UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ - UTFPR
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL
PROFMAT

DIONATAN MIGUEL FIORIN KONAGESKI

EXPERIÊNCIAS CONCRETAS NA ARITMÉTICA MODULAR

CURITIBA

2019

DIONATAN MIGUEL FIORIN KONAGESKI

EXPERIÊNCIAS CONCRETAS NA ARITMÉTICA MODULAR

Dissertação apresentada ao Mestrado Profissional em Matemática em Rede Nacional da Universidade Tecnológica Federal do Paraná em Curitiba - PROFMAT-UTCT como requisito parcial para obtenção do grau de Mestre.
Orientador: Mari Sano, Dra.

CURITIBA

2019

Dados Internacionais de Catalogação na Publicação

Konageski, Dionatan Miguel Fiorin
Experiências concretas na aritmética modular [recurso eletrônico] / Dionatan Miguel Fiorin Konageski.-- 2019.
1 arquivo eletrônico (128 f.) : PDF ; 3,26 MB.

Modo de acesso: World Wide Web.
Texto em português com resumo em inglês.
Dissertação (Mestrado) - Universidade Tecnológica Federal do Paraná. Programa de Mestrado Profissional em Matemática em Rede Nacional, Curitiba, 2019.
Bibliografia: f. 111-113.

1. Matemática - Dissertações. 2. Aritmética modular. 3. Educação básica. 4. Matemática - Programas de atividades. 5. Jogos no ensino de matemática. 6. Jogos educativos. 7. Quebra-cabeças. 8. Jogo de dardos. 9. Aprendizagem. 10. Prática de ensino. I. Sano, Mari, orient. II. Universidade Tecnológica Federal do Paraná. Programa de Mestrado Profissional em Matemática em Rede Nacional. III. Título.

CDD: Ed. 23 – 510

Biblioteca Central do Câmpus Curitiba - UTFPR
Bibliotecária: Luiza Aquemi Matsumoto CRB-9/794

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação

TERMO DE APROVAÇÃO DE DISSERTAÇÃO Nº 70

A Dissertação de Mestrado intitulada “EXPERIÊNCIAS CONCRETAS NA ARITMÉTICA MODULAR”, defendida em sessão pública pelo candidato **Dionatan Miguel Fiorin Konageski**, no dia 11 de outubro de 2019, foi julgada para a obtenção do título de Mestre, área de concentração Matemática, e aprovada em sua forma final, pelo Programa de Pós-Graduação em Matemática em Rede Nacional - PROFMAT.

BANCA EXAMINADORA:

Prof(a). Dr(a). Mari Sano - Presidente – UTFPR

Prof(a). Dr(a). Patrícia Massae Kitani – UTFPR

Prof(a). Dr(a). Marcelo Muniz Silva Alves – UFPR

A via original deste documento encontra-se arquivada na Secretaria do Programa, contendo a assinatura da Coordenação após a entrega da versão corrigida do trabalho.

Curitiba, 11 de outubro de 2019.

Carimbo e Assinatura do(a) Coordenador(a) do Programa

Dedico este trabalho à minha filha Isabella (in memoriam).

AGRADECIMENTOS

Agradeço primeiramente a Deus por me dar sabedoria para vencer todas as barreiras impostas e por todas as coisas que está fazendo em minha vida.

Agradeço aos meus pais Elio e Lori, por me apoiarem em tudo que eu faço e por sempre me incentivarem.

Agradeço à minha esposa Mariane pelo seu amor, pelo companheirismo em casa e nas viagens, pelo incentivo e pela paciência.

Agradeço ao meu irmão Alessandro e ao meu sobrinho Lorenzo.

Agradeço à professora Dra. Mari Sano pela orientação, pela atenção, pelas dicas e pelas sugestões.

Agradeço a todos os professores do PROFMAT da UTFPR Campus Curitiba, que me repassaram conhecimentos capazes de chegar até aqui.

Agradeço à Secretaria de Educação do Estado de Santa Catarina pelo afastamento no período do mestrado, sem isso certamente não conseguiria concluir o curso.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

“A melhor maneira encontrada pelo homem para se aperfeiçoar é aproximando-se de Deus.” (Pitágoras)

RESUMO

KONAGESKI, Dionatan Miguel Fiorin. **Experiências Concretas na Aritmética Modular**. 128 p. Dissertação - Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2019.

A Aritmética Modular possui inúmeras aplicações na educação básica. E para isso faz-se necessário o entendimento dos conceitos básicos da Aritmética Modular. Este trabalho tem como objetivo aplicar de forma lúdica o conteúdo desta teoria nos Chryzodes, no quebra-cabeça de boliche módulo 6 e módulo 10, no jogo de dardos, entre outros. Com essas aplicações procuramos mostrar uma maneira diferente de trabalhar a Aritmética Modular em sala de aula, maneira esta que irá proporcionar ao educando participar de forma mais atrativa das aulas. Acreditamos que tais aplicações deveriam ser abordadas na educação básica, visto sua importância e sua aplicabilidade no cotidiano como podemos perceber neste trabalho e em muitos outros.

Palavras-chave: Aplicações da Aritmética; Chryzodes; Quebra-Cabeça de Boliche; Jogo de Dardos.

ABSTRACT

KONAGESKI, Dionatan Miguel Fiorin. **Concrete Experiences in Modular Arithmetics**. 128 p. Dissertation - Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2019.

Modular arithmetic has numerous applications in basic education. For that, it is necessary to understand the basic concepts of Modular Arithmetic. The aim of this work is to playfully apply the content of this theory in Chryzodes, the module 6 and module 10 bowling pin puzzle, darts game, among others. With these applications we seek to show a different way of working Modular Arithmetic in the classroom, which will provide the student with an attractive way to participate in classes. We belive that such applications should be addressed in basic education, given their importance and applicability in daily life as we can see in this work and many others.

Keywords:Arithmetic Applications; Chryzodes; Bowling Pin Puzzle; Darts Game.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

INTRODUÇÃO

A motivação da escolha do tema e os assuntos abordados se deu pela falta do conhecimento sobre a Aritmética Modular antes de ingressar no PROFMAT. Ao realizar a disciplina de MA-14 (Aritmética) fiquei impressionado com o que estava estudando. Com destaque aos conteúdos de Equações Diofantinas Lineares, Congruências e Teorema Chinês dos Restos, que tinham aplicações diretas no cotidiano. Essa motivação me fez questionar: "Por que esses conteúdos não são enfatizados na educação básica?"

Partindo dessa pergunta apresentamos esse trabalho sobre Aritmética Modular, com enfoque em aplicações lúdicas que podem ser realizadas na educação básica, estimulando o desenvolvimento mental e fazendo com que o aluno construa o conhecimento de uma forma mais prazerosa. Além de apresentar os conteúdos em sala de aula de forma contextualizada nas situações do cotidiano do aluno. O que é afirmado nos Parâmetros Curriculares Nacionais (PCN):

> As necessidades cotidianas fazem com que os alunos desenvolvam capacidades de natureza prática para lidar com a atividade matemática, o que lhes permite reconhecer problemas, buscar e selecionar informações, tomar decisões. Quando essa capacidade é potencializada pela escola, a aprendizagem apresenta melhor resultado. (BRASIL, 1998, p.37)

E ainda:

> A instituição social escola passa a ser um dos espaços privilegiados de formação e informação, isto é, onde a aprendizagem dos conteúdos deve estar relacionada ao cotidiano dos alunos. Assim, ela, além de possibilitar aos alunos a apropriação dos conteúdos de maneira crítica e construtiva, precisa valorizar a cultura de sua própria comunidade, contribuindo para o exercício de cidadania. [(BRASIL, 1997, p.45-46) apud (OLIVEIRA, 2014, p. 44)]

É por isso que um dos principais objetivos deste trabalho é fornecer ferramentas que permitam que os alunos aprendam e visualizem a importância da Aritmética Modular em suas vidas cotidianas. Para isso existem várias atividades que podem ser usadas para se trabalhar em sala de aula, como por exemplo a congruência que existe no relógio e nos Chryzodes, quantos dias se passam no calendário Maia, a congruência no quebra-cabeça de boliche, como descobrir a quantidade de vezes que iremos adicionar ou subtrair dois números dados e assim chegar no resultado desejado e como a precisão e a resolução de uma equação diofantina nos ajudam a ganhar um jogo de dardos.

Com este tipo de atividades procuramos mostrar uma maneira diferente de trabalhar Aritmética na sala de aula, uma maneira que motive e faça com que o aluno participe das aulas. Além de proporcionar uma visão ampla acerca dos conteúdos e mostrar que existem elementos de ligação entre os mesmos, conforme é dito nos Parâmetros Curriculares Nacionais (PCN):

> ··· muitas vezes os conteúdos matemáticos são tratados isoladamente e são apresentados e exauridos num único momento. Quando acontece de serem retomados (geralmente num mesmo nível de aprofundamento, apoiando-se nos mesmos recursos), é apenas com a perspectiva de utilizá-los como ferramentas para a aprendizagem de novas noções. De modo geral, parece não se levar em conta que, para o aluno consolidar e ampliar um conceito, é fundamental que ele o veja em novas extensões, representações ou conexões com outros conceitos. (BRASIL, 1998, p.22 e 23)

Desta forma, o professor pode propor aos alunos atividades que estão no contexto cotidiano de maneira lúdica afim de potencializar a aprendizagem e tornar as aulas mais ricas e atraentes.

A seguir, vamos descrever o trabalho de forma mais detalhada.

OBJETIVO GERAL DO TRABALHO

Apresentar conceitos básicos da Aritmética, bem como algumas aplicações do cotidiano na educação básica.

OBJETIVOS ESPECÍFICOS DO TRABALHO

- Relacionar Aritmética com Geometria e Álgebra;
- Apresentar aplicações da Aritmética;
- Destacar a importância de aplicações para o ensino-aprendizagem;
- Salientar a importância do lúdico para o ensino-aprendizagem;
- Estudar as propriedades dos números inteiros junto com suas operações.

ESTRUTURA DO TRABALHO

No capítulo 1, abordamos os principais conceitos da Aritmética Modular, e alguns de seus aspectos históricos, que são necessários para o entendimento dos demais capítulos. Damos destaque neste capítulo para o Algoritmo Binário de Euclides [1.4] e a Equação Diofantina

Linear com três variáveis [1.8], conteúdos que não são abordados em (HEFEZ, 2016a).

O capítulo 2 visa mostrar várias aplicações dos conceitos trabalhados no capítulo 1, entre eles: Relógios [2.1], Calendário Maia [2.2], Chryzode [2.3], Quebra-Cabeça [2.4], Enigmas de descobertas [2.5] e Jogo de Dardos [2.6]. Todas essas atividades podem ser usadas no ensino dos conceitos do capítulo 1 na educação básica.

O capítulo 3, é destinado a apresentar propostas de atividades no ensino básico que servem para revisar ou fixar os conceitos básicos da Aritmética. Dentre as propostas temos a do Chryzode [3.1], a qual foi realizada com uma turma do 9º ano do ensino fundamental e o resultado dos trabalhos podem ser conferidos no Apêndice do trabalho; proposta de atividade do Quebra-cabeça do boliche módulo m [3.2]; atividade de Números Cruzados [3.3]. Uma observação para esta última atividade é que ela pode ser adaptada para qualquer conteúdo da matemática e não só para conteúdos relacionados com Aritmética. Por fim, sabendo da dificuldade que às vezes o professor enfrenta em criar ou encontrar exercícios para suas aulas resolvemos propor uma atividade de Resolução de Exercícios [3.4] de diferentes níveis de dificuldade para a educação básica sobre Aritmética.

1 CONCEITOS PRELIMINARES DA ARITMÉTICA

Antes de iniciar nossos estudos, é preciso destacar alguns conceitos básicos presentes na Aritmética que serão de grande valia e de suma importância para o entendimento deste trabalho. No decorrer deste capítulo utilizamos as seguintes referências (HEFEZ, 2016a), (SANTOS, 2014) e (DOMINGUES, 2009).

1.1 DIVISIBILIDADE

Sejam a e b dois números inteiros. Diz-se que a divide b, ou que a é divisor de b, ou que b é divisível por a, ou ainda que b é múltiplo de a, se existir um número inteiro k tal que $b = a \cdot k$. Usaremos $a \mid b$ para indicar que a divide b.

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

Exemplo 1.1. Observe os exemplos:

1. $3 \mid 27$;
2. $4 \nmid 15$.

A seguir estabeleceremos algumas propriedades da divisibilidade.

Proposição 1.2. *Dados os números a, b, $c \in \mathbb{Z}$, temos que:*

1. $1 \mid a$, $a \mid a$ e $a \mid 0$;
2. $0 \mid a$ se, e somente se, $a = 0$;
3. $a \mid b$ se, e somente se, $|a| \mid |b|$;
4. se $a \mid b$ e $b \mid c$, então $a \mid c$;
5. se $b \neq 0$ e $a \mid b$, então $|a| \leq |b|$;
6. se $a \mid b$ e $b \mid a$, então $|a| = |b|$.

Demonstração:

1. Decorre imediatamente das igualdades $a = 1 \cdot a$, $a = a \cdot 1$ e $0 = a \cdot 0$;

2. Suponha que 0 | a. Então existe $k \in \mathbb{Z}$ tal que $a = 0 \cdot k$. Como $k \cdot 0 = 0$, para todo inteiro k, então $a = 0$. Reciprocamente, observamos que 0 | 0, o que foi provado no item anterior;

3. Sejam $a, b \in \mathbb{Z}$. Temos que se $a \mid b$, então $b = k \cdot a$, para algum $k \in \mathbb{Z}$. Aplicando módulo a ambos os membros da igualdade, obtemos $|b| = |k \cdot a| = |k| \cdot |a|$. Agora fazendo $|k| = k_1$, (com $k_1 \in \mathbb{Z}$), temos $|b| = k_1 \cdot |a|$, que nos dá que $|a| \mid |b|$.

   Reciprocamente, se $|a| \mid |b|$, então $|b| = k \cdot |a|$ para algum $k \in \mathbb{Z}$. Logo, $b = \pm ka$. De onde temos que $a \mid b$.

4. Suponha que $a \mid b$ e $b \mid c$. Portanto existem k_1 e $k_2 \in \mathbb{Z}$, tais que $b = k_1 \cdot a$ e $c = k_2 \cdot b$. Substituindo o valor de b da primeira equação na segunda equação, obtemos:

$$c = k_2 \cdot b = k_2 \cdot (k_1 \cdot a) = (k_2 \cdot k_1) \cdot a$$

   o que mostra que $a \mid c$.

5. Se $a \mid b$, então existe um inteiro k_1 tal que $b = k_1 \cdot a$. Como $b \neq 0$, temos que nem a e nem k_1 podem ser zero. Daí, $|k_1| \geq 1$. Assim:

$$|b| = |k_1 \cdot a| = |k_1| \cdot |a| \geq |a|.$$

   Portanto, $|a| \leq |b|$.

6. Suponha $a = 0$. Como a | b, devemos ter $b = 0$, logo $|a| = 0 = |b|$.
   Por outro lado, suponhamos $a \neq 0$, logo $b \neq 0$, pois $b \mid a$. Pelo item 5, como $b \mid a$ e $a \mid b$, segue que $|b| \leq |a|$ e $|a| \leq |b|$, o que mostra que $|a| = |b|$.

□

Exemplo 1.3. 1. 1 | (-3); 4 | 4 e 7 | 0;

2. 0 | 0;

3. 2 | 4, assim como (-2) | 4, (-2) | (-4) e 2 | (-4);

4. 7 | 14 e 14 | 28, logo 7 | 28;

5. -5 | 15, temos que $|5| \leq |15|$;

6. (-11) | 11 e 11 | (-11), então $|(-11)| = |11|$.

Proposição 1.4. *Dados os números a, b, c, d* $\in \mathbb{Z}$. *Se a* | *b e c* | *d, então a·c* | *b·d.*

Demonstração: Se $a \mid b$ e $c \mid d$, então existem k_1, $k_2 \in \mathbb{Z}$ tais que $b = k_1 \cdot a$ e $d = k_2 \cdot c$. Sendo assim, temos que:

$$b \cdot d = (k_1 \cdot a)(k_2 \cdot c) = (k_1 \cdot k_2)(a \cdot c).$$

Logo, $a \cdot c \mid b \cdot d$.

$\square$

Exemplo 1.5. Se 3 | 6 e (-2) | 4, então 3 · (-2) | 6 · 4, ou seja (-6) 24.

Proposição 1.6. *Sejam os números a, b, c* $\in \mathbb{Z}$, *tais que* $a \mid (b \pm c)$. *Então* $a \mid b$ *se, e somente se,* $a \mid c$.

Demonstração: Suponha que $a \mid (b - c)$. Portanto, existe $k_1 \in \mathbb{Z}$ tal que $b - c = a \cdot k_1$.

Se $a \mid b$, então existe $k_2 \in \mathbb{Z}$ tal que $b = a \cdot k_2$. Desta forma, $a \cdot k_1 = b - c = a \cdot k_2 - c$, donde segue-se que $c = a \cdot k_2 - a \cdot k_1 \Longrightarrow c = a \cdot (k_2 - k_1)$. Logo $a \mid c$.

Reciprocamente, se $a \mid c$ então existe $k_3 \in \mathbb{Z}$ tal que $c = a \cdot k_3$. Desta forma, $a \cdot k_1 = b - c = b - a \cdot k_3$, donde segue que se $b = a \cdot (k_1 + k_3)$. Logo $a \mid b$.

Se $a \mid (b+c)$, o resultado segue do caso anterior. $\square$

Exemplo 1.7. Sabemos que 3 | (12 - 15), como 3 | 12 temos que 3 | (-15).

Proposição 1.8. *Sendo a, b, c* $\in \mathbb{Z}$, *se* $ac \mid bc$ *então* $a \mid b$, *para todo* $c \in \mathbb{Z}^*$.

Demonstração: Como $a \cdot c \mid b \cdot c$, segue-se que existe $k \in \mathbb{Z}$ tal que $b \cdot c = a \cdot c \cdot k$. Sendo que c é diferente de zero, pela lei do corte, segue que $b = a \cdot k$. Daí, $a \mid b$.

$\square$

Exemplo 1.9. Se 3 · 5 | 9 · 5, então 3 | 9.

Proposição 1.10. *Sejam os números a, b, c* $\in \mathbb{Z}$, *tais que* $a \mid b$ *e* $a \mid c$. *Então para todo x e y* $\in \mathbb{Z}$, *temos que* $a \mid (x \cdot b + y \cdot c)$.

Demonstração: Suponha que $a \mid b$ e $a \mid c$. Portanto, existem k_1 e $k_2 \in \mathbb{Z}$ tais que $b = a \cdot k_1$ e $c = a \cdot k_2$. Sendo assim:

$$x \cdot b + y \cdot c = x \cdot (a \cdot k_1) + y \cdot (a \cdot k_2) = a \cdot (x \cdot k_1 + y \cdot k_2),$$

o que prova o resultado.

□

Exemplo 1.11. Sejam os números 3, 6 e 9, tais que 3 | 6 e 3 | 9. Então $3 \mid (6 \cdot x + 9 \cdot y)$ e assim para $x = 110$ e $y = -2$, temos que $3 \mid (6 \cdot 110 + 9 \cdot (-2))$.

1.2 DIVISÃO EUCLIDIANA

Euclides era um matemático grego, que viveu aproximadamente em 365-300 a.C. Os matemáticos geralmente se referem a ele simplesmente como "Euclides", mas às vezes ele é chamado de Euclides de Alexandria para evitar confusão com o filósofo Euclides de Megara.

Figura 1 – Euclides de Alexandria

Fonte: (WIKIPEDIA, 2018)

Muito pouco se sabe sobre a vida de Euclides, exceto que ele ensinou em Alexandria, no Egito. Ele pode ter sido educado na Academia de Platão, em Atenas, ou possivelmente por alguns dos alunos de Platão. Ele é uma figura histórica importante porque a maioria das regras que usamos hoje em geometria são baseadas nos escritos de Euclides, especificamente no livro intitulado "Os Elementos". Por isso ele é considerado o pai da geometria.

No livro "Os Elementos", reuniu tudo o que se sabia sobre matemática em seu tempo. Assim, recolheu as obras de grandes matemáticos que o precederam. E sua contribuição não era na solução de novos problemas, mas na ordenação de todos os métodos conhecidos, formando um sistema que permitia reunir tudo que era conhecido para descobrir e provar novas ideias.

> Um equívoco que se comete com frequência é pensar que os *Elementos* são uma obra apenas sobre Geometria. Na verdade, há muito de Aritmética e Álgebra em vários dos livros dos *Elementos*. O que é verdade - e isso explica, pelo menos em parte, a origem do equívoco - é que a Matemática grega, na época em que Euclides compôs sua obra, era toda ela geometrizada. (ÁVILA, 2001, p.2)

Para demonstrarmos o Algoritmo da Divisão de Euclides, que diz que é sempre possível efetuar a divisão de *a* por *b* e obter um resto, precisamos antes definir o Princípio da Boa

Ordenação e a Propriedade Arquimediana. Assim:

Princípio da Boa Ordenação

Todo conjunto não-vazio de inteiros positivos contém um elemento mínimo.

Propriedade Arquimediana

Sejam a, $b \in \mathbb{Z}$, com b diferente de zero. Então existe $n \in \mathbb{Z}$ tal que $n \cdot b > a$.

Agora, usaremos esses resultados, para demonstrar esse importante instrumento na obra de Euclides, que é um resultado central da teoria dos números.

Teorema 1.12. *Dado $a,b \in \mathbb{Z}$, $b \neq 0$, existem únicos inteiros q, r chamados respectivamente de quociente e resto, tais que:*

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

Demonstração: Seja o conjunto $M = \{x = a - by \mid y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$.

Existência: Pela *propriedade Arquimediana*, existe $n \in \mathbb{Z}$, tal que $n(-b) > -a$. Portanto, $a - nb > 0$, o que mostra que M é não vazio. Note que o conjunto M é limitado inferiormente por 0. Sendo assim, pelo *Princípio da Boa Ordenação*, temos que M possui um menor elemento r. Suponhamos que $r = a - bq$. É claro que $r \geq 0$, mostremos que $r < |b|$. Suponha, por absurdo, que $r \geq |b|$. Desta forma, existe $m \in \mathbb{N} \cup \{0\}$, tal que $r = |b| + m$ e $0 \leq m < |r|$, o qual contradiz o fato de r ser o menor elemento de M, pois $m = a - (q \pm 1)b \in M$. Logo, $a = bq + r$, com $0 \leq r < |b|$, o que prova a existência de q e r.

Unicidade: Suponha que $a = bq + r = bq_1 + r_1$, onde $q, q_1, r, r_1 \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r_1 < |b|$. Assim, temos que $-|b| < -r \leq r_1 - r \leq r_1 < |b|$. Portanto, $|r_1 - r| < |b|$. Por outro lado, $b \cdot (q - q_1) = r_1 - r$, o que implica que $|b| \cdot |q - q_1| = |r_1 - r| < |b|$, o que é possível quando $q = q_1$ e $r = r_1$. □

Observação 1.13. *O algoritmo acima é chamado* ***Algoritmo da Divisão de Euclides****.*

1.3 MÁXIMO DIVISOR COMUM E O ALGORITMO DE EUCLIDES

1.3.1 MÁXIMO DIVISOR COMUM (MDC)

Diremos que um número natural $d > 0$ é o *máximo divisor comum (mdc)* de $a,\ b \in \mathbb{Z}$ (com $a \neq 0$ ou $b \neq 0$) se possuir as seguintes propriedades:

(i) d é um divisor comum de a e de b;

(ii) Se c é um divisor comum de a e b, então $c \mid d$.

Portanto, se d é o *mdc* de a, b e c é um divisor comum desses números, então $c \leq d$. Isto mostra que o máximo divisor comum de dois números é efetivamente o maior dentre todos os divisores comuns desses números.

Em particular, isto nos mostra que, se d e d' são dois máximos divisor comum de um mesmo par de números, então $d \geq d'$ e $d' \geq d$, logo, $d = d'$. Ou seja, o *mdc* de dois números é único.

O máximo divisor comum de a, $b \in \mathbb{Z}$ é denotado por (a, b). Assim, podemos observar ainda que:

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

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

Exemplo 1.14.

i) $(4, 8) = (8, 4) = 4$;

ii) $(5, 15) = (-5, 15) = (5, -15) = (-5, -15) = 5$;

iii) $(3, 7) = 1$.

Exemplo 1.15. Seja *D(a)* o conjunto dos divisores inteiros de um número inteiro a, então temos que:
$D(40) = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 8, \pm 10, \pm 20 \text{ e } \pm 40\}$.
$D(48) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 16, \pm 24 \text{ e } \pm 48\}$.

Observando os conjuntos dos divisores de 40 e de 48, verifica-se que estes apresentam números comuns, que são: $\{\pm 1, \pm 2, \pm 4, \pm 8\}$. Assim, o $(40,48) = 8$.

A noção de máximo divisor comum entre dois números inteiros pode ser generalizada para *n* inteiros. Assim, um número natural *d* será dito *mdc* de dados números inteiros $a_1, a_2, \ldots, a_n$ todos não nulos, se possuir as seguintes propriedades:

i) *d* é um divisor comum de $a_1, a_2, \ldots, a_n$;

ii) Se *c* é um divisor comum de $a_1, a_2, \ldots, a_n$, então $c \mid d$.

Observação 1.16.

1. *(a,1) = 1;*

2. *(a,0) = $|a|$, se a é diferente de zero;*

3. *a $\mid$ b se, e somente se, (a,b) = $|a|$;*

4. *Se (a,b) = 1, então a e b são denominados primos entre si.*

Exemplo 1.17.

1. (42,1) = 1;

2. (2018,0) = 2018;

3. (7,14) = 7, pois 7 é divisor de 14;

4. (5,9) = 1, então 5 e 9 são primos entre si.

Na continuação apresentaremos algumas propriedades do *mdc*.

Teorema 1.18. ***(Teorema de Bezout):*** *Dados a, b $\in \mathbb{Z}$, seja d = (a,b). Então existem m_0, n_0 $\in \mathbb{Z}$, tais que am_0 + bn_0 = d.*

Demonstração: Considere o conjunto *P* de todos os números inteiros positivos $am + bn$, com $m, n \in \mathbb{Z}$, o qual é diferente do vazio, já que se $m = a$ e $n = b$ temos que $a^2 + b^2$ é positivo e portanto pertence a esse conjunto.

Pelo princípio da Boa Ordenação, existe um menor inteiro positivo $c = am_0 + bn_0$ pertence a *P*. Inicialmente vamos provar que $c \mid a$. Assim, suponha por absurdo que $c \nmid a$. Então, pelo Teorema 1.12, existem *q* e *r*, tais que *a* = *cq* + *r*, isto é, *r* = *a* - *cq*, com 0 < *r* < *c*. Portanto:

$$r = a - cq = a - (am_0 + bn_0)q = a(1 - qm_0) + b(qn_0).$$

Isso mostra que *r* pertence a *P*. Mas isto é uma contradição, pois 0 < *r* < *c*, e pela hipótese *c* é o menor elemento positivo do conjunto, logo $c \mid a$. Analogamente, provamos que $c \mid b$. Agora, só resta provar que *c* = *d*. Como *(a,b)* = *d*, temos que existem $k_1, k_2 \in \mathbb{Z}$, tais que $a = dk_1$ e $b = dk_2$. Então:

$$c = am_0 + bn_0 = dk_1m_0 + dk_2n_0 = d(k_1m_0 + k_2n_0).$$

E isso implica que $d \mid c$. Portanto, como *c* e *d* são positivos e $d \mid c$ então $d \leq c$, note que *d* < *c* é impossível pois *(a,b)* = *d*, assim temos que *d* = *c* = $am_0 + bn_0$.

□

Observação 1.19. *A recíproca do Teorema 1.18 não é válida, pois* $3{\cdot}2+5{\cdot}1 = 11$ *e o* $(3,5) \neq 11$.

Exemplo 1.20. A equação $60m + 42n = 6$ possui solução? Se sim, encontre os valores de m e n que tornam essa equação verdadeira.

Calculando o máximo divisor comum de 60 e 42, obtemos 6. Assim pelo Teorema 1.18 temos que a equação $60m + 42n = 6$, possui solução no conjunto dos números inteiros, $60 \cdot (-2) + 42 \cdot 3 = 6$.

Teorema 1.21. *Se a |bc e (a,b) = 1, então* $a \mid c$.

Demonstração: Da hipótese, temos que (*a*,*b*) = 1, e pelo Teorema 1.18 existem dois números *n* e $m \in \mathbb{Z}$, tais que *na* + *mb* = 1. Multiplicando os dois lados desta igualdade por *c*, temos *n(ac)* + *m(bc)* = *c*. Como $a \mid ac$ e da hipótese $a \mid bc$, então pela Proposição 1.10, temos que $a \mid c$.

□

Exemplo 1.22. Como $2 \mid 3 \cdot 8$ e $(2,3) = 1$, temos pelo Teorema 1.21 que $2 \mid 8$.

Teorema 1.23. *Se a e b* $\in \mathbb{Z}$ *e a = qb + r onde r e q* $\in \mathbb{Z}$*, então (a,b) = (b,r).*

Demonstração: Da relação $a = bq + r$, segue que $r = a - bq$. Assim, seja c um número inteiro tal que $c \mid a$ e $c \mid b$. Sendo assim, da Proposição 1.10, tem-se que $c \mid r$. Portanto, c é um divisor comum de b e r.
Reciprocamente, como $a = bq + r$, 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, $(a,b) = (b,r)$.

□

Exemplo 1.24. Sabemos que $16 = 7 \cdot 2 + 2$, então temos pelo Teorema 1.23 que $(16,7) = (7,2) = 1$.

Proposição 1.25. *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 $(a, b) = d$. 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 $(ac, bc) = dc = c \cdot (a, b)$.

□

Exemplo 1.26. Sendo $(15, 10) = (5 \cdot 3, 5 \cdot 2)$, então pela Proposição 1.25, temos que $(15, 10) = 5 \cdot (3, 2) = 5 \cdot 1 = 5$.

Proposição 1.27. *Dados a, b $\in \mathbb{Z}^*$, tem-se que:*

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

Demonstração: Se *(a,b)* = 1, então a demostração segue diretamente.
Suponha que *(a,b) = d*, com $d \neq 1$ e $d \in \mathbb{N}^*$. Suponha que $\left(\frac{a}{d}, \frac{b}{d}\right)$ = *k*. Então pela Proposição 1.25, segue que *d = (a,b) =* $\left(d.\frac{a}{d}, d.\frac{b}{d}\right)$ = *d.k*. Portanto, temos que *k* = 1.

□

Exemplo 1.28. Aplique a Proposição 1.27, para $a = 20$ e $b = 16$.

Temos que $(20, 16) = 4$, logo:

$$\left(\frac{20}{(20,16)}, \frac{16}{(20,16)}\right) = \left(\frac{20}{4}, \frac{16}{4}\right) = (5, 4) = 1.$$

1.3.2 O ALGORITMO DE EUCLIDES

O Algoritmo de Euclides é um método que usamos para calcular o máximo divisor comum entre dois ou mais números inteiros. Enunciando em forma de regra, o algoritmo de Euclides é o seguinte: *Divida o maior dos dois números inteiros positivos pelo menor e então divida o divisor pelo resto. Continue este processo de dividir o último divisor pelo último resto, até que a divisão seja exata. O divisor final será o máximo divisor comum procurado.*

Teorema 1.29. ***Algoritmo de Euclides*** *Sejam a, b $\in \mathbb{Z}$, com a $\geq$ b > 0. Se o algoritmo da divisão euclidiana for aplicado sucessivamente, então o último resto não nulo r_n é igual ao (a, b), com n $\in \mathbb{N}^*$.*

Demonstração:

Se $b = 1$, ou $b = a$, ou $b \mid a$, sabemos que $(a, b) = b$. Suponhamos que b é diferente de a e que b não divide a. Pelo algoritmo de Euclides existem inteiros q_1 e r_1, tais que:

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

Se $r_1 \mid b$, então $(b, r_1) = r_1$. Pelo Teorema 1.23, temos que $(a, b) = (b, r_1) = r_1$. Se $r_1 \nmid b$, aplicamos o algoritmo de Euclides para b e r_1. Assim, existem inteiros q_2 e r_2 tais que:

$$b = r_1 q_2 + r_2, 0 \leq r_2 < r_1;$$

Que também nos dá duas possibilidades.
Se $r_2 \mid r_1$, então $(r_1, r_2) = r_2$. Pelo Teorema 1.23, segue que $(b, r_1) = (r_1, r_2) = r_2$. Logo:

$$(a, b) = r_2.$$

Se r_2 não divide r_1, então aplicamos novamente o algoritmo de Euclides para r_1 e r_2. Portanto, existem inteiros q_3 e r_3, tais que:

$$r_1 = r_2 q_3 + r_3, 0 \leq r_3 < r_2 < r_1 < b.$$

Este processo é finito, pois pelo Princípio da Boa Ordenação a sequência de números naturais $b > r_1 > r_2 > r_3 > \cdots$ possui um menor elemento. Desta maneira, temos que $r_n \mid r_{n-1}$, para algum n, implicando assim que $(a, b) = r_n$.

$\square$

Ilustrando a demonstração acima, obtemos a seguinte tabela:

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

Exemplo 1.30. Determine o *mdc* de 372 e 162, pelo algoritmo de Euclides.

Pelo Algoritmo de Euclides, temos:

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6	0	

Logo, (372,162) = 6.

1.4 ALGORITMO BINÁRIO DE EUCLIDES

> O algoritmo é conhecido como binário porque, ao contrário do original, ele não usa divisão geral dos inteiros, mas apenas divisão por 2. Já que em um computador os números são representados pelo sistema Binário, você não deve se surpreender ao saber que existe uma instrução de máquina especial que implementa a divisão por 2 de uma maneira altamente eficiente. Isso é conhecido como o deslocamento à direita, em que o bit mais à direita é descarregado, os bits restantes são deslocados para a direita e o bit mais à esquerda é definido como 0. (BOGOMOLNY, 2018)

O algoritmo binário de Euclides foi descoberto por R.Silver e J.Tersian em 1962 mas foi publicado pela primeira vez pelo físico e programador israelense Josef Stein em 1967, por isso também é conhecido como algoritmo de Stein. Este é um algoritmo que calcula o máximo divisor comum (*mdc*) de dois números inteiros positivos, ao qual usa operações aritméticas mais simples que o convencional (1.3.2). Desta forma escreveremos essa seção da adaptação de (MARTÍNEZ, 2013).

De modo geral, esse algoritmo opera pela alteração do *mdc* de dois números inteiros positivos pelo *mdc* de dois números possivelmente menores que os anteriores, porém desta vez subtraímos e dividimos por 2. Vejamos agora, os três Teoremas ao qual o algoritmo binário de Euclides opera:

Teorema 1.31. *Dados $a, b \in \mathbb{N}$, tais que a e b são números pares, então:*

$$mdc(a, b) = 2 \cdot mdc\left(\frac{a}{2}, \frac{b}{2}\right).$$

Demonstração: Decorre imediatamente da Proposição 1.25.

Teorema 1.32. *Dados $a, b \in \mathbb{N}$, tais que a é par e b é ímpar, então:*

$$mdc(a, b) = mdc\left(\frac{a}{2}, b\right).$$

Demonstração: Seja *d* = *mdc(a,b)* e *d'* = *mdc*$\left(\frac{a}{2}, b\right)$. Como *d* | *b* e *b* é ímpar, então *d* é ímpar. Sendo que $a = k \cdot d$ para algum $k \in \mathbb{Z}$, temos que k é par, pois a é par e d é impar, então $\frac{a}{2} = \frac{k}{2} \cdot d$. Portanto $d \mid \frac{a}{2}$ e $d \mid b$, logo $d \leq d'$. Agora, como $d' \mid \frac{a}{2}, \frac{a}{2} = k'd'$ para algum $k' \in \mathbb{Z}$, isto é $a = 2k'd'$, portanto $d' \mid a$, então $d' \mid a$ e $d' \mid b$, assim $d' \leq d$, o que nós dá que $d = d'$.

