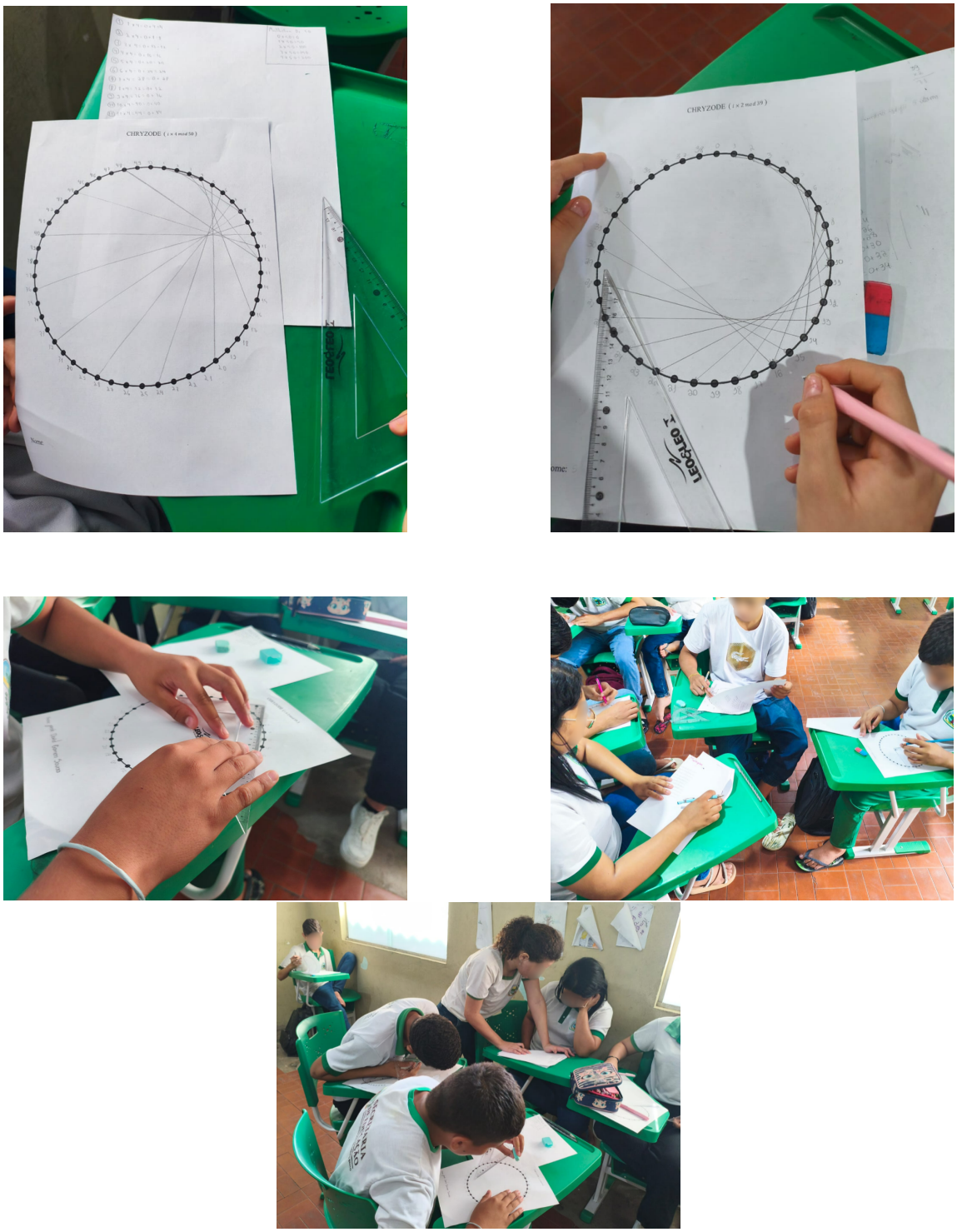
Figura 44 – Realização das operações



Fonte: autor.

Em seguida, os alunos começaram a fazer as conexões $i \to b_i$ utilizando réguas. Alguns alunos apresentaram dificuldades iniciais no manuseio das réguas, porém, gradualmente e por meio da troca de dicas, adaptaram-se à sua utilização.

Figura 45 – Registro das construções



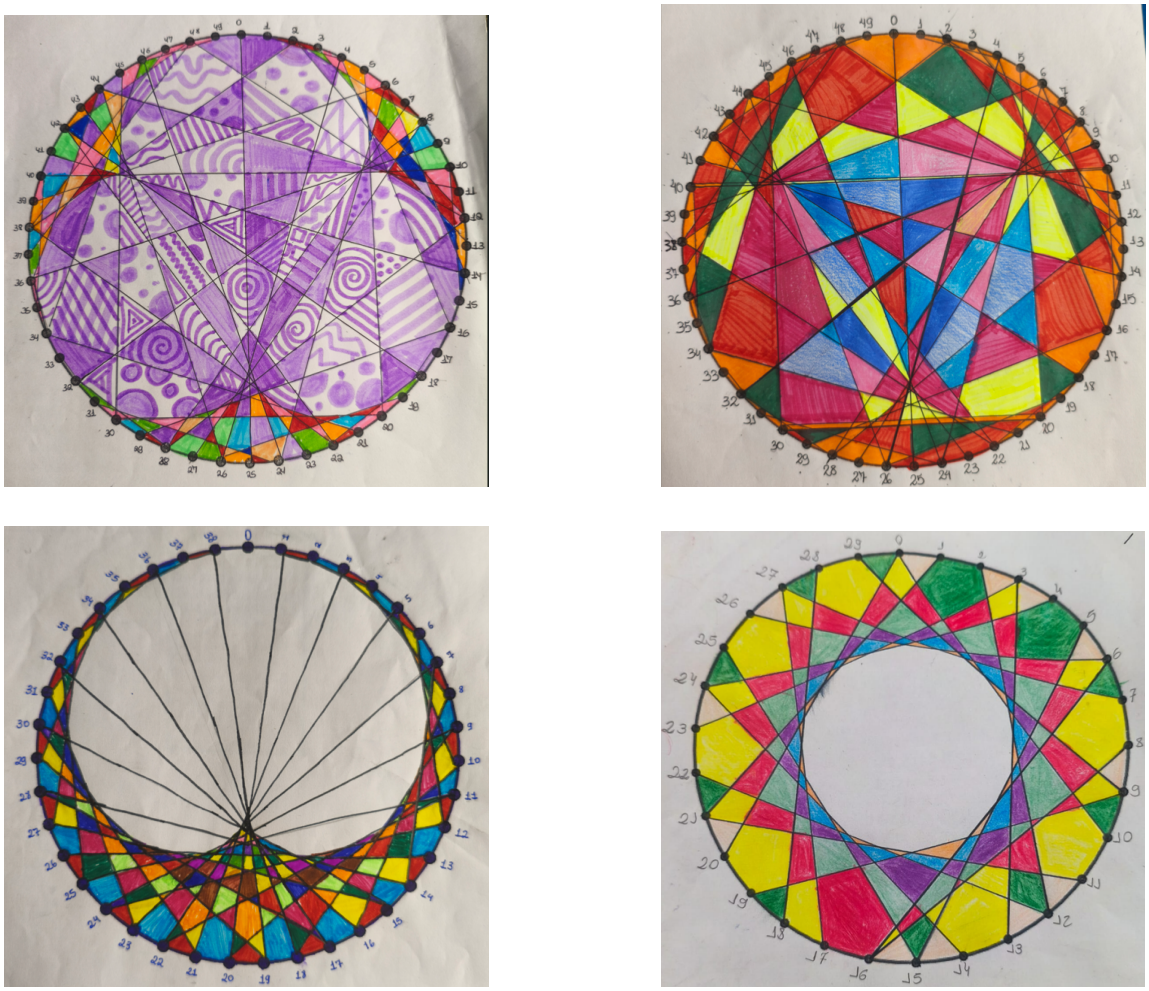
Fonte: autor.

Embora tenham surgido dificuldades pontuais, como no manuseio das réguas, constatou-se que a atividade conseguiu engajar os alunos, que executavam cada cálculo com a expectativa de

visualizar o padrão gráfico resultante. Ao final dessa atividade, referente à etapa 3, solicitou-se que os alunos procurassem circuitos e também colorissem as figuras obtidas de acordo com sua criatividade.

A aplicação da atividade foi bem-sucedida, com a grande maioria dos alunos concluindo todas as etapas propostas.

Figura 46 – Figuras produzidas pelos alunos durante a atividade.



Fonte: autor.

5.4 Construção de mandalas no formato de chryzodes por meio da técnica de String Art

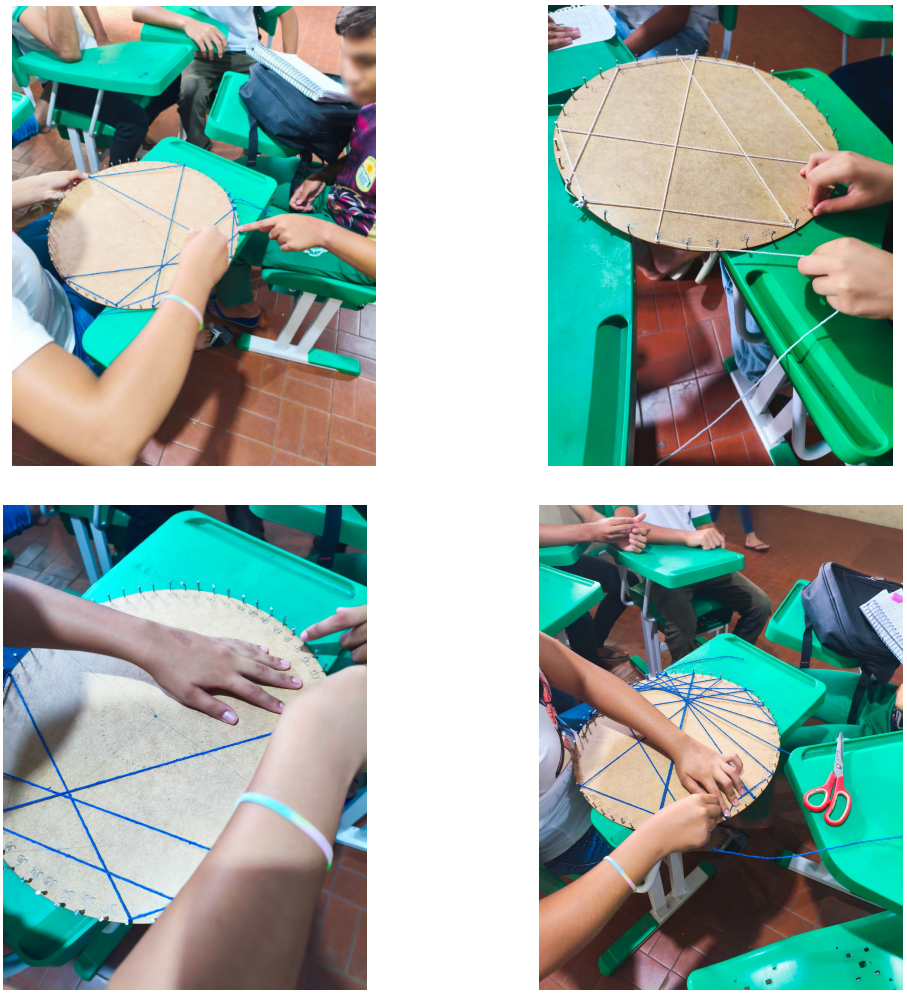
A presente atividade, correspondente à etapa 4 da sequência didática, consiste na criação artística por meio da técnica String Art (arte com cordas), com o objetivo de construir mandalas fundamentadas nos padrões geométricos dos chryzodes.

