UNIVERSIDADE ESTADUAL DE SANTA CRUZ
DEPARTAMENTO DE CIÊNCIAS EXATAS E TECNOLÓGICAS - DCET

COLEGIADO DO MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Fábio Xavier Dos Reis

Aritmética Modular e suas Aplicações no Ensino Médio e Superior

ILHÉUS-BAHIA
2021

Fábio Xavier Dos Reis

Aritmética Modular e suas Aplicações no Ensino Médio e Superior

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, como requisito parcial para a obtenção do Título de Mestre em Matemática pela Universidade Estadual de Santa Cruz.

Orientadora: Profª Drª Fernanda Gonçalves de Paula

ILHÉUS-BAHIA
2021

R375 Reis, Fábio Xavier dos.
Aritmética modular e suas aplicações no ensino médio e superior / Fábio Xavier dos Reis. – Ilhéus, BA: UESC, 2021.
70 f. : il.

Orientadora: Fernanda Gonçalves de Paula.
Dissertação (mestrado) –Universidade Estadual de Santa Cruz. Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT).
Referências: f. 70.

1. Matemática – Estudo e ensino. 2. Aritmética – Problemas, questões, exercícios, etc. 3. Jogos no ensino de matemática. 4. Educação matemática. I.Título.

CDD 510.7

FÁBIO XAVIER DOS REIS

Aritmética Modular e suas Aplicações no Ensino Médio e Superior

Dissertação apresentada ao programa de mestrado profissional em Matemática em Rede nacional, PROFMAT, como requisito parcial para obtenção do Título de Mestre em Matemática pela Universidade Estadual de Santa Cruz

Os componentes da banca de avaliação, abaixo identificados, consideram este trabalho aprovado.

BANCA EXAMINADORA

Profª Drª Fernanda Gonçalves de Paula
UESC

Profª Drª Nazira Hanna Harb
UTFPR

Profº Dr Vinicius Augusto Takahashi Arakawa
UESC

Data da aprovação: em 13 de Abril de 2021, Ilhéus-Bahia.

Ilhéus, Bahia
2021

Dedico esse trabalho a Deus, a minha família, a minha orientadora e aos professores que ministraram aulas no PROFMAT, em especial ao professor Sérgio Mota (*in memoriam*) que tanto colaborou com o mestrado.

Agradecimentos

Agradeço primeiramente a Deus, por ter me sustentado nos momentos difíceis, a minha orientadora, aos meus colegas mestrandos e aos meus professores do PROFMAT.

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

Resumo

Esse trabalho tem como principal objetivo apresentar a Congruência Modular como ferramenta poderosa para auxiliar na resolução de problemas de matemática do Ensino Médio e Superior. Através do material teórico e principalmente prático fornecido nesse trabalho, esperamos facilitar a compreensão da teoria abordada e despertar cada vez mais o interesse pelo estudo dessa fascinante matéria que é a matemática. Propomos nesse trabalho aplicações interessantes da congruência modular em problemas do cotidiano. Fizemos a apresentação de teoremas importantes, como o Pequeno Teorema de Fermat e o Teorema de Wilson com o objetivo de aplicá-los para facilitar a resolução de alguns problemas de congruência modular. Apresentamos o jogo dos restos envolvendo congruência modular e atividades com suas respectivas sequências didáticas para que possam ser aplicadas em sala de aula, facilitando a compreensão do conteúdo. E através de uma gama de atividades resolvidas o leitor terá suporte para um melhor aprofundamento do conteúdo.

Palavras-chave:Congruências; Resolução de Problemas; Educação Matemática.

Abstract

This work has as main objective to present modular congruence as a powerful tool to assist in solving mathematics problems in high school and higher education. Through the theoretical and mainly practical material provided in this work, we hope to facilitate the understanding of the theory addressed and to arouse more and more interest in the study of this fascinating matter that is mathematics. We propose in this work interesting applications of modular congruence in everyday problems. We made the presentation of important theorems, such as Fermat's Little Theorem and Wilson's Theorem with the aim of applying them to facilitate the resolution of some problems of modular congruence. We present the game of remains involving modular congruence and activities with their respective didactic sequences so that they can be applied in the classroom, facilitating the understanding of the content. And through a range of resolved activities the reader will have support for a better deepening of the content.