□

Teorema 1.33. *Dados $a, b \in \mathbb{N}$, tais que a e b são números ímpares, então:*

$$mdc(a, b) = mdc\left(\frac{|a-b|}{2}, a\right) = mdc\left(\frac{|a-b|}{2}, b\right) = mdc\left(\frac{|a-b|}{2}, Mín\{a, b\}\right).$$

Demonstração: Seja *d = mdc(a,b)* e *d' = mdc* $(\frac{|a-b|}{2}, b)$. Como $d \mid a$ e $d \mid b$ então $d \mid |a-b|$. Logo $\mid a-b \mid = kd$ para algum $k \in \mathbb{Z}$, k deve ser par já que a, b e d são números ímpares. Daí podemos dividir ambos os termos da igualdade por dois, ou seja $\frac{|a-b|}{2}$ = $\frac{k}{2} \cdot d$. Portanto, temos que $d \mid \left(\frac{|a-b|}{2}\right)$ e $d \mid b$, então $d \leq d'$. Por outro lado, se $b = k'd'$ e $|a-b|$ = $2k"d'$, substituindo b na última equação, obtemos que $d' \mid a$. Portanto $d' \leq d$ o que prova a igualdade $d = d'$.
A demonstração das outras igualdades é análoga.

□

O algoritmo binário de Euclides prossegue assim: Suponha que $a, b \in \mathbb{Z}$, tais que a $\geq$ 0 e b > 0. Se a e b forem números pares, aplicamos o Teorema 1.31, digamos x vezes, até que um dos números seja ímpar. No final você tem que multiplicar por 2^x como compensação por ter usado o Teorema 1.31, x vezes. Se ainda a ou b for par, aplicamos agora o Teorema 1.32 até que ambos os números sejam ímpares. Quando os dois números forem ímpares, aplicamos o Teorema 1.33. Feito isso alternamos os Teoremas 1.32 e 1.33 conforme for o quociente da divisão $\left(\frac{|a-b|}{2}\right)$ se for par ou se for ímpar. Vamos calcular três *mdc* por esse algoritmo, sendo o primeiro igual ao exemplo 1.30 da seção anterior.

Exemplo 1.34. Determine o *mdc* de 372 e 162, pelo método do algoritmo binário de Euclides.

mdc (372,162)	= 2 · mdc (186,81),	Pelo Teorema 1.31
	= 2 · mdc (93,81),	Pelo Teorema 1.32
	= 2 · mdc (6,81),	Pelo Teorema 1.33
	= 2 · mdc (3,81),	Pelo Teorema 1.32
	= 2 · mdc (39,3),	Pelo Teorema 1.33
	= 2 · mdc (18,3),	Pelo Teorema 1.33
	= 2 · mdc (9,3),	Pelo Teorema 1.32
	= 2 · mdc (3,3),	Pelo Teorema 1.33
	= 2 · mdc (0,3),	Pelo item 2 da Observação 1.16
	= 2 · 3	
	= 6	

Exemplo 1.35. Determine o *mdc* de 22 e 89, pelo método do algoritmo binário de Euclides.

mdc (22,89)	= mdc (11,89),	Pelo Teorema 1.32
	= mdc (39,11),	Pelo Teorema 1.33
	= mdc (14,11),	Pelo Teorema 1.33
	= mdc (7,11),	Pelo Teorema 1.32
	= mdc (2,7),	Pelo Teorema 1.33
	= mdc (1,7),	Pelo item 1 da Observação 1.16
	= 1	

Exemplo 1.36. Determine o *mdc* de 4 e 24, pelo método do algoritmo binário de Euclides.

$$\begin{aligned} \text{mdc }(4{,}24) &= 2 \cdot \text{mdc }(2{,}12), && \text{Pelo Teorema 1.31} \\ &= 4 \cdot \text{mdc }(1{,}6), && \text{Pelo item 1 da Observação 1.16} \\ &= 4 \cdot 1 \\ &= 4 \end{aligned}$$

Diante disso, percebemos que o cálculo do *mdc* termina quando obtemos $mdc(0, d) = d$, conforme o item 2 da Observação 1.16 ou $mdc(1, d) = 1$, de acordo com item 1 da Observação 1.16.

1.5 MÍNIMO MÚLTIPLO COMUM (MMC)

Diremos que um número natural $m \neq 0$ é *mínimo múltiplo comum (mmc)* de $a,b \in \mathbb{Z}^*$, se possuir as seguintes propriedades:

(i) m é um múltiplo comum de a e b;

(ii) Se c é um múltiplo comum de a e b, então $m \mid c$.

Portanto, o *mmc* de a, $b \in \mathbb{Z}$, tal que a, $b > 0$ é o menor número inteiro positivo que é divisível por a e por b. Ao qual denotaremos por $[a,b]$. E pelo Princípio da Boa Ordenação, o conjunto dos múltiplos comuns de a e b sempre possui o menor elemento e ele é único.

Por outro lado, se $[a, b] = m$ e c é um múltiplo comum de a e b, então $m \mid c$. Logo, se c é positivo, temos que $m \leq c$, mostrando que m é o menor múltiplo inteiro positivo comum de a e b.

Exemplo 1.37. Seja *M(a)* o conjunto dos múltiplos inteiros de um número inteiro a, então temos que:
M(40) = $\{\ 0, \pm 40, \pm 80, \pm 120, \pm 160, \pm 200, \pm 240, \pm 280 \cdots\ \}$.
M(48) = $\{\ 0, \pm 48, \pm 96, \pm 144, \pm 192, \pm 240, \pm 288, \cdots\ \}$.

Observando os conjuntos dos múltiplos de 40 e de 48, temos que o menor múltiplo comum de 40 e 48 é 240. Assim, [40,48] = 240.

Diremos também, que um número natural m é *mmc* dos números inteiros não nulos $a_1, a_2, \cdots, a_n$, se m é um múltiplo comum de $a_1, a_2, \cdots, a_n$ e, se para todo múltiplo comum m' desses números, tem-se que $m \mid m'$.

Observação 1.38.

1. $[a, 1] = a$;
2. $[a, b] = 0$ *se, e somente se,* $a = 0$ *ou* $b = 0$;
3. *Se* $a \mid b$, *então* $[a, b] = b$;
4. *Se* $[a, b] = 1$, *então* $a = b = 1$.

Exemplo 1.39.

1. $[14, 1] = 14$;
2. $[12, 0] = 0$;
3. $[3, 6] = 6$;
4. $[1, 1] = 1$;

O seguinte Teorema fornece uma relação entre o *mdc* e o *mmc*.

Teorema 1.40. *Dados a,b,* $\mathbb{N}^*$, *então:*

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

Demonstração: Definindo $m = \frac{ab}{(a,b)}$, queremos provar que $m = [a,b]$. Temos que $a \mid m$ e $b \mid m$. Seja $c \in \mathbb{Z}$, um múltiplo comum entre a e b, então existem k_1, $k_2 \in \mathbb{Z}$, tais que $c = ak_1$ e $c = bk_2$. Segue que: $k_1 \cdot \frac{a}{(a,b)} = k_2 \cdot \frac{b}{(a,b)}$ e pela Proposição1.27, sabemos que $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$. Assim, $\frac{a}{(a,b)}$ divide k_2, ou seja, $\frac{a}{(a,b)}b$ divide $k_2 b$. Logo $m = b\frac{a}{(a,b)}$ divide $k_2 b$, ou seja, $m \mid c$. Portanto, m é o menor dos múltiplos entre a e b, ou seja, $m = [a,b]$.

□

Exemplo 1.41. Sejam $a = 40$ e $b = 48$. Pelo Teorema 1.40, temos que $[40, 48] \cdot (40, 48) =| 40 \cdot 48 |= 1920$. Como $(40, 48) = 8$, segue que $[40, 48] = 240$.

1.6 TEOREMA FUNDAMENTAL DA ARITMÉTICA (TFA)

Um número natural $n > 1$ é chamado primo se seus únicos divisores positivos são 1 e ele próprio. Caso contrário, é chamado composto.

Proposição 1.42. *Se* $p \mid ab$, *onde* p *é primo, então* $p \mid a$ *ou* $p \mid b$.

Demonstração: Se $p \nmid a$, então *(a,p)* = 1, logo pelo Teorema 1.21, temos que $p \mid b$. Analogamente, se $p \nmid b$, então $p \mid a$.

□

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. Por exemplo, 1260 é escrito de maneira única, a menos pela ordem dos fatores, como $2^2 \cdot 3^2 \cdot 5 \cdot 7$.

A ordem dos fatores, pela propriedade comutativa da multiplicação é irrelevante. O que torna o Teorema interessante, pois garante uma representação única para qualquer número inteiro. Vamos então ao Teorema:

Teorema 1.43. *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: Supondo por absurdo, ou seja, 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, certamente ele possui um elemento mínimo. Assim, pelo Princípio da Boa Ordenação, chamamos 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, tais que $x = ab$, com $a < x$ e $b < x$, e como $a \notin A$ e $b \notin A$, eles possuem fatoração e, portanto, $x = ab$, possui fatoração, logo um absurdo, pois $x \in A$. Portanto, A não pode ter elemento mínimo, logo $A = \varnothing$. O que prova a demostração da existência.

Unicidade: Da generalização do Teorema 1.42, temos que $p \mid a_1 a_2 a_3 \ldots a_n$, com p *primo*, então p divide pelo menos um fator a_i do produto, com $i \in \{1, 2, \cdots, n\}$. Assim, sejam $y = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_n$ 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 $p_1 | q_1 q_2 \ldots q_n$ e, portanto, pela generalização da Proposição 1.42 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: $q_1 q_2 \ldots q_k \ldots q_n = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_k$, 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 demostração da unicidade.

□

Contudo, denotando *d(n)* o número de divisores positivos do número natural *n*, segue que se *n* = $p_1^{\alpha_1}\ p_2^{\alpha_2}\ p_3^{\alpha_3}\ \ldots\ p_r^{\alpha_r}$, onde $p_1, \ldots, p_r$ são números primos e $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$, então temos:

$$d(n) = (\alpha_1 + 1)(\alpha_2 +1) \ldots (\alpha_r +1).$$

Exemplo 1.44. Encontre o número de divisores positivos do número natural 360.

Decompondo o número 360 temos que 360 = $2^3 \cdot 3^2 \cdot 5^1$, logo o número de divisores é d(360) = (3+1)(2+1)(1+1) = 4·3·2 = 24.

Assim 360 possui 24 divisores, ao qual são eles: {1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360}.

Proposição 1.45. *Seja n =* $p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\ldots p_r^{\alpha_r}$ *um número natural. Se* n_1 *é um divisor positivo de n, então:*

$$n_1 = p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3}\ldots p_r^{\beta_r},$$

onde $0 \leq \beta_i \leq \alpha_i$*, para i = 1, 2, ..., r.*

Demonstração: Seja n_1 um divisor positivo de *n* e seja p^β a potência de um número primo *p* que pertence à decomposição de n_1 em fatores primos. Como $p^\beta \mid n$, segue que $p^\beta \mid p_i^{\alpha_i}$, por ser primo com os demais $p_j^{\alpha_j}$, e consequentemente, $p = p_i$ e $0 \leq \beta \leq \alpha_i$.

□

Proposição 1.46. *Se a =* $p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\ldots p_n^{\alpha_n}$ *e b =* $p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3}\ldots p_n^{\beta_n}$*, onde* $p_1, p_2, p_3, \ldots, p_n$ *são os primos que ocorrem nas fatorações de a e b, então:*

$$[a,b] = p_1^{max\{\alpha_1,\beta_1\}}p_2^{max\{\alpha_2,\beta_2\}}p_3^{max\{\alpha_3,\beta_3\}}\ldots\ p_n^{max\{\alpha_n,\beta_n\}}$$

Demonstração: Da definição de *mmc* nenhum fator primo p_i deste mínimo poderá ter um expoente que seja inferior nem a α_i e nem a β_i, com $i \in \{1, 2, \cdots, n\}$. Assim, tomando o maior destes dois para expoente de p_i teremos, não apenas um múltiplo comum, mas o menor possível dentre todos.

□

Exemplo 1.47. Calcule o [18,24].

Escrevendo os números como um produto de números primos, assim 18 = $2^1 \cdot 3^2$ e 24 = $2^3 \cdot 3^1$, e pela Proposição 1.46, temos que:

$[18, 24] = 2^3 \cdot 3^2 = 8 \cdot 9 = 72.$

O que também pode ser comprovado encontrando os múltiplos positivo de cada número:

Múltiplos de 18 = {0, 18, 36, 54, 72, ...}.

Múltiplos de 24 = {0, 24, 48, 72, . . . }.
Logo o [18,24] = 72.

1.7 EQUAÇÕES DIOFANTINAS LINEARES COM DUAS VARIÁVEIS

Uma equação diofantina é linear se ela tiver a 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.).

Figura 2 – Diofanto de Alexandria

Fonte: (MORGANA, 2012)

Diofanto foi um matemático e filósofo grego e é considerado o maior algebrista grego, verdadeiro precursor da moderna teoria dos números é visto por alguns como pai da álgebra, devido à sua inovação com notações, e por ser o primeiro a usar símbolos na resolução de problemas algébricos. Mostrou interesse por uma grande variedade de equações indeterminadas que admitem infinitas soluções.

A resolução de muitos problemas de aritmética depende da resolução das equações diofantinas na forma $aX + bY = c$, onde a, b, $c \in \mathbb{Z}$ são dados e X e Y são incógnitas a serem determinadas em $\mathbb{Z}$.

Nem sempre estas equações possuem soluções. É portanto necessário estabelecer condições para que tais equações possuam soluções e, caso tenham, e preciso saber como determiná-las. Para isso, precisamos mostrar as duas proposições a seguir:

Proposição 1.48. *Sejam a, b, c* $\in \mathbb{Z}$*, com* a *e* b *ambos não nulos, e* $d = (a, b)$*. A equação diofantina*

$$aX + bY = c$$

admite solução nos números inteiros se, e somente se, $d \mid c$*.*

Demonstração: Suponhamos que a equação $aX + bY = c$ admite solução em números inteiros, isto é, existem x_0 e $y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = c$. Como $d = (a, b)$, temos que $d \mid a$ e $d \mid b$ e pela Proposição 1.10 segue que $d \mid c$.
Reciprocamente, se $d \mid c$, então existe $l \in \mathbb{Z}$, tal que $dl = c$. Pelo Teorema 1.18, existem x_0 e y_0 $\in \mathbb{Z}$, com $d = ax_0 + by_0$. Disso segue que $c = a(lx_0) + b(ly_0)$, o que implica que lx_0 e ly_0 é uma solução particular de $aX + bY = c$.

$\square$

Proposição 1.49. *Suponha que* $d \mid c$ *e seja* x_0 *e* y_0 *uma solução particular da equação diofantina* $aX + bY = c$*, em que* $a \neq 0$ *e* $b \neq 0$*. Então qualquer solução dessa equação é dada pelo par de inteiros:*

$$x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t, \text{ com } t \in \mathbb{Z}$$

onde d = (a,b).

Demonstração: Sendo x_0 e y_0 uma solução particular e $t \in \mathbb{Z}$, iremos provar que $x = x_0 + \frac{b}{d}t$ e $y = y_0 - \frac{a}{d}t$ é uma solução da equação.
De fato, $aX + bY = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + \frac{b}{d}at + by_0 - \frac{b}{d}at = ax_0 + by_0 = c$.
Reciprocamente, seja x e y uma solução qualquer de $aX + bY = c$. Temos então que $ax_0 + by_0 = c = ax + by$, ou seja:

$$a(x - x_0) = b(y_0 - y).$$

Como $d = (a, b)$, temos que existem r, $s \in \mathbb{Z}$, tais que $a = rd$ e $b = ds$ e da Proposição 1.27 que $(r, s) = (\frac{a}{d}, \frac{b}{d}) = 1$.
Segue que $dr(x - x_0) = ds(y_0 - y)$, ou seja:

$$r(x - x_0) = s(y_0 - y),$$

pois $d \neq 0$.

Assim, supondo que $a \neq 0$, concluímos que $r \mid s(y_0 - y)$, daí $r \mid y_0 - y$, pois $(r, s) = 1$. Portanto, existe $t \in \mathbb{Z}$, tal que $rt = y_0 - y$ de onde vem que $y = y_0 - rt = y_0 - \frac{a}{d}t$.

Segue que $r(x - x_0)$ = $s(y_0 - y) = srt$ e então $x - x_0 = st$, pois $r \neq 0$, assim, $x = x_0 + st = x_0 + \frac{b}{d}t$.
Logo, temos que:

$$x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t, \text{ para algum } t \in \mathbb{Z}.$$

□

Corolário 1.50. *Se d = (a,b) = 1 e x_0, $y_0 \in \mathbb{Z}$ é uma solução particular da equação diofantina linear aX + bY= c, então todas as outras soluções desta equação são dadas por:*

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

Exemplo 1.51. (ENQ 2018/2) Considere a equação diofantina $5x + 3y = 2018$.

(a) Calcule a solução geral em $\mathbb{Z}$.

(b) Quantas soluções existem em $\mathbb{N} \cup \{0\}$?

Solução

(a) Temos que

$$5 \cdot (-1) + 3 \cdot (2) = 1,$$

logo

$$5 \cdot (-2018) + 3 \cdot (4036) = 2018.$$

Fazendo a divisão euclidiana de -2018 por 3,

$$-2018 = 3 \cdot (-673) + 1$$

Substituindo na equação acima, obtemos:

$$5 \cdot (-3 \cdot 673 + 1) + 3 \cdot (4036) = 2018$$

$$5 \cdot (1) + 3\dot{(}4036 - 5 \cdot 673) = 2018$$

$$5 \cdot (1) + 3 \cdot (671) = 2018$$

Portanto, x_0 = 1 e y_0 = 671 é a solução minimal e a solução geral em $\mathbb{Z}$ é dada por:

$$x = 1 + 3t, y = 671 - 5t,$$

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

(b) A solução geral em $\mathbb{N} \cup \{0\}$ é dada por

$$x = 1 + 3t, y = 671 - 5t,$$

onde t $\in \mathbb{N} \cup \{0\}$ e 0 $\leq$ 671 - 5t, logo 0 $\leq$ t $\leq$ 134.

Portanto, existem 135 soluções em $\mathbb{N} \cup \{0\}$.

1.8 EQUAÇÕES DIOFANTINAS LINEARES COM TRÊS VARIÁVEIS

Uma equação diofantina linear de três variáveis é escrita da forma:

$$ax + by + cz = r,$$

onde a, b e c são números inteiros não nulos.

Na Proposição 1.48, vimos que uma equação diofantina do tipo $ax + by = c$ possui solução se, e somente se, *(a,b)* | *c*. E de forma similar, as equações diofantinas lineares de três variáveis admitem soluções se, e somente se, *mdc(a,b,c)* divide *r*. Enunciamos esse resultado na Proposição abaixo:

Proposição 1.52. *Seja ax + by + cz = r, com a, b e c números inteiros não nulos e r um número inteiro qualquer. Assim a equação admite solução se, e somente se, r* = mdc(a,b,c)* | *r*.

Demonstração: Seja r^* = *mdc(a,b,c)* = *mdc(mdc(a,b),c)*, então $r^* \mid$ *mdc(a,b)* e $r^* \mid c$. Logo $r^* \mid a$, $r^* \mid b$ e $r^* \mid c$.

Suponhamos agora, que a equação admite solução, isto é, existem x_0, y_0, $z_0 \in \mathbb{Z}$, tais que $ax_0 + by_0 + cz_0 = r$.

Como $r^* \mid a$, $r^* \mid b$ e $r^* \mid c$, segue que $r^* \mid r$.

Reciprocamente, seja r_1 = *mdc(a,b)*. Então existem k_1, $k_2 \in \mathbb{Z}$, tais que $ak_1 + bk_2 = r_1$. Então r^* = *mdc(r_1,c)* e existem $k, z_0 \in \mathbb{Z}$, tais que $r^* = kr_1 + cz_0 = (ak_1 + bk_2)k + cz_0 = ak_1k + bk_2k + cz_0$.

Sejam $x_0 = k_1k$ e $y_0 = k_2k$, temos que:

$$r^* = ax_0 + by_0 + cz_0.$$

E como $r^* \mid r$, temos que existe $q \in \mathbb{Z}$, tal que $r = r^* \cdot q$. E multiplicando a equação anterior por q, segue que:

$$r = r^*q = a(x_0q) + b(y_0q) + c(z_0q).$$

O que mostra que (x_0q, y_0q, z_0q) é uma das soluções particulares da equação $ax + by + cz = r$.

$\square$

Para obter a solução geral da equação $ax + by + cz = r$, reduzimos essa equação para uma equação de duas variáveis, considerando $ax + by = p$, temos $p + cz = r$ que possui solução, pois $(1, c) = 1$ e 1 divide r. Assim, pela Proposição 1.49 a solução geral da equação $p + cz = r$ é dada por:

$$\{(p_0 + ct_1, z_0 - t_1) \mid t_1 \in \mathbb{Z}\}.$$

Dessa solução geral, escolhemos um valor arbitrário para t_1, que satisfaça, r_2 = *mdc*$(a, b) \mid (p_0 + ct_1)$ e continuamos a encontrar a solução geral da equação $ax + by = p = p_0 + ct_1$, e a partir dessa, a solução geral da equação original. Agora, basta analisar a equação gerada pela substituição feita, $ax + by = p = p_0 + ct_1$ que possui solução geral igual a:

$$\left\{ \left(x_0 + \frac{b}{r_2} t_2, y_0 - \frac{a}{r_2} t_2 \right) |t_2 \in \mathbb{Z} \right\}.$$

Assim, a solução geral da equação original é:

$$\left\{ \left(x_0 + \frac{b}{r_2} t_2, y_0 - \frac{a}{r_2} t_2, z_0 - t_1 \right) |t_1, t_2 \in \mathbb{Z} \right\}.$$

Logo para encontrarmos a solução geral de uma equação diofantina de três variáveis, devemos seguir os passos abaixo:

- Reduzir a equação original a uma equação com duas variáveis, por meio de uma substituição, e resolvê-la;
- Dessa solução, retornamos na substituição acima e resolvemos outra equação com duas variáveis. Obtendo assim a solução geral da equação.

Exemplo 1.53. Determine a solução geral da equação diofantina de três variáveis $56x + 72y + 21z = 317$.

Solução: Agora vamos resolver por partes, para encontrar a solução geral da equação diofantina $56x + 72y + 21z = 317$. Considere $p = 56x + 72y$, que gera a equação $p + 21z = 317$, que também possui solução, pois *mdc*(1,21) = 1 e 1 | 317. Então, conseguimos encontrar uma solução particular da equação $p + 21z = 317$, fazendo:

$$1 = 1 \cdot (-20) + 1 \cdot 21 \Longrightarrow 317 = 1 \cdot (-20 \cdot 317) + 317 \cdot 21 \Longrightarrow 317 = 1 \cdot (-6340) + 317 \cdot 21.$$

que nos leva a solução geral de $p + 21z = 317$, que é:

$$\{(-6340 + 21t_1, 317 - t_1), |t_1 \in \mathbb{Z}\}$$

Para encontrar a solução geral da equação diofantina $56x + 72y + 21z = 317$, devemos encontrar a solução geral da equação $56x + 72y = p = -6340 + 21t_1$. E para que essa equação possua solução, o *mdc*(56,72) = 8 deve dividir $-6340 + 21t_1$.

Satisfazendo a condição acima, basta encontrar a solução geral, assim pelo algoritmo de Euclides, temos que 8 = 4 · 56 - 3 · 72. Portanto:

$$8 = 56 \cdot 4 + 72 \cdot (-3) \Longrightarrow$$

$$8 \cdot \left(\frac{-6340 + 21t_1}{8}\right) = 56 \cdot 4\left(\frac{-6340 + 21t_1}{8}\right) + 72 \cdot (-3) \cdot \left(\frac{-6340 + 21t_1}{8}\right) \Longrightarrow$$

$$-6340 + 21t_1 = 56 \cdot \left(\frac{-25360 + 84t_1}{8}\right) + 72 \cdot \left(\frac{19020 - 63t_1}{8}\right).$$

Assim temos que a solução geral de $56x + 72y = p = -6340 + 21t_1$ é:

$$\left\{\left(\frac{-25360 + 84t_1}{8} + \frac{72t_2}{8}, \frac{19020 - 63t_1}{8} - \frac{56t_2}{8}\right) | t_1, t_2 \in \mathbb{Z}\right\}$$

Com isso, concluímos que a solução geral da equação diofantina de três variáveis é:

$$\left\{\left(\frac{-25360 + 84t_1}{8} + 9t_2, \frac{19020 - 63t_1}{8} - 7t_2, 317 - t_1\right) | t_1, t_2 \in \mathbb{Z}\right\}.$$

1.9 CONGRUÊNCIAS

O conceito de congruência, assim como a notação da qual se torna um dos instrumentos mais fortes da teoria dos números, foi introduzida por Johann Carl Friedrich Gauss (1777-1855) em um trabalho publicado em 1801 intitulado de *Disquisitiones Arithmeticae*.

Figura 3 – Johann Carl Friedrisch Gauss

Fonte: (WIKIPEDIA, 2019)

No livro, Gauss introduz a noção de congruência; desenvolve a teoria dos resíduos quadráticos, demonstrando a *Lei da Reciprocidade Quadrática*; estuda as formas quadráticas binárias, deduzindo dentro de um quadro bem mais geral, o Teorema de Fermat.

Definição 1.54. *Se a e b são inteiros, dizemos que a é congruente a b módulo m, para m > 1, se* $m \mid (a-b)$*. Ao qual denotamos por* $a \equiv b \pmod{m}$.

Por outro lado, se m $\nmid$ *(a - b), dizemos que a é incongruente b módulo m. E denotamos por* $a \not\equiv b \pmod{m}$.

Exemplo 1.55.

- $15 \equiv 3 \pmod{2}$, pois 2 | (15-3);
- $19 \not\equiv 7 \pmod{5}$, pois 5 $\nmid$ (19-7).

Observação 1.56. *Se* $a, b \in \mathbb{Z}$*, então* $a \equiv b \pmod{m}$ *se, e somente se,* a *e* b *possuem o mesmo resto na divisão euclidiana por* m.
Portanto, uma outra maneira de verificar que $15 \equiv 3 \pmod{2}$ *é vendo que os restos da divisão de 15 e de 3 por 2 são iguais a 1.*

Os seguintes resultados demonstram algumas propriedades elementares das Congruências.

Proposição 1.57. *Se a, b* $\in \mathbb{Z}$*, temos que* $a \equiv b \pmod{m}$ *se, e somente se, existe k* $\in \mathbb{Z}$*, tal que a = b + km.*

Demonstração: Se $a \equiv b \pmod{m}$, então *m* | (a - b), o que implica na existência de um número *k* $\in \mathbb{Z}$, tal que *a - b = km*, ou seja, *a = b + km*.

Reciprocamente, temos que da existência de um número *k* $\in \mathbb{Z}$, o qual satisfaz $a = b+km$, segue que $km = a - b$, ou seja, *m* | *(a - b)*, isto é $a \equiv b \pmod{m}$.

□

Exemplo 1.58. Como $63 = 3 + 12 \cdot 5$, temos pela Proposição 1.57 que $63 \equiv 3 \pmod{5}$.

Proposição 1.59. *Se a, b, d, m* $\in \mathbb{Z}$*, com m > 0, então:*

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

Demonstração:

1. Como *m* | 0, então *m* | *(a - a)*, implica em $a \equiv a \pmod{m}$;
2. Suponhamos que $a \equiv b \pmod{m}$, isto é, $m \mid a - b$. Logo, $m \mid -(a - b)$, o qual implica que $b \equiv a \pmod{m}$;
3. Se $a \equiv b \pmod{m}$ e $b \equiv d \pmod{m}$, então existem k_1 e $k_2 \in \mathbb{Z}$ tais que *a - b* = k_1*m* e *b - d* = k_2*m*. Somando, membro a membro, estas duas equações, obtemos *a - d* = *(*k_1 + k_2*)m*, que implica em $a \equiv d \pmod{m}$.

□

Exemplo 1.60.

1. $7 \equiv 7 \pmod{9}$;
2. $9 \equiv 3 \pmod{6}$, assim como $3 \equiv 9 \pmod{6}$;
3. $73 \equiv 13 \pmod{5}$ e $13 \equiv 3 \pmod{5}$, assim como, $73 \equiv 3 \pmod{5}$.

Observe que a Proposição acima afirma que a relação de congruência satisfaz as propriedades reflexiva, simétrica e transitiva. Ou seja, a relação de congruência, no conjunto dos números inteiros é uma relação de equivalência em $\mathbb{Z}$. Note também que podemos descrever as classes de equivalência assim: dado $0 \leq a < m$, a inteiro,

$$\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

é igual ao conjunto de inteiros cujo resto dividido por m é igual a a.

Teorema 1.61. *Se a, b, c, d, m* $\in \mathbb{Z}$*, com m>1, tais que* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$*, então:*

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

Demonstração:

1. De $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ temos *a - b* = k_1*m* e *c - d* = k_2*m*, com $k_1, k_2 \in \mathbb{Z}$. Somando-se ambos os lados da igualdade, obtemos *(a + c) - (b + d)* = (k_1 + k_2)*m* e isto implica $a + c \equiv b + d \pmod{m}$.

2. Subtraindo as igualdades *a - b* = k_1*m* e *c - d* = k_2*m*, obtemos *(a - b) - (c - d)* = *(*k_1 *-* k_2*)m*, que implica em, $a - c \equiv b - d \pmod{m}$.

3. Multiplicando a igualdade *a - b* = k_1*m* por *c* e *c - d* = k_2*m* por *b*, obtemos *ac - bc* = *c*k_1*m* e *bc - bd* = *b*k_2*m*. Agora somando as duas igualdades obtemos *ac - bc + bc - bd* = *(c*k_1 + *b*k_2*)m*, que implica em, $ac \equiv bd \pmod{m}$. □

Exemplo 1.62.

1. Sendo $19 \equiv 4 \pmod{5}$ e $12 \equiv 2 \pmod{5}$, segue do Teorema 1.61 (1) que $19+12 \equiv 4+2 \pmod{5}$, ou seja, $31 \equiv 6 \equiv 1 \pmod{5}$.

2. Visto que $19 \equiv 4 \pmod{5}$ e $12 \equiv 2 \pmod{5}$, temos do Teorema 1.61 (2) que $19 - 12 \equiv 4 - 2 \pmod{5}$, ou seja, $7 \equiv 2 \pmod{5}$.

3. Note que $19 \equiv 4 \pmod{5}$ e $12 \equiv 2 \pmod{5}$, temos do Teorema 1.61 (3) que $19{\cdot}12 \equiv 4{\cdot}2 \pmod{5}$, ou seja, $228 \equiv 8 \equiv 3 \pmod{5}$.

Alguns casos particulares do Teorema 1.61 é dado pela Observação abaixo:

Observação 1.63. *Se a, b, c, k, m* $\in \mathbb{Z}$*, tais que* $a \equiv b \pmod{m}$*, então:*

1. $a + c \equiv b + c \pmod{m}$*;*

2. $a - c \equiv b - c \pmod{m}$*;*

3. $ac \equiv bc \pmod{m}$.

Exemplo 1.64.

1. Sendo $10 \equiv 3 \pmod{7}$, da Observação 1.63 (1), temos que $10 + 2 \equiv 3 + 2 \pmod{7}$, ou seja, $12 \equiv 5 \pmod{7}$.

2. Visto que $10 \equiv 3 \pmod{7}$, da Observação 1.63 (2), temos que $10 - 2 \equiv 3 - 2 \pmod{7}$, ou seja, $8 \equiv 1 \pmod{7}$.

3. Note que $10 \equiv 3 \pmod{7}$, da Observação 1.63 (3), temos que $10 \cdot 2 \equiv 3 \cdot 2 \pmod{7}$, ou seja, $20 \equiv 6 \pmod{7}$.

Teorema 1.65. *Se a, b, c e m* $\in \mathbb{Z}$*, com m > 1, temos que:*

$$ac \equiv bc \pmod{m}$$

se, e somente se,

$$a \equiv b \pmod{\frac{m}{(c, m)}}.$$

Demonstração: Se $ac \equiv bc \pmod{m}$ temos *ac - bc = km*, com $k \in \mathbb{Z}$. Dividindo por *(c,m)*, temos:

$$\frac{c}{(c,m)}(a-b) = k\frac{m}{(c,m)} \Longleftrightarrow \frac{m}{(c,m)} \mid \frac{c}{(c,m)}(a-b).$$

Sendo que

$$\left(\frac{m}{(c,m)}, \frac{c}{(c,m)}\right) = 1,$$

temos que

$$\frac{m}{(c,m)} \mid (a-b).$$

Daí

$$a \equiv b \pmod{\frac{m}{(c,m)}}.$$

$\square$

Exemplo 1.66. Note que $144 \equiv 36 \pmod{12}$ e $(9,12) = 3$. Pelo Teorema 1.65,

$$\frac{144}{9} \equiv \frac{36}{9} \pmod{\frac{12}{(9,12)}},$$

ou seja, $16 \equiv 4 \pmod{4}$.

Proposição 1.67. *Se a, b, m* $\in \mathbb{Z}$*, com* $m > 1$ *e* $a \equiv b \pmod{m}$*, então tem-se que:*

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

para todo $n \in \mathbb{N}$.

Demonstração: Vamos provar essa Proposição, pelo princípio de Indução Finita sobre n.

Para $n = 1$ a propriedade é válida pela hipótese.

Suponhamos que a propriedade é válida para um certo $n = k$, isto é, $a^k \equiv b^k \pmod{m}$. Mostremos que $a^{k+1} \equiv b^{k+1} \pmod{m}$.

Pelo Teorema 1.61, item 3, o fato que $a \equiv b \pmod{m}$ e a hipótese indutiva $a^k \equiv b^k \pmod{m}$ obtemos o resultado.

$\square$

Exemplo 1.68. Vamos determinar o algarismo das unidades de:

- 101^{101}

  Para encontrarmos o algarismo das unidades de um número, basta encontrarmos a congruência, módulo 10 desse número. Assim, sabemos que o algarismo das unidades de 101 é 1, pois $101 \equiv 1 \pmod{10}$. Logo, para sabermos o algarismo das unidades de 101^{101}, vamos usar a Proposição 1.67 na congruência $101 \equiv 1 \pmod{10}$, ou seja, $101^{101} \equiv 1^{101} \equiv 1 \pmod{10}$. Então, o último algarismo de 101^{101} é 1.

- 99^{101}

  Sabendo que $99 \equiv -1 \pmod{10}$, pela Proposição 1.67, temos que $99^{101} \equiv (-1)^{101} \equiv -1 \equiv 9 \pmod{10}$. Assim, o último algarismo de 99^{101} é 9.

Proposição 1.69. *Seja m um número inteiro maior do que 1. E sejam a e b números inteiros quaisquer. Temos que, se $a \equiv b \pmod{m}$ e se $n \mid m$, então $a \equiv b \pmod{n}$.*

Demonstração: Se $a \equiv b \pmod{m}$, então $m \mid b - a$. Como $n \mid m$, segue-se que $n \mid b - a$. Portanto, $a \equiv b \pmod{n}$.

□

Exemplo 1.70. Se $35 \equiv 7 \pmod{14}$, temos que $7 \mid 14$, então da Proposição 1.69 temos $35 \equiv 7 \pmod{7}$.

Teorema 1.71. *Se $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\ldots$, $a \equiv b \pmod{m_n}$, onde a, b, m_1, m_2,$\ldots$, $m_n \in \mathbb{Z}$, com $m_i > 1$ para $i = 1, 2, \cdots, n$. Então*

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_n]},$$

onde $[m_1, m_2, \ldots, m_n]$ é o mmc dos números $m_1, m_2, \ldots, m_n$.

Demonstração: Se $a \equiv b \pmod{m_i}$, $i = 1, 2, \cdots, r$, então $m_i \mid b - a$ para todo i. Sendo $b - a$ um múltiplo de cada m_i, segue-se que $[m_1, \cdots, m_r] \mid b - a$, o que prova que $a \equiv b \pmod{[m_1, \cdots, m_r]}$.

□

Exemplo 1.72. Sendo $45 \equiv 9 \pmod{2}$; $45 \equiv 9 \pmod{3}$ e $45 \equiv 9 \pmod{4}$.

Temos também que $[2, 3, 4] = 12$, logo pelo Teorema 1.71, $45 \equiv 9 \pmod{12}$.