Inicialmente, a turma foi organizada em quatro grupos, e cada um recebeu os materiais necessários para a atividade: lápis, borracha, régua, tesouras, suportes de MDF com marcações prévias, barbante e folhas A4 para rascunho. Em seguida, foram apresentados os conceitos artísticos e religiosos associados às mandalas, mencionando seu uso no Budismo e Hinduísmo como suportes

visuais para meditação, representações da ordem cósmica e da jornada espiritual do exterior ao centro (do mundano ao divino), e sua presença no Cristianismo, nas rosáceas das catedrais e em ícones de estrutura circular, que simbolizam a glória divina, a ordem celestial e a centralidade de Deus.

Em seguida, iniciou-se a construção das mandalas, com cada membro do grupo participando ativamente da técnica, realizando conexões com o barbante sobre o suporte de MDF, vivenciando, assim, a aplicação prática do String Art.

Figura 47 – Construção das mandalas.



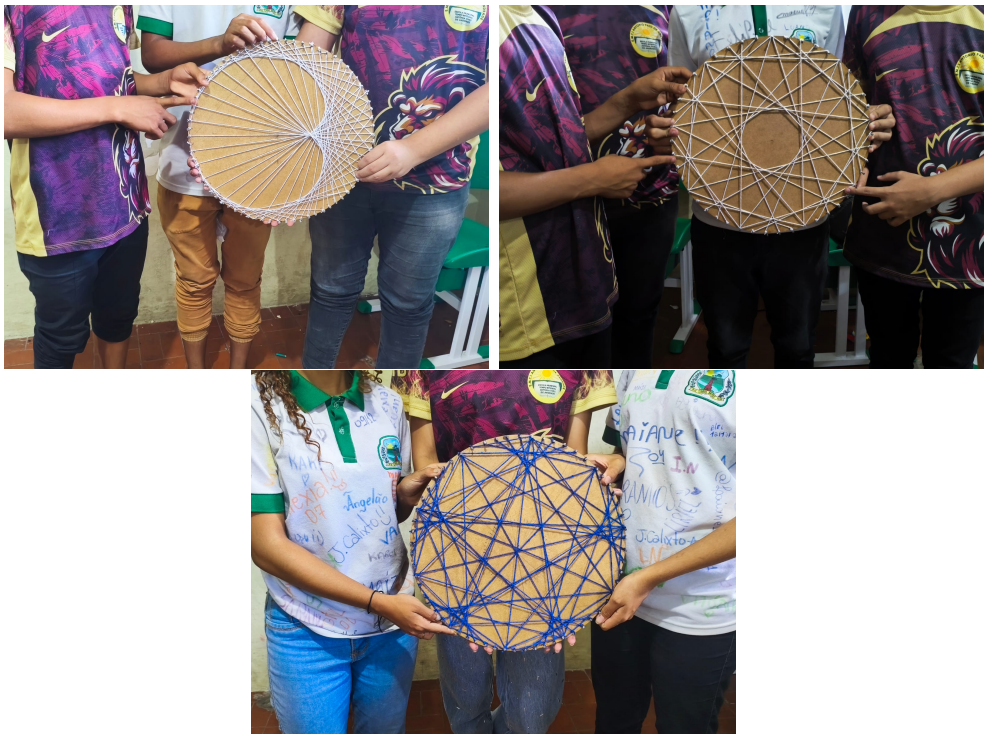
Fonte: autor.

Depois de concluírem as mandalas, os alunos participaram de uma *gallery walk*, onde cada grupo organizou sua própria estação de exposição. Cada estação inclui: A mandala em formato de chryzode e o seu padrão.

Começamos com um momento de observação silenciosa, em que os alunos percorreram as estações individualmente, absorvendo as mandalas sem conversar. Na sequência, retornaram às estações para ouvir as explicações dos grupos criadores sobre a construção e os padrões representados. Esse processo gerou um diálogo vivo entre os participantes, que compartilharam

impressões e debateram os conceitos matemáticos envolvidos, criando um ambiente de comunicação rica e contextualizada.

Figura 48 – Mandalas feitas pelos alunos.



Fonte: Autor.

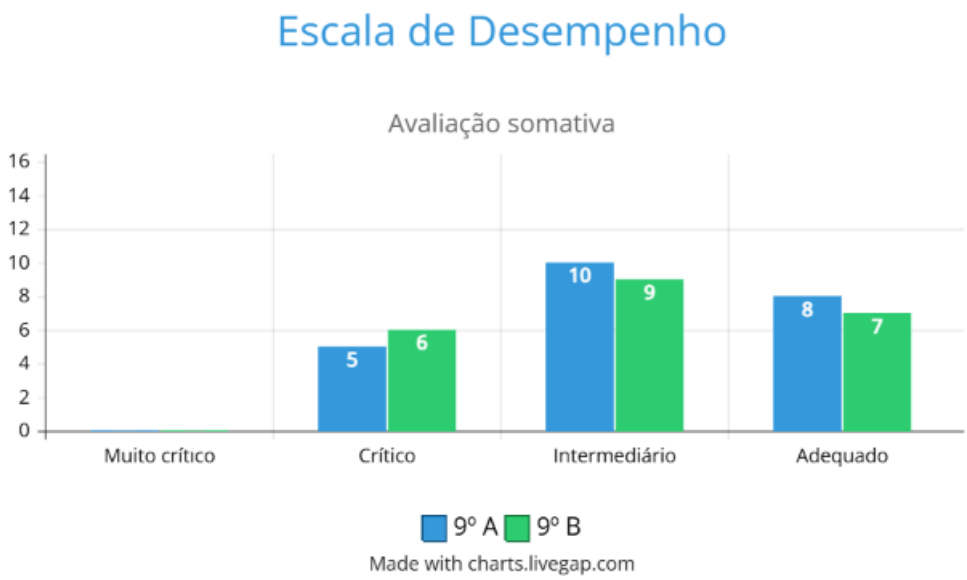
Os alunos não apenas exibiram suas mandalas, mas vivenciaram a matemática como linguagem universal, percebendo que os mesmos padrões que criam beleza artística também regem operações numéricas e estruturas do mundo real.

5.5 Avaliação somativa

A última etapa consistiu na aplicação da avaliação somativa, disponível no apêndice E, com o objetivo de mensurar o desempenho dos alunos ao final da sequência didática, acerca dos conhecimentos prévios essenciais ao tema. O gráfico a seguir exibe os resultados conforme a seguinte escala de desempenho:

- **Muito crítico**: até 25% de acertos ($\leq 25\%$)
- **Crítico**: mais de 25% e até 50% acertos ($> 25\%$ e $\leq 50\%$)
- **Intermediário**: mais de 50% e até 75% acertos ($> 50\%$ e $\leq 75\%$)
- **Adequado**: mais de 75% de acertos ($> 75\%$)

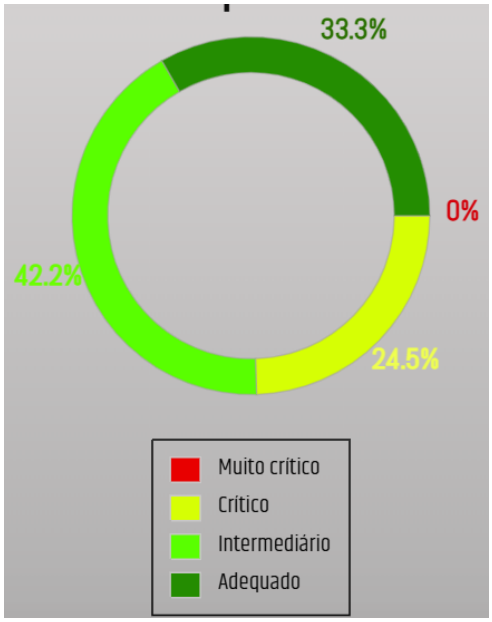
Gráfico 3 – Resultado da avaliação somativa.



Fonte : Feito pelo autor no site "charts.livegap.com".

O Gráfico 4 exibe a distribuição percentual consolidada dos resultados das duas turmas.

Gráfico 4 – Resultados da avaliação somativa em taxa percentual.



Fonte : Feito pelo autor no site "charts.livegap.com".

Observa-se que aproximadamente 24,5% dos estudantes (11 de 45) encontram-se em patamares críticos ou muito críticos, enquanto aproximadamente 75,5% (34 de 45) situam-se nos níveis intermediário e adequado. Em comparação com a avaliação diagnóstica no Gráfico 1, constata-se um avanço notável: o nível muito crítico foi completamente superado, o quantitativo no nível crítico foi reduzido e o número de alunos nos níveis intermediário e adequado aumentou

significativamente.

Os dados quantitativos obtidos através da avaliação somativa aplicada ao final da sequência didática revelam impactos significativos na aprendizagem dos conceitos matemáticos trabalhados. A análise comparativa com os resultados da avaliação diagnóstica inicial permite não apenas mensurar o progresso cognitivo, mas também avaliar a eficácia da metodologia empregada.

A análise quantitativa, contextualizada pedagogicamente, vai além de percentuais isolados, revelando uma trajetória coletiva de avanço. A sequência didática com chryzodes demonstrou ser não só viável, mas também transformadora, ao ressignificar a relação dos estudantes com a matemática básica. A persistência de desafios pontuais não minimiza as conquistas alcançadas; antes, indica direções para o aprimoramento contínuo da prática docente.

As evidências coletadas corroboram a premissa de que metodologias que articulam dimensões estéticas, colaborativas e visuais têm o potencial de reestruturar significativamente os processos de ensino e aprendizagem em matemática, especialmente no âmbito das operações fundamentais e de suas múltiplas representações.

24

6 CONSIDERAÇÕES FINAIS

O objetivo deste trabalho é disponibilizar, através de uma sequência didática, recursos que apoiem a aprendizagem das operações básicas pelos estudantes via divisão euclidiana. Com foco na natureza epicicloidal dos chryzodes, propõe-se ilustrar suas aplicações em diversos contextos do dia a dia, inclusive na expressão artística. Apesar de as congruências aritméticas não integrarem explicitamente o currículo do ensino básico, os padrões visuais intrigantes resultantes da construção dos chryzodes servem como representações gráficas das operações de soma, subtração, multiplicação e divisão, funcionando como ferramentas eficazes para uma assimilação mais significativa desses conteúdos. A realização dessas atividades oferece uma experiência rica e produtiva para alunos e professores.

Ao elaborar as atividades, buscamos integrar práticas lúdicas com as técnicas de construção dos chryzodes, facilitando assim a percepção visual dos padrões. As propostas são flexíveis e podem ser adequadas a distintas realidades de sala de aula, permitindo aplicação em múltiplos contextos educativos.

A organização em grupos possibilitou que os alunos assumissem uma postura ativa perante os desafios, promovendo trocas de ideias, expressão de pensamentos e a dedução conjunta de estratégias variadas. Com isso, traçaram caminhos diversos para atingir os resultados, aprendendo também a gerir opiniões diferentes e a negociar para alcançar pontos de acordo.