Keywords: Congruences; Problem Solving; Mathematics Education.

Lista de figuras

Lista de tabelas

Sumário

INTRODUÇÃO

A motivação desta dissertação surgiu do interesse em relacionar a Matemática estudada durante as aulas do PROFMAT com a Matemática da Educação Básica, mais especificamente no que se refere ao conteúdo de Aritmética Modular, o qual pode ser utilizado para simplificar e agilizar a resolução de alguns problemas matemáticos. Acreditamos que através do conteúdo teórico e prático abordado no presente trabalho, se tornará mais fácil a compreensão e aplicabilidade dos problemas tratados não só no Ensino Médio, mas também no Ensino Superior, onde a abordagem é mais complexa.

Nesse sentido, apresentaremos vários recursos tais como atividades práticas para o Ensino Médio, listas de exercícios e jogo com o objetivo de auxiliar os professores em sala de aula. No âmbito do Ensino Superior apresentaremos também material teórico e diversas atividades resolvidas como ferramenta auxiliadora.

Mas especificamente:

- Definiremos congruência modular, mostraremos algumas propriedades e teoremas da aritmética modular como ferramenta para resolver problemas que envolvam: divisibilidade, resto, números complexos, trigonometria e problemas do cotidiano como verificação da validade do CPF e aplicação no calendário.
- Mostraremos como alguns problemas difíceis que diz respeito a divisibilidade podem ser resolvidos de maneira bem mais fácil quando utiliza-se as propriedades e os teoremas abordados nesse trabalho.
- Esperamos contribuir para o Ensino - Aprendizagem da Matemática na Educação Básica e Superior através da aplicação da aritmética modular com confecção de sequências didáticas envolvidas.

O presente trabalho está divido como se segue. No **Capítulo** 1 falaremos um pouco da história dos principais matemáticos que contribuíram com assuntos relacionados a congruência modular, apresentaremos a definição de congruência modular, sistema completo de restos, operações em $\mathbb{Z}_m$, aplicação de congruência modular em critérios de divisibilidade, apresentaremos teoremas com suas demonstrações e daremos exemplos de como aplicá-los. Falaremos também de algumas aplicações de congruência modular no cotidiano, tais como no calendário e no CPF. No **Capítulo** 2 propomos sequências didáticas que poderão ser aplicadas no Ensino Médio, envolvendo o jogo dos restos, a aritmética do relógio, aritmética aplicada na trigonometria e nos números complexos. Apresentamos também listas de exercícios com conteúdo de revisão e com o conteúdo de congruência

modular que podem ser aplicadas em sala de aula. No **Capítulo** 3, apresentaremos alguns dos principais teoremas que envolvem o conceito da aritmética modular, como o Pequeno Teorema de Fermat, o Teorema de Wilson, o Teorema de Euler e o Teorema Chinês dos Restos (aqui, falaremos da congruência linear) de modo a levar os alunos do ensino superior a ampliar sua compreensão acerca destes resultados. Para tanto, falaremos um pouco sobre o autor de cada teorema, além de obviamente enunciar e demonstrar cada teorema. Por fim, serão resolvidos vários exercícios de nível superior. No **Capítulo** 4, trazemos nossas Considerações Finais acerca do trabalho desenvolvido, onde esperamos que o trabalho tenha acrescentado mais conhecimento para o leitor.

1 Noções de Congruência Modular

Iniciaremos este capítulo apresentando alguns aspectos históricos da congruência modular. Posteriormente, faremos sua definição, resolveremos exercícios, mostraremos a caracterização de inteiros congruentes, mostraremos algumas propriedades e operações em $\mathbb{Z}_m$ e demonstraremos alguns resultados que consideramos mais relevantes. Posteriormente, demonstraremos alguns critérios de divisibilidade utilizando as noções de congruência modular. Terminamos o capítulo mostrando algumas aplicações de congruência modular no nosso cotidiano.

1.1 Aspectos Históricos

No decorrer da história tivemos muitas contribuições dadas por diversos estudiosos para o enriquecimento do conhecimento matemático, no que se trata da Aritmética Modular. Carl Friedrich Gauss (1777, 1855), foi o grande introdutor do conceito de congruência modular, e começou a mostrar ao mundo as congruências a partir de um trabalho realizado em 1801, (GOLDSTEIN et al., 2007) quando tinha apenas 24 anos de idade.