1.10 CONGRUÊNCIA LINEAR

Definição 1.73. *A forma da congruência linear é:*

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

onde a, b, m $\in \mathbb{Z}$, com $m > 1$, são dados.

Exemplo 1.74. Resolva a congruência $6X \equiv 3 \pmod{15}$.

Por tentativa e erro, ou seja, variando o valor de $X = 1, 2, \cdots$, temos que uma solução para a congruência $6X \equiv 3 \pmod{15}$ é $X = 8$.

Exemplo 1.75. Resolva a congruência $2X \equiv 7 \pmod{4}$.

Podemos escrever a congruência acima na forma $2X - 7 \equiv 0 \pmod{4}$, a qual não possui solução pois para qualquer X temos que $2X - 7$ é um número ímpar que não é divisível por 4.

A Proposição, a seguir, fornece um critério que nos permite decidir se uma congruência linear admite ou não soluções.

Proposição 1.76. *Dados m $\in \mathbb{N}$, e a e b $\in \mathbb{Z}$, com m > 1, a congruência $aX \equiv b \pmod{m}$ possui solução se, e somente se, (a,m) | b.*

Demonstração: Suponha que $aX \equiv b \pmod{m}$ tenha uma solução x, logo temos que $m \mid ax - b$ que equivale a existência de k, com $k \in \mathbb{Z}$, tal que $ax - mk = b$, o que implica que a equação $aX + mK = b$ admite solução e pela Proposição 1.48, temos que $(a, m) \mid b$.

Reciprocamente, suponha que $(a, m) \mid b$. Da Proposição 1.48, a equação $aX + mK = b$ admite uma solução $\{x, k_1\}$. Portanto, $ax = b - mk_1$ e, consequentemente, x é uma solução de $aX \equiv b \pmod{m}$.

□

Observação 1.77. *A equação $aX \equiv 1 \pmod{m}$, tem solução se, e somente se, mdc$(a, m) = 1$. Isto é, a tem um "inverso"módulo m se, e somente se, mdc$(a, m) = 1$.*

Proposição 1.78. *Sejam $d = (a, m)$ com $m \in \mathbb{N}$ e a, b $\in \mathbb{Z}$, com m > 1. Se d | b, então $aX \equiv b \pmod{m}$, possui d soluções incongruentes entre si módulo m. Se $x_0 \in \mathbb{Z}$ é uma solução particular (solução minimal), então as d soluções incongruentes são obtidas por:*

$$x_0,\ x_0 + \tfrac{m}{d},\ x_0 + \tfrac{2m}{d},\ x_0 + \tfrac{3m}{d},\ \ldots,\ x_0 + \tfrac{m(d-1)}{d}.$$

Demonstração: Toda solução x da congruência $aX \equiv b \pmod{m}$ é congruente, módulo m, a $x_0 + i\frac{m}{d}$ para algum $0 \leq i < d$. Assim, se x é uma solução qualquer da congruência, então,

$$ax \equiv ax_0 \pmod{m}.$$

Logo, do Teorema 1.65, temos que:

$$x \equiv x_0 \pmod{\frac{m}{d}}.$$

Portanto, $x - x_0 = \frac{km}{d}$. E pela divisão euclidiana, existe $0 \leq i < d$ tal que $k = qd + i$ e, assim:

$$x = x_0 + qm + i\frac{m}{d} \equiv x_0 + i\frac{m}{d} \pmod{m}.$$

Reciprocamente, temos que os números $x_0 + i\frac{m}{d}$, com $0 \leq i < d$, são soluções da congruência $aX \equiv b \pmod{m}$, pois substituindo, temos que:

$$a \cdot \left(x_0 + i\frac{m}{d}\right) = ax_0 + i\frac{a}{d}m \equiv ax_0 \equiv b \pmod{m}.$$

Por fim, esses números são dois a dois incongruentes módulo m, pois se, para $0 \leq i, j < d$, obtemos:

$$x_0 + i\frac{m}{d} \equiv x_0 + j\frac{m}{d} \pmod{m},$$

então

$$i\frac{m}{d} \equiv j\frac{m}{d} \pmod{m}.$$

Sendo que $0 \leq i, j < d$, obtemos $0 \leq i\frac{m}{d}, j\frac{m}{d} < m$, e como m divide $|i\frac{m}{d} - j\frac{m}{d}|$, segue-se que $i\frac{m}{d} = j\frac{m}{d}$, ou seja, $i = j$.

□

Exemplo 1.79. Resolva a congruência $6X \equiv 3 \pmod{15}$, encontrando todas as soluções inteiras.

Observe que $d = (6, 15) = 3$ e $3 \mid 3$. Portanto, a congruência tem $d = 3$ soluções incongruentes módulo 15.

Do exemplo 1.74, temos que $x_0 = 8$ é uma solução.

Logo, as soluções incongruentes módulo 15 são:

$$8, 8 + \frac{15}{3}, 8 + 2 \cdot \frac{15}{3}.$$

Assim, todas as soluções inteiras são dadas por:

$$8 + 15t, 13 + 15t, 18 + 15t,$$

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

1.11 SISTEMAS DE CONGRUÊNCIAS

Agora, podemos pensar em resolver sistemas de congruências lineares que possuem a seguinte forma genérica:

$$\begin{cases} a_1X \equiv b_1 \pmod{m_1} \\ a_2X \equiv b_2 \pmod{m_2} \\ \vdots \\ a_rX \equiv b_r \pmod{m_r} \end{cases}$$

onde $a_i, b_i, m_i \in \mathbb{Z}$, com $m_i > 1$, para $i = 1, 2, \cdots, r$.

Uma solução desse sistema de congruências é um inteiro x_0 tal que seja solução para cada uma das congruências que dele fazem parte. Assim, se uma de suas congruências não admite solução, o mesmo ocorrerá com o sistema de congruências.

Proposição 1.80. *Se a congruência linear do tipo $aX \equiv b \pmod{m}$ admite solução, então ela é equivalente a uma congruência da forma*

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

Demonstração: Se $aX \equiv b \pmod{m}$ tem solução, ou seja, $d = (a, m) \mid b$. Fazendo

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

tem-se que a congruência $aX \equiv b \pmod{m}$ é equivalente a $a'X \equiv b' \pmod{n}$. Como $(a', n) = 1$, a' é invertível, ou seja, existe um a" tal que $a' \cdot a" \equiv 1 \pmod{n}$. Daí, multiplicando a congruência $a'X \equiv b' \pmod{n}$ por a", tem-se $a'a"X \equiv ba" \pmod{n}$, isto é,

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

onde $c = ba"$, com a" o inverso multiplicativo de a' módulo n.

$\square$

Os sistemas de congruências lineares do tipo

$$a_iX \equiv b_i \pmod{m_i},$$

para $i = 1, \cdots, r$, possuem solução quando $(a_i, m_i) \mid b_i$, para todo $i = 1, \cdots, r$.

Nesse caso, pela Proposição 1.80, o sistema é equivalente a um sistema reduzido escrito na forma

$$X \equiv c_i \pmod{n_i},$$

para $i = 1, \cdots, r$.

A partir dessa equivalência dos sistemas de congruência, apresentaremos o Teorema Chinês dos Restos, que fornece um método de resolução dos Sistemas de Congruências.

1.11.1 TEOREMA CHINÊS DOS RESTOS

A mais antiga declaração conhecida desse Teorema é do matemático chinês Sun-Tsu, no século 3 d.C. Então, vamos ao Teorema:

Teorema 1.81. *Sejam $m_1, m_2, \ldots, m_r$ números inteiros maiores que um e tais que (m_i, m_j) = 1, sempre que $i \neq j$, com i, j $\in \mathbb{N}^*$. Sejam $M = m_1 m_2 \ldots m_r$ e $b_1, b_2, \ldots, b_r$, respectivamente, soluções das congruências lineares:*

$$\frac{M}{m_j} b_i \equiv 1 \pmod{m_j}.$$

Então o sistema:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

admite uma única solução módulo M e as soluções são dadas por

$$x = a_1 b_1 \frac{M}{m_1} + a_2 b_2 \frac{M}{m_2} + \cdots + a_r b_r \frac{M}{m_r} + tM.$$

Demonstração: Notemos que, como (m_j, m_i) = 1, para $i \neq j$, com i, j $\in \mathbb{N}^*$, então:

$$\left(m_j, \tfrac{M}{m_j}\right) = 1.$$

O que implica na existência de soluções para cada congruência linear:

$$\tfrac{M}{m_j} b \equiv 1 \pmod{m_j},$$

as quais estamos indicando por b_j. Assim:

$$\tfrac{M}{m_j} b_j \equiv 1 \pmod{m_j}.$$

Portanto,

$$\tfrac{M}{m_j} a_j b_j \equiv a_j \pmod{m_j}.$$

Por outro lado, se $i \neq j$, temos que:

$$\tfrac{M}{m_i} \equiv 0 \pmod{m_j} \Longrightarrow a_i b_i \tfrac{M}{m_i} \equiv 0 \pmod{m_j}.$$

Logo, temos que:

$$a_1 b_1 \tfrac{M}{m_1} + \cdots + a_j b_j \tfrac{M}{m_j} + \cdots + a_r b_r \tfrac{M}{m_r} \equiv a_j \pmod{m_j},$$

para todo j, tal que $1 \leq j \leq r$. Assim,

$$x_0 = \textstyle\sum_{i=1}^{r} a_i b_i \tfrac{m}{m_i},$$

é uma solução particular do sistema.

Para demonstrar a unicidade desta solução, suponhamos que x' é outra solução qualquer do sistema considerado, então

$$x \equiv x' \pmod{m_i}$$

para todo $i = 1, \cdots, r$.

Como $(m_i, m_j) = 1$, para todo $i \neq j$, segue-se que $[m_1, \cdots, m_r] = m_1 \cdots m_r = M$ e, consequentemente, pelo Teorema 1.71, temos que $x \equiv x' \pmod{M}$.

□

Agora vamos resolver um exemplo que abrange algumas definições vistas acima.

Exemplo 1.82. (ENQ 2018/1) O objetivo deste problema é encontrar o número natural *x*, menor do que 1700 e que deixe restos 2, 2, 1 e 0 quando dividido por 5, 6, 7 e 11, respectivamente. Para tanto, faça os itens a seguir:

(a) Escreva um sistema de congruências que tenha *x* como uma solução.

(b) Determine a solução geral do sistema do item (a).

(c) A partir da solução geral do sistema, calcule o valor de *x*.

Solução

(a) Temos que $0 < x < 1700$ é uma solução do seguinte sistema de congruências:

$$\begin{cases} X \equiv 2 \pmod{5} \\ X \equiv 2 \pmod{6} \\ X \equiv 1 \pmod{7} \\ X \equiv 0 \pmod{11} \end{cases}$$

(b) Como 5, 6, 7, 11 são coprimos dois a dois, usaremos o Teorema 1.81 para determinar a solução geral do sistema.

Tomamos $M = 5 \cdot 6 \cdot 7 \cdot 11 = 2310$, $M_1 = 6 \cdot 7 \cdot 11 = 462$, $M_2 = 5 \cdot 7 \cdot 11 = 385$, $M_3 = 5 \cdot 6 \cdot 11 = 330$ e $M_4 = 5 \cdot 6 \cdot 7 = 210$. Continuando, temos a_1 = 2, a_2 = 2, a_3 = 1 e a_4 = 0, temos que a solução geral do problema é dado por:

$$X \equiv M_1b_1a_1 + M_2b_2a_2 + M_3b_3a_3 + M_4b_4a_5 \pmod{M},$$

onde cada b_i é solução de $M_i{\cdot}b_i \equiv 1 \pmod{m_i}, i = 1, 2, 3, 4.$

Como a_4 = 0 precisaremos determinar apenas b_1, b_2 e b_3, onde:

$$\begin{cases} 6 \cdot 7 \cdot 11 \cdot b_1 \equiv 1 \pmod 5 \\ 5 \cdot 7 \cdot 11 \cdot b_2 \equiv 1 \pmod 6 \\ 5 \cdot 6 \cdot 11 \cdot b_3 \equiv 1 \pmod 7 \end{cases}$$

O que equivale ao sistema:

$$\begin{cases} 2 \cdot b_1 \equiv 1 \pmod 5 \\ 1 \cdot b_2 \equiv 1 \pmod 6 \\ 1 \cdot b_3 \equiv 1 \pmod 7 \end{cases}$$

Que possui solução para, b_1 = 3, b_2 = b_3 = 1 e, assim:

$$X \equiv 462 \cdot 3 \cdot 2 + 385 \cdot 1 \cdot 2 + 330 \cdot 1 \cdot 1 \equiv 3872 \pmod{2310}.$$

(c) Temos que X = 3872 + 2310t, com t $\in \mathbb{Z}$. Como 0 < x < 1700, obtemos x = 3872 - 2310 = 1562, tendo assim solução única.

Os conceitos acima descritos nos dão o suporte que desejamos para o melhor entendimento do trabalho proposto a partir de agora. Além de acreditar que essa área da matemática seja de fundamental importância na educação básica.

> A existência de uma Aritmética da rua e uma Aritmética da escola permite verificar um campo de grande tensão e conflito nesse espaço aberto. O que se vê é que os algarismos tratados na escola são da escola e mecanismo que possibilitam fazer as contas nas ruas são das ruas. [...]. Dessa forma, não se pode pensar o ensino de Matemática de acordo com o sistema tradicional de Educação, o mundo é outro, os recursos tecnológicos estão aí, muitos deles inclusive acessíveis. E, um ensino voltado para a repetição e verbalização de conteúdo, é algo que não deve mais pertencer a este tempo. (SANTANA, 2016, p.3)

Destacamos a prática demonstrativa nesta unidade, pois ela tange as habilidades referentes à argumentação matemática, que é de suma importância na prática docente e na utilização das demonstrações matemáticas como uma abordagem metodológica contribuindo tanto no processo de formação acadêmica como na potencialização profissional.

> Resolver situações-problemas, sabendo validar estratégias e resultados, desenvolvendo formas de raciocínio e de processos, como dedução, indução, intuição, analogia, estimativa, e utilizando conceitos e procedimentos matemáticos, bem como instrumentos tecnológicos disponíveis. (BRASIL, 1998, p.48)

Sendo assim, prosseguimos com a proposta do trabalho.

2 ALGUMAS APLICAÇÕES DA ARITMÉTICA

Neste Capítulo, apresentaremos algumas aplicações cotidianas para os conceitos da Aritmética, que vimos no primeiro capítulo. Assim aplicaremos o conteúdo de Aritmética na programação das horas do relógio e na elaboração do calendário Maia. Essas duas aplicações foram adaptadas de (MEDRANO, 2013). Também aplicamos na construção de Chryzodes, adaptado de (BELLO, 2011); na ludicidade do jogo Puzzle (Quebra-cabeças), adaptado de (DELGADO, 2019); no descobrimento da quantidade de números com equações diofantinas lineares, adaptado de (MATHEMATICS; COMPUTING, 2012); e por fim na aplicação do jogo de dardos, conteúdo adaptado de (CHOW, 2009).

2.1 ARITMÉTICA DO RELÓGIO

O tempo é um conceito presente no cotidiano diário de todas a pessoas pois é através do tempo que nos organizamos nas tarefas do dia-a-dia. Ou seja, vivemos correndo contra o tempo, cada vez com mais tarefas a serem realizadas e com menos tempo para as realizar. E um dos aparelhos usado para medir o tempo é o relógio analógico que serve para indicar horas, minutos e segundos.

Figura 4 – Relógio Analógico

Fonte: O autor

Sabendo dessa importância iremos relacionar o conceito de congruência com o relógio analógico. Por exemplo, 15 é congruente com 3 módulo 12 (15 = 12 + 3), ao qual representamos do seguinte modo:

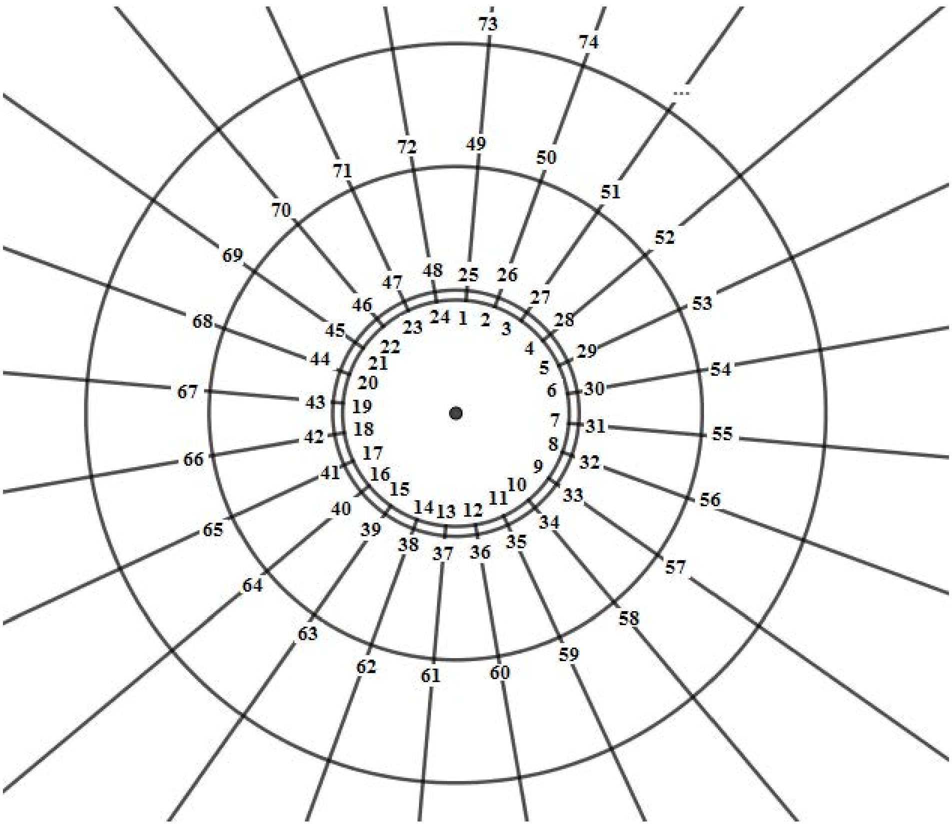
$$15 \equiv 3 \pmod{12}.$$

Se pensarmos no dia como 24 horas poderemos fazer módulo 24. Por exemplo, 74 é congruente com 2 módulo 24 (74 = 24 + 24 + 24 + 2), ao qual representamos:

$$74 \equiv 2 \pmod{24}.$$

Podemos usar a Figura 5 para entender a aritmética do relógio. Observe que ela nos ajuda a enxergar quais números têm a mesma posição no relógio. Por exemplo: 26, 50 e 74 possuem a mesma posição no relógio de 24 horas.

Figura 5 – Exemplo de relógio analógico de 24 horas com a sua continuação



Fonte: O autor

Se pensarmos nos dias da semana, faremos módulo 7; dias do mês comercial, faremos módulo 30; dias do ano comercial, faremos módulo 360. Esses são alguns exemplos de "aritmética módulo n". Abordaremos somente a aritmética com o relógio módulo 12, devido aos outros exemplos serem resolvidos de maneira análoga. Denominaremos este estudo de "Aritmética do Relógio".

Vamos verificar algumas situações interessantes que acontecem na aritmética do relógio, ou seja, as congruências módulo doze. Se forem 5 horas e tiver decorrido 9 horas, então o relógio marcará 2 horas ($5 + 9 \equiv 2 \pmod{12}$). Isso significa que cada vez que passam 12 horas começamos a contagem novamente.

De fato, em um relógio analógico há apenas 12 horas, então basta usar os números 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 e 11 para informar as horas. Assim o 12 passa a ser o 0, o 13 passa a ser o 1, e assim sucessivamente. Ao qual representamos da forma de congruências:

$$12 \equiv 0 \pmod{12}, 13 \equiv 1 \pmod{12}, 14 \equiv 2 \pmod{12}, \dots$$

Generalizado, diremos que dois números inteiros **a** e **b** são congruentes módulo 12, e escreveremos da seguinte forma

$$a \equiv b \pmod{12}.$$

Na aritmética do relógio podemos somar, subtrair e multiplicar os números (horas). Em alguns casos podemos até mesmo dividir os números (horas). Em todas as operações vamos considerar **a**, **b** e **c** $\in \mathbb{Z}$ e **c** compreendido entre 0 e 11.

Adição: Se $a + b = 12q + c$, para algum $q \in \mathbb{Z}$, então $(a + b) \equiv c \pmod{12}$. Assim, para somar 8 e 10 horas, começaremos em zero hora, em seguida avançamos 8 horas e depois as outras 10 horas. Isto é 8 + 10 = 18 = 12 + 6, logo o resultado é 6.

$$(8 + 10) \equiv 6 \pmod{12}.$$

Subtração: Possui a seguinte propriedade $(a - b) \equiv c \pmod{12}$. Assim para subtrair 7 e 9 horas, começaremos em zero horas, em seguida avançamos 7 horas, para logo depois atrasar 9 horas. Isto dará 7 - 9 = -2 = 10 - 12, logo o resultado é 10.

$$(7 - 9) \equiv -2 \equiv 10 \pmod{12}.$$

Podemos dizer que o sinal negativo significa que devemos atrasar o relógio.

Multiplicação: Possui a seguinte propriedade $(a \cdot b) \equiv c \pmod{12}$. A multiplicação é uma soma repetida várias vezes, então sabendo somar, você também sabe como multiplicar na aritmética do relógio. Se você quiser calcular, na aritmética do relógio 7 · 14, você pode primeiro fazer a multiplicação 7 · 14 = 98, e pelo Teorema 1.12, temos que 98 = 12 · 8 + 2. Que é o mesmo que dar 8 voltas no sentido horário, parando no zero e em seguida avançar as 2 horas restantes. Assim:

$$(7 \cdot 14) \equiv 2 \pmod{12}.$$

Também podemos resolver da seguinte forma:

$$(7 \cdot 14) \equiv 7 \cdot (12 + 2) \equiv (7 \cdot 12) + (7 \cdot 2) \pmod{12}.$$

Como dar 7 voltas completas no relógio é o mesmo que não avançar nenhuma hora, temos que:

$$(7 \cdot 14) \equiv (7 \cdot 2) \pmod{12}.$$

Assim,

$$(7 \cdot 2) \equiv 14 \equiv (1 \cdot 12) + 2 \equiv 2 \pmod{12}.$$

Divisão: Se $(b, 12) = 1$, então pela Observação 1.77 temos que $c \cdot b^{-1} \equiv a \pmod{12}$. Assim, sendo a divisão a operação inversa da multiplicação e considerando o valor de $5 \div 7$ na aritmética do relógio, o que queremos fazer é encontrar o número **c**, compreendido entre 0 e 11, tal que

$$(c \cdot 7) \equiv 5 \pmod{12}.$$

Uma maneira de resolvermos essa congruência é resolver os 12 possíveis valores de **c**, observe:

$$(0 \cdot 7) \equiv 0 \pmod{12};$$

$$(1 \cdot 7) \equiv 7 \pmod{12};$$

$$(2 \cdot 7) \equiv 14 \equiv 2 \pmod{12};$$

$$(3 \cdot 7) \equiv 21 \equiv 9 \pmod{12};$$

$$(4 \cdot 7) \equiv 28 \equiv 4 \pmod{12};$$

$$(5 \cdot 7) \equiv 35 \equiv 11 \pmod{12};$$

$$(6 \cdot 7) \equiv 42 \equiv 6 \pmod{12};$$

$$(7 \cdot 7) \equiv 49 \equiv 1 \pmod{12};$$

$$(8 \cdot 7) \equiv 56 \equiv 8 \pmod{12};$$

$$(9 \cdot 7) \equiv 63 \equiv 3 \pmod{12};$$

$$(10 \cdot 7) \equiv 70 \equiv 10 \pmod{12};$$

$$(11 \cdot 7) \equiv 77 \equiv 5 \pmod{12};$$

Assim, percebemos que **c** é igual a 11.

Outra forma de resolvermos a congruência

$$(c \cdot 7) \equiv 5 \pmod{12}$$

é através da Definição 1.73, Congruência Linear.

Assim seja:

$$(c \cdot 7) \equiv 5 \pmod{12} \Leftrightarrow 7X - 12Y = 5$$

Como (7,12) = 1 e 1 | 5, então a equação admite solução. Vamos achar uma solução particular x_0, $y_0 \in \mathbb{Z}$ desta equação. Assim, pelo Algoritmo de Euclides, temos:

	1	1	2	2
12	7	5	2	1
5	2	1	0	

De onde temos:
5 = 12 - 7 · 1
2 = 7 - 5 · 1
1 = 5 - 2 · 2

Substituindo as equações acima uma nas outras, obtemos:

1 = 3 · 12 - 5 · 7,

portanto, multiplicando por 5, temos:

5 = 15 · 12 - 25 · 7.

Logo, x_0 = -25 e y_0 = -15 é solução particular da equações, consequentemente, as soluções são:

$$\begin{cases} X = -25 - 12t \\ Y = -15 - 7t \end{cases}$$

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

Como **c** está compreendido entre 0 e 11, então **X** está compreendido entre 0 e 11, logo:

Se t = -1, então X = -13;
Se t = -2, então X = -1;
Se t = -3, então X = 11.

Logo **c** é igual a 11.

2.2 CALENDÁRIO MAIA

O calendário consiste em um conjunto de unidades de tempo, como dias, meses e anos. Através dessas unidades podemos dividir o ano em quatro estações (Outono, Inverno, Primavera e Verão). De uma maneira geral podemos dizer que o calendário teve origem da necessidade de medir e registrar eventos ao longo de pequenos e grandes períodos.

Segundo alguns especialistas o calendário teve origem com os sumérios - povo da Mesopotâmia - em 2700 a.C.. Abaixo adaptamos de (NETWORKS, 2000) um pouco da história de alguns calendários, que introduzirá a nossa proposta de aplicação de congruências no calendário, mais especificamente no Calendário Maia. Visto que os outros calendários já foram objeto de estudo em outras dissertações de mestrado deste mesmo programa.

Calendário Solar: Esse calendário foi criado pelos egípcios e possui 12 meses de 30 dias cada, ou seja um total de 360 dias por ano acrecidos de mais 5 dias no final do ano, isso para trazê-lo mais de acordo com o ano solar. Não havia ano bissexto pois em vez de ter um único dia bissexto a cada quatro anos para dar conta do dia fracionado (como fazemos agora), eles deixavam acumular o dia e depois de 1460 anos solares, ou quatro períodos de 365 anos, tinham passado na verdade 1461 anos egípcios. Isto significa que, como o passar dos anos, os meses egípcios caiam fora de sincronia com as estações do ano, de modo que os meses do verão, eventualmente, caiam durante o inverno. Assim, somente a cada 1460 anos o seu calendário coincide precisamente com o ano solar.

Figura 6 – Calendário Solar

Fonte: (EUGENESERGEEV, 2012)

Calendário Romano ou Juliano: Quando Roma emergiu como uma potência mundial, as dificuldades de fazer um calendário eram bem conhecidas, mas os romanos complicaram suas vidas por causa de sua superstição de que até os números eram infelizes. Assim, seus meses foram de 29 ou 31 dias, com exceção de fevereiro, que teve 28 dias. No entanto, quatro meses de 31 dias, sete meses de 29 dias e um mês de 28 dias somaram apenas 355 dias. Por isso, os romanos inventaram um mês extra chamado "Mercedonius"de 22 ou 23 dias. Ao qual foi adicionado a cada dois anos.

Aconselhado pelo astrônomo Sosigenes, Júlio César ordenou no ano de 46 a.C. uma reforma radical no calendário, foi refeito com 445 dias por decreto imperial, trazendo o calendário de volta em sintonia com as estações do ano. Então o ano solar (com o valor de 365 dias e 6 horas) foi feito a base do calendário. Os meses tinham 30 ou 31 dias de duração, e para cuidar das 6 horas, a cada quatro anos era feito um ano de 366 dias. Além disso, César decretou que o ano começasse no dia primeiro de janeiro, e não mais no final de março.

Este calendário foi nomeado como Calendário Juliano, depois de Júlio César, e continua a ser usado por igrejas ortodoxas orientais para cálculos de feriados. No entanto, apesar da correção, o Calendário Juliano ainda é 111/2 minutos a mais que o ano solar.

Calendário Cristão ou Gregoriano: No século XV, o calendário Juliano havia se atrasado em torno de uma semana em relação ao calendário solar, de modo que o equinócio vernal caía por volta de 12 de março, em vez de 20 de março. O Papa Sisto IV (que reinou de 1471 a 1484) decidiu que outra reforma era necessário e chamou o astrônomo alemão Regiomontanus a Roma para aconselhá-lo. Regiomontanus chegou em 1475, mas infelizmente ele morreu pouco depois, e os planos do Papa para a reforma morreram com ele.

Então, em 1545, o Concílio de Trento autorizou o papa Paulo III a reformar o calendário mais uma vez. A maior parte do trabalho matemático e astronômico foi feito pelo Padre Christopher Clavius, S.J. A correção imediata, aconselhada pelo padre Clávio e ordenada pelo papa Gregório XIII(por esse motivo também é conhecido como calendário gregoriano), era que a quinta-feira, 4 de outubro de 1582, seria o último dia do Calendário Juliano. O dia seguinte seria sexta-feira, 15 de outubro. Para uma precisão de longo alcance, uma fórmula sugerida pelo bibliotecário do Vaticano Aloysius Giglio foi adotada: o ano ao qual é acrescentado um dia extra, ficando ele com 366 dias, um dia a mais do que os anos normais de 365 dias, ocorrendo a cada quatro anos (exceto anos múltiplos de 100 que não são múltiplos de 400). Essa regra elimina três anos bissextos em quatro séculos, tornando o calendário suficientemente preciso.

A contagem dos anos deveria ser iniciada por um acontecimento de grande valor, de modo que, como cristãos foi considerado que o ano 1 deveria ser o ano do nascimento de Jesus

Figura 7 – Calendário Juliano para o Gregoriano

Fonte: (AMILMIUQ, 2013)

Cristo. Esse é o calendário usado atualmente no Brasil e em grande parte do mundo.

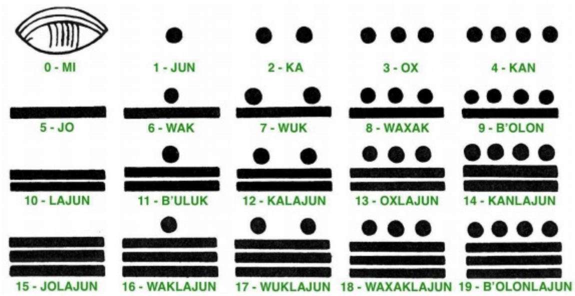
Mas estes calendários, já foram estudadas em outras dissertações de mestrado do PROFMAT. Assim, vamos inovar os estudos e aplicar os conteúdos de aritmética, mais precisamente o Teorema Chinês dos Resto no Calendário Maia.

Calendário Maia: É composto por dois calendários: o Haab, que é o calendário civil, e o Tzolk'in, que é o calendário sagrado, ou calendário religioso. Enquanto o Haab conta com 365 dias divididos entre 18 meses com 20 dias cada um, num total de 360 (5 dias não pertencem a mês algum), o Tzolk'in conta com 260 dias divididos em treze períodos de 20 dias cada um, em que cada dia é contado de 1 a 13.

O sistema matemático Maia é formado por 20 dígitos, de 0 a 19. Por isso, é de base vigesimal. Os dígitos maias são representados a partir de um sistema de ponto e barra, em que um ponto representa uma unidade, e uma barra significa cinco unidades. Assim, o número 4 é representado por quatro pontos ($4 \cdot 1$), enquanto o número 17 é representado por três barras e dois pontos ($3 \cdot 5 + 2$).

Na figura 8, é possível ver a representação dígitos Maias, acompanhados pelos seus nomes em língua maia *Yukateka*.

Figura 8 – Representação dos 20 dígitos maias



Fonte: (CAVALCANTI, 2014, p.52)

> É importante começar a falar do calendário de 260 dias [...], uma vez recorrido o percurso "clássico" de introdução à matemática e sua aplicação calendárica mais objetiva, a conta longa. A ilustração de que números também são pessoas (sejam humanas ou não-humanas) para xs maias é fundamental para compreender a própria matemática do tempo maia e mesoamericana, seja – por exemplo – aquela dxs maias clássicxs, dxs mexicas ou dxs maias de hoje.(CAVALCANTI, 2014, p.64 e 65)

Figura 9 – Glifos dos 20 dias do Tzolk'in

Fonte: (CAVALCANTI, 2014, p.64)

> O calendário de 260 dias deve ser entendido como oriundo de permutações ou intersecções entre dois ciclos distintos: precisamente os de 13 e de 20 dias. Há pouco, viu-se que estes (mais o zero) têm centralidade na cosmovisão maia, e é exatamente no Tzolk'in que isto se demonstra com maior força.[...]
> Diga-se que os 20 glifos aqui expostos são também vinte faces, rostos, identidades dos dias. E que cada um dos 260 dias têm uma identidade específica que, por sua vez, combina um dos 13 números com um dos 20 glifos. Como 260 é o mínimo múltiplo comum (doravante MMC) entre os dois ciclos, esta é uma razão matemática para sua duração.(CAVALCANTI, 2014, p.65)

A Figura 10 mostra a sequência dos 260 dias do Tzolk'in, contada com o início em 1 Imix.