As principais conclusões evidenciaram a progressão dos alunos quanto aos conceitos abordados, viabilizando a aquisição de conhecimentos pertinentes aos temas. Os estudantes apresentaram resoluções diversificadas, recorrendo a múltiplas formas de representação, o que contribuiu para o aprimoramento de seus raciocínios e ideias matemáticas. Adicionalmente, destacaram que o engajamento proporcionado pela metodologia *gallery walk* e a maneira colaborativa de resolver as tarefas favoreceriam uma retenção mais duradoura dos saberes adquiridos.

Por fim, conclui-se que a construção de chryzodes constitui uma alternativa viável de conteúdo a ser trabalhada com alunos da educação básica, uma vez que permite aplicar, de forma contextualizada, os conhecimentos sobre as operações fundamentais adquiridos em sala de aula, além de funcionar como uma porta de entrada motivadora para a aprendizagem de novos conceitos matemáticos.

REFERÊNCIAS

AMARAL, D. A. **Gauss, Carl Friedrich**. 2023. Acesso em: 1 out. 2025. Disponível em: <https://sites.fem.unicamp.br/~em313/paginas/person/gauss.htm>.

BELLO, M. G. **La aritmética modular y algunas de sus aplicaciones**. Dissertação (Mestrado) — Universidad Nacional de Colombia, 2011.

BEZERRA, J. **Mandala**. s.d. Disponível em: <https://www.todamateria.com.br/mandala/>.

BRASIL. **Parâmetros Curriculares Nacionais: Ensino Médio**. Brasília, 1998. Disponível em: <https://portal.mec.gov.br/seb/arquivos/pdf/matematica.pdf>. Acesso em: 13 nov. 2025.

BRASIL. **Parâmetros Curriculares Nacionais: Ensino Médio**. Brasília, 2000.

BRASIL. **Base Nacional Comum Curricular: Educação Infantil e Ensino Fundamental**. Brasília, 2018.

DECOR, C. **String Art- Mandalas, Nomes, Cactus e Como Fazer Passo a Passo**. 2024. Disponível em: <https://construindodecor.com.br/string-art/>.

FERRETTO, D. **CURVAS: estudo e visualização com o software Cabri-Géomètre II**. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2003.

HEFEZ, A. **Aritmética**. 3ª ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2022.

JESUITA, F. T. P. **CAN'T STOP: uma proposta de sequência didática para o ensino de probabilidade**. Dissertação (Mestrado) — Universidade Rural do Semi-Árido, 2022.

ODUENYI, V. O. **Diofanto de Alexandria**. 2017. Disponível em: <https://www.sapaviva.com/diophantus-of-alexandria/>.

OLIVEIRA, L. M. da S. **ENSINANDO GEOMETRIA COM RÉGUA E COMPASSO, UMA PROPOSTA PARA O 8º ANO**. Dissertação (Mestrado) — Universidade Estadual do Norte Fluminense Darcy Ribeiro, 2015.

Organisation for Economic Co-operation and Development. **PISA 2022 Results**. [S.l.]: OECD Publishing, 2022.

PANKOVA, A. **Sol e Lua**. 2025. Disponível em: <https://sl1nk.com/ukq91yt>.

PONTE, J. P. da. **Matemática: uma disciplina condenada ao insucesso**. Dissertação (Mestrado) — Noesis, 1994.

PUTNOKI, J. C. **Elementos de Geometria e Desenho Geométrico: volume especial para o vestibulando: caderno de atividades.** [S.l.]: Scipione, 1990.

RAMOS, F. da S. **FORMA E ARQUÉTIPO: um estudo sobre a mandala**. Dissertação (Mestrado) — Universidade Estadual de Campinas, 2006.

REIS, M. V. dos. **Conjunto de Mandelbrot**. Dissertação (Mestrado) — Universidade Federal de Goiás, 2016.

ROCHA, R. S.; CARDOSO, I. M. D.; MOURA, M. A. E. de. **O uso da gallery walk como metodologia ativa em sala de aula: uma análise sistemática no processo de ensino-aprendizagem**. Dissertação (Mestrado) — Revista Sítio Novo, 2019.

SCIENCEPHOTO. **Pierre de Fermat**. 2025. Disponível em: <https://www.sciencephoto.com/media/776354/view/pierre-de-fermat-french-mathematician>. Acesso em: 14 out. 2025.

SELINA; FACTS.NET. **Euclid Facts**: Mathematical symbols. 2024. Disponível em: <https://facts.net/euclid-facts/>. Acesso em: 17 set. 2025.

SOUZA, A. L. de. **Teoria dos Grafos e Aplicações**. Dissertação (Mestrado) — UNIVERSIDADE FEDERAL DO AMAZONAS, 2013.

STEGMAYER, C. **O que é um microfone cardióide? (Exemplos de padrão polar + microfone)**. s.d. Disponível em: <https://sl1nk.com/qszkopa>.

VIEIRA, F. de B. **Diofanto de Alexandria**. 2018. Disponível em: <https://clubes.obmep.org.br/blog/b_diofanto-de-alexandria/>.

WIKIPéDIA. **Leonhard Paul Euler**. 2020. Disponível em: <https://pt.wikipedia.org/wiki/Leonhard_Euler/>.

WIKIPéDIA. **Étienne Bézout**. 2024. Disponível em: <https://pt.wikipedia.org/wiki/%C3%89tienne_B%C3%A9zout>.

WIKIPéDIA. **Carl Friedrich Gauss**. 2025. Disponível em: <https://pt.wikipedia.org/wiki/Carl_Friedrich_Gauss>.

YOON, J. **Samsara**. 2017. Disponível em: <https://artlecture.com/artworks/2580>.

YOSHIKO. **Grafos Hamiltoniano**. 2020. Disponível em: <https://www.ime.usp.br/~yw/2020/grafinhos/aulas/cap4-slides.pdf>.

ZABALA, A. **A prática educativa: como ensinar**. [S.l.]: Artmed, 2010.

APÊNDICE A – AVALIAÇÃO DIAGNÓSTICA

Avaliação Diagnóstica

Nome: Turma:

1. Sara comprou 8 cadernos iguais, pagando com uma nota de $R\$$ 50,00 e recebeu $R\$$ 16,00 de troco. Qual era o preço de cada caderno ?

2. Em uma divisão exata, o divisor é 15 e o quociente é 28. Qual é o dividendo?

3. Um agricultor colheu 1.845 laranjas e quer embalá-las em caixas que cabem 15 laranjas cada. Quantas caixas ele poderá encher completamente?

4. Um cinema tem 24 fileiras com 32 poltronas em cada fileira. Se em uma sessão foram vendidos 689 ingressos, quantas poltronas ficaram vazias?

5. Um campeonato de futebol com 5 times usa um sistema em que cada time joga contra todos os outros uma vez. Cada jogo é representado por uma aresta em um grafo, onde os vértices são os times. Quantos jogos haverá no total?

6. Para realizar um campeonato de vôlei em uma escola o professor de educação física decidiu dividir os 96 alunos em grupos. Sabendo que cada equipe para esse esporte deve ser composta por 6 pessoas, quantas equipes o professor conseguiu formar?

7. Para um aniversário, as 30 mesas disponíveis em um salão de festa foram distribuídas de modo que cada mesa seria para 6 convidados e, mesmo assim, ainda restariam 2 convidados para acomodar. Sabendo disso, calcule quantas pessoas foram convidadas para festa.

8. Determine se 2 491 é múltiplo de 57.

9. Analisando a sequência {A, B, C, D, A, B, C, D, A, B, C, D,...}, qual é o termo de poisção 1686^{o} ?

10. Na divisão de A por B, números inteiros estritamente positivos, foram obtidos quociente 2 e resto 9. Obtém-se quociente 2 e resto 5, dividindo-se A por B acrescido de quanto?

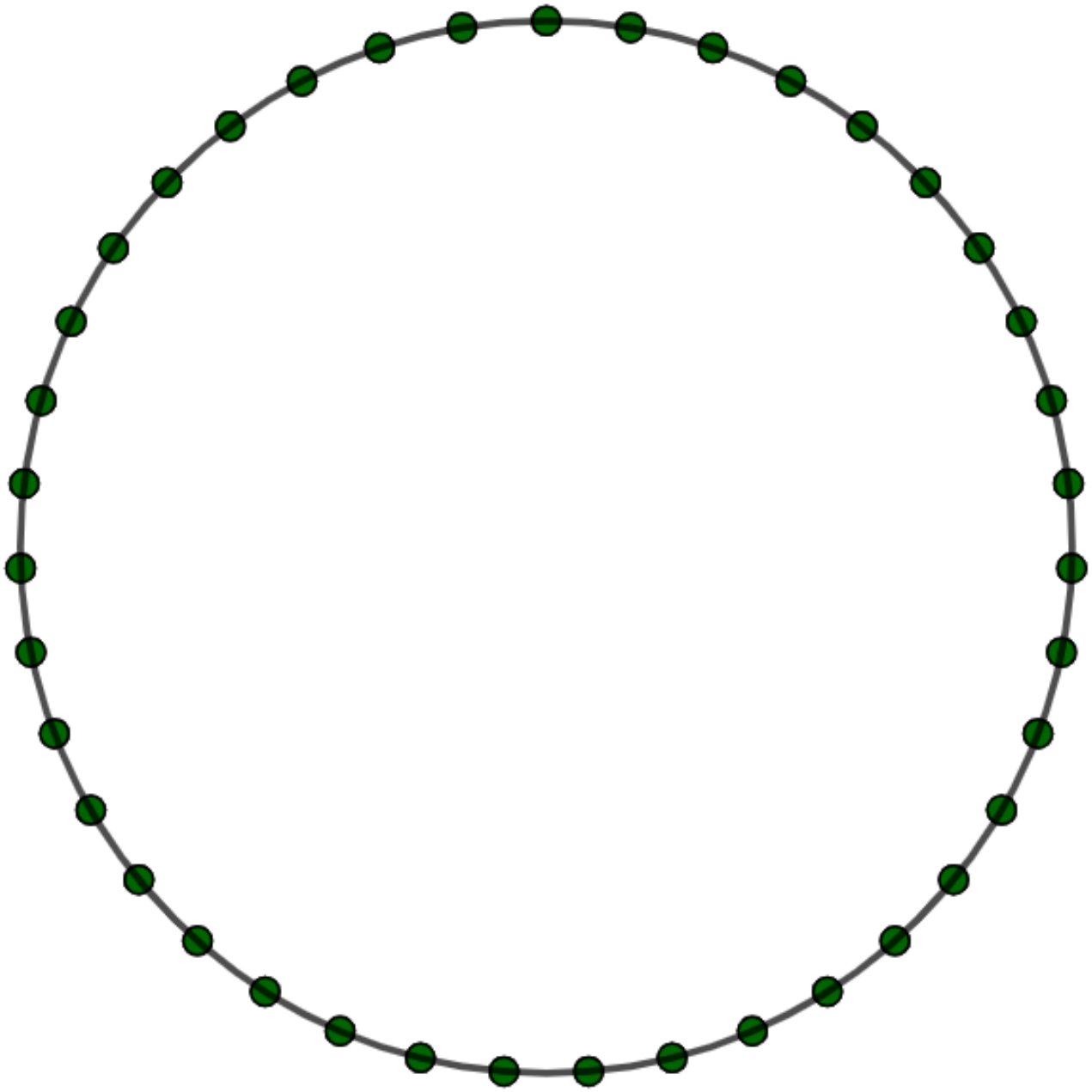
11. Um labirinto tem 5 salas (A, B, C, D, E) com portas entre: A $\rightleftharpoons$ B, A$\rightleftharpoons$C, B$\rightleftharpoons$D, C$\rightleftharpoons$D, D$\rightleftharpoons$E.

    a) Desenhe o grafo.

    b) É possível visitar todas as salas passando por cada porta apenas uma vez?