Várias ideias de grande importância usadas na teoria dos números, foram introduzidas e são utilizadas até hoje (assim como o símbolo usado na congruência atualmente, foi o que Gauss usou naquela época). Um uso familiar da aritmética modular é no relógio de ponteiro, no qual o dia é divido em dois períodos de 12 horas cada. Se são 7 horas agora, então daqui a 8 horas serão 3 horas. A adição usual sugere que o tempo futuro deveria ser $7 + 8 = 15$, mas esta é a resposta errada por que o relógio "volta para trás" a cada 12 horas; não existe "15 horas" no relógio de ponteiro. Da mesma forma, se o relógio começa em 12:00 (meio dia) e 21 horas se passam, então a hora será 9:00 do dia seguinte, em vez de 33:00. Como o número de horas começa de novo depois que atinge 12, esta aritmética é chamada aritmética módulo 12. O número 12 é congruente não só a ele mesmo, mas também a 0, assim a hora chamada "12:00" pode também ser chamada "0:00", pois $0 \equiv 12 \pmod{12}$. (GAUSS, 1801). Atento às relações existentes entre os números, Gauss observou que frequentemente eram usados termos como a dá o mesmo resto que b quando dividimos por m. Essa afirmação o intrigou, levando-o a desenvolver o pensamento e as bases da aritmética modular. Como isso é possível? Ora, ao demonstrar que números diferentes divididos por um outro número distinto dos anteriores produzia o mesmo resto. Assim concluiu que esses números eram congruentes, iguais, em termos de divisibilidade por aquele divisor. Não se pode descartar, nas discussões sobre aritmética modular, as contribuições de Pierre de Fermat, advogado francês que tinha a matemática como um hobby, já que matemáticos de épocas posteriores debruçavam sobre suas proposições para

fazerem demostrações e comprovações. É de Fermat o enunciado do famoso Pequeno Teorema de Fermat, que afirma "Se p é primo e a é um número inteiro não divisível por p, então o número $a^{p-1} - 1$ é divisível por p". Tal enunciado, atualizando a linguagem, foi declarado em uma carta a Frenicle de Bessy em 18 de outubro de 1640. A demonstração desse Teorema foi publicado pela primeira vez por Leonhard Euler, cerca de 100 anos mais tarde. Tempos depois, Gauss propôs que o Pequeno Teorema de Fermat é um caso de congruência, pois "se p é um número primo e a é um número inteiro qualquer, então a afirmação p divide $(a^p - a)$, pode ser escrita usando uma notação de congruência como $a^p \equiv a \pmod{p}$".

1.2 Embasamento Teórico

Geralmente, a aritmética modular é abordada apenas no ensino superior, mas acreditamos que, devido à facilidade de compreensão do conceito, suas noções também podem ser introduzidas no ensino médio, desde que com uma linguagem matemática apropriada para esta etapa do ensino e sem que sejam feitas todas as demonstrações. Nessa seção trataremos das primeiras noções de congruência modulares, iniciando pela definição de congruência modular, passando por algumas propriedades, teoremas e sistema completo de restos.

Definição 1.1 *Sejam a e b inteiros quaisquer e seja $m > 1$ um inteiro positivo fixo. Diz-se que a é congruente a b módulo m, se m divide $(a - b)$, isto é, se existe um inteiro k tal que $a - b = k.m$.* □

Notação: $a \equiv b \pmod{m}$

Exemplo 1.1 *Temos os seguintes exemplos de congruências:*

i) $24 \equiv 3 \pmod{7}$, *pois* $7|(24 - 3)$, *ou seja* $7|21$, *já que* $3.7 = 21$;

ii) $31 \equiv -11 \pmod{6}$, *pois* $6|[(31 - (-11)]$, *ou seja* $6|42$, *já que* $7.6 = 42$;

iii) $-63 \equiv -15 \pmod{8}$, *pois* $8|[-63 - (-15)]$, *ou seja* $8|-48$, *já que* $(-6).8 = -48$.