Figura 10 – Os 260 dias do Tzolk'in

Dia 1 1 Imix	Dia 27 1 Manik'	Dia 53 1 B'en	Dia 79 1 Kawak	Dia 105 1 Chikchan	Dia 131 1 Chuwen	Dia 157 1 Kab'an	Dia 183 1 Akb'al	Dia 209 1 Muluk	Dia 235 1 Men
Dia 2 2 Ik'	Dia 28 2 Lamat	Dia 54 2 Ix	Dia 80 2 Ajaw	Dia 106 2 Kimi	Dia 132 2 Eb'	Dia 158 2 Etz'nab'	Dia 184 2 K'an	Dia 210 2 Ok	Dia 236 2 Kib'
Dia 3 3 Akb'al	Dia 29 3 Muluk	Dia 55 3 Men	Dia 81 3 Imix	Dia 107 3 Manik'	Dia 133 3 B'en	Dia 159 3 Kawak	Dia 185 3 Chikchan	Dia 211 3 Chuwen	Dia 237 3 Kab'an
Dia 4 4 K'an	Dia 30 4 Ok	Dia 56 4 Kib'	Dia 82 4 Ik'	Dia 108 4 Lamat	Dia 134 4 Ix	Dia 160 4 Ajaw	Dia 186 4 Kimi	Dia 212 4 Eb'	Dia 238 4 Etz'nab'
Dia 5 5 Chikchan	Dia 31 5 Chuwen	Dia 57 5 Kab'an	Dia 83 5 Akb'al	Dia 109 5 Muluk	Dia 135 5 Men	Dia 161 5 Imix	Dia 187 5 Manik'	Dia 213 5 B'en	Dia 239 5 Kawak
Dia 6 6 Kimi	Dia 32 6 Eb'	Dia 58 6 Etz'nab'	Dia 84 6 K'an	Dia 110 6 Ok	Dia 136 6 Kib'	Dia 162 6 Ik'	Dia 188 6 Lamat	Dia 214 6 Ix	Dia 240 6 Ajaw
Dia 7 7 Manik'	Dia 33 7 B'en	Dia 59 7 Kawak	Dia 85 7 Chikchan	Dia 111 7 Chuwen	Dia 137 7 Kab'an	Dia 163 7 Akb'al	Dia 189 7 Muluk	Dia 215 7 Men	Dia 241 7 Imix
Dia 8 8 Lamat	Dia 34 8 Ix	Dia 60 8 Ajaw	Dia 86 8 Kimi	Dia 112 8 Eb'	Dia 138 8 Etz'nab'	Dia 164 8 K'an	Dia 190 8 Ok	Dia 216 8 Kib'	Dia 242 8 Ik'
Dia 9 9 Muluk	Dia 35 9 Men	Dia 61 9 Imix	Dia 87 9 Manik'	Dia 113 9 B'en	Dia 139 9 Kawak	Dia 165 9 Chikchan	Dia 191 9 Chuwen	Dia 217 9 Kab'an	Dia 243 9 Akb'al
Dia 10 10 Ok	Dia 36 10 Kib'	Dia 62 10 Ik'	Dia 88 10 Lamat	Dia 114 10 Ix	Dia 140 10 Ajaw	Dia 166 10 Kimi	Dia 192 10 Eb'	Dia 218 10 Etz'nab'	Dia 244 10 K'an
Dia 11 11 Chuwen	Dia 37 11 Kab'an	Dia 63 11 Akb'al	Dia 89 11 Muluk	Dia 115 11 Men	Dia 141 11 Imix	Dia 167 11 Manik'	Dia 193 11 B'en	Dia 219 11 Kawak	Dia 245 11 Chikchan
Dia 12 12 Eb'	Dia 38 12 Etz'nab'	Dia 64 12 K'an	Dia 90 12 Ok	Dia 116 12 Kib'	Dia 142 12 Ik'	Dia 168 12 Lamat	Dia 194 12 Ix	Dia 220 12 Ajaw	Dia 246 12 Kimi
Dia 13 13 B'en	Dia 39 13 Kawak	Dia 65 13 Chikchan	Dia 91 13 Chuwen	Dia 117 13 Kab'an	Dia 143 13 Akb'al	Dia 169 13 Muluk	Dia 195 13 Men	Dia 221 13 Imix	Dia 247 13 Manik'
Dia 14 1 Ix	Dia 40 1 Ajaw	Dia 66 1 Kimi	Dia 92 1 Eb'	Dia 118 1 Etz'nab'	Dia 144 1 K'an	Dia 170 1 Ok	Dia 196 1 Kib'	Dia 222 1 Ik'	Dia 248 1 Lamat
Dia 15 2 Men	Dia 41 2 Imix	Dia 67 2 Manik'	Dia 93 2 B'en	Dia 119 2 Kawak	Dia 145 2 Chikchan	Dia 171 2 Chuwen	Dia 197 2 Kab'an	Dia 223 2 Akb'al	Dia 249 2 Muluk
Dia 16 3 Kib'	Dia 42 3 Ik'	Dia 68 3 Lamat	Dia 94 3 Ix	Dia 120 3 Ajaw	Dia 146 3 Kimi	Dia 172 3 Eb'	Dia 198 3 Etz'nab'	Dia 224 3 K'an	Dia 250 3 Ok
Dia 17 4 Kab'an	Dia 43 4 Akb'al	Dia 69 4 Muluk	Dia 95 4 Men	Dia 121 4 Imix	Dia 147 4 Manik'	Dia 173 4 B'en	Dia 199 4 Kawak	Dia 225 4 Chikchan	Dia 251 4 Chuwen
Dia 18 5 Etz'nab'	Dia 44 5 K'an	Dia 70 5 Ok	Dia 96 5 Kib'	Dia 122 5 Ik'	Dia 148 5 Lamat	Dia 174 5 Ix	Dia 200 5 Ajaw	Dia 226 5 Kimi	Dia 252 5 Eb'
Dia 19 6 Kawak	Dia 45 6 Chikchan	Dia 71 6 Chuwen	Dia 97 6 Kab'an	Dia 123 6 Akb'al	Dia 149 6 Muluk	Dia 175 6 Men	Dia 201 6 Imix	Dia 227 6 Manik'	Dia 253 6 B'en
Dia 20 7 Ajaw	Dia 46 7 Kimi	Dia 72 7 Eb'	Dia 98 7 Etz'nab'	Dia 124 7 K'an	Dia 150 7 Ok	Dia 176 7 Kib'	Dia 202 7 Ik'	Dia 228 7 Lamat	Dia 254 7 Ix
Dia 21 8 Imix	Dia 47 8 Manik'	Dia 73 8 B'en	Dia 99 8 Kawak	Dia 125 8 Chikchan	Dia 151 8 Chuwen	Dia 177 8 Kab'an	Dia 203 8 Akb'al	Dia 229 8 Muluk	Dia 255 8 Men
Dia 22 9 Ik'	Dia 48 9 Lamat	Dia 74 9 Ix	Dia 100 9 Ajaw	Dia 126 9 Kimi	Dia 152 9 Eb'	Dia 178 9 Etz'nab'	Dia 204 9 K'an	Dia 230 9 Ok	Dia 256 9 Kib'
Dia 23 10 Akb'al	Dia 49 10 Muluk	Dia 75 10 Men	Dia 101 10 Imix	Dia 127 10 Manik'	Dia 153 10 B'en	Dia 179 10 Kawak	Dia 205 10 Chikchan	Dia 231 10 Chuwen	Dia 257 10 Kab'an
Dia 24 11 K'an	Dia 50 11 Ok	Dia 76 11 Kib'	Dia 102 11 Ik'	Dia 128 11 Lamat	Dia 154 11 Ix	Dia 180 11 Ajaw	Dia 206 11 Kimi	Dia 232 11 Eb'	Dia 258 11 Etz'nab'
Dia 25 12 Chikchan	Dia 51 12 Chuwen	Dia 77 12 Kab'an	Dia 103 12 Akb'al	Dia 129 12 Muluk	Dia 155 12 Men	Dia 181 12 Imix	Dia 207 12 Manik'	Dia 233 12 B'en	Dia 259 12 Kawak
Dia 26 13 Kimi	Dia 52 13 Eb'	Dia 78 13 Etz'nab'	Dia 104 13 K'an	Dia 130 13 Ok	Dia 156 13 Kib'	Dia 182 13 Ik'	Dia 208 13 Lamat	Dia 234 13 Ix	Dia 260 13 Ajaw

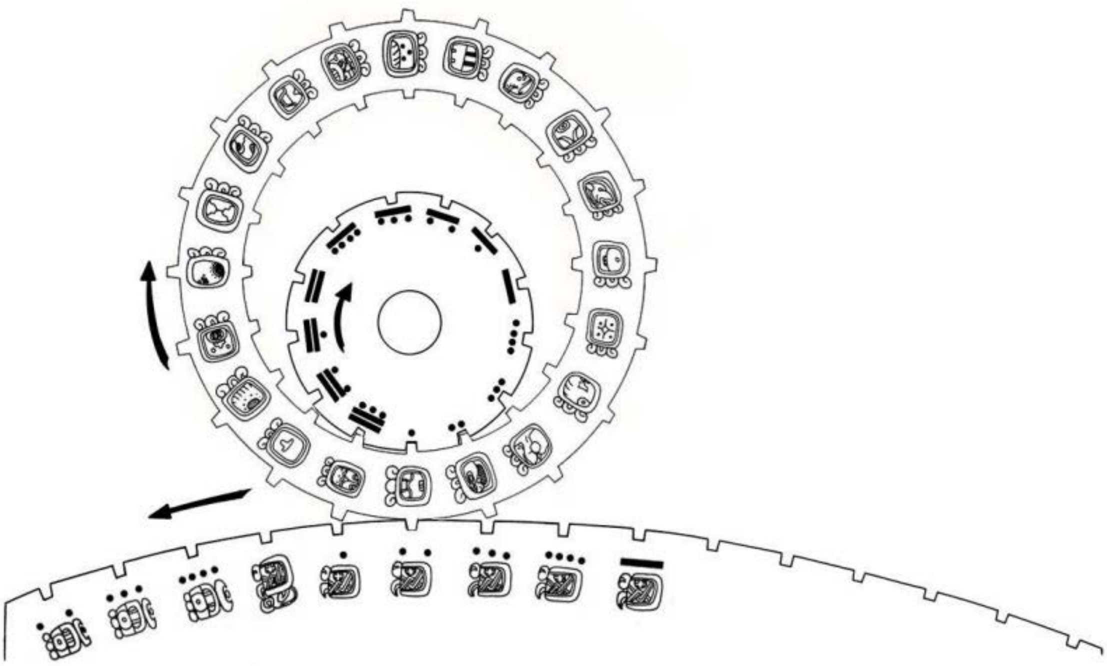
Fonte: (CAVALCANTI, 2014, p. 68)

É preciso observar, aqui, uma dinâmica da matemática mesoamericana do tempo: todos os ciclos sempre estão correndo paralelamente. Dito de outra forma, o dia de hoje não é apenas um dia no Tzolk'in, mas também um dia no Ja'ab', na conta longa e em todas as outras contas calendáricas. Por conseguinte, também todos os ciclos "encontram-se" em alguma altura, o que é constatado mais sistematicamente a partir da marcação de pontos de partida específicos (e aqui se dá uma forma de marcação da diferença a partir do calendário).

No caso do Junab', isto significa dizer que sua duração, 18.980 dias, é na verdade o MMC entre 260 e 365. Constatei, anteriormente, que a própria razão matemática para o Tzolk'in ter 260 dias está no fato de que ele é efetivamente o MMC entre 13 e 20. Assim, posso concluir que a observação do MMC entre dois ciclos é uma prática antiga que remonta aos tempos de oralidade primária e que contribuiu para a posterior construção do registro infinito – e escrito

> – do tempo. Cada novo ciclo engendrado a partir da combinação de ciclos menores gera um ciclo maior, e este ciclo maior por sua vez é sempre passível de ser combinado com outros ciclos (sejam previamente oriundos ou não do MMC entre dois ou mais ciclos), tornando impossível definir o "maior ciclo mesoamericano".
> O ciclo de 52 anos faz coincidir os calendários de 260 e 365 dias a partir da marcação de uma data específica, composta pelo encontro entre um determinado dia entre os 260 e outro dia oriundo dos 365. Entretanto, é preciso compreender de que maneira isto ocorre e qual é o significado do Junab'. Por isso, vou adentrar aspectos da relação entre os dois calendários. Para efeito de ilustração, a interação entre o Tzolk'in e o Ja'ab' é mostrada a partir de rodas dentadas na Figura 11.
> Assim, entende-se ainda melhor que o primeiro dia de cada ano no Ja'ab' sempre equivalerá a um dos 260 dias do Tzolk'in, uma vez que os ciclos correm paralelamente. No contexto das sociedades mesoamericanas que combinaram o uso dos calendários de 260 e 365 dias, o dia da conta ritual torna-se algo além de um dia que apenas acompanha e compõe a data, tornando-se um dia que simbolicamente pode influenciar todo o ano de 365 dias em questão, ou parte dele. (CAVALCANTI, 2014, p. 80)

Figura 11 – Roda calendárica mostrando a interação entre o Tzolk'in (com as duas rodas menores, uma dos 20 glifos e a interna de 13 números) e o Ja'ab'. O dia aqui ilustrado é 1 K'an 2 Pop, terceiro dia de um ano 12 Ik'.



Fonte: (CAVALCANTI, 2014, p. 80)

Observando a Figura 11 percebemos que a roda maior aparecem os 20 dias que correspondem ao calendário Tzolk'in e na roda pequena que está dentro do interior aparecem números de um a treze (escrita Maia). Na figura aparece no primeiro dia do calendário correspondente ao primeiro Imix , no segundo dia as duas rodas giram na mesma direção, no sentido horário, então o segundo dia é o segundo de Ik'. Ou seja, para cada dia seguinte, o dia e o mês mudam.

Um problema que surge no calendário Tzolk'in seria: **Quantos dias se passaram desde o 7 MANIK' até o 5 KIMI?** Em geral, devemos encontrar o número de dias **x** desde Tzolk'in (d, p), onde 1 < d < 20 e 1 < p < 13 para Tzolk'in (d',p'), onde 1 < d'< 20 e 1 < p'< 13, sendo p e p' os períodos e d e d' os dias.

Devido ao comportamento cíclico dos períodos, o problema pode ser colocado como uma congruência do tipo:

$$x \equiv (p' - p) \pmod{13}.$$

E devido ao comportamento cíclico dos dias, a congruência pode ser escrita:

$$x \equiv (d' - d) \pmod{20}.$$

Para responder à pergunta, devemos ter em mente que no 7º dia MANIK é o casal (7,7) e no 5º dia o KIMI é representado como o casal (6,5), assim podemos escrever as congruências:

$$\begin{cases} x \equiv -2 \pmod{13} \\ x \equiv -1 \pmod{20} \end{cases}$$

Como (13,20) = 1, podemos resolver a congruência pelo Teorema Chinês dos Restos. Que neste caso temos que M = 13 x 20 = 260, M_1 = 20 e M_2 = 13. Por outro lado y_1 = 2 e y_2 = 17 são soluções, respectivamente, das congruências $20y_1 \equiv 1 \pmod{13}$ e $13y_2 \equiv 1 \pmod{20}$, logo:

$$x = 20 \cdot 2 \cdot (-2) + 13 \cdot 17 \cdot (-1) + 260t, t \in \mathbb{Z}.$$

Do qual obtemos:

$$x = 219 + 260t, t \in \mathbb{Z}.$$

O que responde a pergunta, pois quer dizer que entre o sétimo dia MANIK' e quinto dia KIMI, transcorrem 219 dias.

2.3 CHRYZODES

A palavra Chryzode deriva do grego "Chrysos"(escrito em ouro) e "zooide"(círculo), ou seja, escrita de ouro em um círculo e são as representações geométricas e gráficas de números e operações aritméticas modulares por meio de um círculo dividido em arcos iguais. Tal representação permite dar uma visão alternativa (fato artístico) às classes de congruências e às operações entre elas.

Assim uma maneira de construirmos um Chryzode é dividir uma circunferência em *m* pontos equidistantes, ordenados e numerados de 0 a $m - 1$. Feito isto, escolhemos um número natural *a*, que multiplicará a sequência de números 1, 2, 3, 4, 5, $\cdots$, *m*-1. Em seguida, resolvemos as congruências módulo *m* para essa sequência de números. Por fim, para obter o Chryzode, basta ligar a sequência de números 1, 2, 3, 4, 5, $\cdots$, *m*-1 com o resultado de seu módulo. Ou seja:

$$\begin{aligned}
a \cdot 1 &\equiv b_1 \pmod{m};\\
a \cdot 2 &\equiv b_2 \pmod{m};\\
a \cdot 3 &\equiv b_3 \pmod{m};\\
&\vdots\\
a \cdot (m-2) &\equiv b_{m-2} \pmod{m};\\
a \cdot (m-1) &\equiv b_{m-1} \pmod{m}.
\end{aligned}$$

De maneira simplificada,

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

para i = 1, 2, $\cdots$, $m-1$.

Resolvendo as congruências e ligando os pontos 1 com b_1, 2 com b_2, 3 com b_3, e assim sucessivamente, teremos um conjunto de linhas desenhadas no círculo inicial, do qual forma o Chryzode.

Então o Chryzode pode ser representado desenhando as linhas, ou (quando o número de linhas for muito grande), plotando com um computador apenas os pontos de intersecção entre as linhas (para essa finalidade podemos utilizar o *software* Chryzodus, disponível em: <https://chryzodus-a-chryzode-explorer.soft112.com/>). Assim podemos desenhar diferentes Chryzodes, para isso basta variar o valor de *a* e de *m*.

Através de um exemplo vamos criar um Chryzode, utilizando a explicação acima.

Exemplo 2.1. Vamos desenhar o Chryzode representando a multiplicação por 2 no módulo 11.

Assim, temos que *a* = 2 e *m* = 11. Logo:

$$\begin{aligned}
2 \cdot 1 &\equiv 2 \pmod{11};\\
2 \cdot 2 &\equiv 4 \pmod{11};\\
2 \cdot 3 &\equiv 6 \pmod{11};\\
2 \cdot 4 &\equiv 8 \pmod{11};
\end{aligned}$$

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

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

$$2 \cdot 7 \equiv 14 \equiv 3 \pmod{11};$$

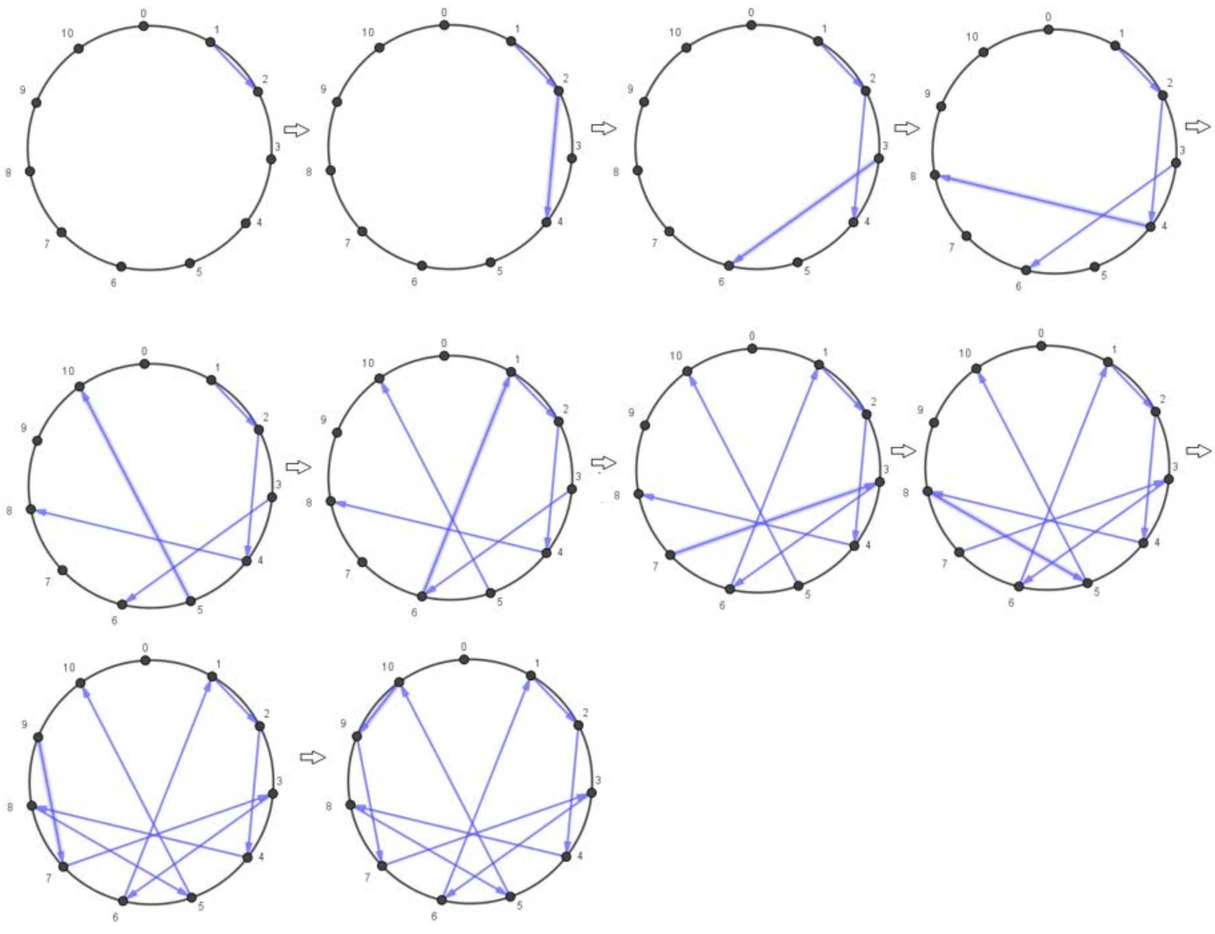
$$2 \cdot 8 \equiv 16 \equiv 5 \pmod{11};$$

$$2 \cdot 9 \equiv 18 \equiv 7 \pmod{11};$$

$$2 \cdot 10 \equiv 20 \equiv 9 \pmod{11}.$$

Por outro lado, desenhamos uma linha de cada número da sequência 1, 2, 3, 4, 5, $\cdots$, m-1 com o seu módulo, ou seja uma linha de 1 à 2, de 2 à 4, de 3 à 6, de 4 à 8, de 5 à 10, de 6 à 1, de 7 à 3, de 8 à 5, de 9 à 7 e de 10 à 9. O resultado da construção do Chryzode é mostrado na figura 12.

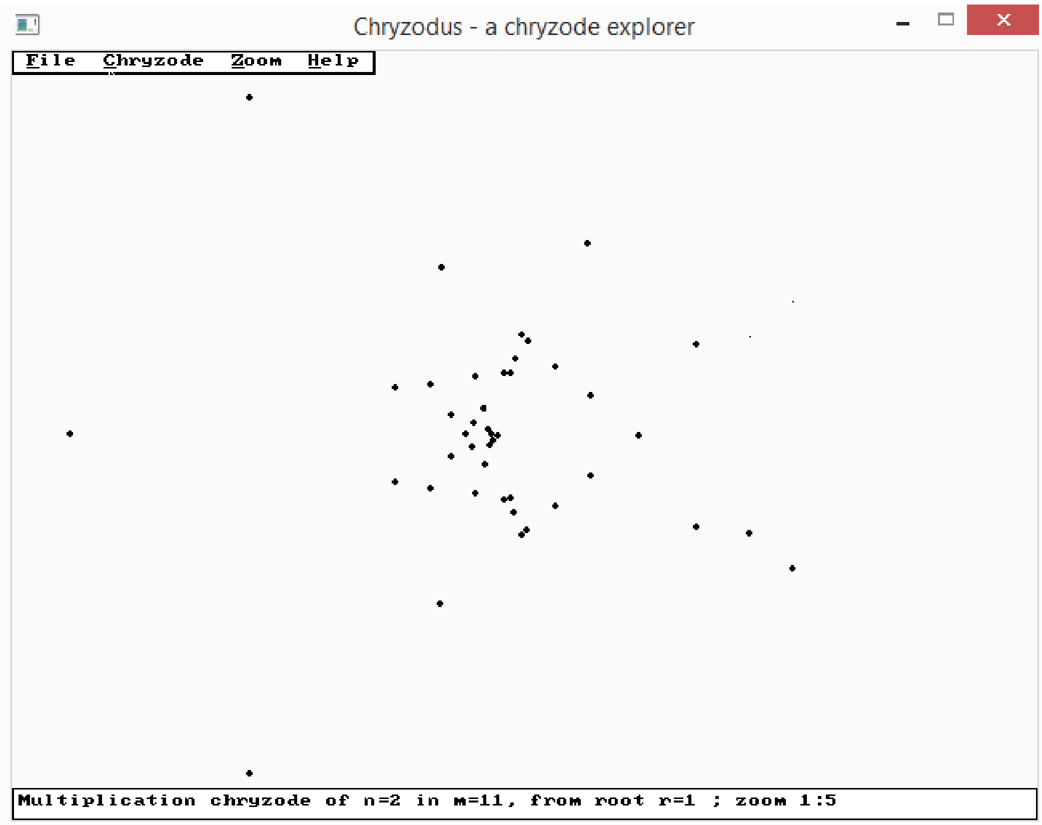
Figura 12 – Chryzode, produto por 2 no módulo 11, em linha.



Fonte: O autor

No *software* Chryzodus, obtemos o resultado conforme a figura 13.

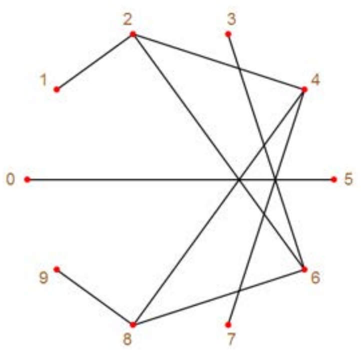
Figura 13 – Pontos de interseção das linhas do Chryzode, produto por 2 no módulo 11 obtido pelo *software* Chryzodus



Fonte: O autor

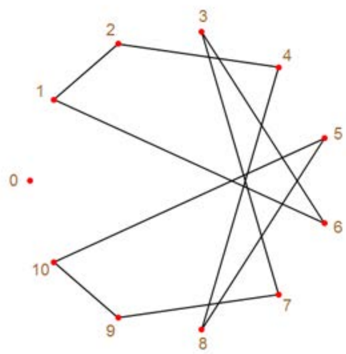
Para uma melhor visualização vamos "esconder"a circunferência e variar o valor de *m* (do módulo). Assim teremos os Chryzodes para módulo 10, 11, 12, 13, 14, 15, 20, 30, 40, 50 e 70. Conforme podemos visualizar nas figuras 14 à 24.

Figura 14 – Chryzode, produto por 2 no módulo 10



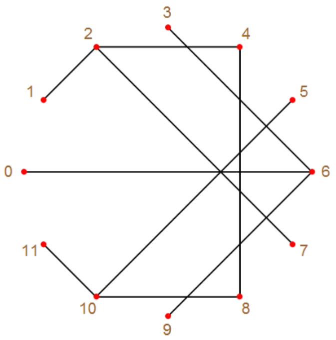
Fonte: O autor

Figura 15 – Chryzode, produto por 2 no módulo 11



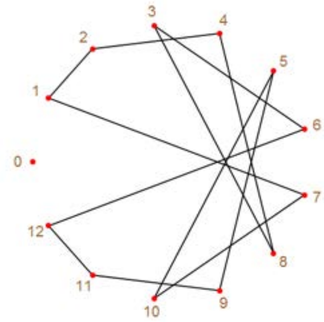
Fonte: O autor

Figura 16 – Chryzode, produto por 2 no módulo 12



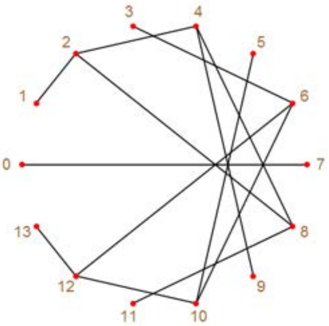
Fonte: O autor

Figura 17 – Chryzode, produto por 2 no módulo 13



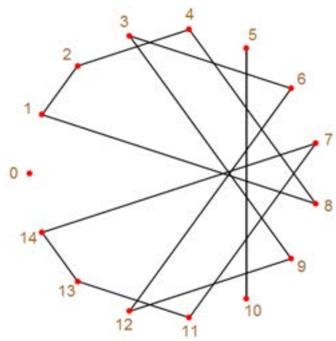
Fonte: O autor

Figura 18 – Chryzode, produto por 2 no módulo 14



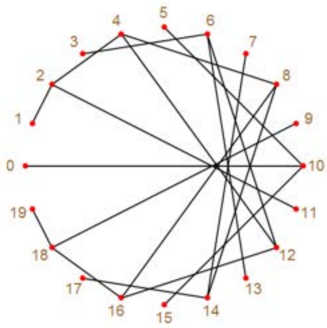
Fonte: O autor

Figura 19 – Chryzode, produto por 2 no módulo 15



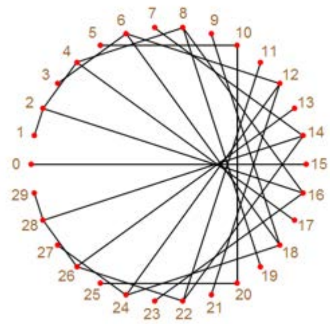
Fonte: O autor

Figura 20 – Chryzode, produto por 2 no módulo 20



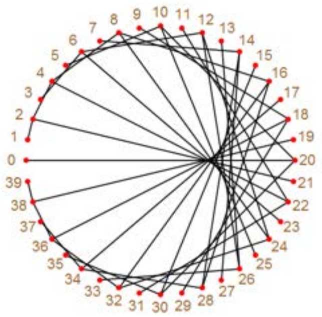
Fonte: O autor

Figura 21 – Chryzode, produto por 2 no módulo 30



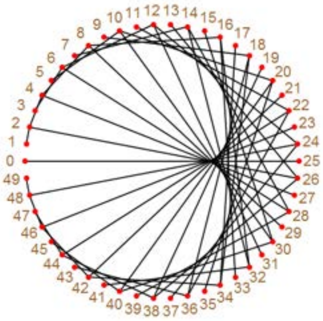
Fonte: O autor

Figura 22 – Chryzode, produto por 2 no módulo 40



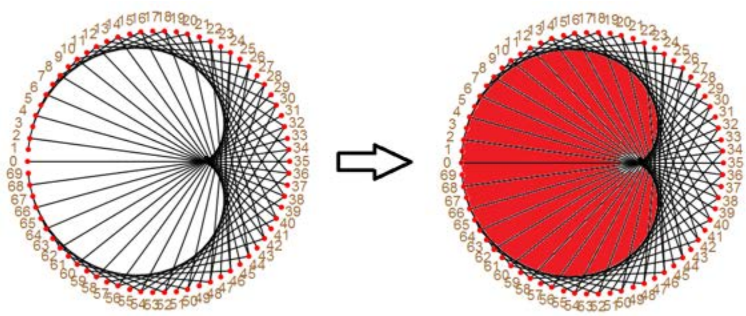
Fonte: O autor

Figura 23 – Chryzode, produto por 2 no módulo 50



Fonte: O autor

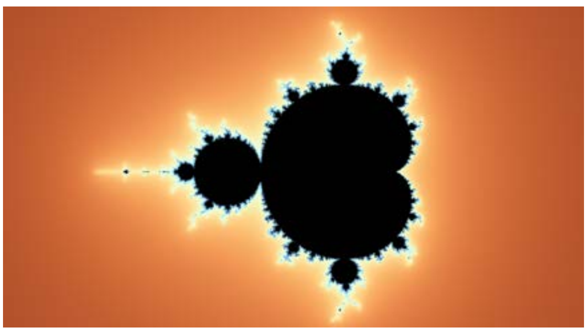
Figura 24 – Chryzode, produto por 2 no módulo 70



Fonte: O autor

Quanto maior o valor de *m* mais a curva se parece com um coração (o que fica mais visível, conforme a pintura da Figura 24), por esse motivo esse tipo de Chryzode recebe o nome de Cardioide, que aparece em muitos lugares do cotidiano, tais como as Figuras 25, 26 e 27.

Figura 25 – Conjunto de Mandelbrot[1]do tipo $z^2 + c$



Fonte: O autor

[1] Foge do escopo desse trabalho, relatar e demonstrar propriedades desse conjunto. Mas para aguçar o interesse do leitor, definimos por Conjunto de Mandelbrot um fractal definido como o conjunto de pontos c no plano complexo para o qual a sucessão é definida por $z_{n+1} = z_n^n + c$. Ou pode ser consultado (REIS, 2016)

.

Figura 26 – Espuma do café no formato de um Cardioide

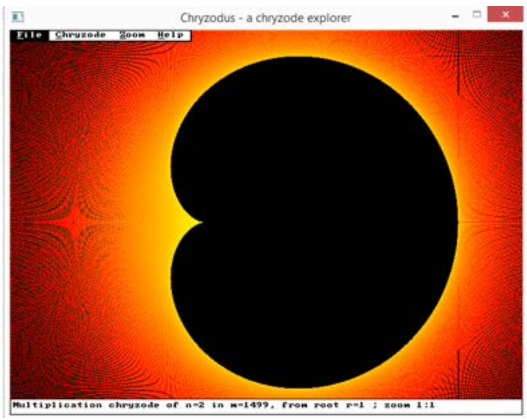
Fonte: (IMAGENS, 2018)

Figura 27 – Microfone Cardioide

Fonte: (IMAGENS, 2019)

No *software* Chryzodus quanto maior o valor de m e com as cores certas, mais bonito e definido o Chryzode se parece com um cardioide, conforme podemos ver na Figura 28.

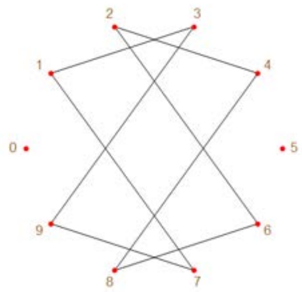
Figura 28 – Chryzode (Cardioide), produto por 2 no módulo 1499



Fonte: O autor

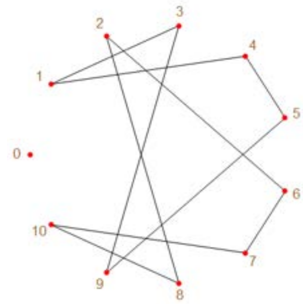
Agora em vez de fazer a tabela de multiplicação por 2, conforme todos os exemplos acima, analogamente, vamos fazer a tabela da multiplicação por 3. E da mesma forma, iremos "esconder"a circunferência e variar o valor de m (do módulo). Assim teremos os Chryzodes para módulo 10, 11, 12, 13, 14, 15, 20, 30, 40, 50 e 70, conforme as Figuras abaixo:

Figura 29 – Chryzode, produto por 3 no módulo 10



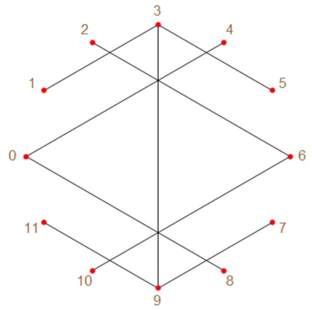
Fonte: O autor

Figura 30 – Chryzode, produto por 3 no módulo 11



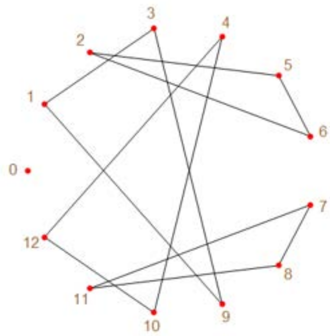
Fonte: O autor

Figura 31 – Chryzode, produto por 3 no módulo 12



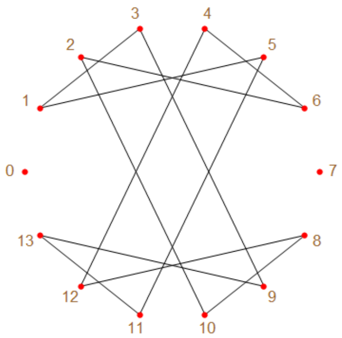
Fonte: O autor

Figura 32 – Chryzode, produto por 3 no módulo 13



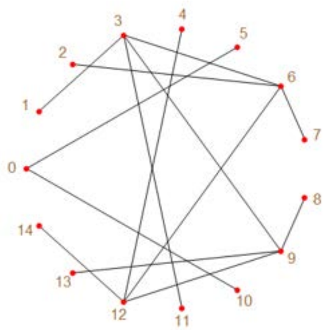
Fonte: O autor

Figura 33 – Chryzode, produto por 3 no módulo 14



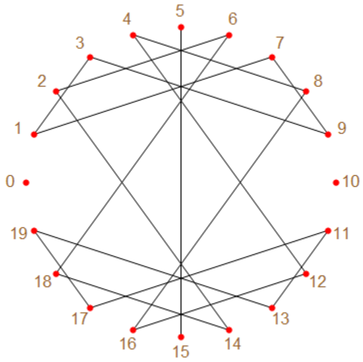
Fonte: O autor

Figura 34 – Chryzode, produto por 3 no módulo 15



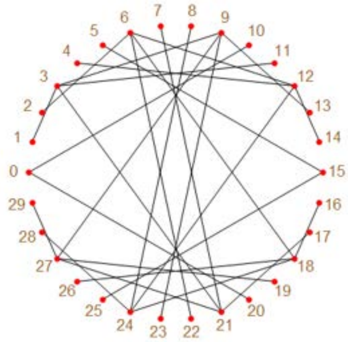
Fonte: O autor

Figura 35 – Chryzode, produto por 3 no módulo 20



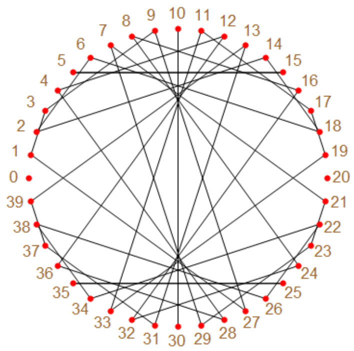
Fonte: O autor

Figura 36 – Chryzode, produto por 3 no módulo 30



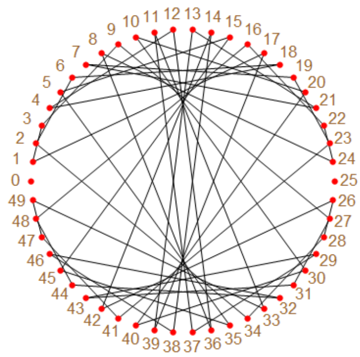
Fonte: O autor

Figura 37 – Chryzode, produto por 3 no módulo 40



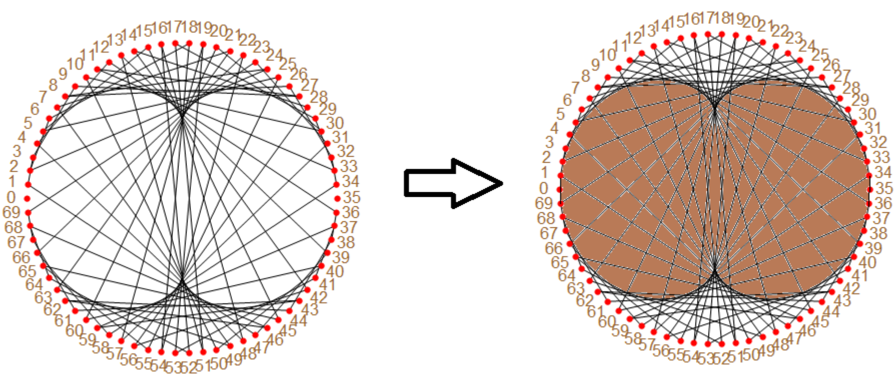
Fonte: O autor

Figura 38 – Chryzode, produto por 3 no módulo 50



Fonte: O autor

Figura 39 – Chryzode, produto por 3 no módulo 70

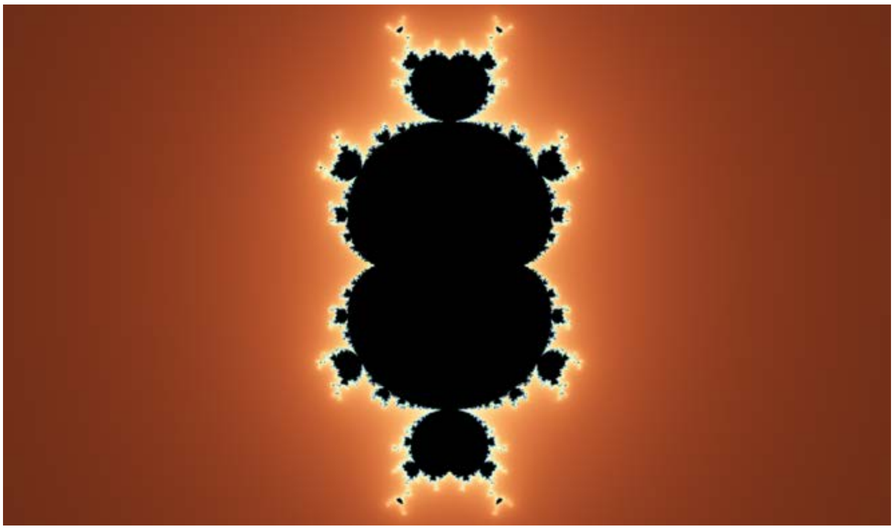


Fonte: O autor

Assim variando o valor de *m*, obtemos outra curva parecida com um Rim, por esse motivo esse tipo de Chryzode recebe o nome de Nefroide, cujo nome significa *forma de rim*, ao qual podemos visualizar na pintura da Figura 39.