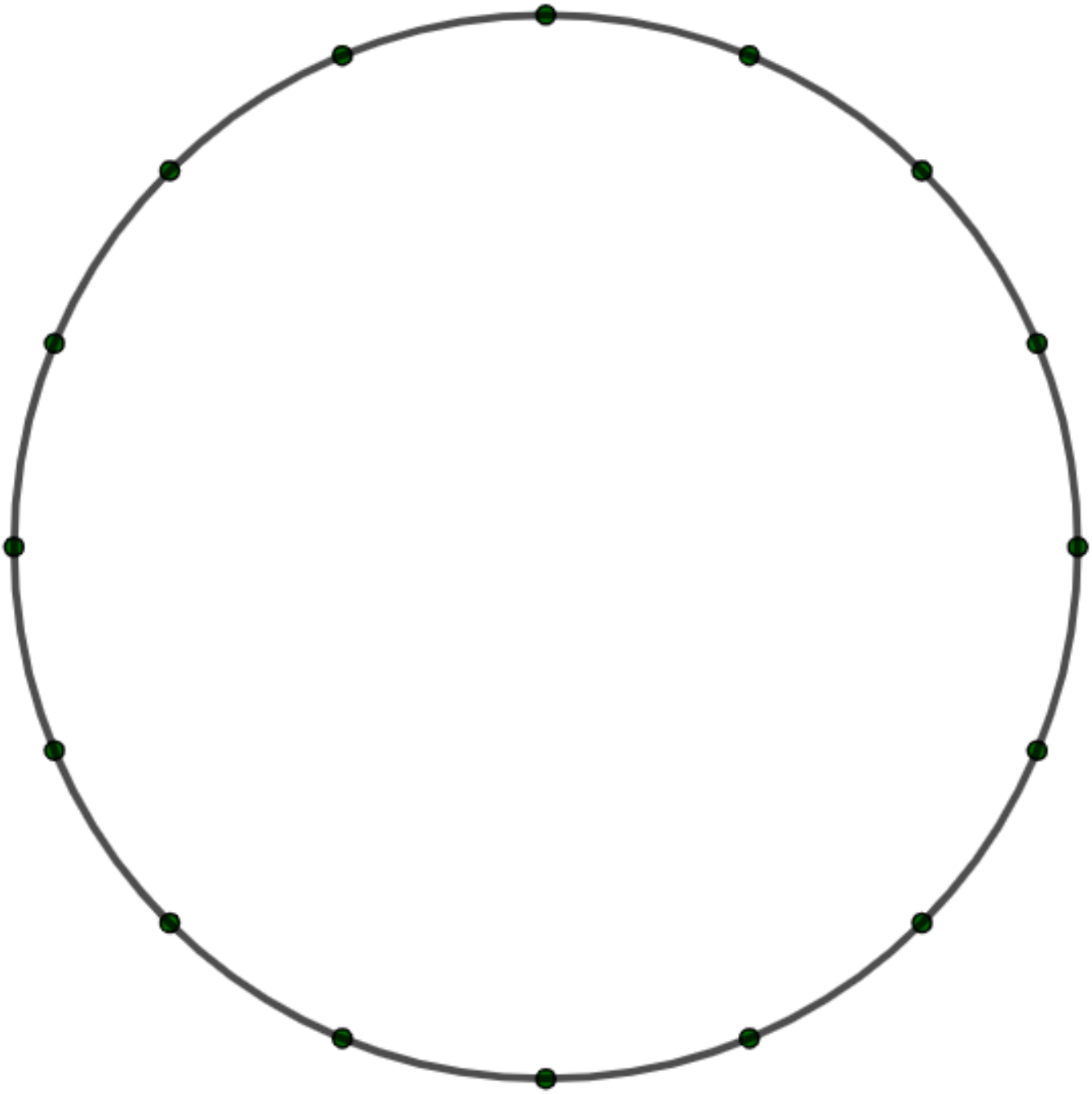
APÊNDICE B – IMPRESSÕES PARA A ATIVIDADE 1

CHRYZODE ($i \times 2 \, mod \, 39$)



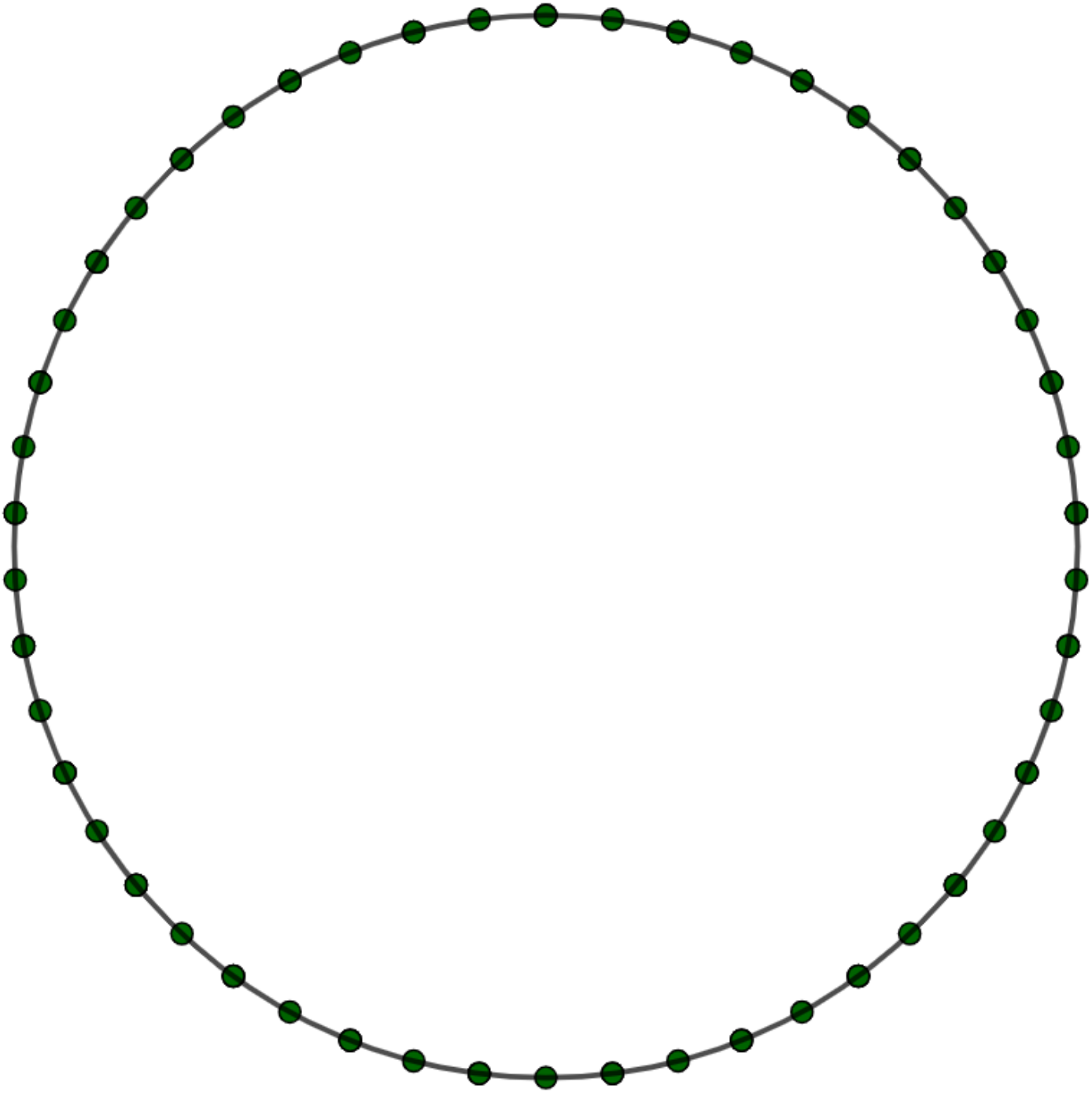
Nome:

CHRYZODE ($i \times 3 \, mod \, 16$)



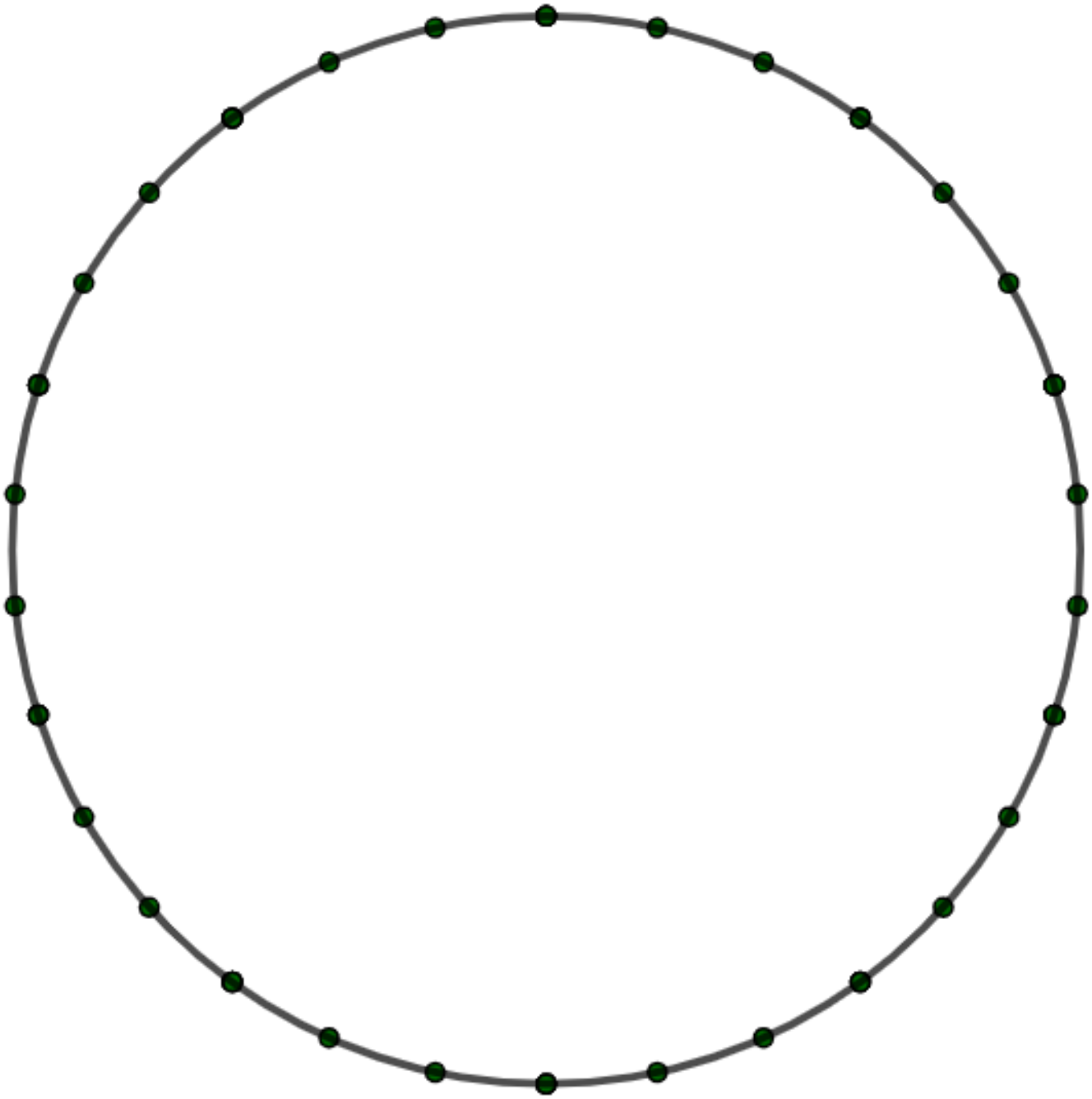
Nome:

CHRYZODE ($i \times 4 \, mod \, 50$)



Nome:

CHRYZODE ($i \times 21 \, mod \, 30$)

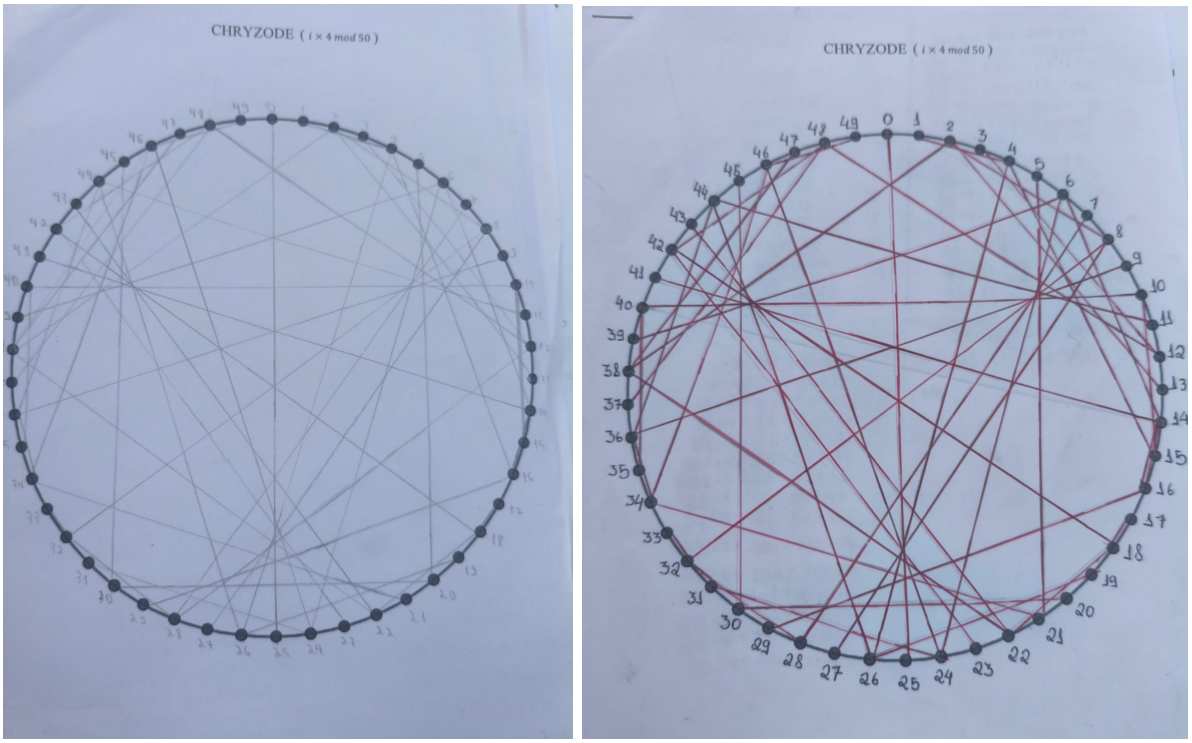


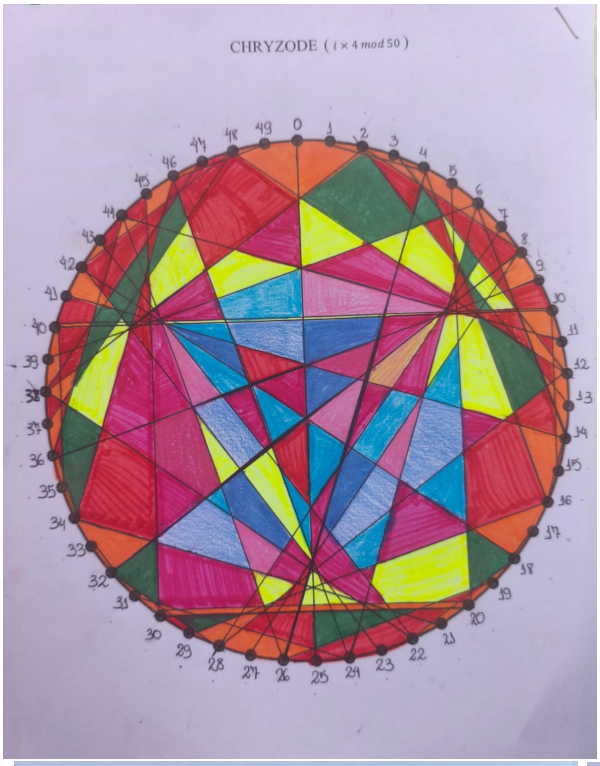
Nome:

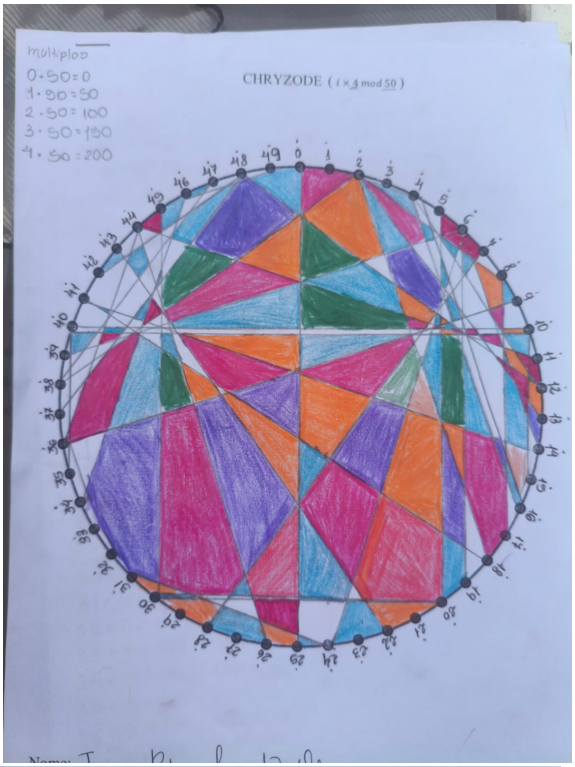
APÊNDICE C – CHRYZODES FEITOS DURANTE A ATIVIDADE DA ETAPA 3

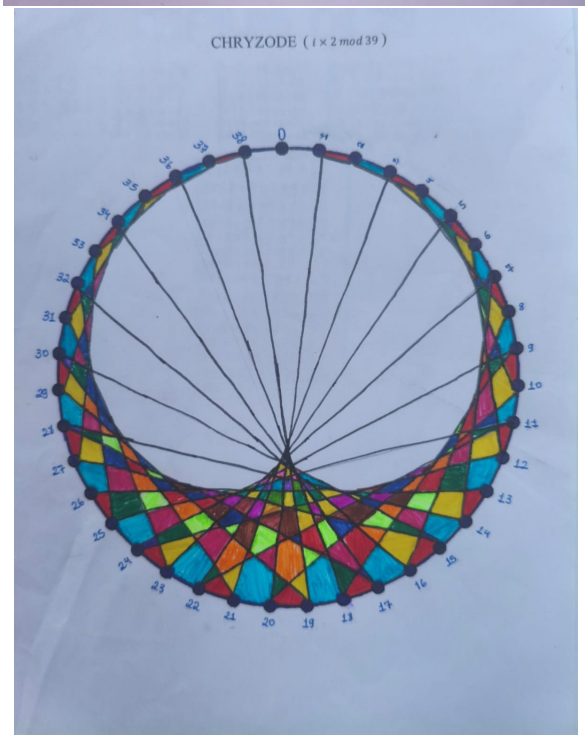
Aqui contemplamos algumas produções sobre Chryzodes dos discentes dos 9º anos A e B do Ensino Fundamental da Escola Municipal de Tempo Integral Antonio Paes de Andrade. Os trabalhos revelam a interdependência entre habilidades técnicas com instrumentos de precisão e competências socioemocionais como concentração e criatividade.

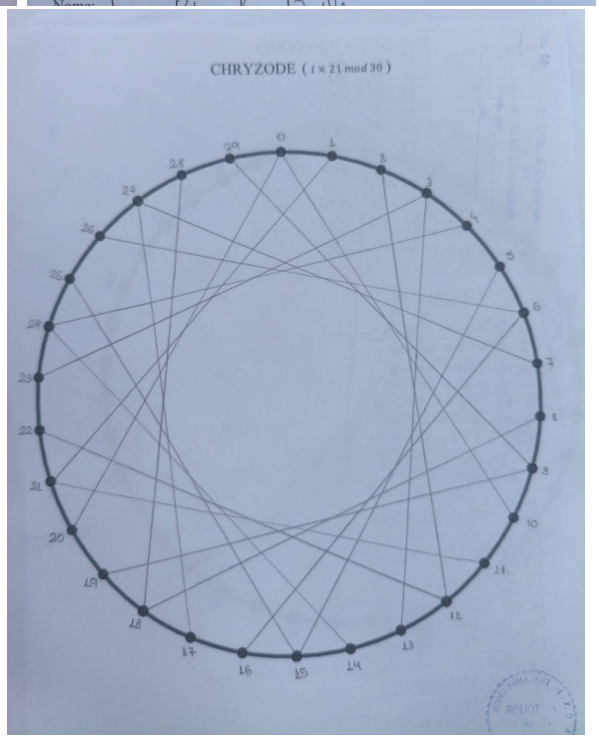
Figura 49 – Alguns dos Chryzodes produzidos pelos alunos.