Definição 1.2 *Sejam a e b inteiros quaisquer. Se $m > 1$ não divide a diferença $a - b$, então diz-se que a é incongruente a b módulo m.* □

Notação: $a \not\equiv b \pmod{m}$

Exemplo 1.2 *Veja que* $10 \not\equiv 3 \pmod 6$*, pois* $6 \nmid (10-3)$*, ou seja* $6 \nmid 7$.

Observações: É fácil ver que:

1. Dois inteiros quaisquer são congruentes $\pmod 1$.
2. Dois inteiros são congruentes $\pmod 2$ se ambos são pares ou ambos são ímpares.
3. $a \equiv 0 \pmod m$ se, e somente se, $m|a$.

Veremos a seguir um resultado que nos fornece uma caracterização de inteiros congruentes. Para tanto, precisamos do seguinte resultado:

Algoritmo da Divisão de Euclides: Dados $a, b \in \mathbb{Z}$, $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$ tais que $a = b.q + r$ e $0 \leq r < |b|$.

Para maiores detalhes, veja (MARTINS, 2015).

Teorema 1.1 *Dois inteiros a e b são congruentes módulo m se, e somente se, a e b deixam o mesmo resto quando divididos por m.*

Demonstração:

($\Rightarrow$) Suponhamos que $a \equiv b \pmod m$. Então, pela definição:

$$a - b = k.m, \text{ existe } k \in \mathbb{Z}.$$

Seja r o resto da divisão de b por m; então pelo Algorítimo da Divisão de Euclides, existe $q \in \mathbb{Z}$ tal que

$$b = m.q + r, 0 \leq r < m.$$

Portanto:

$$a = k.m + b = k.m + m.q + r = (k+q).m + r$$

e isto significa que r também é o resto da divisão de a por m, isto é, os inteiros a e b divididos por m deixam o mesmo resto r.

($\Leftarrow$) Reciprocamente, suponhamos que a e b divididos por m deixam o mesmo resto r. Então, podemos escrever:

$$a = m.q_1 + r \text{ e } b = m.q_2 + r, 0 \leq r < m$$

e, portanto:

$$a - b = (q_1 - q_2)m \Rightarrow m|(a - b) \Rightarrow a \equiv b \pmod{m} \blacksquare$$

Teorema 1.2 *Seja m um inteiro positivo fixo ($m > 1$) e sejam a, b, c, d inteiros quaisquer. Valem as seguintes propriedades:*

1. *Se $a \equiv b \pmod{m}$ e se $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$ e $a.c \equiv b.d \pmod{m}$.*
2. *Se $a \equiv b \pmod{m}$ e c um inteiro qualquer, então $a + c \equiv b + c \pmod{m}$ e $a.c \equiv b.c \pmod{m}$.*
3. *Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$ para todo inteiro positivo n.*

Demonstração:

1. Se $a \equiv b \pmod{m}$ e se $c \equiv d \pmod{m}$, então existem inteiros h e k tais que $a - b = h.m$ e $c - d = k.m$. Portanto:

   $$(a + c) - (b + d) = (a - b) + (c - d) = (h + k).m$$

   e

   $$a.c - b.d = (b + h.m)(d + k.m) - b.d = (b.k + d.h + h.k.m).m$$

   o que implica:

   $$a + c \equiv b + d \pmod{m} \text{ e } a.c \equiv b.d \pmod{m}$$

2. Temos:

   $$a \equiv b \pmod{m} \text{ e } c \equiv c \pmod{m}$$

   Logo, pela propriedade anterior:

   $$a + c \equiv b + c \pmod{m} \text{ e } a.c \equiv b.c \pmod{m}$$

   Em particular, se $c = -1$, então:

   $$a.(-1) \equiv b.(-1) \pmod{m} \text{ ou } -a \equiv -b \pmod{m}$$

3. Provando por indução sobre n, a proposição é verdadeira para $n = 1$, e suposta verdadeira para o inteiro positivo k temos:

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

Portanto, pela propriedade 1 acima

$$a^k.a \equiv b^k.b \pmod{m} \text{ ou } a^{k+1} \equiv b^{k+1} \pmod{m}$$

isto é, a proposição é verdadeira para o inteiro positivo $k+1$. Logo, a proposição é verdadeira para todo inteiro positivo n . ■