Generalizando no conjunto de Mandelbrot, temos a equação $z^3 + c$, diferente do conjunto anterior que tinha expoente dois. Como agora estamos falando da tabela de multiplicação por três, então mudamos o expoente para três. O que de fato nós dá o bulbo principal do conjunto de Mandelbrot como um Nefroide, conforme podemos visualizar na Figura 40.

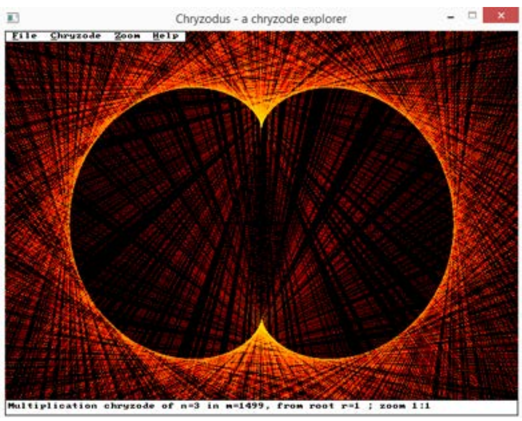
Figura 40 – Conjunto de Mandelbrot do tipo $z^3 + c$



Fonte: O autor

No *software* Chryzodus, também é possível construir o Nefroide, conforme podemos ver na Figura 41.

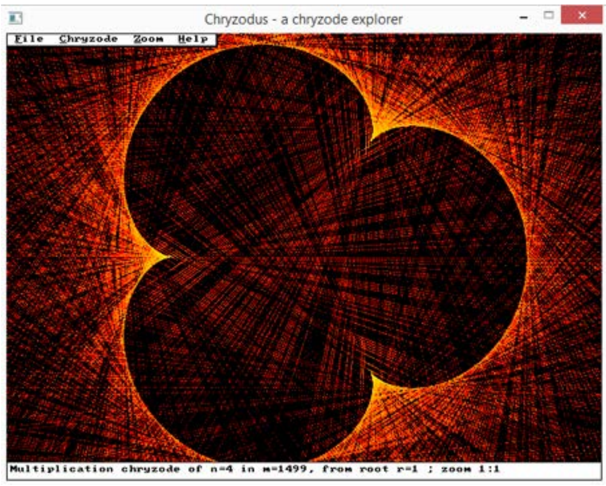
Figura 41 – Chryzode (Nefroide), produto por 3 no módulo 1499



Fonte: O autor

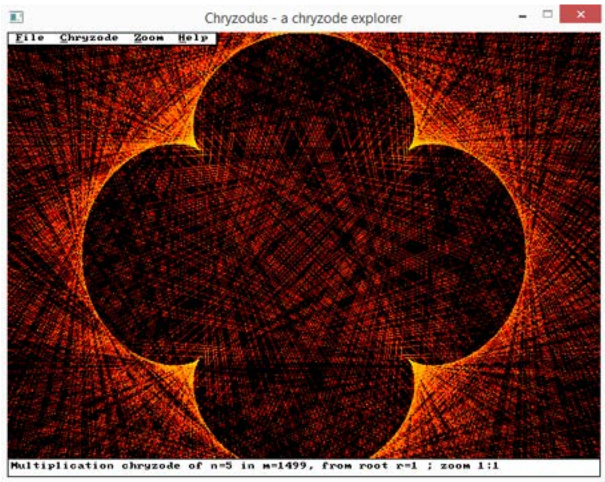
Observando os Chryzodes quando multiplicamos por dois, percebemos que o mesmo possui uma "pétala", quando multiplicamos por três forma duas "pétalas". Seguindo esse padrão, temos que: Multiplicando por quatro, teremos três "pétalas". Multiplicando por cinco, teremos quatro "pétalas", etc, o que podemos verificar nas Figuras 42 e 43.

Figura 42 – Chryzode, produto por 4 no módulo 1499



Fonte: O autor

Figura 43 – Chryzode, produto por 5 no módulo 1499



Fonte: O autor

Para visualizarmos o que acontece de uma forma mais tecnológica e lúdica, foi criado o vídeo que varia o valor de *a* e o valor de *m* dos Chryzodes, o que está disponível em: <https://www.youtube.com/watch?v=sSq3DCkpS-g&t=12s>.

Já no Conjunto de Mandelbrot observamos exatamente esse tipo de padrão, sendo que se tendermos o expoente *n* da fórmula $z_{n+1} = z_n^n + c$, para o infinito positivo o conjunto tende à virar um grande círculo. O que pode ser visualizado no *software* FRAQTIVE, disponível em: <https://fraqtive.mimec.org/>, ao qual foi variado o valor real de *n*, para o infinito positivo.

Para um maior entendimento do *software* e da criação dos Conjuntos de Mandelbrot, foi desenvolvido um breve vídeo disponível em: <https://www.youtube.com/watch?v=t31ulWRs4mY>.

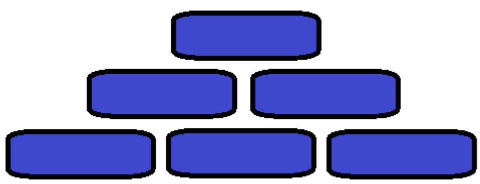
2.4 QUEBRA-CABEÇA DE BOLICHE MÓDULO 6 E 10

Ouvimos falar que a matemática é uma matéria de difícil aprendizagem e temida por grande parte dos alunos. Por esse motivo cabe ao professor inovar a maneira de ensinar. E a prática lúdica pode ser uma maneira de estimular o desenvolvimento mental, fazendo com que o aluno construa o conhecimento de uma forma mais prazerosa. Além de tornar as aulas menos cansativas e mais atraentes, aproximando o professor do aluno o que por si acaba com os bloqueios e medos dos alunos em relação a matemática. Segundo (MENDES, 2011):

> O educador deve priorizar o ato de encorajar a criança a pensar autonomamente em todos os tipos de situação. Cabe a ele buscar formas didáticas diferenciadas para ensinar, que estimulem as formas de pensamento das crianças, fazendo com que elas pensem por si. Não apenas limitando a um mesmo raciocínio, mas propiciando atividades diferenciadas para estimular a mente da criança, que está em pleno desenvolvimento, para que a criança sinta o desejo de pensar logicamente. [· · ·] Pois no momento do jogo as crianças não se sentem intimidadas e sentem maior desejo de participar da brincadeira, porque durante a aplicação das atividades elas se sentem iguais acabando com os medos, deixando transparecer apenas a vontade de brincar, e acabam por aprender de forma que nem imaginavam.

Pensando nisso, este tópico serve para ensinar/aprender de uma maneira lúdica a aritmética modular, através do quebra-cabeça modular. Vamos começar com a pirâmide módulo 6, que consiste em 6 blocos empilhados como pirâmide: três blocos na linha inferior, dois blocos na linha do meio e um bloco no topo. Conforme podemos perceber na Figura 44.

Figura 44 – Pirâmide *mod* 6.



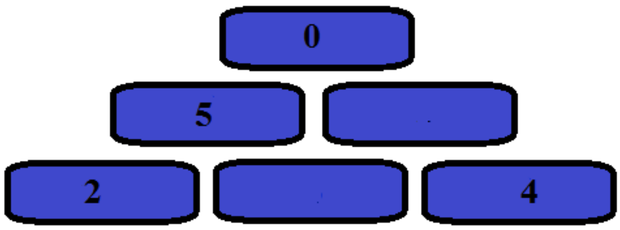
Fonte: O autor

A resolução da pirâmide se dá pelo preenchimento de todos os blocos da pirâmide com números, tal que a regra da pirâmide segue de um triângulo reverso de Pascal, isto é, qualquer bloco é a soma dos dois blocos diretamente abaixo dele *mod* 6. O objetivo é usar todos os números 0, 1, 2, 3, 4 e 5 exatamente uma vez tal que eles satisfaçam a regra da pirâmide.

O seguinte exemplo mostra como funciona a regra da pirâmide, mas não é uma solução do quebra-cabeça.

Exemplo 2.2. Vamos completar a pirâmide da Figura 45, pela regra da pirâmide.

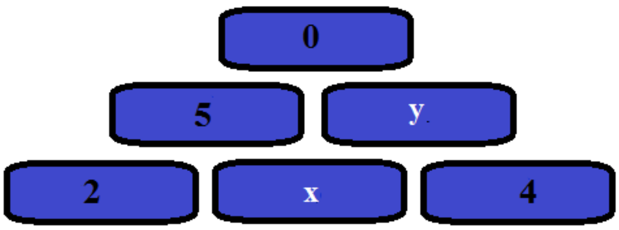
Figura 45 – Exemplo de pirâmide *mod* 6.



Fonte: O autor

Solução: Primeiramente vamos colocar incógnitas nos blocos ao qual queremos solução, assim obtemos uma pirâmide conforme a Figura 46.

Figura 46 – Exemplo de pirâmide *mod* 6.

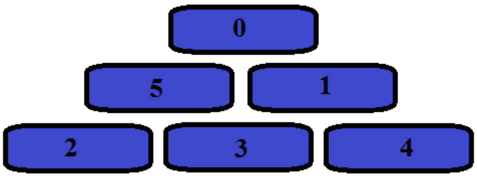


Fonte: O autor

Agora basta pensarmos na congruência $2 + x \equiv 5 \mod 6$, ao qual possui a solução minimal igual a 3. Analogamente, temos que $5 + y \equiv 0 \pmod 6$, logo $y = 1$.

Assim, completamos a pirâmide, conforme a Figura 47.

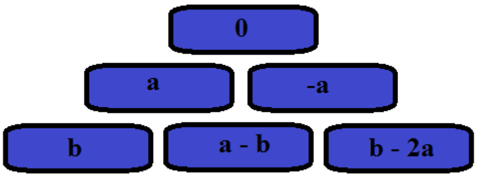
Figura 47 – Resolução pela regra da pirâmide *mod* 6.



Fonte: O autor

Agora, vamos tentar resolver o quebra-cabeça usando as propriedades dos inteiros módulo 6. O zero deve estar no topo da pirâmide, caso contrário não poderíamos garantir que os números 0, 1, 2, 3, 4 e 5 sejam usados exatamente uma vez. Isto implica que na próxima linha teremos um número a e seu inverso $-a$. Na linha de baixo, vamos deixar o bloco inferior esquerdo ser outro número, digamos b, em seguida, pelas regras do triângulo, o próximo bloco deve ser $a - b$ e o bloco da direita deve ser $b - 2a$. O que podemos melhor visualizar na Figura 48.

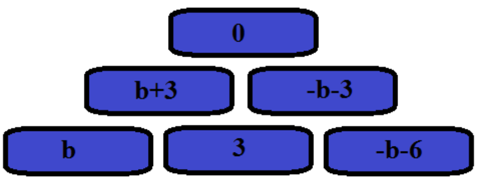
Figura 48 – Quebra cabeça *mod* 6, resolvido por álgebra com duas incógnitas.



Fonte: O autor

Assim os possíveis valores dos blocos $\pmod 6$, são 0, 1, 2, 3, 4 e 5. Suponha que cada bloco possua um desse valores. Se somarmos os valores de todos os blocos, obtemos $5 + 4 + 3 + 2 + 1 + 0 = (5 + 0) + (4 + 1) + (3 + 2) = 5 \cdot 3 = 15 \equiv 3 \pmod 6$. Por outro lado, somando os valores dos blocos $0 + a + (-a) + b + (a - b) + (b - 2a)$, fica $b - a$. Logo, $b - a = 3$ módulo 6. Assim, $a = b - 3$ módulo 6 ou $a = b + 3$ módulo 6. Substituindo $a = b + 3$ na pirâmide, temos a pirâmide conforme a Figura 49.

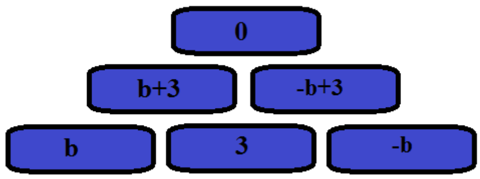
Figura 49 – Quebra cabeça *mod* 6, reduzido a uma incógnita.



Fonte: O autor

Observe que podemos mudar o -3 pelo $+3$ no bloco a direita da segunda linha e -6 pelo 0 no último bloco (da esquerda para a direita) da terceira linha, conforme podemos visualizar na Figura 50.

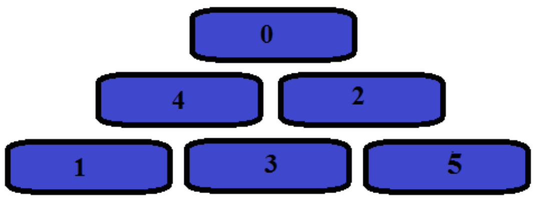
Figura 50 – Quebra cabeça *mod* 6, resolvido por álgebra.



Fonte: O autor

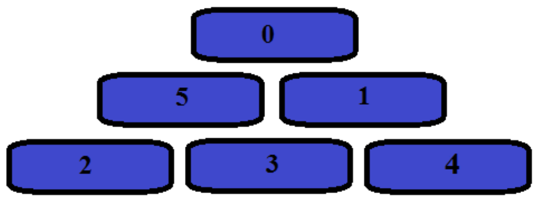
Substituindo b= 1, 2, 4 e 5 obtemos quatro soluções diferentes contando reflexões.

Figura 51 – Quebra cabeça *mod* 6, com $b = 1$



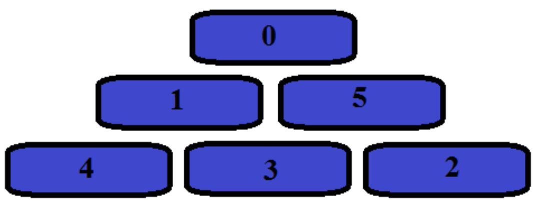
Fonte: O autor

Figura 52 – Quebra cabeça *mod* 6, com $b = 2$



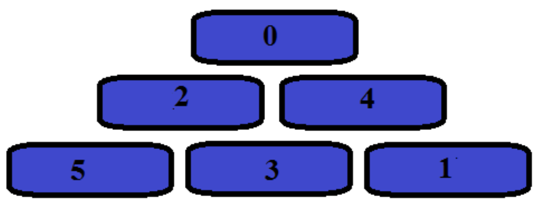
Fonte: O autor

Figura 53 – Quebra cabeça *mod* 6, com $b = 4$



Fonte: O autor

Figura 54 – Quebra cabeça *mod* 6, com $b = 5$



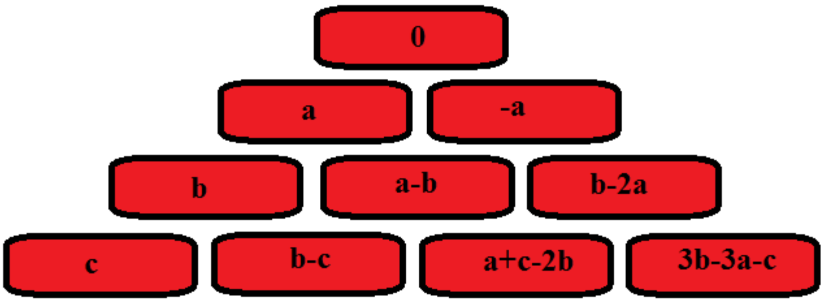
Fonte: O autor

De maneira semelhante, podemos encontrar um padrão para o quebra-cabeça $\pmod{10}$, aumentando assim um pouco o nível de dificuldade. Essa é uma boa maneira para os alunos da educação básica se familiarizarem com a aritmética modular, pois faz com que todos os alunos se envolvam com o jogo, o que acabam pensando que estão jogando, mas na verdade estão revisando conceitos matemáticos disfarçados do jogo de quebra-cabeça.

A seguir, vamos obter as soluções do quebra-cabeças módulo 10. O raciocínio é análogo ao quebra-cabeças módulo 6.

Sabendo que o zero tem que estar no topo da pirâmide obtemos a seguinte configuração:

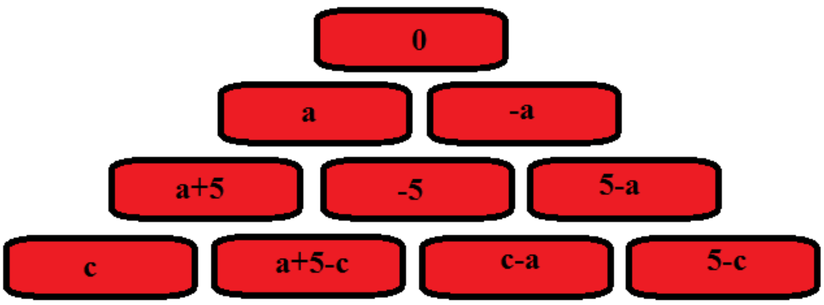
Figura 55 – Pirâmide *mod* 10, com três variáveis.



Fonte: O autor

Como cada bloco possui um dos valores entre 0 e 9, sem repetições, segue que $9+8+7+6+5+4+3+2+1+0 = (0+9)+(8+1)+(7+2)+(6+3)+(5+4) = 9 \cdot 5 = 45 \equiv 5 \pmod{10}$ ao somarmos todos esses valores. De outro modo, somando os valores dos blocos $0 + a + (-a) + b + (a-b) + (b-2a) + c + (b-c) + (a+c-2b) + (-c-3a+3b)$, fica $3 \cdot (b-a)$. Assim, $3 \cdot (b-a) \equiv 5 \pmod{10}$. Sendo 7 o inverso de 3 módulo 10, temos que $b - a \equiv 35 \pmod{10}$ ou $b - a \equiv 5 \pmod{10}$. Substituindo $b = a + 5$ na pirâmide, obtemos uma pirâmide conforme a Figura 56.

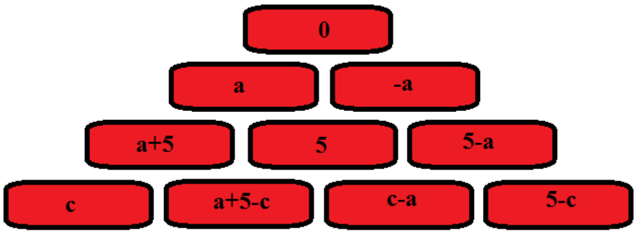
Figura 56 – Pirâmide *mod* 10, com duas variáveis.



Fonte: O autor

Note que podemos mudar -5 por $+5$ na pirâmide, assim obtemos a pirâmide conforme a Figura 57.

Figura 57 – Pirâmide *mod* 10, reescrita com duas variáveis.

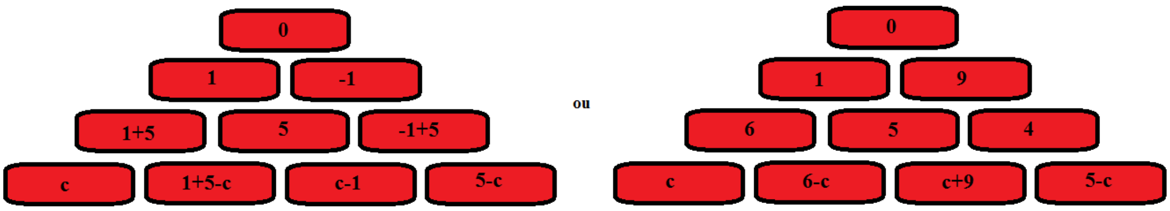


Fonte: O autor

Agora, analisaremos as possíveis soluções da pirâmide, variando os valores de a entre 1 à 9, pois se a for igual a zero teremos que $a = -a = 0$ e esse valor aparece mais de uma vez na pirâmide. E variando os valores de c, entre 0 à 9. Assim:

Para $a = 1$, temos:

Figura 58 – Pirâmide *mod* 10, para $a = 1$.

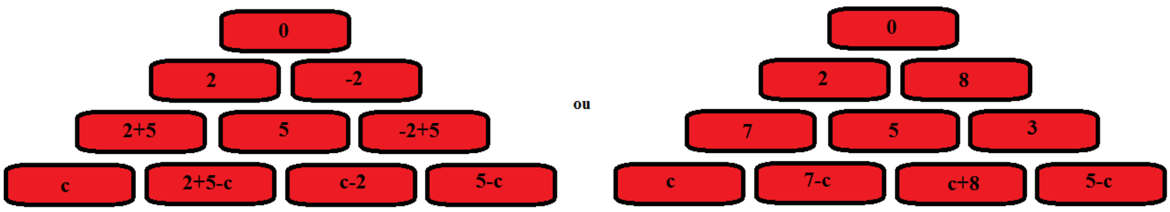


Fonte: O autor

Ao qual percebemos que não tem solução, pois não existe c tal que os números $0, 1, 2, 3, 4, 5, 6, 7, 8$ e 9, apareçam exatamente uma vez.

Para $a = 2$, temos:

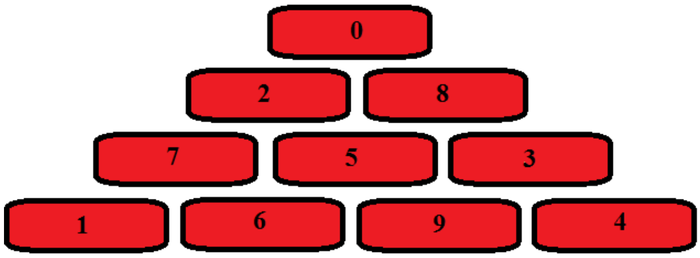
Figura 59 – Pirâmide *mod* 10, para $a = 2$.



Fonte: O autor

Ao qual temos solução para $c = 1$, e podemos perceber na Figura 60.

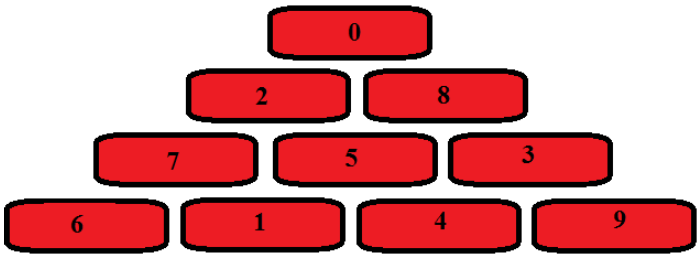
Figura 60 – Pirâmide *mod* 10, para $a = 2$ e $c = 1$.



Fonte: O autor

E temos solução para $c = 6$, ao qual notamos na Figura 61.

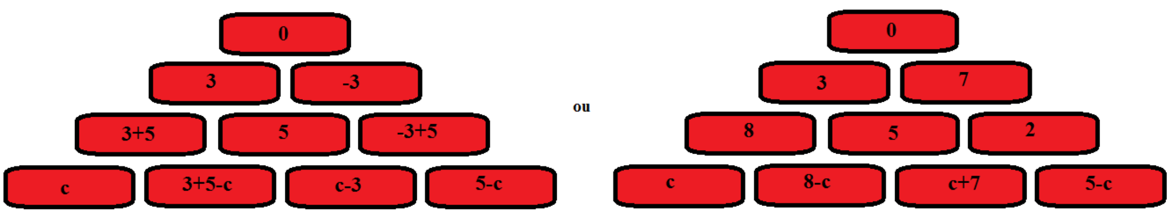
Figura 61 – Pirâmide *mod* 10, para $a = 2$ e $c = 6$.



Fonte: O autor

Para $a = 3$, temos:

Figura 62 – Pirâmide *mod* 10, para $a = 3$.

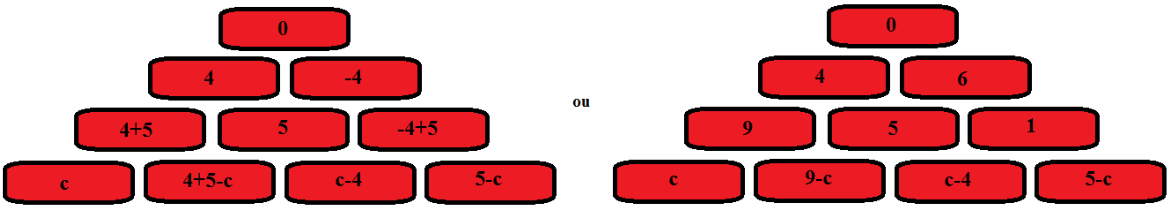


Fonte: O autor

Ao qual também percebemos que não tem solução, pois não existe c tal que os números $0, 1, 2, 3, 4, 5, 6, 7, 8$ e 9, apareçam exatamente uma vez.

Para $a = 4$, temos:

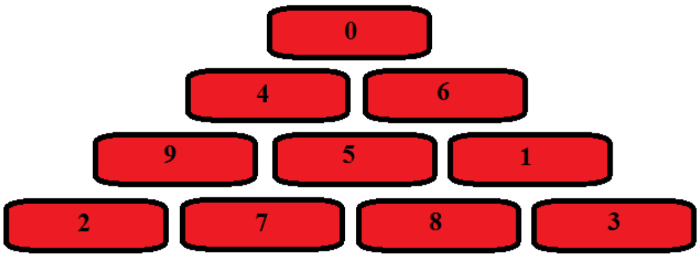
Figura 63 – Pirâmide *mod* 10, para $a = 4$.



Fonte: O autor

O que tem solução para $c = 2$, e notamos na Figura 64.

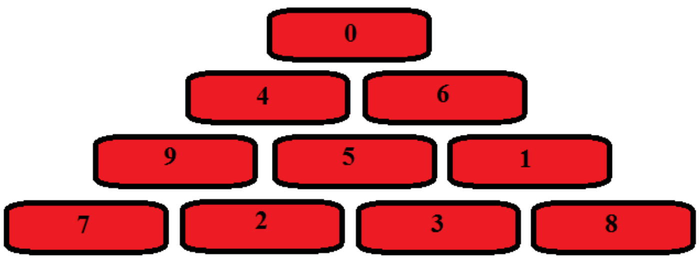
Figura 64 – Pirâmide *mod* 10, para $a = 4$ e $c = 2$.



Fonte: O autor

E também temos solução para $c = 7$, ao qual também notamos na Figura 65.

Figura 65 – Pirâmide *mod* 10, para $a = 4$ e $c = 7$.

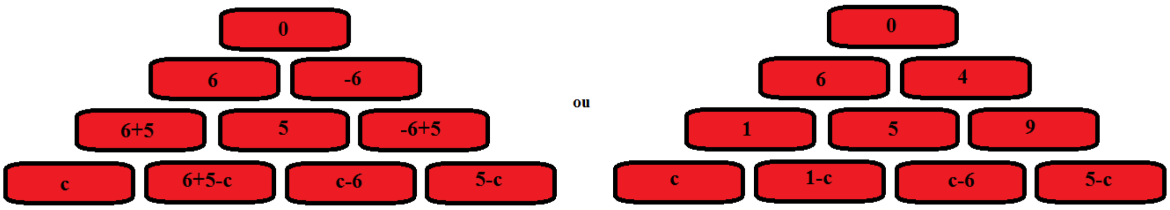


Fonte: O autor

Para $a = 5$, é visível que a pirâmide não tem solução pelo fato de $a = -a = 5$.

Para $a = 6$, temos:

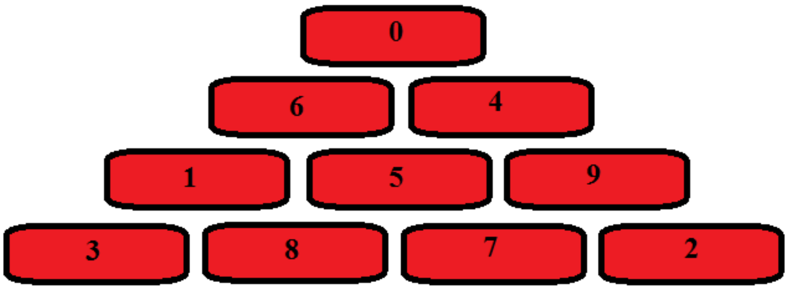
Figura 66 – Pirâmide *mod* 10, para $a = 6$.



Fonte: O autor

Note que existe solução para $c = 3$, o que pode ser notado na Figura 67.

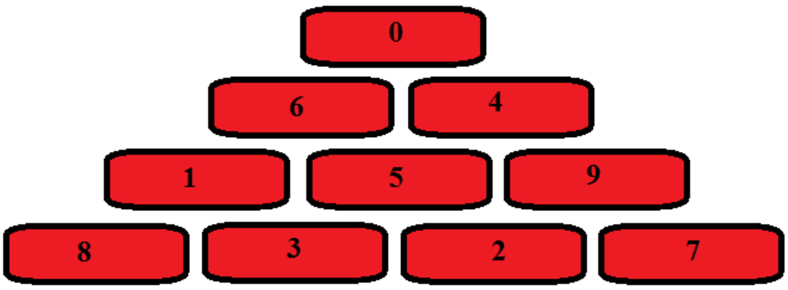
Figura 67 – Pirâmide *mod* 10, para $a = 6$ e $c = 3$.



Fonte: O autor

E também existe solução para $c = 8$, o que também pode ser notado na Figura 68.

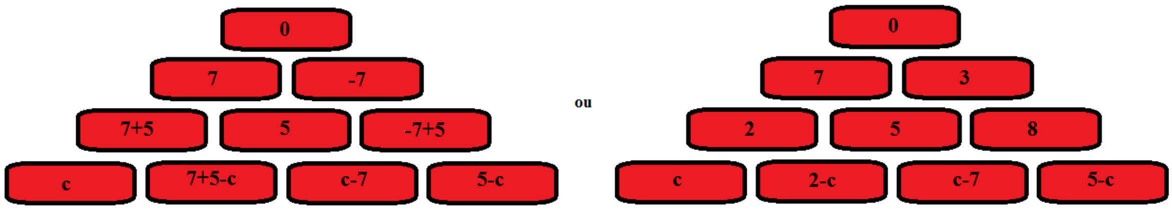
Figura 68 – Pirâmide *mod* 10, para $a = 6$ e $c = 8$.



Fonte: O autor

Para $a = 7$, temos:

Figura 69 – Pirâmide *mod* 10, para $a = 7$.

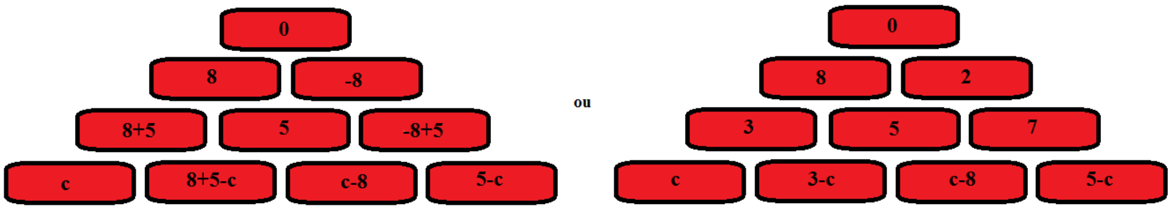


Fonte: O autor

Aqui também percebemos que não tem solução, pois não existe c tal que os números $0, 1, 2, 3, 4, 5, 6, 7, 8$ e 9, apareçam exatamente uma vez.

Para $a = 8$, temos:

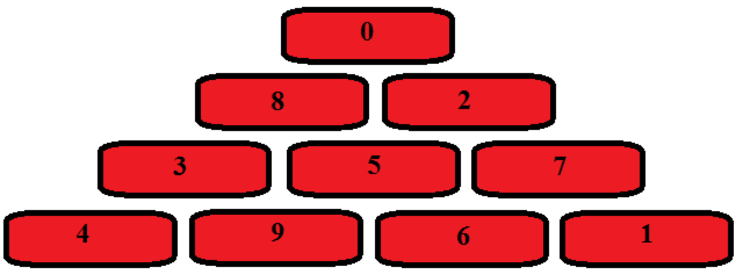
Figura 70 – Pirâmide *mod* 10, para $a = 8$.



Fonte: O autor

Que possui solução para $c = 4$, e percebemos na Figura 71.

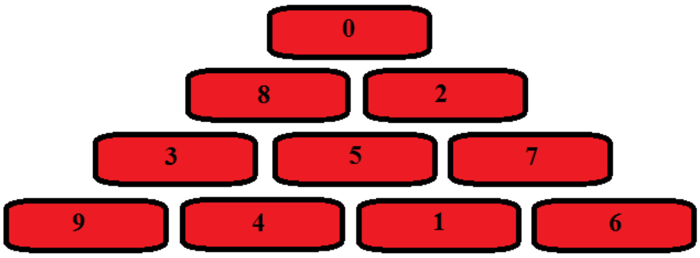
Figura 71 – Pirâmide *mod* 10, para $a = 8$ e $c = 4$.



Fonte: O autor

E solução para $c = 9$, ao qual é possível perceber na Figura 72.

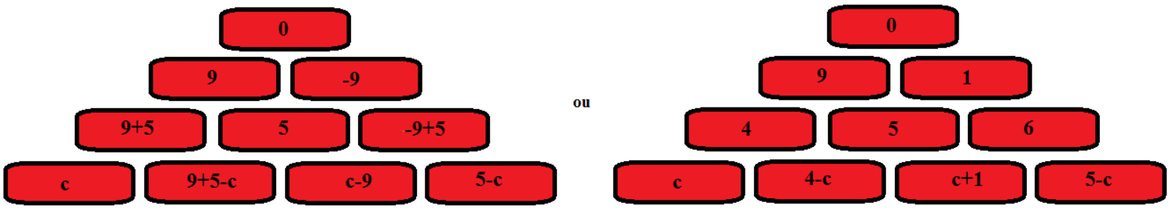
Figura 72 – Pirâmide *mod* 10, para $a = 8$ e $c = 9$.



Fonte: O autor

E por fim, para $a = 9$, temos:

Figura 73 – Pirâmide *mod* 10, para $a = 9$.



Fonte: O autor

Novamente percebemos que não tem solução, pois não existe c tal que os números $0, 1, 2, 3, 4, 5, 6, 7, 8$ e 9, apareçam exatamente uma vez.