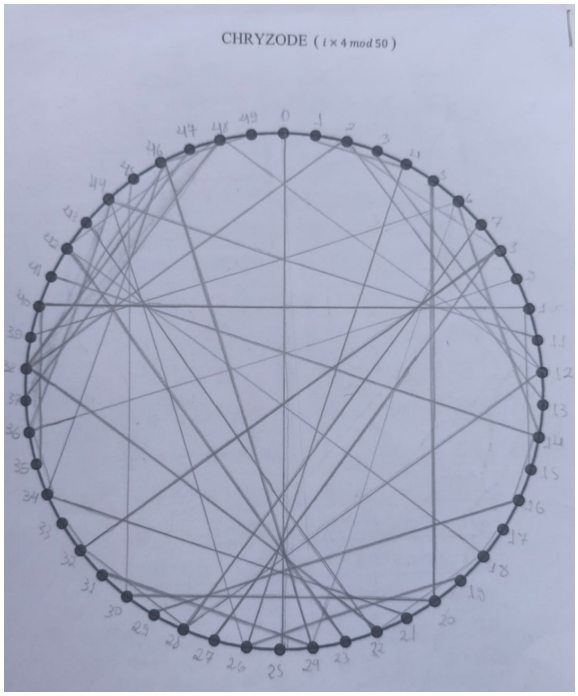

CHRYZODE (i × 4 mod 50)


multiples
0 · 50 = 0
1 · 50 = 50
2 · 50 = 100
3 · 50 = 150
4 · 50 = 200
CHRYZODE (i × 4 mod 50)


CHRYZODE (i × 2 mod 39)


CHRYZODE (i × 21 mod 30)

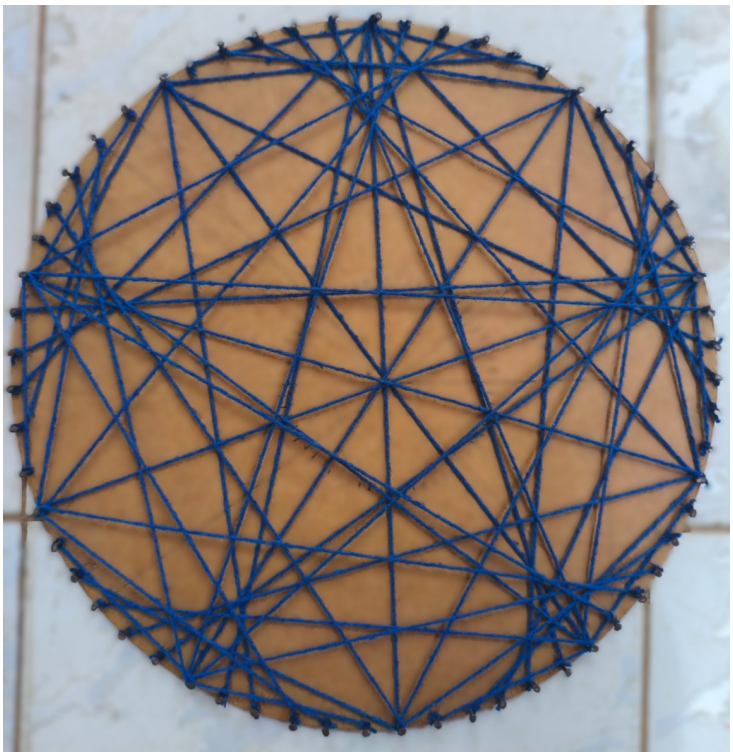

CHRYZODE ($i \times 2 \bmod 39$)

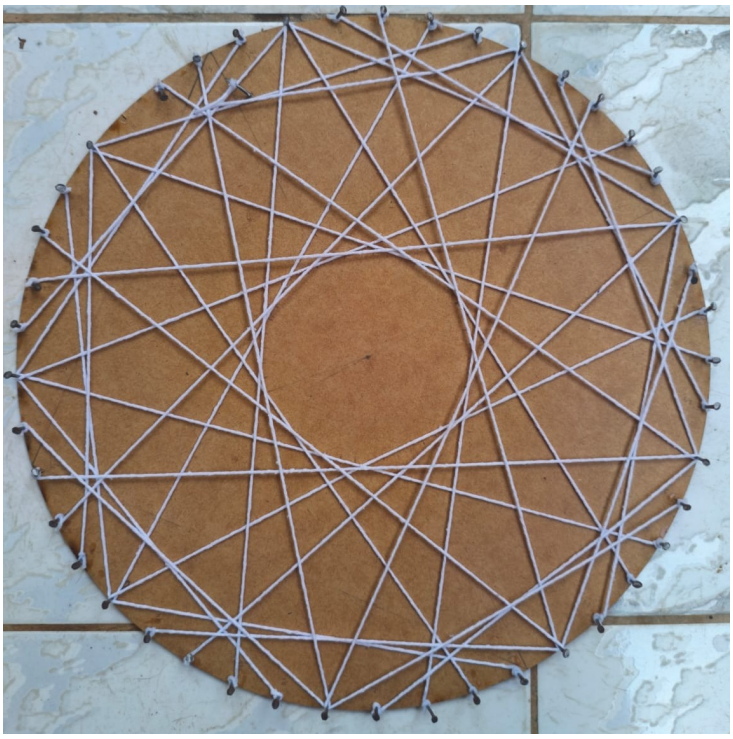

CHRYZODE ($i \times 4 \bmod 50$)

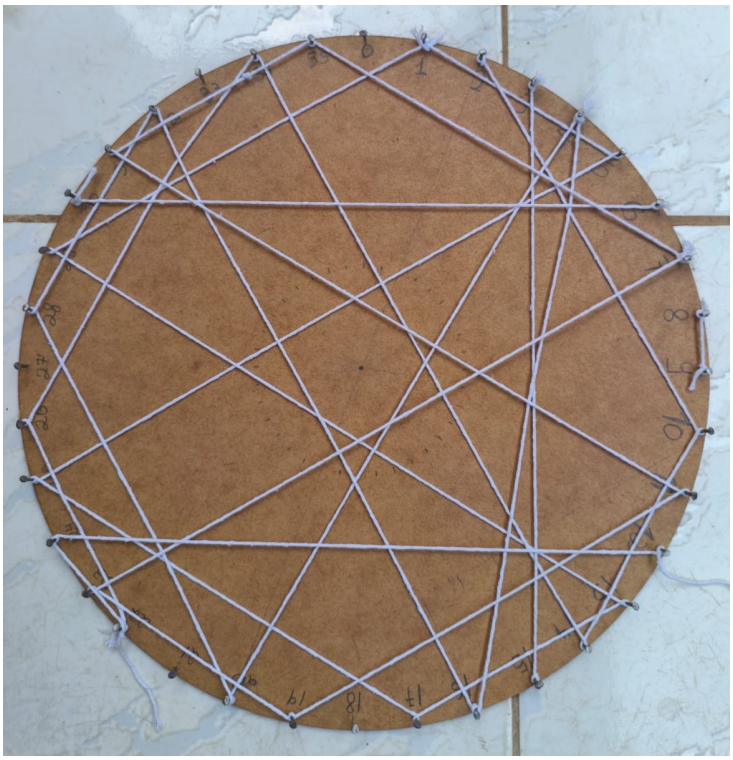
APÊNDICE D – CONSTRUÇÕES DE MANDALAS REALIZADA NA ATIVIDADE DA ETAPA 4

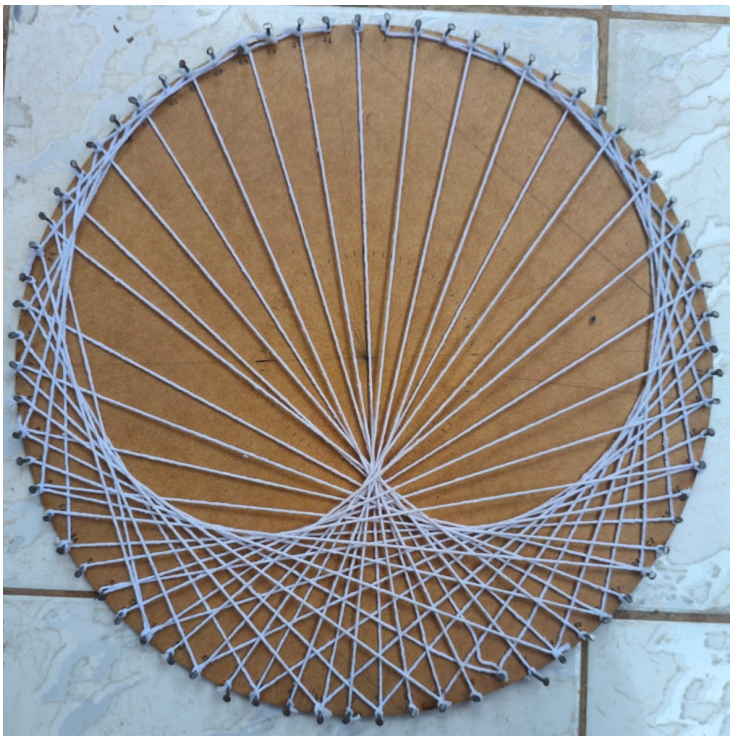
Aqui contemplamos algumas mandalas inspiradas em Chryzodes dos discentes dos 9º anos A e B do Ensino Fundamental da Escola Municipal de Tempo Integral Antonio Paes de Andrade.

Figura 50 – Mandalas produzidas pelos alunos.









APÊNDICE E – AVALIAÇÃO SOMATIVA

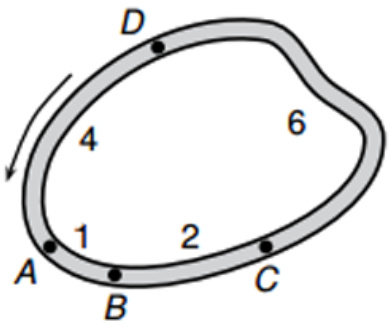
Avaliação Somativa

Nome: Turma:

1. Formalize matematicamente o Algoritmo da Divisão Euclidiana.

2. Encontre o número natural que ao ser dividido por 7 resulta um quociente 4 e resto maior possível.

3. (OBMEP 2006 – N1Q6 – 2ªfase)A figura abaixo representa o traçado de uma pista de corrida.



Os postos A, B, C e D são usados para partidas e chegadas de todas as corridas. As distâncias entre postos vizinhos, em quilômetros, estão indicadas na figura e as corridas são realizadas no sentido indicado pela flecha. Por exemplo, uma corrida de 17 quilômetros pode ser realizada com partida em D e chegada em A.

(a) Quais são os postos de partida e chegada de uma corrida de 14 quilômetros?

(b) E para uma corrida de 100 quilômetros, quais são estes postos?

(c) Mostre que é possível realizar corridas com extensão igual a qualquer número inteiro de quilômetros.

4. João tem R$ 350 e quer comprar jogos que custam R$ 48 cada. Quantos jogos ele pode comprar? Quanto dinheiro sobrará?

5. Quatro times (T1, T2, T3, T4) vão jogar entre si. Cada time joga uma vez contra cada outro.

   a) Quantos jogos haverá no total?

   b) Desenhe o grafo onde vértices são times e arestas são jogos.

6. Numa divisão, o divisor é 23, o quociente é 15 e o resto é o maior possível. Qual é o dividendo?

7. Um carteiro precisa entregar cartas em 5 ruas. As conexões entre as ruas são:

   - Rua 1 conectada com 2 e 3;
   - Rua 2 conectada com 1, 3 e 4;
   - Rua 3 conectada com 1, 2 e 5
   - Rua 4 conectada com 2 e 5
   - Rua 5 conectada com 3 e 4

   É possível que ele faça um trajeto passando por todas as ruas sem repetir nenhuma?

APÊNDICE F – DEMONSTRAÇÃO DO TEOREMA 3.3.3.

Antes de iniciar a demonstração, é necessário compreender alguns conceitos.

O *envelope* de uma família de curvas a um parâmetro é uma curva que, em cada um de seus pontos, é tangente a pelo menos um membro da família. É como a "silhueta" ou o contorno limite que envolve toda a família. O chryzode $C_a(m)$ resultante quando $m \to +\infty$ é a curva limite para a qual convergem as poligonais construídas em cada iteração. Essa curva limite atua como o envelope da família de curvas (as poligonais de cada etapa). Cada poligonal (de uma iteração finita) é tangente ao chryzode em múltiplos pontos, e no limite, o chryzode toca todas elas.