(KONAGESKI et al., 2019)

Teorema 1.3 *Seja m um inteiro positivo fixo ($m > 1$) e sejam a, b e c inteiros quaisquer. Valem as seguintes propriedades:*

1. $a \equiv a \pmod{m}$ *(Reflexiva)*
2. *Se* $a \equiv b \pmod{m}$, *então* $b \equiv a \pmod{m}$ *(Simétrica)*
3. *Se* $a \equiv b \pmod{m}$ *e se* $b \equiv c \pmod{m}$, *então* $a \equiv c \pmod{m}$ *(Transitiva)*

Demonstração:

1. É fácil ver que $a|0$. Assim, podemos escrever $a|(a-a)$, o que implica: $a \equiv a \pmod{m}$.
2. Se $a \equiv b \pmod{m}$, então existe $k \in \mathbb{Z}$ tal que $a - b = k.m$. Portanto: $b - a = -(k.m) = (-k).m \Rightarrow b \equiv a \pmod{m}$.
3. Se $a \equiv b \pmod{m}$ e se $b \equiv c \pmod{m}$, então existem inteiros h e k tais que $a - b = h.m$ e $b - c = k.m$.

   Assim $a - c = (a - b) + (b - c) = h.m + k.m = (h + k).m$

   e isto significa que $a \equiv c \pmod{m}$. ■
   (KONAGESKI et al., 2019)

Sistema Completo de Restos

Definição 1.3 *Chama-se sistema completo de restos módulos m todo conjunto $S = \{r_1, r_2, ..., r_m\}$ de m inteiros tal que um inteiro qualquer a é congruente módulo m a um único elemento de S.* □

Em outras palavras, um conjunto $S \subset \mathbb{Z}$ é um sistema completo de restos módulo m se para todo $a \in \mathbb{Z}$ existe um, e só um, $b \in S$ tal que $a \equiv b \pmod{m}$.

Exemplo 1.3 *Cada um dos conjuntos:*

$$\{1,2,3\},\{0,1,2\},\{-1,0,1\},\{1,5,9\}$$

é um sistema completo de restos $(\text{mod } 3)$.

Pois cada um dos elementos de um desses conjuntos é congruente a 0*, ou a* 1*, ou a* 2 $(\text{mod } 3)$*, que são todos os restos menores que* 3.

Já o conjunto $\{1,4,7\}$ *não é um sistema completo de resto* $(\text{mod } 3)$.

Pois $1 \equiv 1 \ (\text{mod } 3)$*,* $4 \equiv 1 \ (\text{mod } 3)$ *e* $7 \equiv 1 \ (\text{mod } 3)$*, forma só um conjunto unitário* $\{1\}$.

Aritmética Módulo m

A ideia primária da aritmética modular é bem simples. Fixado um inteiro m, todos os demais números inteiros a são substituídos pelo resto de sua divisão euclidiana por m. Desse modo, o conjunto $\mathbb{Z}$ dos números inteiros se transforma no conjunto $\mathbb{Z}_m = \{0,1,...,m-1\}$, denominado conjunto dos inteiros módulo m (cujos elementos são os restos possíveis da divisão de um inteiro a qualquer por m).

Definição 1.4 *Seja a um inteiro. Chama-se classe de congruência de a módulo,* $(m > 1)$ *ao conjunto formado por todos os inteiros que são congruentes à a módulo* m. □

Denotamos esse conjunto por $\overline{a}$*. Temos, então:*

$$\overline{a} = \{x \in \mathbb{Z} \ ; \ x \equiv a \ (\text{mod } m)\}$$

Como $x \equiv a \ (\text{mod } m)$, se e somente se, x é da forma $x = a + k.m$, para algum $k \in \mathbb{Z}$, também podemos escrever:

$$\overline{a} = \{a + k.m | k \in \mathbb{Z}\}$$

Mostraremos a seguir que a relação de congruência entre números é uma igualdade no que se diz respeito a divisibilidade.

Proposição 1.1 *Sejam a e b inteiros. Então* $a \equiv b \ (\text{mod } m)$*, se e somente se,* $\overline{a} \equiv \overline{b}$.