Observação 2.3. *Para o quebra-cabeça de boliche módulo 15, não encontramos solução.*

2.5 APLICAÇÃO DE EQUAÇÕES DIOFANTINAS LINEARES COM DUAS VARIÁVEIS - DESCOBRINDO A QUANTIDADE DE NÚMEROS

Nessa seção abordaremos uma aplicação de Equação Diofantina Linear com duas variáveis. Essa aplicação tem como objetivo descobrir a quantidade de vezes que iremos adicionar ou subtrair dois números dados e assim chegar no resultado desejado. Então vamos aos exemplos:

Exemplo 2.4. Comece do número 0 e, a cada passo, você pode adicionar ou subtrair o número 5 ou o número 17. É possível chegar como resultado no número 1? Se sim, descreva os passos utilizados.

$$0 \xrightarrow{+5} 5 \xrightarrow{+17} 22 \longrightarrow \cdots$$

Solução: Para resolvermos esse problema, devemos verificar se existe solução para a equação diofantina linear $5x + 17y = 1$.

Assim da Proposição 1.48, a equação admite solução se o *mdc*(5, 17) | 1. E pelo algoritmo de Euclides (Teorema 1.29), temos:

	3	2	2
17	5	2	1
2	1	0	

Logo, temos que o *mdc*(5, 17) = 1. Daí a equação diofantina possui solução. Então:

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

$$5 = 2 \cdot 2 + 1 \Longrightarrow 1 = 5 - 2 \cdot 2$$

Assim substituindo a primeira igualdade na segunda igualdade, temos:

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (17 - 3 \cdot 5) = 5 - 2 \cdot 17 + 6 \cdot 5 = 7 \cdot (5) - 2 \cdot (17).$$

O que nos dá 1 = 7 · (5) - 2 · (17).

Portanto, $x_0 = 7$ e $y_0 = -2$ é uma solução particular e a solução geral em $\mathbb{Z}$ é dada por:

$$x = 7 + 17t, y = -2 - 5t,$$

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

Portanto é possível chegar ao número 1. O processo de adicionar ou subtrair o número 5 ou o número 17 pode ser feito de várias formas. Os diagramas, a seguir, são exemplos de visualizações do processo.

Para $t = 0$, temos:

$$0 \xrightarrow{+5} 5 \xrightarrow{+5} 10 \xrightarrow{+5} 15 \xrightarrow{+5} 20 \xrightarrow{+5} 25 \xrightarrow{+5} 30 \xrightarrow{+5} 35 \xrightarrow{-17} 18 \xrightarrow{-17} 1$$

Outra forma de chegar no resultado é para $t = -1$

$$0 \xrightarrow{+17} 17 \xrightarrow{+17} 34 \xrightarrow{+17} 51 \xrightarrow{-5} 46 \xrightarrow{-5} 41 \xrightarrow{-5} 36 \xrightarrow{-5}$$

$$31 \xrightarrow{-5} 26 \xrightarrow{-5} 21 \xrightarrow{-5} 16 \xrightarrow{-5} 11 \xrightarrow{-5} 6 \xrightarrow{-5} 1$$

Exemplo 2.5. Comece do número 0 e, a cada passo, você pode adicionar ou subtrair o número 4 ou o número 6. É possível chegar como resultado no número 3? Se sim, descreva os passos utilizados.

$$0 \xrightarrow{+4} 4 \xrightarrow{-6} -2 \longrightarrow \cdots$$

Solução: Para resolvermos esse problema, devemos verificar se existe solução para a equação diofantina linear $4x + 6y = 3$.

Então da Proposição 1.48, a equação admite solução se o *mdc*(4, 6) | 3. E pelo algoritmo de Euclides (Teorema 1.29), temos:

	1	2	
6	4	2	
2	0		

Assim, temos que o *mdc*(4, 6) = 2 e 2 $\nmid$ 3. Logo a equação diofantina não possui solução e consequentemente a adição e a subtração dos números 4 e 6 nunca terão como resultado o número 3. O que é válido, pois considere *a* e *b*, números pares, tal que $a = k_1$ e $b = k_2$, assim $a - b$ = $2k_1 - 2k_2$ = $2 \cdot (k_1 - k_2)$ = $2k_3$.

□

2.6 APLICAÇÃO DE EQUAÇÕES DIOFANTINAS LINEARES COM TRÊS VARIÁVEIS - JOGO DE DARDOS

Vivemos em um país em que o Jogo de Dardos não é um jogo popular e conhecido entre a população. Mas então, porque torná-lo um objeto de estudo? A resposta dessa pergunta é simples. Para o jogador de dardos ganhar uma partida ele deve resolver uma equação diofantina linear. Portanto, nessa seção abordaremos uma aplicação de equação diofantina linear com duas e três variáveis através do jogo de Dardos.

Antes de mais nada, vamos explicar a forma de como funciona para aqueles que não conhecem o jogo de dardos. O princípio do jogo é jogar um pequeno projétil pontudo em um quadro de destino enumerado, conforme a figura 74.

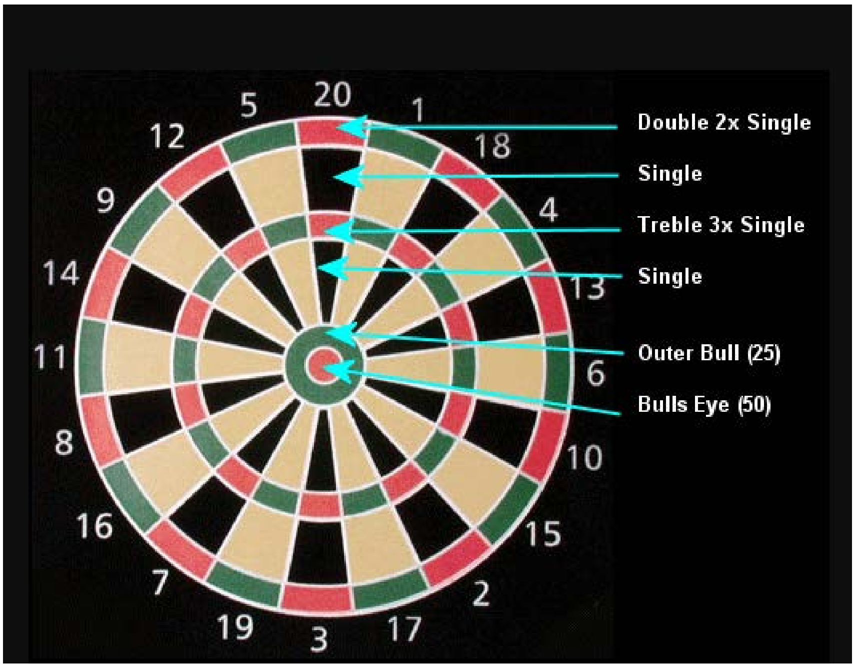
Percebemos que o tabuleiro de dardos é redondo e é dividido em 20 setores, ao qual cada setor vale de 1 à 20 pontos. Esses setores são divididos em quatro partes. Ao qual cada parte possui uma pontuação: O anel externo do setor vale o dobro do valor do setor (Double 2X Single) e o anel do meio do setor vale o triplo do valor do setor (Treble 3X Single).

Figura 74 – Tabuleiro do jogo de dardos

Fonte: <www.walmart.com.br/jogo-de-dardos-western-tabuleiro-alvo-duplo/4419471/pr>

As outras duas partes valem o valor normal do setor (Single). O círculo central do tabuleiro chamado Bulls Eye (olho de touros) vale 50 pontos e o anel ao redor do Bull Eye é chamado de Outer Bull (Touro exterior) ao qual vale 25 pontos. Conforme podemos visualizar na figura 75.

Figura 75 – Pontuação do tabuleiro do jogo de dardos



Fonte: <https://flordoexilio.wordpress.com/tag/dardos/>

Cada jogador inicia com zero pontos e ganha o jogo quem somar primeiro 501 pontos. O jogo é dividido em rodadas, sendo que em cada rodada o jogador tem três dardos para serem jogados. Um dardo que cai em um determinado setor no tabuleiro obterá essa pontuação. No entanto, se você pousar no anel do meio, você ganha o triplo da pontuação do setor e se você pousar no anel externo você recebe o dobro da pontuação. Assim, o número máximo de pontos para um dardo é o triplo de vinte, ou seja 60 pontos.

Como cada jogador lança três dardos por rodada, o número máximo de pontos por rodada é 180 pontos. Além disso, o jogador deve acertar o Double 2X Single ou o Bulls Eye pelo menos uma vez na última rodada para ganhar o jogo.

Nas primeiras rodadas, eles buscam o triplo de vinte, de modo que, em cada rodada se consiga 180 pontos. Supondo que isso se concretize, teríamos 180 pontos na primeira rodada, mais 180 pontos na segunda rodada o que restaria 141 pontos para a última rodada. Isso poderia ser feito por exemplo com um triplo de 19 para obter 57 pontos, um triplo de vinte, que chega a 117 pontos, e finalmente um duplo 12 para chegar a 141 pontos. (Observe que foi acertado em Double 2X Single, no caso o dobro de 12). Note que nove dardos é o número mínimo para se ganhar uma partida, já que a pontuação máxima com 8 dardos é 480 (8 x 60). Assim, um jogo de dardos perfeito termina em três rodadas e 9 lançamentos dos dardos.

Observação 2.6. *Nos torneios de jogos de dardos (ou em partidas) existe um narrador que aponta o número de pontos somados em cada rodada. E quando o máximo de 180 pontos é atingido, é como se o jogador tivesse marcado um gol.*

Mas o que isso tem a ver com Matemática? Ou melhor onde usamos Equações Diofantinas Lineares? A resposta está na última rodada, ao qual a resolução de uma equação diofantina e a precisão na mira darão a vitória ao jogador.

Assim, suponha que eles precisem marcar n pontos para vencer. Então eles precisam resolver a equação $2X + aY + bZ = n$, onde a e $b \in \{0, 1, 2, 3\}$ e $X, Y, Z \in \{1, 2, \ldots, 20\}$. Observe que o dobro de X aparece na equação devido o critério da última rodada. Daí vocês me perguntarão e se eu acertar um Bulls Eye na última rodada? Neste caso a equação se reduz a uma equação diofantina de duas variáveis do tipo $aX + bY = n_1$, onde n_1 são os pontos faltantes e a, $b \in \{0, 1, 2, 3\}$ e $X, Y, Z \in \{1, 2, \ldots, 20\}$.

Exemplo 2.7. Suponha que em um jogo de dardos o jogador tenha feito 360 pontos nas duas primeira rodadas, ou seja, para ganhar o jogo o jogador precisa de 141 pontos na terceira rodada. Encontre as possíveis combinações que darão a vitória ao jogador.

Solução: Devemos resolver a equação diofantina do tipo $2X + aY + bZ = 141$ onde *a*, *b* ∈ {0, 1, 2, 3 } e *X*, *Y*, *Z* ∈ {1, 2, . . . , 20 }. Vamos resolver a equação de tal maneira que o jogador consiga um "Double 2X Single"e dois "Treble 3X Single", ou seja, a equação $2X + 3Y + 3Z = 141$.

Sendo o *mdc*(2,3,3) = 1 e que 1 | 141, então conforme a Proposição 1.52 essa equação diofantina de três variáveis possui solução. Por outro lado o *mdc*(2,3) = 1, pois 2 e 3 são primos entre si e *mdc*(*mdc*(2,3),3) = *mdc* (1,3) = 1. Fazendo as devidas substituições temos que $1 = 2 \cdot (-1) + 3 \cdot (1) + 3 \cdot (0)$. Assim, $(-1 \cdot 141, 1 \cdot 141, 0 \cdot 141)$ = (-141, 141, 0) é uma solução particular da equação dada.

Agora vamos resolver por partes, para encontrar a solução geral da equação diofantina $2X + 3Y + 3Z = 141$. Assim, considere $p = 2X + 3Y$, que gera a equação $p + 3Z = 141$, que também possui solução, pois *mdc*(1,3) = 1 e 1 | 141. Então, conseguimos encontrar uma solução particular da equação $p + 3Z = 141$, fazendo:

$$1 = 1 \cdot (-2) + 3 \cdot 1 \Longrightarrow 141 = 1 \cdot (-2 \cdot 141) + 141 \cdot 3 \Longrightarrow 141 = 1 \cdot (-282) + 3 \cdot 141.$$

que nos leva a solução geral de $p + 3Z = 141$, que é:

$$S_1 = \{(-282 + 3t_1, 141 - t_1) | t_1 \in \mathbb{Z}\}$$

Para encontrar a solução geral da equação diofantina $2X + 3Y + 3Z = 141$, devemos encontrar a solução geral da equação $2X + 3Y = p = -282 + 3t_1$. E para que essa equação possua solução, o *mdc*(2,3) = 1 deve dividir $-282 + 3t_1$, o que é válido.

Logo:

$$1 = 2 \cdot (-1) + 3 \cdot (1),$$

multiplicando por $(-282 + 3t_1)$, temos:

$$1 \cdot (-282 + 3t_1) = 2 \cdot (-1) \cdot (-282 + 3t_1) + 3 \cdot (1) \cdot (-282 + 3t_1) \Longrightarrow$$

$$-282 + 3t_1 = 2 \cdot (282 - 3t_1) + 3 \cdot (-282 + 3t_1).$$

Assim temos que a solução geral de $2x + 3y = p = -282 + 3t_1$ é:

$$S_2 = \{(282 - 3t_1 + 3t_2, -282 + 3t_1 - 2t_2) | t_1, t_2 \in \mathbb{Z}\}.$$

Com isso, concluímos que a solução geral da equação diofantina de três variávies é:

$$S = \{(282 - 3t_1 + 3t_2, -282 + 3t_1 - 2t_2, 141 - t_1) | t_1, t_2 \in \mathbb{Z}\}.$$

Por outro lado, sabendo a solução geral da equação e considerando a pontuação máxima e miníma, temos que:

$$141 - t_1 \geq 0 \Longrightarrow t_1 \leq 141$$

$$141 - t_1 \leq 20 \Longrightarrow t_1 \geq 121$$

Então, $121 \leq t_1 \leq 141$.

Da mesma forma temos:

$$282 - 3t_1 + 3t_2 \geq 0 \Longrightarrow 3t_2 \geq -282 + 3t_1 \Longrightarrow t_2 \geq \frac{-282 + 3t_1}{3},$$

$$282 - 3t_1 + 3t_2 \leq 20 \Longrightarrow 3t_2 \leq -262 + 3t_1 \Longrightarrow t_2 \leq \frac{-262 + 3t_1}{3}$$

e

$$-282 + 3t_1 - 2t_2 \geq 0 \Longrightarrow 2t_2 \leq -282 + 3t_1 \Longrightarrow t_2 \leq \frac{-282 + 3t_1}{2},$$

$$-282 + 3t_1 - 2t_2 \leq 20 \Longrightarrow -302 + 3t_1 \leq 2t_2 \Longrightarrow t_2 \geq \frac{-302 + 3t_1}{2}.$$

Na tabela abaixo, vamos variar t_1 nas desigualdades acima e descobrir quais os valores podemos ter para t_2.

t_1	$\frac{-282+3t_1}{2}$	$\frac{-302+3t_1}{2}$	$\frac{-282+3t_1}{3}$	$\frac{-262+3t_1}{3}$
121	40,5	30,5	27	33,66$\cdots$
122	42	32	28	34,66$\cdots$
123	43,5	33,5	29	35,66$\cdots$
124	45	35	30	36,66$\cdots$
125	46,5	36,5	31	37,66$\cdots$
126	48	38	32	38,66$\cdots$
127	49,5	39,5	33	39,66$\cdots$
128	51	41	34	40,66$\cdots$
129	52,5	42,5	35	41,66$\cdots$
130	54	44	36	42,66$\cdots$
131	55,5	45,5	37	43,66$\cdots$
132	57	47	38	44,66$\cdots$
133	58,5	48,5	39	45,66$\cdots$
134	60	50	40	46,66$\cdots$
135	61,5	51,5	41	47,66$\cdots$
136	63	53	42	48,66$\cdots$
137	64,5	54,5	43	49,66$\cdots$
138	66	56	44	50,66$\cdots$
139	67,5	57,5	45	51,66$\cdots$
140	69	59	46	52,66$\cdots$
141	70,5	60,5	47	53,66$\cdots$

Observe que variando t_1, nas desigualdades obtemos intervalos válidos para $t_2 \in \mathbb{Z}$, apenas para $121 \leq t_1 \leq 126$. Para t_1 maior que 126, temos que não existe um t_2 que satisfaça o mesmo intervalo. Assim, o problema tem solução, conforme a tabela abaixo:

t_1	t_2	S
121	31,32 e 33	(12,19,20), (15,17,20) e (18,15,20)
122	32,33 e 34	(12,20,19), (15,18,19) e (18,16,19)
123	34 e 35	(15,19,18) e (18,17,18)
124	35 e 36	(15,20,17) e (18,18,17)
125	37	(18,19,16)
126	38	(18,20,15)

Portanto, se quisermos um "Double 2X Single"e dois "Treble 3X Single"para chegarmos na pontuação igual a 141, temos essas doze possíveis soluções de acertos no jogo de dardos. Obviamente para outras configurações de acertos teríamos que calcular outras equações diofantinas lineares.

Existem alguns sites que disponibilizam o jogo de dardos para se praticar, um deles está disponível em: <https://www.transum.org/Maths/Game/Darts/>.

Com essa aplicação, ficam algumas indagações:

- Será que os jogadores de dardos resolvem a equação diofantina em suas cabeças enquanto jogam ou apenas lembram das combinações necessárias? Pois analisando os jogos percebemos que eles parecem fazer essas contas instantaneamente;
- Os jogadores se adaptam em tempo real, porque se eles perderem um alvo pretendido em um lance, eles teriam que resolver uma equação diofantina linear com duas variáveis;
- Por fim, se os jogares de dardos não memorizam as combinações possíveis no jogo, então ao que tudo parece esses jogadores são melhores em aritmética do que os que não são jogadores de dardos. Portanto, essa atividade é um ótimo estimulo para começar a encorajar as pessoas a jogar dardos.

3 PROPOSTAS DE ATIVIDADES NO ENSINO BÁSICO

Neste capítulo, daremos enfoque ao ensino dos conteúdos de Aritmética, através de Planos de Aula, focados para a Educação Básica (ou seja, Ensino Fundamental e Médio) que seguem os Parâmetros Curriculares Nacionais (PCN's) .

Mas e onde surgiu a palavra Aritmética? E quais são os conteúdos que a Aritmética abrange?

Conforme (MORAES, 2018, p. 38):

> A etimologia do termo Aritmética procede do latim *arithmetica*, com origem na palavra grega *aritmetikos*, que por sua vez é composta por *arithmos* que se refere a *número*,e por *tiko* que se remete a ciência, portanto, Aritmética significa *ciência dos números*. A Aritmética surgiu naturalmente pela necessidade do homem de contar, esta é a base de toda a Matemática, nela se estabelecem conceitos importantes, como os sistemas de base posicional, representações dos algarismos, operações, estudo de frações, conceitos sobre múltiplos e divisores, dentre outros.

Estando estes conteúdos nos PCN's, pretendemos aborda-lós de modo que os alunos tenham mais interesse e curiosidade sobre o assunto e que percebam a presença da matemática no cotidiano ou aprendam de maneira lúdica.

Essas propostas pedagógicas, terão como público alvo os alunos da educação básica, levando a esses alunos a oportunidade de aplicar conhecimentos matemáticos adquiridos em sala de aula em situações do cotidiano, ou aprender e revisar esses conhecimentos de forma lúdica, pois, em concordância com (BRASIL, 1998, p. 24): "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". Assim vamos aos planos:

3.1 ATIVIDADE 1 - CHRYZODE

CONTEÚDOS:

Congruências, Comprimento de uma circunferência e Arco de uma circunferência.

OBJETIVO GERAL:

Exercitar ou revisar conteúdos matemáticos através de representações (Chryzodes) que permitem dar uma visão alternativa (uma imagem artística).

OBJETIVO ESPECÍFICO:

1. Calcular o perímetro de uma circunferência;
2. Reconhecer arco de circunferência e calcular seu comprimento;
3. Dividir uma circunferência em m partes iguais;
4. Calcular diferentes congruências;
5. Familiarizar-se com régua e compasso;
6. Potencializar a concentração;
7. Provocar/estimular a criatividade.

MATERIAIS NECESSÁRIOS:

- Cartolina ou papel A4, A3, A2, A1;
- Régua e compasso;
- Lápis, caneta, lápis de cor, giz de cera, canetinhas coloridas;
- Calculadora (opcional);
- Barbante.

METODOLOGIA:

Distribuir para os alunos ou grupos o Chryzode a ser desenhado, ou seja, multiplicação por a no módulo m. Em seguida seguir os passos abaixo:

- Com o compasso desenhar uma circunferência em um papel do tamanho que desejar;
- Calcular o comprimento[1]da circunferência pela fórmula $C = d\pi$, onde C é o comprimento da circunferência e d é o diâmetro da circunferência;

.

[1] Foge do escopo desse trabalho, relatar e demonstrar esse cálculo. Mas o leitor interessado poderá consultar (MARANGON, 2017)

- Dividir o comprimento da circunferência por *m*;
- Medir o barbante com o resultado acima e cortá-lo;
- Estipular o ponto 0 na circunferência e com o barbante cortado determinar os $(m-1)$ pontos;
- Resolver as congruências:

$$
\begin{aligned}
a \cdot 1 &\equiv b_1 \pmod{m};\\
a \cdot 2 &\equiv b_2 \pmod{m};\\
a \cdot 3 &\equiv b_3 \pmod{m};\\
&\vdots\\
a \cdot (m-2) &\equiv b_{m-2} \pmod{m};\\
a \cdot (m-1) &\equiv b_{m-1} \pmod{m}.
\end{aligned}
$$

- Ligar os pontos 1 com b_1, 2 com b_2, 3 com b_3, $\cdots$ e $m-1$ com b_{m-1}, formando assim o Chryzode.
- Depois de construído o Chryzode, preenche-lo da maneira que a criatividade mandar.

Abaixo construiremos em uma tábua cortada em forma circular, o Chryzode do Exemplo 2.1, onde *a* é igual a 2 e *m* é igual a 11.

Assim, medimos o diâmetro da tábua que deu 48,6cm, calculando a circunferência encontramos 152,68cm, dividindo esse valor por 11, encontramos que cada comprimento de arco é igual a 13,88cm. Após isso cortamos um barbante com essa medida e fizemos as marcações na tábua e em seguida pregamos um prego em cima de cada marcação.

Logo conforme os cálculos do Exemplo 2.1, amarramos um barbante de 1 à 2, de 2 à 4, de 3 à 6, de 4 à 8, de 5 à 10, de 6 à 1, de 7 à 3, de 8 à 5, de 9 à 7 e de 10 à 9.

O passo a passo e o resultado final pode ser conferido na Figura 76 à 85.

Na mesma tábua, porém no lado contrário construímos outro Chryzode com *a* igual a 25 e *m* igual a 20. O resultado final pode ser visualizado na Figura 86.

Nos apêndices, podemos visualizar alguns Chryzodes construídos por alunos do 9º ano, ao qual sou o professor regente.

Figura 76 – Linha de 1 à 2.

Fonte: O autor

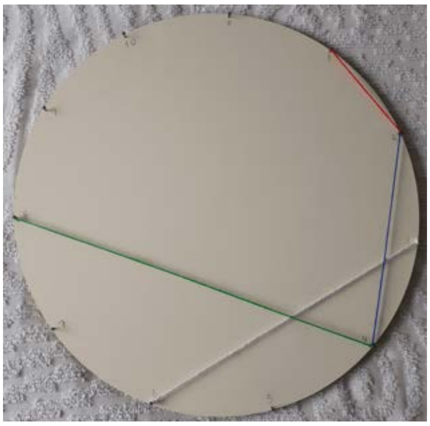
Figura 77 – Linha de 2 à 4.

Fonte: O autor

Figura 78 – Linha de 3 à 6.

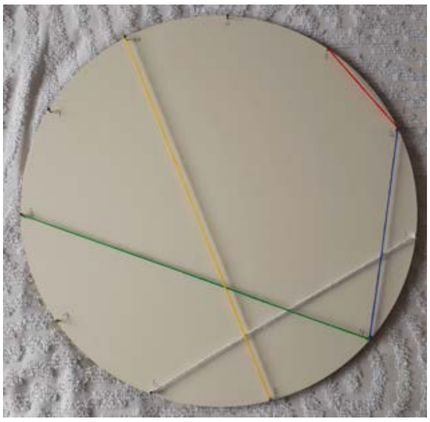
Fonte: O autor

Figura 79 – Linha de 4 à 8.



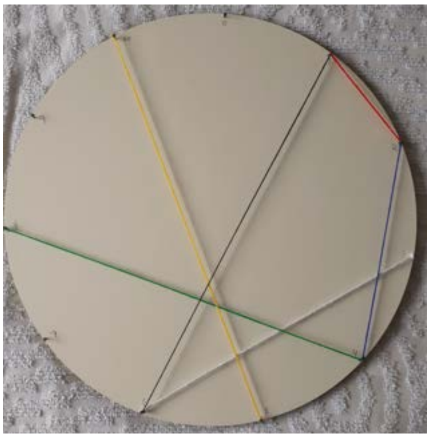
Fonte: O autor

Figura 80 – Linha de 5 à 10.



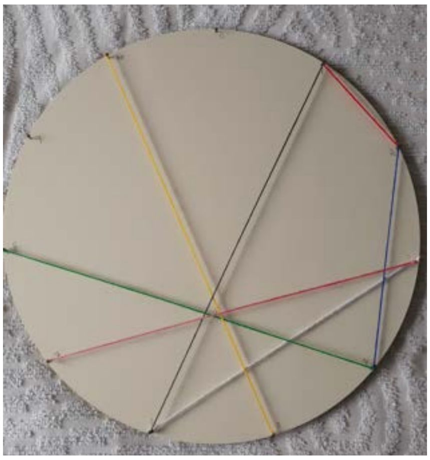
Fonte: O autor

Figura 81 – Linha de 6 à 1.



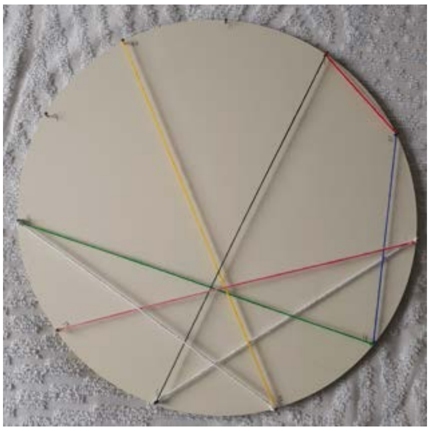
Fonte: O autor

Figura 82 – Linha de 7 à 3.



Fonte: O autor

Figura 83 – Linha de 8 à 5.

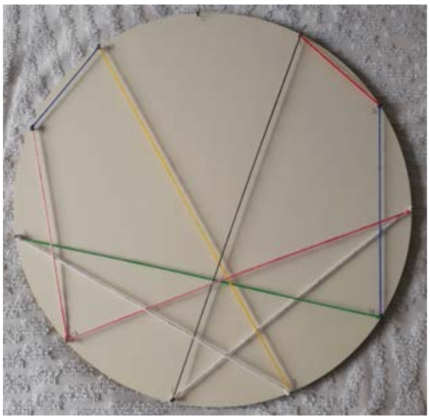


Fonte: O autor

Figura 84 – Linha de 9 à 7.

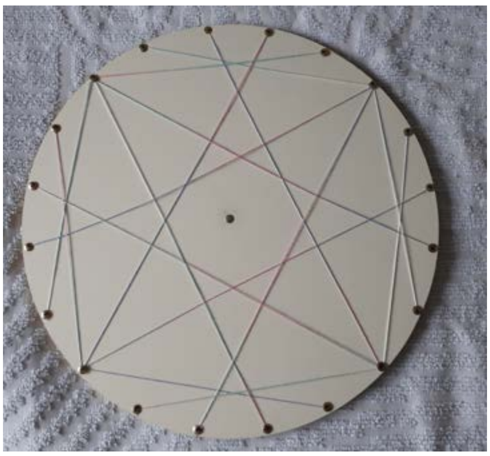
Fonte: O autor

Figura 85 – Linha de 10 à 9.



Fonte: O autor

Figura 86 – Chryzode multiplicação por 25 módulo 20



Fonte: O autor

3.2 ATIVIDADE 2 - QUEBRA-CABEÇA DE BOLICHE MÓDULO M

CONTEÚDOS:

Congruências.

OBJETIVO GERAL:

Propor de forma lúdica a resolução de problemas sobre congruência, com um conjunto de habilidades.

OBJETIVO ESPECÍFICO:

1. Estimular a aprendizagem;
2. Desenvolver a atenção e o pensamento lógico;
3. Revisar e ou exercitar os conceitos de congruências de maneira lúdica;
4. Modelar problemas com álgebra;
5. Desenvolver diferentes habilidades do pensamento como: observar, comparar, analisar e sintetizar.
6. Trabalhar o espírito competitivo;
7. Resolver exercícios de maneira lúdica.

MATERIAIS NECESSÁRIOS:

- Folhetos de quebra-cabeça (um por grupo);
- Lápis;
- Calculadora e papel de rascunho (opcional).

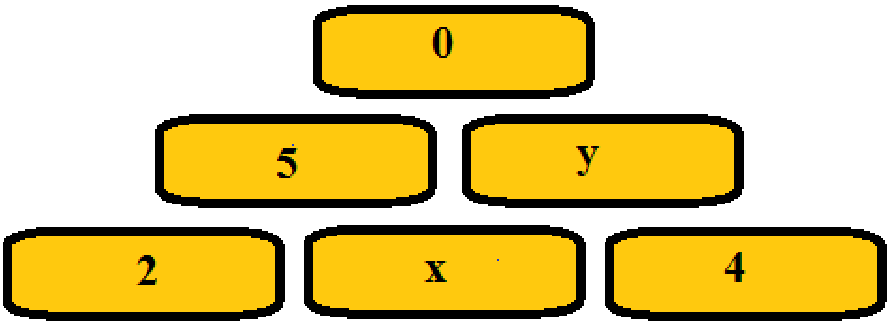
METODOLOGIA:

- Entregar para cada grupo um folheto por "rodada";
- Vence a rodada o grupo que entregar primeiro e corretamente o quebra-cabeça;
- Cada "rodada"valerá uma pontuação de acordo com o nível de dificuldade do quebra cabeça;

- Vence a equipe que conseguir mais pontos em todas as rodadas.

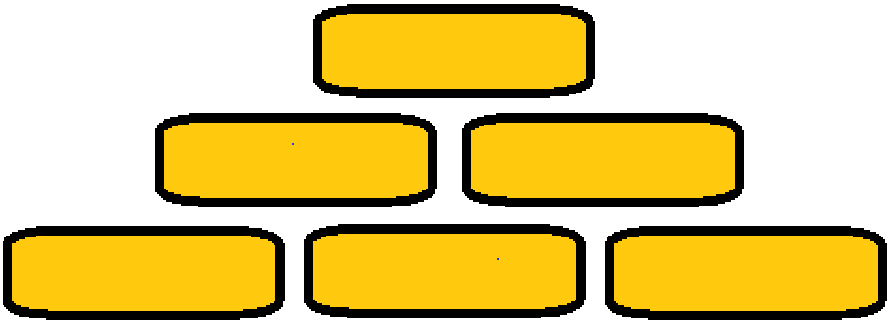
Abaixo segue alguns exemplos de pirâmides e quebra-cabeças de boliche módulo 6 e 10.

1. Encontre o valor de **x** e de **y**, na pirâmide abaixo:

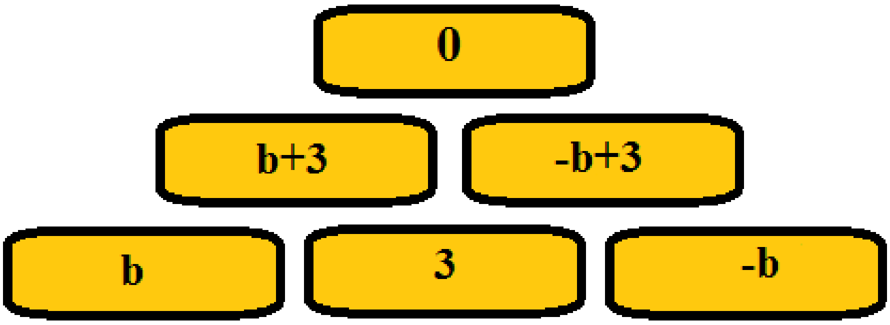


Solução: x = 3 e **y** = 1.

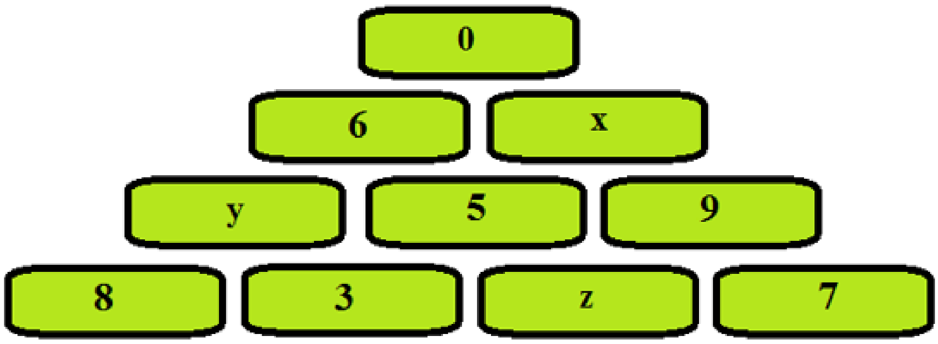
2. Generalize algebricamente a pirâmide abaixo, com uma incógnita. Tendo no topo da pirâmide o número zero.



Solução:

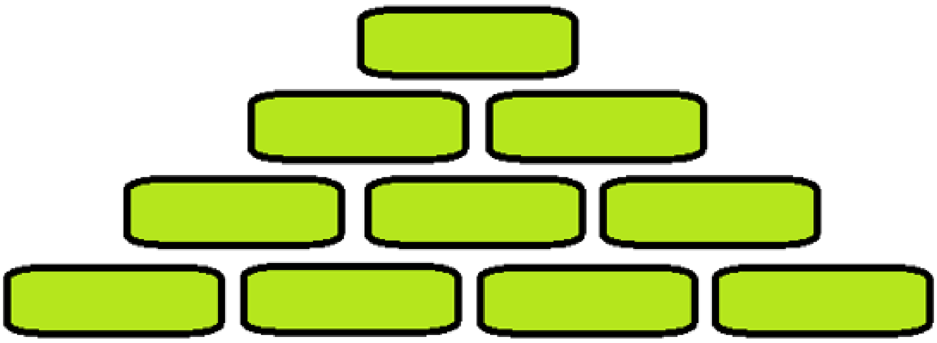


3. Encontre o valor de **x**, **y** e de **z** na pirâmide abaixo:

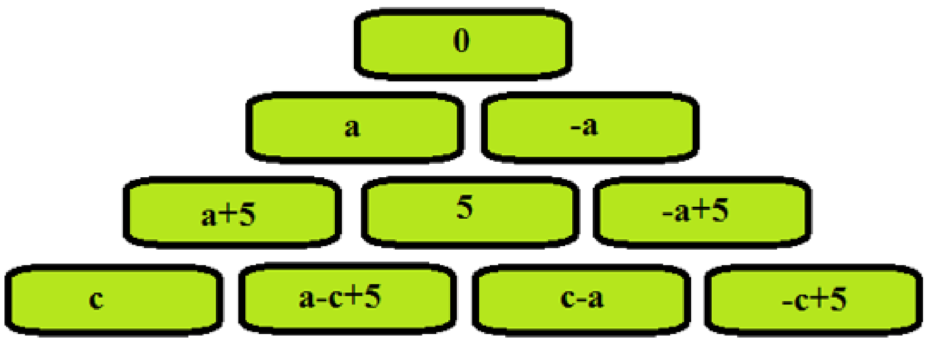


Solução: x =4, **y** = 1 e **z** = 2.

4. Generalize algebricamente a pirâmide abaixo, com duas incógnitas. Tendo no topo da pirâmide o número 0.



Solução:



3.3 ATIVIDADE 3 - NÚMEROS CRUZADOS

Todos nós conhecemos os enigmas das palavras cruzadas, usando pistas escrevemos palavras na horizontal e na vertical, onde preenchemos uma letra em cada quadradinho dentro de um quadrado grande. Assim, cada vez que se preenche uma palavra corretamente, você descobre letras de outras palavras que se cruzam.