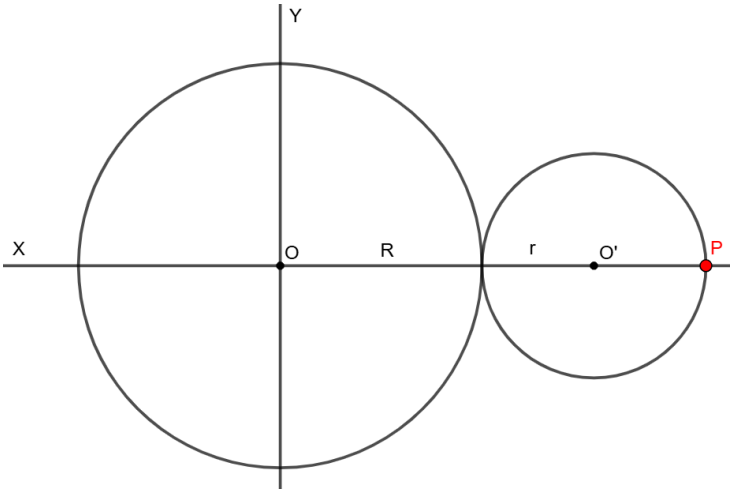
Teorema do Envelope: Considere uma família de curvas dada implicitamente por $F(x,y,\theta) = 0$, onde θ é o parâmetro que identifica cada curva da família. O envelope dessa família é obtido resolvendo o sistema:

$$\begin{cases} F(x,y,\theta) = 0 \\ \frac{\partial F(x,y,\theta)}{\partial \theta} = 0 \end{cases}$$

onde a primeira equação garante que o ponto (x, y) pertence a uma curva da família, e a segunda assegura que, nesse ponto, a curva da família é tangente ao envelope.

A figura abaixo representa as circunferências de centro *O*' (circunferência geradora, que rola) e de centro *O* (circunferência diretora, fixa), no instante inicial, antes do início do movimento de rolamento."

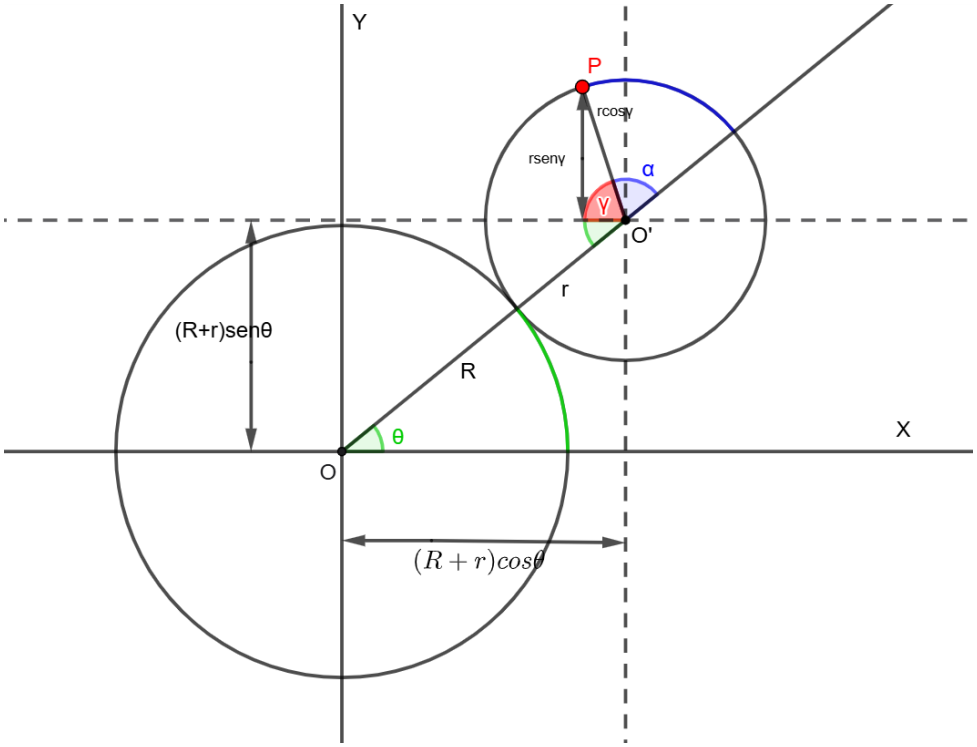
Figura 51 – Circunferência geradora e diretora antes do início do rolamento.



Fonte: autor.

Vamos deduzir as equações paramétricas da involuta de uma epicicloide, em que o ponto gerador P está posicionado, no instante inicial, no lado oposto à interseção entre a circunferência diretora e a circunferência geradora. Consulte a figura abaixo para referência.

Figura 52 – Circunferência diretora com um rolamento de θ graus da circunferência geradora .



Fonte: autor.

Assumimos que a posição do ponto P é o que queremos solucionar, α (ângulo azul) é o ângulo em radiano a partir do ponto Inicial até o ponto móvel P, e θ (ângulo verde) é o ângulo em radiano do rolamento da circunferência geradora sobre a diretora.

Como não há deslizamento entre os dois círculos, os arcos l_R (arco verde da circunferência diretora) e l_r (arco azul da circunferência geradora) são iguais, isso é,

$$l_R = l_r. \tag{2}$$

A partir da definição de radiano (tamanho do arco sobre o raio), temos que

$$l_R = \theta \cdot R \ e \ l_r = \alpha \cdot r. \tag{3}$$

A partir das condições (2) e (3), temos

$$\theta \cdot R = \alpha \cdot r \Rightarrow \alpha = \frac{R}{r} \cdot \theta. \tag{4}$$

Observando a Figura 52, vemos a posição do ponto P,

$$x = (R+r)cos\theta \ - \ rcos\gamma,$$

$$y = (R+r)sen\theta \ + \ rsen\gamma.$$

Perceba que $\gamma = 180^\circ - (\alpha+\theta)$, portanto

$$x = (R+r)cos\theta \ - \ rcos(180^\circ - (\alpha+\theta)); \tag{5}$$

$$y = (R+r)sen\theta \ + \ rsen(180^\circ - (\alpha+\theta)). \tag{6}$$

Sabemos das expressão trigonométrica que $sen(180^\circ - \mu) = sen(\mu)$ e $cos(180^\circ - \mu) = -cos(\mu)$, portanto, das equações (5) e (6), e utilizado em seguida (4) teremos

$$x = (R+r)cos\theta \ + \ rcos(\alpha+\theta) \quad \Rightarrow \quad x = (R+r)cos\theta \ + \ rcos\left(\tfrac{(R+r)}{r}\theta\right);$$

$$y = (R+r)sen\theta \ + \ rsen(\alpha+\theta) \quad \Rightarrow \quad y = (R+r)sen\theta \ + \ rsen\left(\tfrac{(R+r)}{r}\theta\right).$$

Portanto as equações paramétricas da involuta de uma epicicloide, são

$$x(\theta) = (R+r)cos\theta \ + \ rcos\left(\frac{(R+r)}{r}\theta\right); \tag{7}$$

$$y(\theta) = (R+r)sen\theta \ + \ rsen\left(\frac{(R+r)}{r}\theta\right). \tag{8}$$

Por curiosidade, caso o ponto P estivesse na interseção das circunfêrencias diretora e geradora no instante inicial, antes do início do movimento de rolamento. As equações seriam

$$x(\theta) = (R+r)cos\theta \ - \ rcos\left(\tfrac{(R+r)}{r}\theta\right);$$

$$y(\theta) = (R+r)sen\theta \ - \ rsen\left(\tfrac{(R+r)}{r}\theta\right).$$

A posição de um ponto no plano complexo é dada por $z = x + iy$. Substituindo as equações paramétricas (7) e (8) na expressão de z:

$$z(\theta) = \left[(R+r)\cos(\theta) + r\cos\left(\tfrac{(R+r)}{r}\theta\right)\right] + i\left[(R+r)\sin(\theta) + r\sin\left(\tfrac{(R+r)}{r}\theta\right)\right].$$

Reorganizando os termos para agrupar as partes com $(R+r)$ e r:

$$z(\theta) = (R+r)(\cos(\theta) + i\sin(\theta)) + r\left(\cos\left(\tfrac{R+r}{r}\theta\right) + i\sin\left(\tfrac{R+r}{r}\theta\right)\right).$$

Usando a fórmula de Euler, $e^{i\phi} = \cos(\phi) + i\sin(\phi)$, podemos converter as expressões trigonométricas para a forma exponencial complexa:

$$z(\theta) = (R+r)e^{i\theta} + re^{i\left(\frac{R+r}{r}\theta\right)} \tag{9}$$

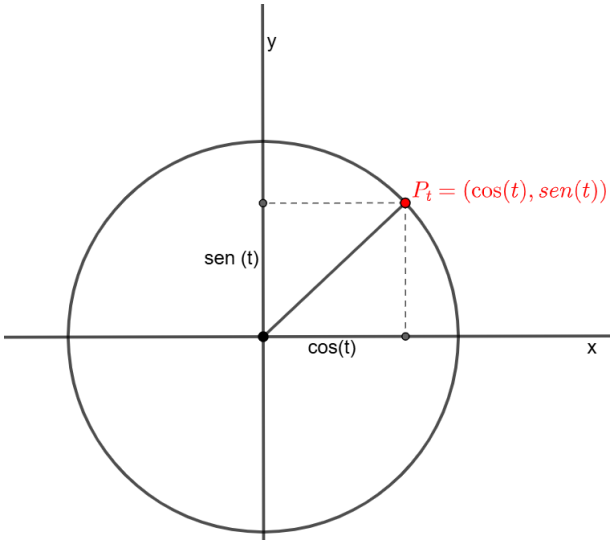
Portanto $z(\theta)$ é a equação complexa da epicicloide.

Teorema 3.3.3. Dado um chryzode $C_a(m)$ onde $a, m \in \mathbb{N}$ e $2 \leq a \leq m-1$, este converge para uma epicicloide simples de $n = a-1$ ciclos quando $m \to +\infty$.

Demonstração: Para $m \to +\infty$ a distribuição dos pontos na circunferência se torna contínua. Logo o chryzode $a \cdot t \equiv b_t \pmod{m}$ de conexões $t \to b_t$ torna-se, no contínuo, o conjunto de segmentos de conexões $t \to a \cdot t$, pois como m é suficiente grande podemos fazer $a \cdot t = m \cdot 0 + b_t$ com $0 \leq b_t < m$, resultando em $a \cdot t = b_t$ (para evitar confusão com a unidade imaginária, trocamos o parâmetro i por t, na definição de chryzodes).

No círculo unitário onde a epicicloide estará no seu interior, definimos os pontos $P_t = (cos(t),\ sen(t))$, com $t \in [0, 2\pi]$. (Observe que a parametrização $P_t = \left(sen\frac{2\pi t}{m}, cos\frac{2\pi t}{m}\right)$ apresentada na **Definição 3.1.1** nada mais é do que uma rotação de 90° da circunferência, o que faria com que P_0 ficasse no topo. Contudo, essa escolha não afeta os conceitos fundamentais dos chryzodes, uma vez que rotações são transformações geométricas admissíveis na definição de equivalência).

Figura 53 – Representação dos pontos P_t



Fonte: autor.