Demonstração:

Suponhamos que $a \equiv b \pmod{m}$, queremos provar que $\overline{a} = \overline{b}$, isto é, uma igualdade entre conjuntos. Dado $x \in \overline{a}$, temos por definição que $x \equiv a \pmod{m}$. Da propriedade transitiva de congruência e da hipótese, segue imediatamente que $x \in \overline{b}$. Logo, $\overline{a} \subset \overline{b}$. A inclusão $\overline{b} \subset \overline{a}$ segue de forma análoga. Reciprocamente, se $\overline{a} = \overline{b}$, como $a \in \overline{a}$, temos também que $a \in \overline{b}$, logo, $a \equiv b \pmod{m}$. ■

Corolario 1.1 *Sejam a e b inteiros. Se $\overline{a} \neq \overline{b}$, então $\overline{a} \cap \overline{b} = \varnothing$.*

Demonstração:

Suponhamos por absurdo que $\overline{a} \cap \overline{b} \neq \varnothing$. Considere um inteiro c que pertença à ambas as classes. Como $c \in \overline{a}$, temos que $c \equiv a \pmod{m}$ e, de forma análoga, $c \equiv b \pmod{m}$. Portanto, $a \equiv b \pmod{m}$ e, da proposição acima, $\overline{a} = \overline{b}$. Absurdo! Pois $\overline{a} \neq \overline{b}$. Logo, $\overline{a} \cap \overline{b} = \varnothing$. ■

Note que, por exemplo, para as classes $\pmod 7$, temos que $\overline{0} = \overline{7} = \overline{14} = \overline{-7} = ...$ etc. Mais precisamente, dada uma classe $\overline{a}$, para qualquer inteiro x tal que $x \in \overline{a}$, temos que $\overline{x} = \overline{a}$. Por causa disto, cada inteiro pertencente a uma dada classe é chamado de representante daquela classe. Por exemplo, 11 e -3 são representantes da classe $\overline{4} \pmod 7$.

Consideremos um sistema completo de classes ou resíduos módulo m, por exemplo, os inteiros $0, 1, ..., m-1$ e suas respectivas classes:

$$\overline{0} = \{0, \pm m, \pm 2.m, \pm, 3.m, ...\}$$

$$\overline{1} = \{1, 1 \pm m, 1 \pm 2.m, 1 \pm 3.m, ...\}$$

$$...$$

$$\overline{m-1} = \{m-1, m-1 \pm m, m-1 \pm 2.m, m-1 \pm 3.m, ...\}$$

Conforme já foi considerado, cada inteiro pertence a uma e apenas uma das m classes. Por exemplo, se $m = 7$, todas as classes possíveis, $\pmod 7$, são as seguintes:

$\overline{0} = \{0, \pm 7, \pm, 14, \pm 21, ...\}$

$\overline{1} = \{1, 1 \pm 7, 1 \pm 14, 1 \pm 21, ...\}$

$\overline{2} = \{2, 2 \pm 7, 2 \pm 14, 2 \pm 21, ...\}$

$$\overline{1} = \{3, 3 \pm 7, 3 \pm 14, 3 \pm 21, ...\}$$

$$\overline{4} = \{4, 4 \pm 7, 4 \pm 14, 4 \pm 21, ...\}$$

$$\overline{5} = \{5, 5 \pm 7, 5 \pm 14, 5 \pm 21, ...\}$$

$$\overline{6} = \{6, 6 \pm 7, 6 \pm 14, 6 \pm 21, ...\}$$

Denotamos pelo símbolo $\mathbb{Z}_m$ o conjunto das classes de congruência módulo m e o chamaremos de Conjunto dos Inteiros Módulo m.

Assim, $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$.

Note que, por exemplo,

$\overline{0} = \overline{7}, \overline{1} = \overline{15}, \overline{2} = \overline{9}, \overline{3} = \overline{-11}, \overline{4} = \overline{25}, \overline{5} = \overline{-16}$, $\overline{6} = \overline{-8}$.

e também podemos escrever:

$\mathbb{Z}_7 = \{\overline{7}, \overline{15}, \overline{9}, \overline{-11}, \overline{25}, \overline{-16}, \overline{-8}\}$

Em geral, se $\{a_1, a_2, ..., a_m\}$ é um sistema completo de restos módulo m, temos que:

$$\mathbb{Z}_m = \{\overline{a_1}, \overline{a_2}, ..., \overline{a_m}\}$$

Tomando o sistema de restos mais simples, podemos escrever:

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$$

Note que, conforme as observações acima, o conjunto $\mathbb{Z}_m$ tem precisamente m elementos.