Nesta atividade, em vez de preencher palavras, os alunos resolverão problemas de matemática e preencherão números nos quadradinhos, um algarismo por caixa. Então vamos lá.

CONTEÚDOS:

Números primos, Múltiplos, Divisores, MDC, MMC e Algoritmo de Euclides.

OBJETIVO GERAL:

Propor uma maneira lúdica a resolução de exercícios.

OBJETIVO ESPECÍFICO:

1. Estimular a aprendizagem;
2. Desenvolver a atenção e o pensamento lógico;
3. Despertar o raciocínio dedutivo;
4. Revisar e ou exercitar diferentes conteúdos de maneira lúdica;
5. Fixar conteúdos;
6. Desenvolver diferentes habilidades do pensamento como: observar, comparar, analisar e sintetizar.
7. Trabalhar o espírito competitivo;
8. Resolver exercícios de maneira lúdica.

MATERIAIS NECESSÁRIOS:

- Folhetos dos números cruzados a serem preenchidos (um por aluno ou um por grupo);
- Folhetos com os problemas para preencher os números cruzados (um por aluno ou um por grupo);

- Lápis (um por aluno);
- Calculadora e papel de rascunho (opcional).

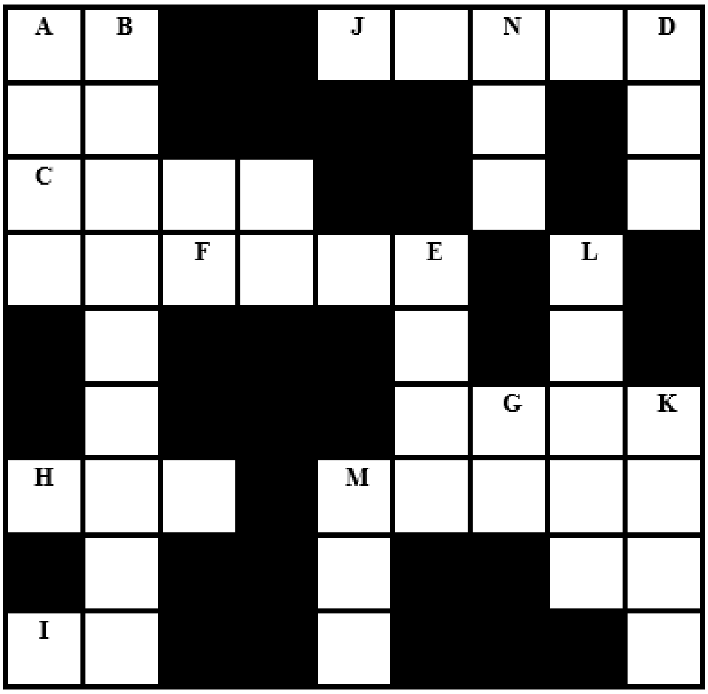
METODOLOGIA:

Esta atividade pode ser feita em grupos ou individual. Cada grupo ou estudante deve ter uma folha de problemas para resolver o quebra-cabeça. À medida que os alunos resolvam os problemas, eles vão preenchendo o quebra-cabeça numérico. Cada problema que eles solucionam lhes dará pelo menos um dígito da resposta de outro problema, assim os alunos saberão que possuem um erro se duas respostas que se sobrepõem possuem dígitos distintos no mesmo espaço. Se os alunos não conseguirem resolver algum problema (e consequentemente encontrar um número), eles poderão tentar alguns algarismos, descobrindo os números que se cruzam.

Cada quebra-cabeça possui um conjunto com vários problemas de diferentes níveis de dificuldade. Na nossa proposta de atividade temos um conjunto com 18 problemas, mas isso pode ser adaptado, assim como os conteúdos a serem abordados.

Abaixo segue uma atividade sobre Números Cruzados envolvendo os conteúdos vistos neste trabalho.

Números Cruzados



HORIZONTAIS	VERTICAIS
A - Dados os números A = $2^3 . 3^{10} . 5 . 7^2$ e B = $2^5 . 3 . 11$, encontre o *mdc*(A,B).	**A** – Qual é o mínimo múltiplo comum de 2, 3, 4, 5, 6, 7, 8 e 9 mais um?
B – Qual é o último algarismo do número 2^{50}?	**B** – Dados os números A = $2^8 . 5^3 . 7$ e B = $2^5 . 3 . 5^7$, encontre o *mmc*(A,B).
C - Qual é o múltiplo de 15 que mais se aproxima de 2009?	**D** – Qual é o único primo de três algarismos ao qual o primeiro e o último algarismo são iguais e está compreendido entre 100 e 150?
D – Encontre o resto da divisão de 2^{100} por 3?	**E** – Encontre um número de quatro algarismos que é um quadrado perfeito, onde os dois primeiros algarismos são iguais e os dois últimos algarismos também são iguais.
F - Qual é o maior produto possível de quaisquer dois números primos distintos menores de 40?	**G** – Qual é o dobro do mínimo múltiplo comum de 10 e 15?
H - Qual é a soma dos dois maiores fatores de 231?	**L** - A soma de quatro números inteiros consecutivos pares é 596. Qual é o produto do menor e do maior desses números inteiros?
I - Qual é o menor inteiro positivo que é divisível por 2, 5, 6 e 9?	**K** - Qual é o maior número de quatro dígitos divisível por 12?
J - Euclides escolhe um inteiro positivo de dois dígitos, adiciona 200 e eleva ao quadrado o resultado. Qual é o maior número que Euclides pode obter?	**M** - Qual é o maior número primo de três dígitos que pode ser formado usando cada um dos dígitos 1, 2 e 7 exatamente uma vez?
M – Qual é o triplo de 8000 mais o triplo de 33?	**N** – O número primo entre 62 e 70, multiplicado pelos dois primeiros primos é igual a quanto?

A atividade acima possui como solução o seguinte quebra-cabeça:

A 2	B 4			J 8	9	N 4	0	D 1
5	2					0		3
C 2	0	1	0			2		1
1	0	F 1	1	4	E 7		L 2	
	0				7		2	
	0				4	G 6	1	K 9
H 3	0	8		M 2	4	0	9	9
	0			7			2	9
I 9	0			1				6

3.4 ATIVIDADE 4 - RESOLUÇÃO DE EXERCÍCIOS

CONTEÚDOS:

Números primos, Divisibilidade, MDC, MMC, Algoritmo de Euclides e Equações diofantinas lineares.

OBJETIVO GERAL:

Estudar e fixar as propriedades dos números inteiros junto com as suas operações, enfatizando as questões relacionadas com a divisibilidade. Definir as equações diofantinas lineares e desenvolver o método de tentativa e erro e encontrar suas soluções gerais.

OBJETIVO ESPECÍFICO:

1. Perceber as diferentes formas de utilização dos números no cotidiano;
2. Perceber a importância dos números na vida do ser humano;
3. Utilizar o dispositivo prático para encontrar o m.m.c. entre dois ou mais números;
4. Economizar tempo e cálculos utilizando os critérios de divisibilidade;

5. Conceituar o número primo;
6. Encontrar divisores de um número natural e o m.d.c. entre os dois ou mais números naturais, aplicando esse conhecimento na resolução de problemas;
7. Escrever números naturais como produto de fatores primos;
8. Identificar o menor número que é múltiplo de dois outros e suas aplicações;
9. Registrar conclusões usando a linguagem matemática adequadamente;
10. Conceituar equações diofantinas lineares;
11. Fazer com que o aluno pense nas possíveis soluções das equações apresentadas;
12. Resolver equações com duas incógnitas;
13. Analisar se uma equação diofantina linear tem solução;
14. Encontrar as possíveis soluções das equações diofantinas lineares;
15. Encontrar a solução minimal das equações diofantinas lineares;
16. Resolução de exercícios com aplicação das equações diofantinas lineares;
17. Generalizar uma forma de resolver equações diofantinas lineares.

METODOLOGIA:

O professor deverá iniciar sua aula motivando os alunos a quererem aprender matemática, mais especificamente a Aritmética. Depois que o aluno estiver motivado, empolgado e curioso o professor deve abordar os conteúdos de números primos, múltiplos, divisores, MDC, MMC, algoritmo de Euclides e equações diofantinas lineares. Tais conteúdos podem ser definidos conforme foi visto no primeiro capítulo deste trabalho.

Definidos e entendidos estes conceitos, os alunos terão conhecimento para resolver os exercícios abaixo da melhor maneira que o professor julgar.

Exercicío 1. *Encontrar os divisores dos números 15, 18 e 40.*

Exercicío 2. *Encontrar o máximo divisor comum entre 32 e 58.*

Exercicío 3. *Encontrar o quociente e o resto da divisão de 550 por 20.*

Exercicío 4. *Escreva os números 24, 120 e 169 na forma de fatores primos.*

Exercicío 5. *Quais são os 10 primeiros múltiplos de 12.*

Exercicío 6. *Determinar o mínimo múltiplo comum entre 64 e 80.*

Exercicío 7. *Verifique se 189 é divisível por 8.*

Exercicío 8. *Qual é o maior múltiplo de 13 menor que 500?*

Exercicío 9. *Achar os elementos do conjunto A =* $\{1; 2; 3; 4; 5\}$ *que são primos com 15.*

Exercicío 10. *O número 923 é um número primo?*

Exercicío 11. *Decomponha o número 432 em fatores primos.*

Exercicío 12. *A fatoração completa do número 1800 é* $2^a \cdot 3^b \cdot 5^c$*. Qual é o valor de* $a + b + c$*?*

Exercicío 13. *Seja o conjunto A =* $\{1; 2; 3; 4; 5; 6\}$*. Enumerar os elementos do conjunto X =* $\{x \in A | mdc(x; 12) = 1\}$.

Exercicío 14. *Em uma viagem da turma do 6º ano, para o Instituto de Matemática Pura e Aplicada (IMPA) no RJ, podemos contar os alunos de 8 em 8 ou de 10 em 10. Quantos alunos haviam na viajem?*

Exercicío 15. *O relógio de Luiz bate a cada 15 minutos, o relógio de Mariana a cada 25 minutos, e o relógio de Carlos bate a cada 40 minutos. Qual é, em horas, o menor intervalo de tempo decorrido entre duas batidas simultâneas dos três relógios?*

Exercicío 16. *Para fazer uma bandeira, Jair precisa de 30 m de fita verde e 24 m de fita amarela. Porém ele quer cortar essas fitas de modo que os pedaços tenham o mesmo tamanho, que sejam o maior tamanho possível e que não sobre pedaços da fita. Quantos metros deve ter cada pedaço de fita?*

Exercicío 17. *Achar o maior inteiro positivo pelo qual se devem dividir os inteiros 160, 198 e 370 para que os restos sejam respectivamente 7, 11 e 13.*

Exercicío 18. *Usando o método de tentativa e erro, encontre algumas soluções para as equações a seguir:*

1. $X + 3Y = 5$;
2. $12X + 7Y = 9$;
3. $2X + Y = 6$;
4. $4X + 6Y = 3$;
5. $30X + 17Y = 201$;
6. $2X + 3Y + 5Z = 11$.

Exercicío 19. *Maria e João receberam R\$ 10,00 de seus pais para comprar picolés. Cada picolé de água custa R\$2,00 e cada picolé de creme custa R\$3,00. Quais são as possíveis combinações de picolés que eles podem comprar gastando todo o dinheiro? E se tivessem recebido R\$15,00?*

Exercicío 20. *Uma sorveteria vende sorvetes de uma bola por R\$2,00 e de duas bolas por R\$3,00. Se as sobrinhas de dona Maria comprarem R\$48,00 em sorvetes, quais as possíveis combinações dos sorvetes de uma bola e dos sorvetes de duas bolas?*

Exercicío 21. *Uma caixa contém formigas e aranhas. Sabendo que existem 46 patas na caixa, quantos são as formigas e quantas são as aranhas, sabendo que as formigas têm seis patas e as aranhas têm oito patas?*

Exercicío 22. *Divida R\$100,00 em 2 parcelas, de modo que uma seja múltiplo de sete e a outra de onze .*

Exercicío 23. *Verificar se as equações abaixo apresentam ou não soluções inteiras.*

1. $X + 3Y = 5$;
2. $2X + 5Y = 8$;
3. $8X + 13Y = 23$.

Exercicío 24. *Encontrar as soluções particulares e gerais para a Equação Diofantina* $69X + 111Y = 9000$.

Exercicío 25. *Explique porque as equações podem ou não ter soluções inteiras, e caso tenham solução, encontrá-las.*

1. $15X + 27Y = 1$;
2. $5X - 6Y = -1$;
3. $15x - 51y = 41$;
4. $5X + 6y = 1$;
5. $2X + 3Y = 4$;
6. $3X + 5y = 7$;
7. $3X - 12Y = 7$;
8. $1900X - 173Y = 11$;
9. $21X + 48Y = 6$

Exercicío 26. *Determinar todas as soluções inteiras e positivas das seguintes Equações Diofantinas Lineares:*

1. $15x + 16y = 17$;
2. $6x + 15y = 51$.

Exercicío 27. *Suponha que existam notas de R$10,00 e de R$13,00. Como podemos pagar uma conta de R$107,00 com essas notas?*

Exercicío 28. *(Retirando de (VANSAN, 2014)) Encontrar todos os números inteiros N, tais que o resto da divisão de N por 37 é 9, e o resto da divisão de N por 52 é 15.*

Exercicío 29. *(Retirando de (VANSAN, 2014)) Determinar o menor inteiro positivo que dividido por 8 e por 15 deixa os restos 6 e 13, respectivamente.*

Exercicío 30. *(Retirado de (HEFEZ, 2016b)) Resolva o sistema de equações diofantinas:*

$$\begin{cases} 6X - Y + 5Z = 3 \\ 2X + Y - Z = 9 \end{cases}$$

Exercicío 31. *(Retirando de (VANSAN, 2014)) Um pato pode ser comprado por 5 reais, uma galinha por 1 real, e 20 codornas por 1 real. Você possui 100 reais e deseja comprar 100 aves. Quantas aves de cada tipo você pode adquirir?*

Exercicío 32. *(Retirando de (VANSAN, 2014)) Quando 100 quilogramas de grãos são distribuídos entre 100 pessoas de modo que cada homem recebe 3 quilogramas, cada mulher recebe 2 quilogramas, e cada criança recebe meio quilograma, quantos homens, mulheres e crianças haviam?*

4 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo, apresentar aplicações da Aritmética Modular na educação básica, conforme nos sugere a Base Nacional Comum Curricular, que tem como uma de suas finalidades, no ensino/aprendizado da matemática, o despertar da curiosidade dos alunos com problemas interessantes e que estejam relacionadas de situações concretas do seu dia-a-dia.

Assim, sabendo das diversas dificuldades presentes no ensino da matemática, procuramos desenvolver técnicas de aulas mais atrativas, através de assuntos relacionados com a Aritmética Modular que provoquem a curiosidade ou que estejam ligados diretamente no cotidiano dos alunos como é o caso do Relógio, Chryzodes e Quebra-Cabeça (que são aplicações de Congruências), Calendário (que é uma aplicação do Teorema Chinês dos Restos), Enigmas (que é uma aplicação de Equações Diofantinas Lineares com duas variáveis) e Jogo de Dardos (que é uma aplicação das Equações Diofantinas de duas e três variáveis). Além de propor um método de atividade que visa despertar o interesse dos alunos na resolução de exercícios que é o caso dos números cruzados, que podem ser adaptados para qualquer conteúdo matemático.

Também foi apresentada outra técnica para se calcular o Máximo Divisor Comum *(MDC)* pelo Algoritmo Binário de Euclides, que se utiliza de operações aritméticas mais simples para o cálculo do *MDC* de dois números inteiros.

Foram usadas e indicadas ferramentas computacionais para desenvolver a atividade dos Chryzodes. Ao qual serviram para dar uma noção de como a tecnologia pode nos ser útil em sala de aula. Sendo assim, sugere-se ao professor que busque outros *softwares* para que possa, de maneira eficaz, estimular o ensino/aprendizagem da matemática através da sua interação com outras áreas do conhecimento.

Espera-se que as atividades propostas neste trabalho, sejam o ponta-pé inicial para que o professor busque outras formas de explanação dos conteúdos relacionados à Aritmética Modular, pois ao inserirmos novos métodos de ensino, a matemática se torna cada vez mais atrativa.

> ··· é preciso tornar os alunos pessoas capazes de enfrentar situações e contextos variáveis, que exijam deles a aprendizagem de novos conhecimentos e habilidades. Por isso, os alunos que hoje aprenderem a aprender estarão, previsivelmente, em melhores condições de adaptar-se às mudanças culturais, tecnológicas e profissionais que nos aguardam na virada do milênio. (POZO, 1998, p.9)

Diante de tudo, percebemos a importância da Aritmética Modular e por isso acreditamos que esse ramo da Matemática, poderia ser enfatizado na educação básica, pois permite exercitar o raciocínio lógico-dedutivo, com diferentes graus de dificuldade. Abrindo espaço a cada atividade proposta, a introdução de outras atividades com um grau mais elevado de dificuldade, dessa forma o aluno é instigado a pensar e rever estratégias para tentar resolver estas atividades, as quais podem desenvolver potencialidades tanto na interpretação de situações problema, como na organização dos dados o que acarreta uma melhora no seu desempenho dentro e fora de sala de aula.

Portanto, esperamos que este trabalho sirva como material de apoio para os professores no ensino/aprendizagem da Aritmética Modular em suas aulas. Entendemos e sabemos da dificuldade de se mudar a estrutura curricular do ensino básico, mas a ideia é que esses assuntos da Aritmética Modular possam ter maior ênfase no currículo da educação básica.

REFERÊNCIAS

AMILMIUQ. **Mensagens Bíblicas Redentoras**. 2013. Disponível em: <https://mensagensbiblicasredentoras.wordpress.com/2013/12/02/o-sabado-no-calendario-juliano-e-gregoriano/>. Acesso em: 17 dez. 2018. 58

BELLO, M. G. **LA ARITMÉTICA MODULAR Y ALGUNAS DE SUS APLICACIONES**. Dissertação (MAESTRIA EN ENSEÑANZA DE LAS CIENCIAS EXACTAS Y NATURALES) — Universidad Nacional de Colombia, 2011. 51

BOGOMOLNY, A. **Binary Euclid's Algorithm**. [S.l.], 2018. Disponível em: <https://www.cut-the-knot.org/blue/binary.shtml>. Acesso em: 28 fev. 2019. 27

BRASIL, S. d. E. F. **Parâmetros curriculares nacionais - Apresentação dos temas tranversais e ética**. Brasília: MEC/SEF, 1997. Disponível em: <http://portal.mec.gov.br/seb/arquivos/pdf/livro081.pdf>. Acesso em: 16 maio 2019. 14

BRASIL, S. d. E. F. **Parâmetros curriculares nacionais - Matemática**. Brasília: MEC/SEF, 1998. Disponível em: <http://portal.mec.gov.br/seb/arquivos/pdf/matematica.pdf>. Acesso em: 10 out. 2018. 14, 15, 50, 92

CAVALCANTI, T. J. B. **“La Zona Maya no es museo Etnográfico, sino pueblos en marcha": Introdução ao "Calendário Maia"e à diversidade Pan-Maia na Mesoamérica**. Dissertação (Curso de Graduação em Antropologia) — Universidade Federal Fluminense, 2014. Disponível em: <http://acervomesoamericano.org/bitstream/handle/AM/38/CAVALCANTI2014.pdf?sequence=3&isAllowed=y>. Acesso em: 11 Dez. 2018. 59, 60, 61

CHOW, C. C. **Darts and Diophantine equations**. 2009. Disponível em: <https://sciencehouse.wordpress.com/2009/10/24/darts-and-diophantine-equations/>. Acesso em: 04 abril. 2019. 51

DELGADO, J. **Math Circle Lesson Bowling Pin Puzzle**. [S.l.], 2019. Disponível em: <http://math.sfsu.edu/cm2/papers/JessicaDelgado_termpaper_Final.pdf>. Acesso em: 30 jan. 2019. 51

DOMINGUES, H. H. **Fundamentos de Aritmética**. Florinópolis: UFSC, 2009. 17

EUGENESERGEEV. **Calendario Solar**. 2012. Disponível em: <https://pt.dreamstime.com/foto-de-stock-calend%C3%A1rio-solar-antigo-image28296700>. Acesso em: 17 dez. 2018. 56

HEFEZ, A. **Aritmética**. Rio de Janeiro: SBM, 2016. 16, 17

HEFEZ, A. **Exercícios Resolvidos de Aritmética**. Rio de Janeiro: SBM, 2016. 108

IMAGENS, G. **Café em forma de coração**. 2018. Disponível em: <https://pt.depositphotos.com/88814800/stock-photo-a-cup-of-coffee-with.html>. Acesso em: 31 jan. 2019. 68

IMAGENS, G. **Microfone Cardioide**. 2019. Disponível em: <https://www.google.com/search?q=microfone+cardioide&rlz=1C1GCEA_enBR757BR757&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiC9oyio5bgAhVNLLkGHR0SAyAQ_AUIDigB&biw=1366&bih=657>. Acesso em: 17 dez. 2018. 68

MARANGON, M. D. **O número** Π. Dissertação (PROFMAT) — Universidade Federal de Juiz de Fora, 2017. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=160390774>. Acesso em: 23 abril. 2019. 93

MARTÍNEZ, A. R. **Números y hoja de cálculo: Algoritmo de Euclides binario**. [S.l.], 2013. Disponível em: <http://hojaynumeros.blogspot.com/2013/03/algoritmo-de-euclides-binario.html>. Acesso em: 28 fev. 2019. 27

MATHEMATICS, T. C. for EDUCATION in; COMPUTING. **Intermediate Math Circles**. 2012. Disponível em: <https://cemc.math.uwaterloo.ca/events/mathcircles/2011-12/Winter/Intermediate_Feb29-Solns.pdf>. Acesso em: 25 mar. 2019. 51

MEDRANO Álvaro A. **El maravilloso mundo de las congruencias modulares y sus aplicaciones**. Costa Rica: [s.n.], 2013. Disponível em: <https://pt.calameo.com/books/002628221ee0ab06cf7f1>. Acesso em: 13 Dez. 2018. 51

MENDES, L. M. da C. **A IMPORTÂNCIA DO LÚDICO NO ENSINO DA MATEMÁTICA**. [S.l.], 2011. Disponível em: <http://www.lambaridoeste.mt.gov.br/secretarias/educacao-e-cultura/artigos-dos-professores/59/view/630>. Acesso em: 28 jan. 2019. 73

MORAES, M. M. de. **Análise de Erros em Problemas de Aritmética:**: Uma abordagem na 2a fase da obmep no oeste do pará. Dissertação (PROFMAT) — Universidade Federal de São João Del Rei, 2018. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=160040897>. Acesso em: 05 fev. 2019. 92

MORGANA, N. e. a. **Diofato de Alexandria**. 2012. Disponível em: <http://amatematicagrega.blogspot.com/2012/01/diofanto-de-alexandria.html>. Acesso em: 10 nov. 2018. 33

NETWORKS, I. S. **History of the Calendar**. [S.l.], 2000. Disponível em: <https://www.infoplease.com/calendar-holidays/calendars/history-calendar>. Acesso em: 10 Dez. 2018. 56

OLIVEIRA, F. G. de. **Psicologia da educação e da aprendizagem**. Indaial: Uniasselvi, 2014. 14

POZO, J. I. **A Solução de problemas: Aprender a resolver, resolver para aprender**. Porto Alegre: [s.n.], 1998. 109

REIS, M. V. dos. **Conjunto de Mandelbrot**. Dissertação (PROFMAT) — Universidade Federal de Goiás, 2016. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=95006>. Acesso em: 17 jan. 2019. 67

SANTANA, N. A. d. S. **Pensamento aritmético e sua importância para o ensino de matemática**. Minas Gerais, 2016. Disponível em: <http://www.ufjf.br>. Acesso em: 10 out. 2018. 49

SANTOS, J. P. d. O. **Introdução à Teoria dos Números**. Rio de Janeiro: IMPA, 2014. 17

VANSAN, A. H. **EQUAÇÕES DIOFANTINAS: UM PROJETO PARA A SALA DE AULA E O USO DO GEOGEBRA**. Dissertação (PROFMAT) — UNIVERSIDADE ESTADUAL DE MARINGÁ, 2014. Disponível em: <https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?id=61>. Acesso em: 11 fev. 2019. 108

WIKIPEDIA. **Euclides**. 2018. Disponível em: <https://pt.wikipedia.org/wiki/Euclides>. Acesso em: 30 jan. 2019. 20

WIKIPEDIA. **Carl Friedrich Gauss**. 2019. Disponível em: <https://pt.wikipedia.org/wiki/Carl_Friedrich_Gauss>. Acesso em: 30 jan. 2019. 38

ÁVILA. Euclides, geometria e fundamentos. Revista do Professor de Matemática, 45, 2001. Disponível em: <http://www.educadores.diaadia.pr.gov.br/arquivos/File/2010/veiculos_de_comunicacao/RPM/RPM45/RPM45_01.PDF>. Acesso em: 13 out. 2018. 20

5 APÊNDICES

Aqui veremos alguns trabalhos sobre Chryzodes desenvolvidos por alguns alunos do 9º ano do ensino fundamental. Neles podemos perceber a importância das habilidades com régua, compasso e lápis além das habilidades de concentração e criatividade.

Podemos perceber também que alguns erros acontecem e cabe ao professor corrigir antes que seja tarde de mais. Que é o caso das figuras 96, 97 e 98, onde os alunos dividiram a circunferência de 0 à 72, e o correto seria de 0 à 71, e na figura 99, em que os alunos ligaram erroneamente o ponto 0 ao ponto 5. Mesmo erro que ocorre na figura 100, a qual os alunos ligam o número 22 com o número 24. Erros que não comprometem a beleza dos trabalhos.

Figura 87 – Multiplicação por 2 módulo 39

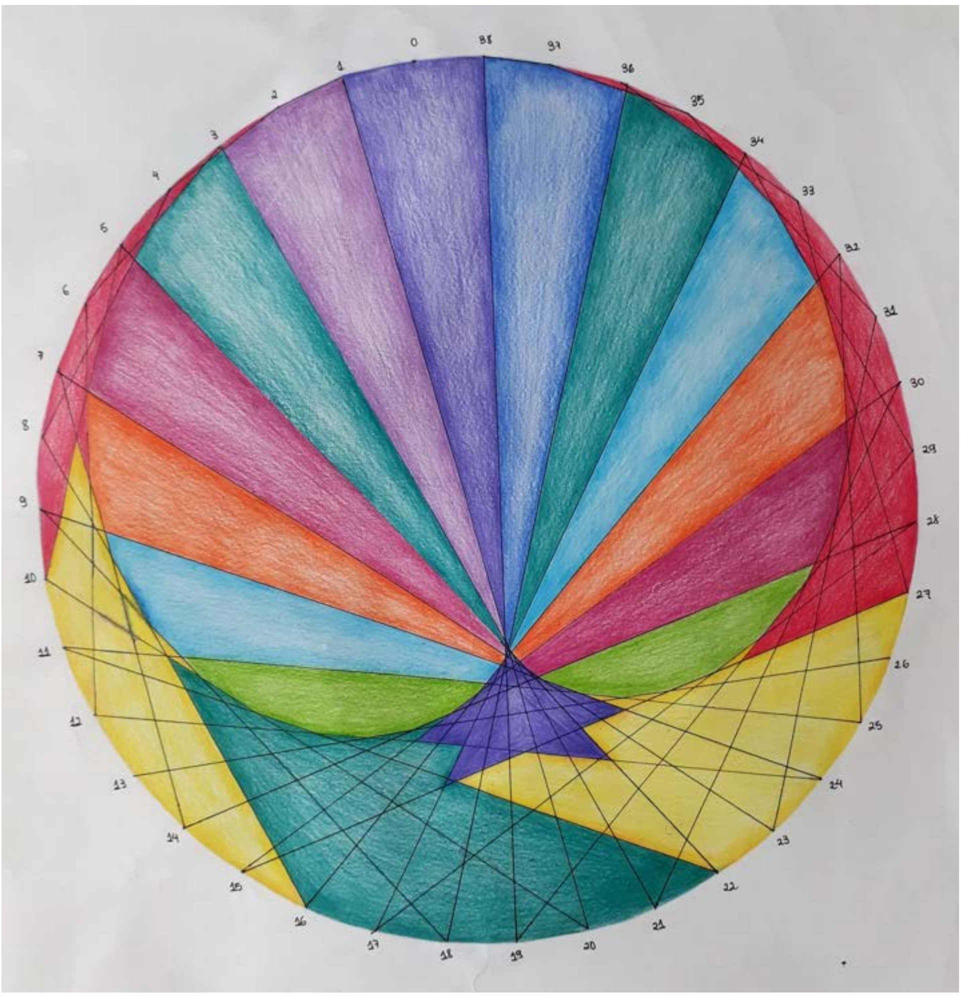


Figura 88 – Multiplicação por 16 módulo 50

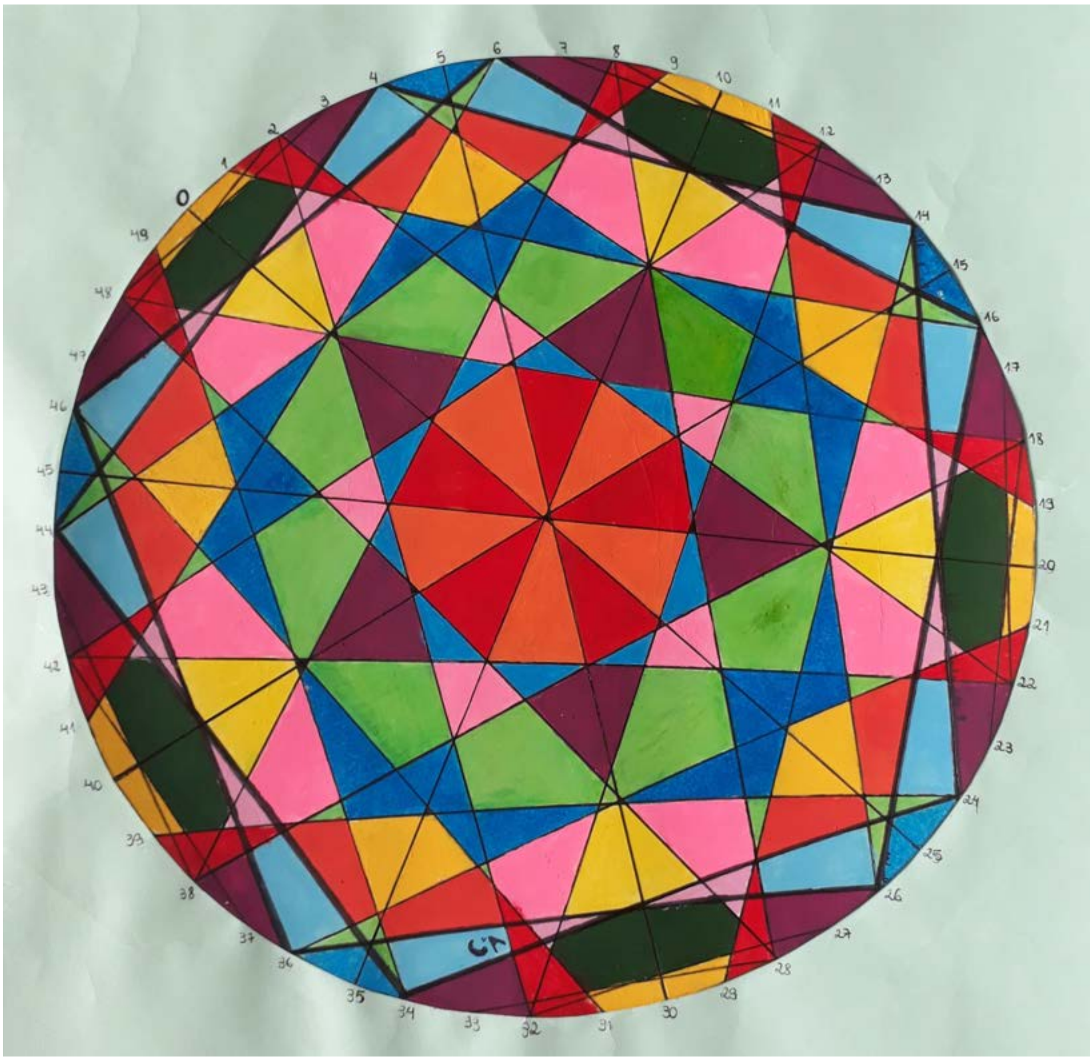


Figura 89 – Multiplicação por 16 módulo 50

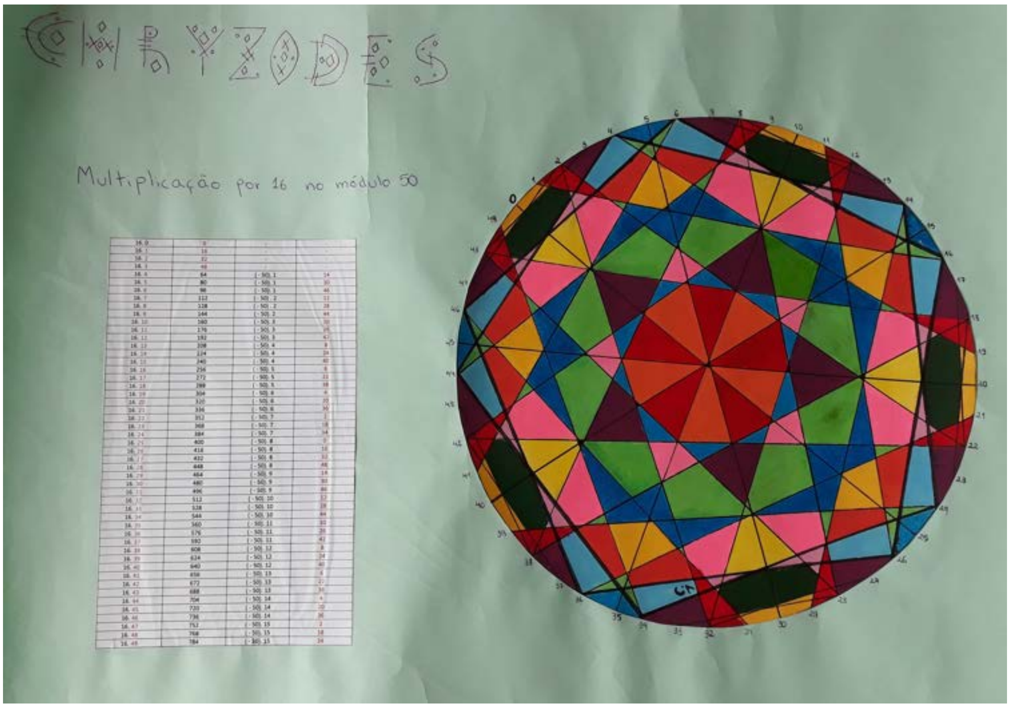
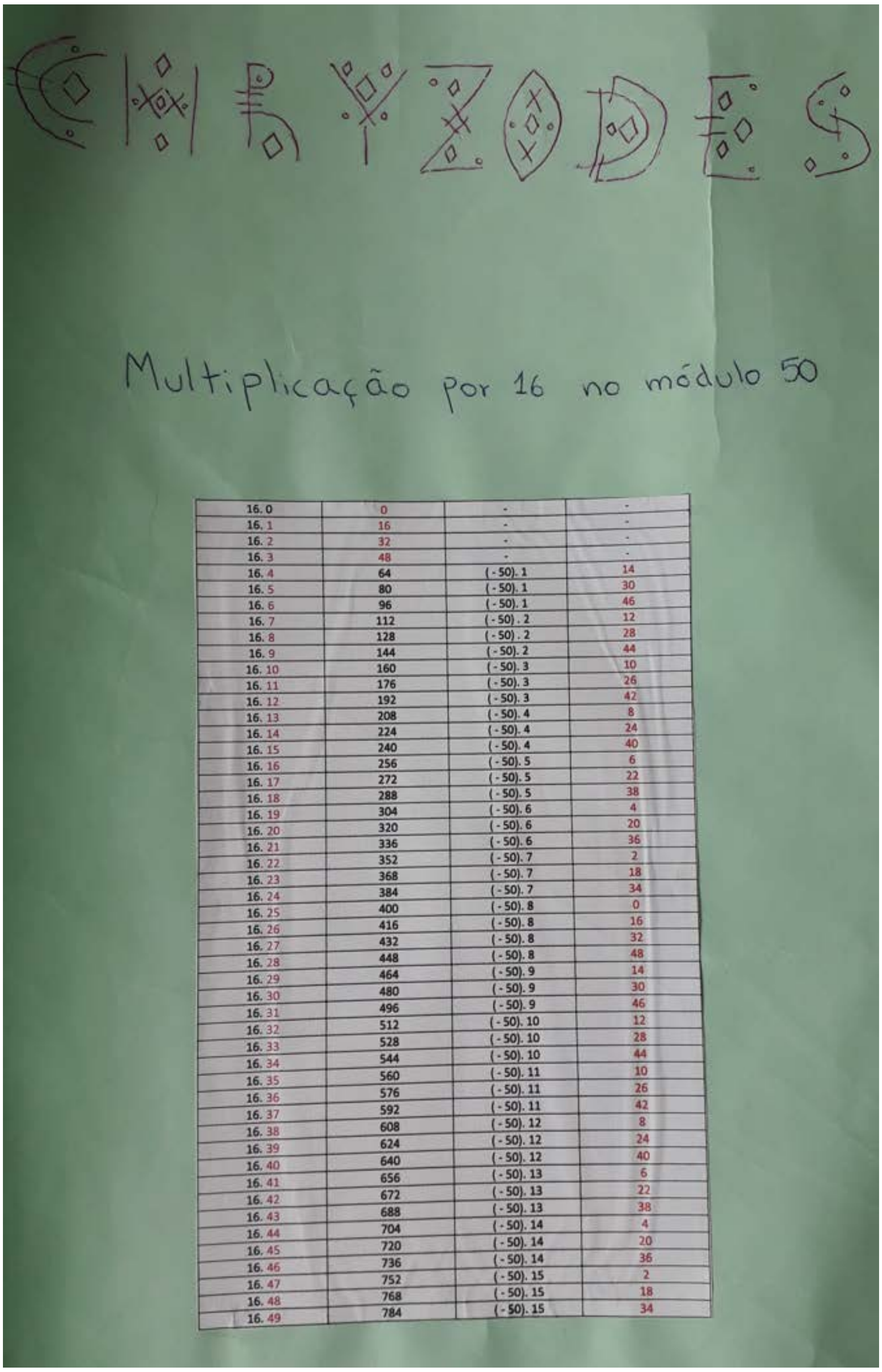