Seja $a \in \mathbb{Z}$, e $a \geq 2$. Definimos as retas L_t que passa pelos pontos $P_t = (cos(t),\ sen(t))$ e $P_{at} = (cos(at),\ sen(at))$. A equação da reta L_t passando por P_t e P_{at} é dado por:

$$\begin{vmatrix} x & y & 1 \\ cos(t) & sen(t) & 1 \\ cos(at) & sen(at) & 1 \end{vmatrix} = 0.$$

Assim, temos

$$xsen(t) + ycos(at) + sen(at)cos(t) - cos(at)sen(t) - xsen(at) - ycos(t) = 0$$

$$\Rightarrow x[sen(t) - sen(at)] - y[cos(t) - cos(at)] + [sen(at)cos(t) - sen(t)cos(at)] = 0. \quad (10)$$

Utilizando a identidade

$$sen(p-q) = sen(p)cos(q) - sen(q)cos(p),$$

teremos que o último termo da equação (10) é

$$[sen(at)cos(t) - sen(t)cos(at)] = sen(at - t) = sen((a-1)t).$$

Portanto,

$$F(x,\ y,\ t) = x[sen(t) - sen(at)] - y[cos(t) - cos(at)] + sen((a-1)t) = 0. \quad (11)$$

Utilizando as identidades,

- $sen(p) - sen(q) = 2cos\left(\frac{p+q}{2}\right) \cdot sen\left(\frac{p-q}{2}\right)$
- $cos(p) - cos(q) = -2sen\left(\frac{p+q}{2}\right) \cdot sen\left(\frac{p-q}{2}\right)$

fazendo $p = t$ e $q = at$, teremos:

- $sent(t) - sen(at) = 2cos\left(\frac{(a+1)t}{2}\right) \cdot sen\left(\frac{(1-a)t}{2}\right)$;
- $cos(t) - cos(at) = -2sen\left(\frac{(a+1)t}{2}\right) \cdot sen\left(\frac{(1-a)t}{2}\right)$.

Note que $sen\left(\frac{(1-a)t}{2}\right) = -sen\left(\frac{(a-1)t}{2}\right)$, pois a função seno é impar. Logo,

$$sent(t) - sen(at) = -2cos\left(\frac{(a+1)t}{2}\right) \cdot sen\left(\frac{(a-1)t}{2}\right) \quad (12)$$

$$cos(t) - cos(at) = 2sen\left(\frac{(a+1)t}{2}\right) \cdot sen\left(\frac{(a-1)t}{2}\right). \quad (13)$$

Da relação do seno da soma de dois arcos, obtemos

$$sen\left(\frac{(a-1)t}{2}+\frac{(a-1)t}{2}\right)=2sen\left(\frac{(a-1)t}{2}\right)\cdot cos\left(\frac{(a-1)t}{2}\right)$$

$$\Rightarrow sen((a-1)t)=2sen\left(\frac{(a-1)t}{2}\right)\cdot cos\left(\frac{(a-1)t}{2}\right) \tag{14}$$

Substituindo (12), (13) e (14) em (11), obtemos

$$F(x,\ y,\ t)=x\left[-2cos\left(\frac{(a+1)t}{2}\right)\cdot sen\left(\frac{(a-1)t}{2}\right)\right]-$$
$$y\left[2sen\left(\frac{(a+1)t}{2}\right)\cdot sen\left(\frac{(a-1)t}{2}\right)\right]+2sen\left(\frac{(a-1)t}{2}\right)\cdot cos\left(\frac{(a-1)t}{2}\right)=0,$$

dividindo tudo por $\left[-2sen\left(\frac{(a-1)t}{2}\right)\right]$ (onde é $\neq 0$),

$$F(x,\ y,\ t)=xcos\left(\frac{(a+1)t}{2}\right)+ysen\left(\frac{(a+1)t}{2}\right)-cos\left(\frac{(a-1)t}{2}\right)=0.$$

Fazendo $\alpha=\frac{(a+1)t}{2}$ e $\beta=\frac{(a-1)t}{2}$, teremos

$$F(x,\ y,\ t)=xcos(\alpha)+ysen(\alpha)-cos(\beta)=0. \tag{15}$$

Pelo teorema do envelope sabemos que o envelope na família $F(x,\ y,\ t)=0$, satisfaz $\frac{\partial F}{\partial t}=0$. Calculemos:

$$\frac{\partial F}{\partial t}=x(-sen(\alpha)\cdot\alpha')+y(cos(\alpha)\cdot\alpha')+sen(\beta)\cdot\beta'=0,$$

onde $\alpha'=\frac{a+1}{2}$ e $\beta=\frac{a-1}{2}$. Substituindo α' e β' e em seguida multiplicar a equação por 2, obtemos:

$$\frac{\partial F}{\partial t}=-(a+1)xsen(\alpha)+(a+1)y(cos\alpha)+(a-1)sen(\beta)=0. \tag{16}$$

Portanto, o sistema formado por $F(x,y,t)=0$ e $\frac{\partial F}{\partial t}=0$ é dado por,

$$\begin{cases} xcos(\alpha)+ysen(\alpha)-cos(\beta)=0 \\ -(a+1)xsen(\alpha)+(a+1)y(cos\alpha)+(a-1)sen(\beta)=0. \end{cases}$$

Dividindo a segunda equação do sistema por $(a+1)$, e organizando os termos, resultamos no sistema a seguir:

$$\begin{cases} xcos(\alpha)+ysen(\alpha)=cos(\beta) \\ -xsen(\alpha)+ycos(\alpha)=-\dfrac{(a-1)}{a+1}sen(\beta). \end{cases}$$

Escrevendo o sistema acima na forma de matriz e tomando $u = xcos(\alpha)+ysen(\alpha)=cos(\beta)$ e $v=-xsen(\alpha)+ycos(\alpha)=-\dfrac{(a-1)}{a+1}sen(\beta)$, fica

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} cos(\alpha) & sen(\alpha) \\ -sen(\alpha) & cos(\alpha) \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

Perceba que a matriz acima é o resultado de uma rotação de α no sentido anti-horário. Ou seja, utilizando a matriz de rotaçao a um ângulo $-\alpha$, obtemos a matriz acima, isto é,

$$\begin{pmatrix} cos(-\alpha) & -sen(-\alpha) \\ sen(-\alpha) & cos(-\alpha) \end{pmatrix} \Rightarrow \begin{pmatrix} cos(\alpha) & sen(\alpha) \\ -sen(\alpha) & cos(\alpha) \end{pmatrix}.$$

Da geometria analítica, sabemos que a matriz de rotação é ortogonal, ou seja, sua inversa é sua transposta. Multiplicando a forma matricial do sistema pela inversa da matriz de rotação de $-\alpha$ (no caso a transposta), ficará da seguinte forma,

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} cos(\alpha) & sen(\alpha) \\ -sen(\alpha) & cos(\alpha) \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \Rightarrow \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} cos(\alpha) & -sen(\alpha) \\ sen(\alpha) & cos(\alpha) \end{pmatrix} \cdot \begin{pmatrix} u \\ v \end{pmatrix}$$

isso é,

$$\begin{aligned} x &= ucos(\alpha)-vsen(\alpha) \\ y &= usen(\alpha)+vcos(\alpha). \end{aligned}$$

Como $u = cos(\beta)$ e $v=-\dfrac{(a-1)}{a+1}sen(\beta)$, teremos as equações:

$$x = cos(\beta)cos(\alpha)+\frac{(a-1)}{a+1}sen(\beta)\cdot sen(\alpha) \tag{17}$$

e

$$y = cos(\beta)sen(\alpha)-\frac{(a-1)}{a+1}sen(\beta)\cdot cos(\alpha) \tag{18}$$

Vamos encontrar a forma nos complexos, pois devemos comparar com a equação da epicicloide nos complexos. Seja $z = x+iy$, então

$$z = \left[cos(\beta)cos(\alpha) + \frac{(a-1)}{a+1}sen(\beta)\cdot sen(\alpha)\right] + i\left[cos(\beta)sen(\alpha) - \frac{(a-1)}{a+1}sen(\beta)\cdot cos(\alpha)\right]$$

$$\Rightarrow z = cos(\beta)\cdot(cos(\alpha) + isen(\alpha)) + \frac{(a-1)}{a+1}sen(\beta)\cdot(sen(\alpha) - icos(\alpha)).$$

Sabendo que $(-i)^2 = 1$, note que, $sen(\alpha) - icos(\alpha) = -i(cos(\alpha) + isen(\alpha))$ e da fórmula de Euler $e^{i\alpha} = \cos(\alpha) + i\sin(\alpha)$, obtemos

$$sen(\alpha) - icos(\alpha) = -ie^{i\alpha}.$$

Então,

$$z = cos(\beta)\cdot e^{i\alpha} - i\frac{(a-1)}{a+1}sen(\beta)\cdot e^{i\alpha}$$

$$\Rightarrow z = e^{i\alpha}\cdot\left[cos(\beta) - i\frac{(a-1)}{a+1}sen(\beta)\right] \tag{19}$$

Usando as relações,

- $cos(\beta) = \dfrac{e^{i\beta} + e^{-i\beta}}{2}$ (origina-se somando as relações $e^{i\beta}$ com $e^{-i\beta}$)
- $sen(\beta) = \dfrac{e^{i\beta} - e^{-i\beta}}{2i}$ (origina-se subtraindo as relações $e^{i\beta}$ com $e^{-i\beta}$)

obtemos que,

$$cos(\beta) - i\frac{(a-1)}{a+1}sen(\beta) = \frac{e^{i\beta} + e^{-i\beta}}{2} - i\frac{(a-1)}{a+1}\left(\frac{e^{i\beta} - e^{-i\beta}}{2i}\right)$$

$$\Rightarrow cos(\beta) - i\frac{(a-1)}{a+1}sen(\beta) = \frac{e^{i\beta} + e^{-i\beta}}{2} - \frac{(a-1)}{a+1}\left(\frac{e^{i\beta} - e^{-i\beta}}{2}\right)$$

$$\Rightarrow cos(\beta) - i\frac{(a-1)}{a+1}sen(\beta) = \left(\frac{1 - \left(\frac{a-1}{a+1}\right)}{2}\right)e^{i\beta} + \left(\frac{1 + \left(\frac{a-1}{a+1}\right)}{2}\right)e^{-i\beta}$$

Portanto,

$$cos(\beta) - i\frac{(a-1)}{a+1}sen(\beta) = \left(\frac{1}{a+1}\right)e^{i\beta} + \left(\frac{a}{a+1}\right)e^{-i\beta}. \tag{20}$$

Substituindo a equação (20) na equação (19), resulta na equação

$$z = e^{i\alpha}\cdot\left[\left(\frac{1}{a+1}\right)e^{i\beta} + \left(\frac{a}{a+1}\right)e^{-i\beta}\right],$$

$$\Rightarrow z = \frac{e^{i(\alpha+\beta)}}{a+1} + \frac{ae^{i(\alpha-\beta)}}{a+1},$$

mas $\alpha = \frac{(a+1)t}{2}$ e $\beta = \frac{(a-1)t}{2}$, logo, $\alpha+\beta = at$ e $\alpha-\beta = t$. Portanto, teremos

$$z = \frac{e^{iat}}{a+1} + \frac{ae^{it}}{a+1},$$

resultando na equação complexa de $F(x,y,t)$, dada por:

$$z(t) = \left(\frac{1}{a+1}\right)e^{iat} + \left(\frac{a}{a+1}\right)e^{it}. \tag{21}$$

Sabendo de (9) que, no plano complexo, a epicicloide é descrita como

$$z(\theta) = (R+r)e^{i\theta} + re^{i(\frac{R+r}{r})\theta},$$

comparando as equações (21) e (9), teremos a igualdade quando:

- $\theta = t$;
- $R+r = \frac{a}{a+1}$;
- $r = \frac{1}{a+1} \Rightarrow R = \frac{a-1}{a+1}$,

consequentemente $\dfrac{R+r}{r} = a$. Portanto, pela **Definição 3.3.2** o número de ciclos é dado por

$$n = \frac{R}{r} = \frac{\frac{a-1}{a+1}}{\frac{1}{a+1}} = a-1.$$

□