Figura 90 – Multiplicação por 16 módulo 50



16. 0	0	-	-
16. 1	16	-	-
16. 2	32	-	-
16. 3	48	-	-
16. 4	64	(- 50). 1	14
16. 5	80	(- 50). 1	30
16. 6	96	(- 50). 1	46
16. 7	112	(- 50) . 2	12
16. 8	128	(- 50) . 2	28
16. 9	144	(- 50). 2	44
16. 10	160	(- 50). 3	10
16. 11	176	(- 50). 3	26
16. 12	192	(- 50). 3	42
16. 13	208	(- 50). 4	8
16. 14	224	(- 50). 4	24
16. 15	240	(- 50). 4	40
16. 16	256	(- 50). 5	6
16. 17	272	(- 50). 5	22
16. 18	288	(- 50). 5	38
16. 19	304	(- 50). 6	4
16. 20	320	(- 50). 6	20
16. 21	336	(- 50). 6	36
16. 22	352	(- 50). 7	2
16. 23	368	(- 50). 7	18
16. 24	384	(- 50). 7	34
16. 25	400	(- 50). 8	0
16. 26	416	(- 50). 8	16
16. 27	432	(- 50). 8	32
16. 28	448	(- 50). 8	48
16. 29	464	(- 50). 9	14
16. 30	480	(- 50). 9	30
16. 31	496	(- 50). 9	46
16. 32	512	(- 50). 10	12
16. 33	528	(- 50). 10	28
16. 34	544	(- 50). 10	44
16. 35	560	(- 50). 11	10
16. 36	576	(- 50). 11	26
16. 37	592	(- 50). 11	42
16. 38	608	(- 50). 12	8
16. 39	624	(- 50). 12	24
16. 40	640	(- 50). 12	40
16. 41	656	(- 50). 13	6
16. 42	672	(- 50). 13	22
16. 43	688	(- 50). 13	38
16. 44	704	(- 50). 14	4
16. 45	720	(- 50). 14	20
16. 46	736	(- 50). 14	36
16. 47	752	(- 50). 15	2
16. 48	768	(- 50). 15	18
16. 49	784	(- 50). 15	34

Figura 91 – Multiplicação por 2 módulo 30

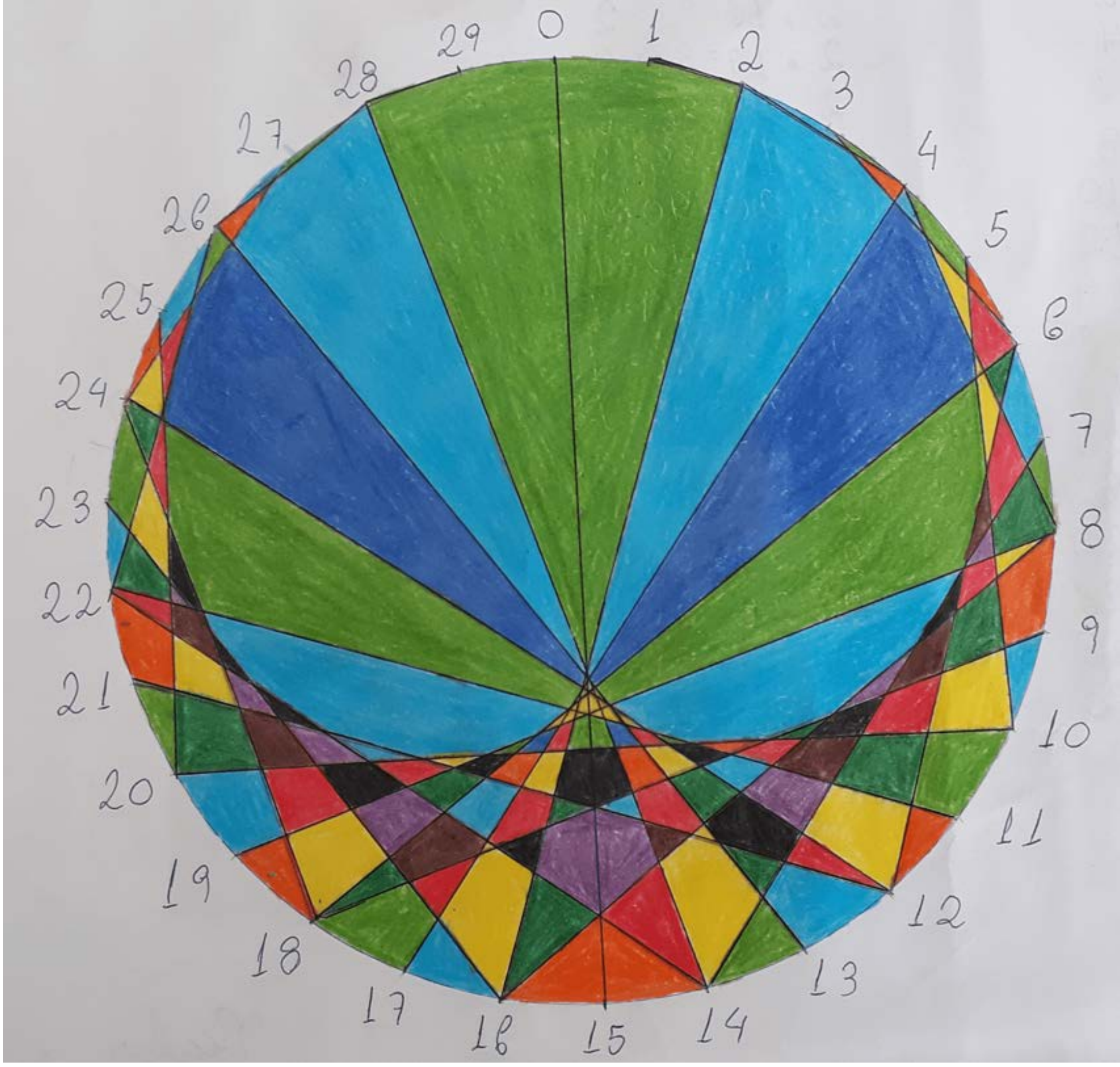


Figura 92 – Multiplicação por 4 módulo 40

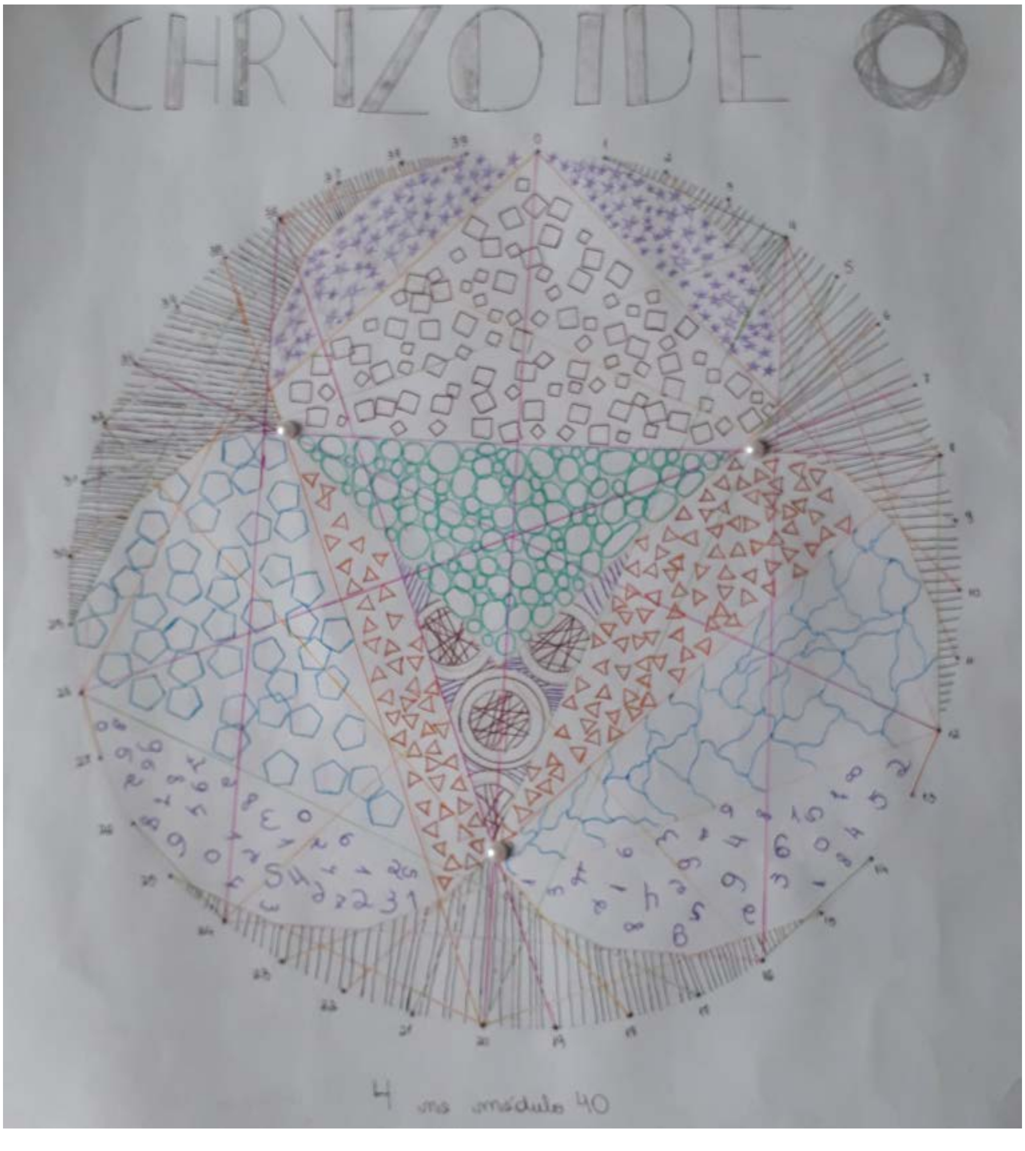


Figura 93 – Multiplicação por 3 módulo 10

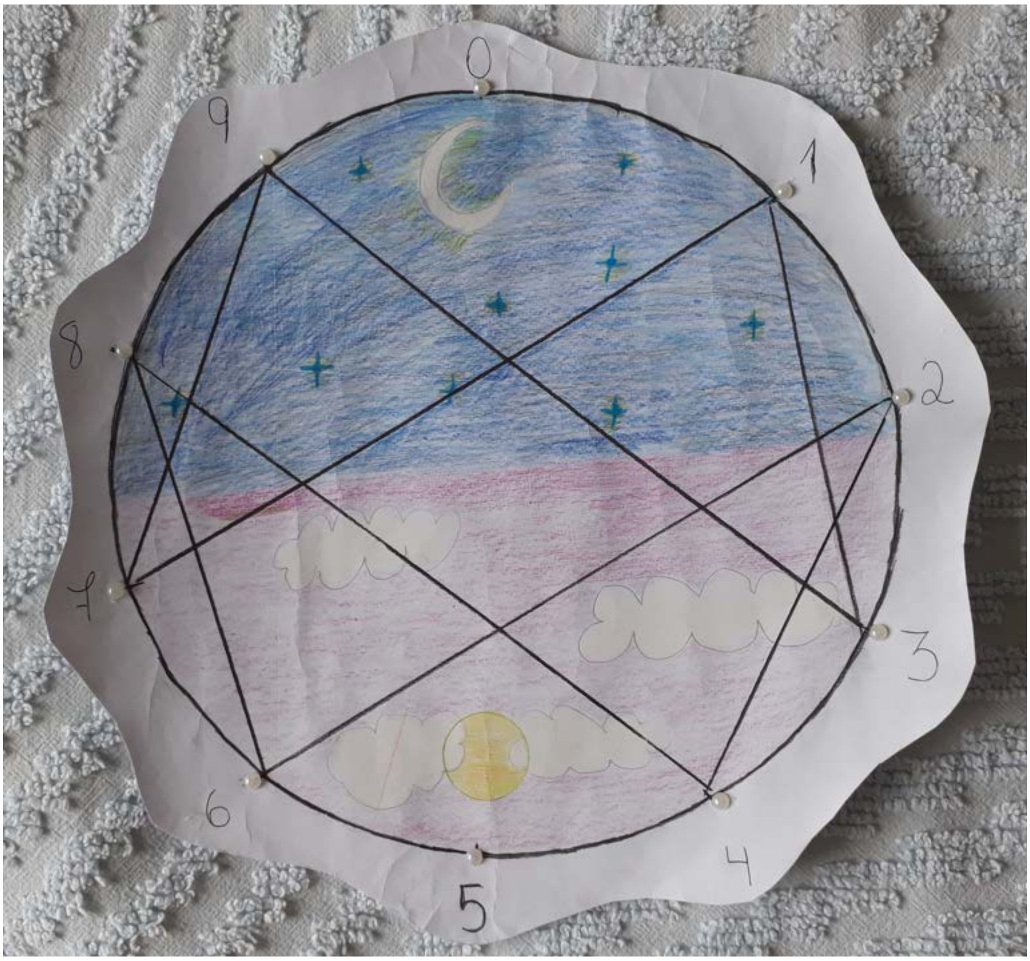


Figura 94 – Multiplicação por 3 módulo 10

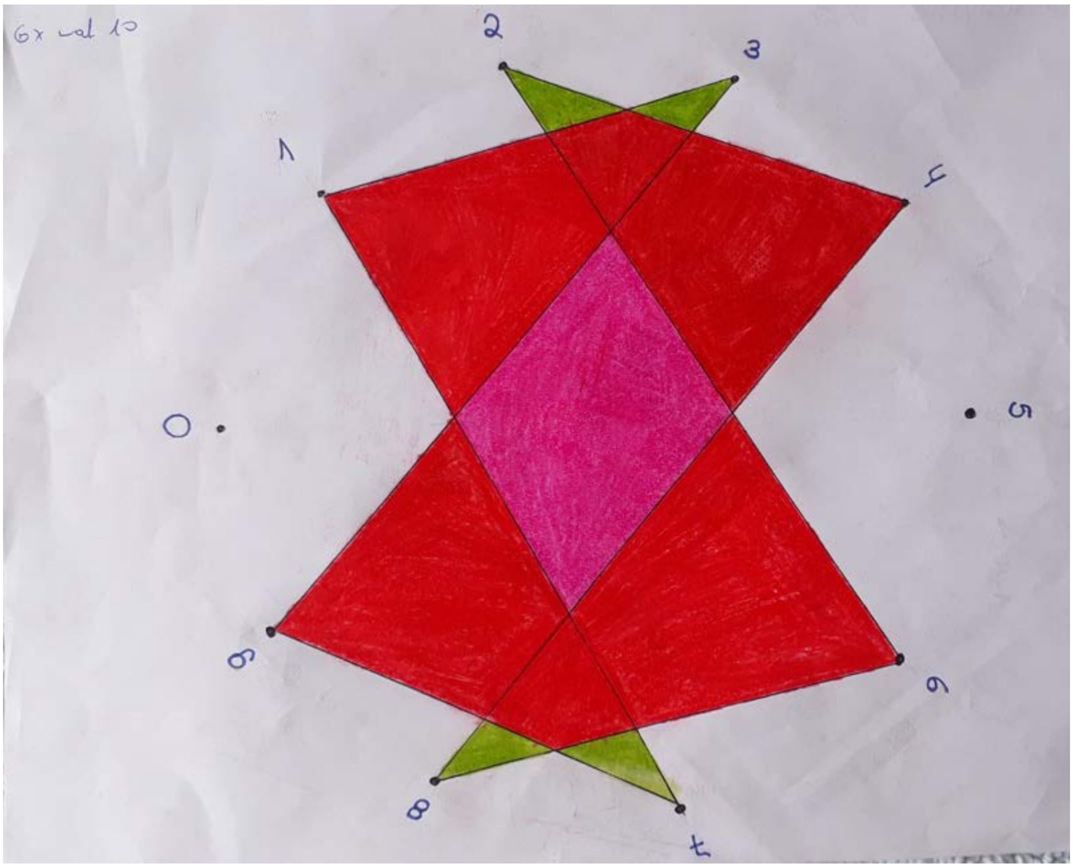


Figura 95 – Multiplicação por 2 módulo 20

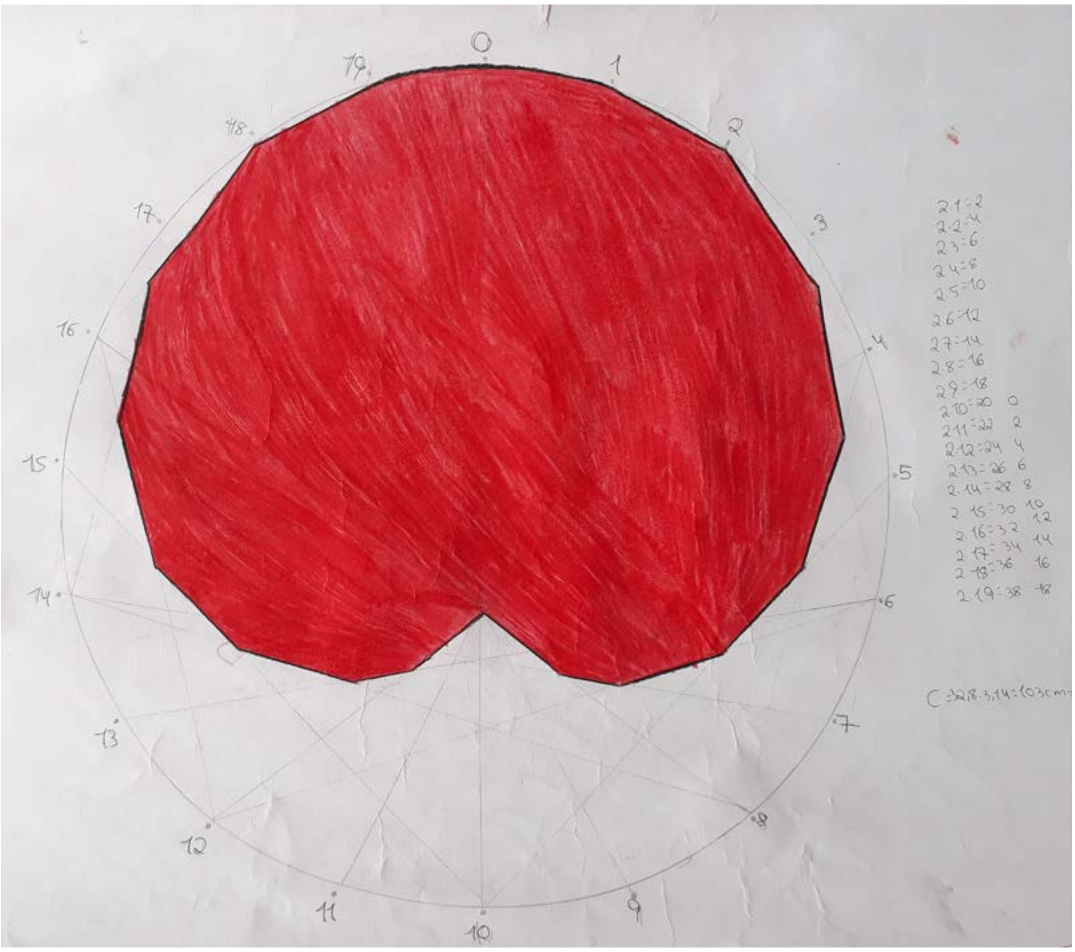


Figura 96 – Multiplicação por 5 módulo 73

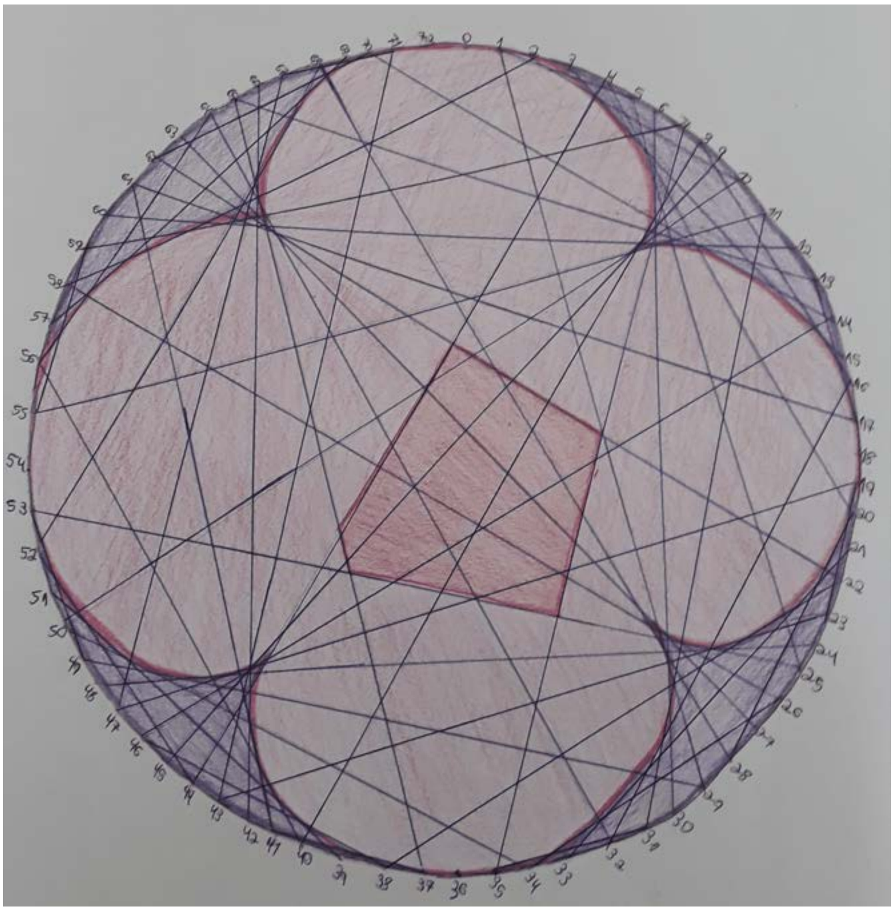


Figura 97 – Multiplicação por 5 módulo 73

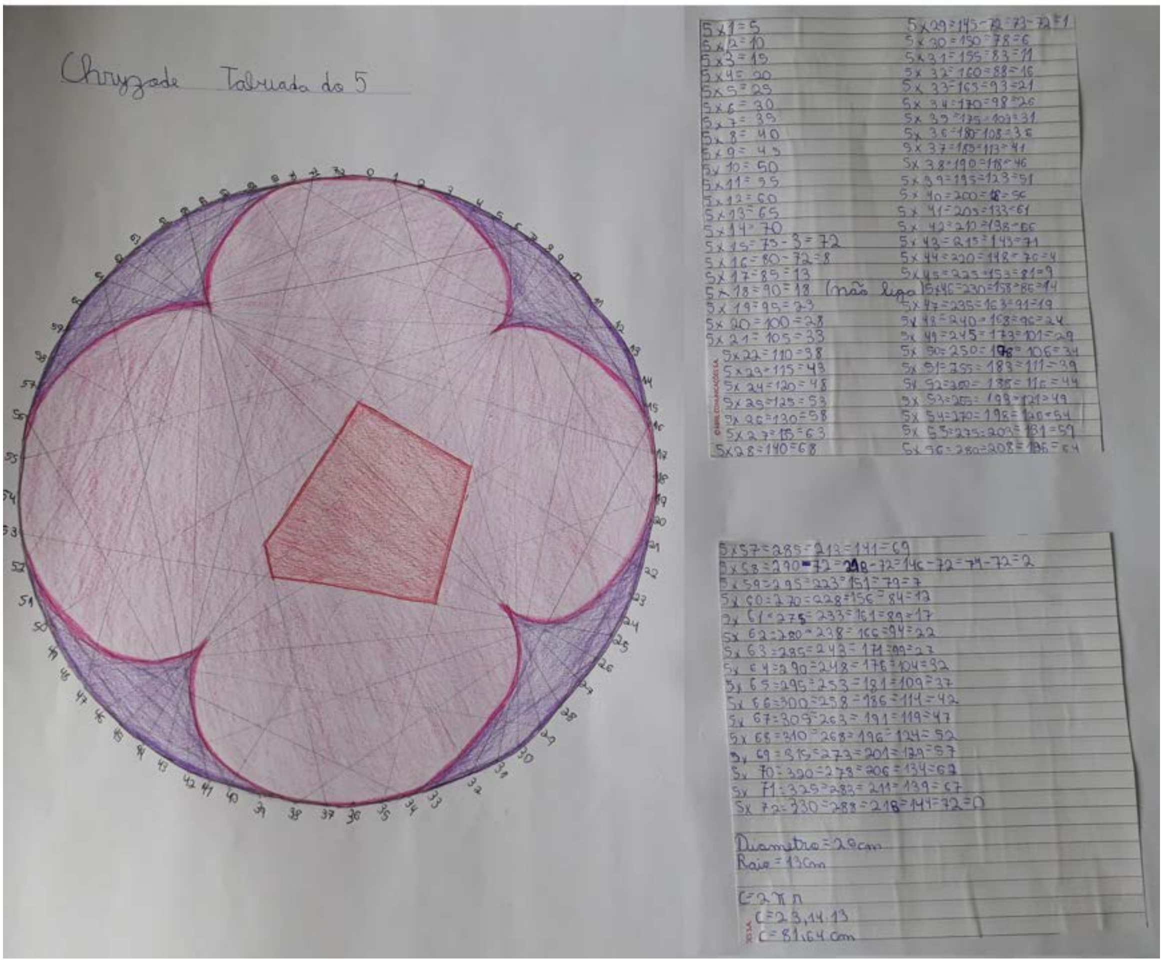
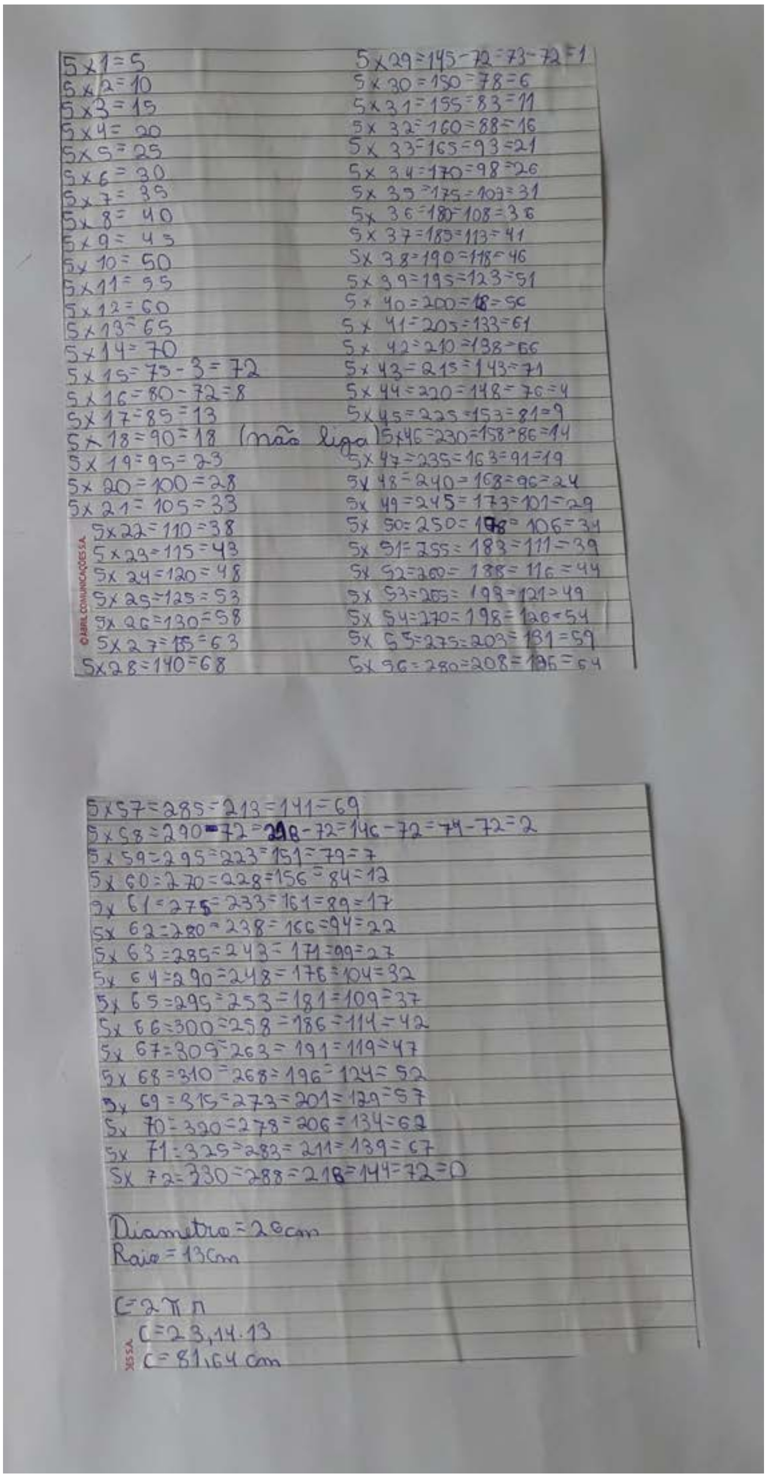


Figura 98 – Multiplicação por 5 módulo 73



5x1=5
5x2=10
5x3=15
5x4=20
5x5=25
5x6=30
5x7=35
5x8=40
5x9=45
5x10=50
5x11=55
5x12=60
5x13=65
5x14=70
5x15=75-3=72
5x16=80-72=8
5x17=85=13
5x18=90=18 (não liga)
5x19=95=23
5x20=100=28
5x21=105=33
5x22=110=38
5x23=115=43
5x24=120=48
5x25=125=53
5x26=130=58
5x27=135=63
5x28=140=68

5x29=145-72=73-72=1
5x30=150=78=6
5x31=155=83=11
5x32=160=88=16
5x33=165=93=21
5x34=170=98=26
5x35=175=103=31
5x36=180=108=36
5x37=185=113=41
5x38=190=118=46
5x39=195=123=51
5x40=200=128=56
5x41=205=133=61
5x42=210=138=66
5x43=215=143=71
5x44=220=148=76=4
5x45=225=153=81=9
5x46=230=158=86=14
5x47=235=163=91=19
5x48=240=168=96=24
5x49=245=173=101=29
5x50=250=178=106=34
5x51=255=183=111=39
5x52=260=188=116=44
5x53=265=193=121=49
5x54=270=198=126=54
5x55=275=203=131=59
5x56=280=208=136=64

5x57=285=213=141=69
5x58=290-72=218-72=146-72=74-72=2
5x59=295=223=151=79=7
5x60=270=228=156=84=12
5x61=275=233=161=89=17
5x62=280=238=166=94=22
5x63=285=243=171=99=27
5x64=290=248=176=104=32
5x65=295=253=181=109=37
5x66=300=258=186=114=42
5x67=309=263=191=119=47
5x68=310=268=196=124=52
5x69=315=273=201=129=57
5x70=320=278=206=134=62
5x71=325=283=211=139=67
5x72=330=288=218=144=72=0

Diametro=26cm
Raio=13cm

C=2πr
C=2.3,14.13
C=81,64 cm

Figura 99 – Multiplicação por 5 módulo 20

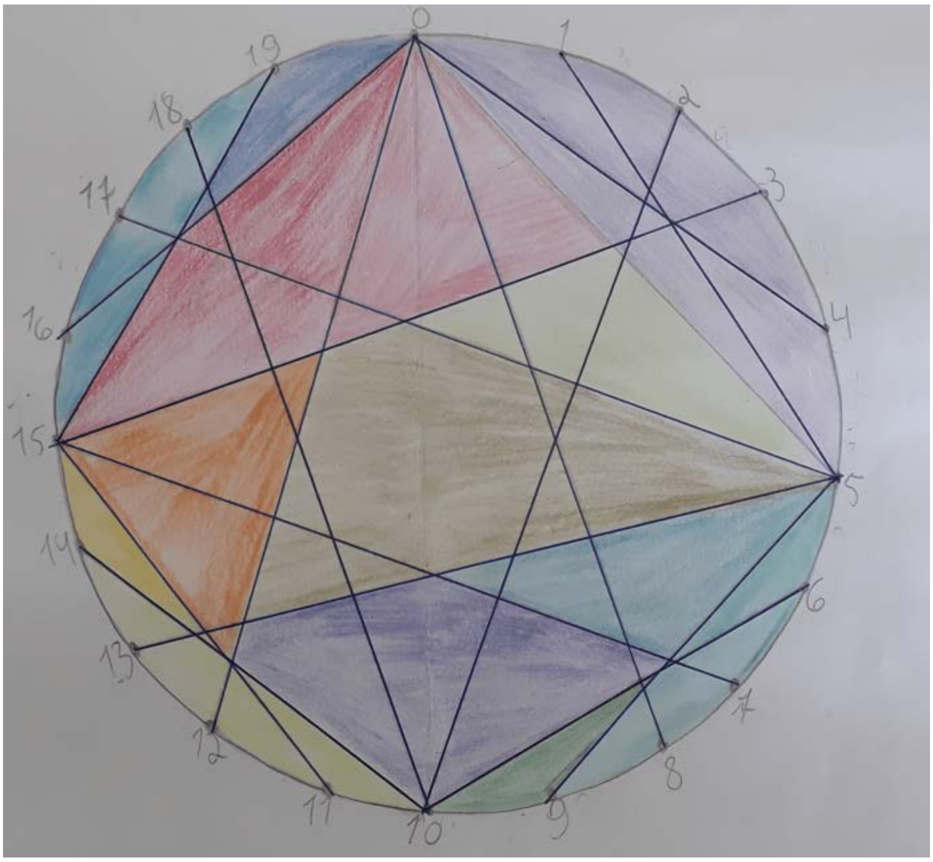


Figura 100 – Multiplicação por 3 módulo 30