Adição e Multiplicação em $\mathbb{Z}_m$

Vamos entender as operações de soma e produto em $\mathbb{Z}_m$ estudando suas propriedades. Tem uma forma natural de compreender. Por exemplo, para somar e multiplicar $\overline{3}$ e $\overline{6}$ em $\mathbb{Z}_7$, faríamos:

$\overline{3} + \overline{6} = \overline{9} = \overline{2}$

$\overline{3} \times \overline{6} = \overline{18} = \overline{4}$

Exemplificando a adição e a multiplicação em uma "tabela" (mod 7) :

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tabela 1 – Adição (mod 7)

∗	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tabela 2 – Multiplicação (mod 7)

Observações:

Perceba, na tabela de adição, o conceito de inverso aditivo módulo m. Dizemos que dois elementos de $\mathbb{Z}_m$ são inversos aditivos, se e somente se, $\overline{a+b} = 0 \pmod{m}$. Assim, por exemplo, 4 e 3 são inversos aditivos (mod 7), uma vez que $\overline{4+3} = 0 \pmod{7}$.

Portanto para efetuar a soma de duas classes módulo m, tomamos representantes (quaisquer) **a** e **b** dessas classes, efetuamos a soma **a**+**b** em $\mathbb{Z}$ e consideremos como resultado da soma a classe de **a**+**b** módulo m. A operação de produto se faz de forma análoga. Pode se questionar: será que o resultado das operações não depende dos representantes escolhidos? De volta ao exemplo de $\mathbb{Z}_7$, para somar $\overline{3}+\overline{6}$, poderíamos tomar 38 como um representante de $\overline{3}$ e 27 como representante de $\overline{6}$. Será que $\overline{38}+\overline{27} = \overline{65}$ é o mesmo resultado que aquele obtido acima, $\overline{3}+\overline{6} = \overline{2}$? A resposta é afirmativa. Como $65 \equiv 2 \pmod{7}$, claramente o resultado é o mesmo. O lema abaixo garante esse bom comportamento das operações.

Lema 1.1 *Sejam a, a', b, b' inteiros tais que* $\overline{a} = \overline{a'}$ *e* $\overline{b} = \overline{b'}$. *Então,* $\overline{a+b} = \overline{a'+b'}$ *e* $\overline{a.b} = \overline{a'.b'}$.

1.3 Critérios de Divisibilidade

Nessa seção faremos a demonstração de alguns critérios de divisibilidade fazendo uso da congruência linear. Esta abordagem visa preparar o professor para sanar questionamentos do tipo "Por que essas regras ensinadas dão certo?", ou "de onde surgem essas regras?"
Esperamos que o conteúdo aqui abordado possa preparar o professor para melhor respondê-las.

Critério de divisibilidade por 2

Um número é divisível por dois quando for par, ou seja seu último algarismo terminar com um desses algarismos $0, 2, 4, 6$ *ou* 8.

Seja $n = a_n a_{n-1}...a_0$ um número natural com $n+1$ dígitos, sendo a_i esses dígitos, então $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Podemos escrever n na forma $n = a_n a_{n-1}...a_0 = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10a_1 + a_0$.

Exemplo 1.4 $123 = 100 + 20 + 3 = 1.10^2 + 2.10^1 + 3.10^0$

Dado $n = a_n a_{n-1}...a_0 = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10a_1 + a_0$. Como $10 \equiv 0 \pmod 2$, temos então que $n \equiv a_0 \pmod 2$. Portanto para que n seja divisível por 2, a_0 tem que ser par, ou seja um dos algarismos $0, 2, 4, 6$ ou 8.

Exemplo 1.5 *O número* $2.456.856.888$ *é divisível por* 2*, pois seu último algarismo é o* 8 *que é divisível por* 2*. E o número* 345.679 *não é divisível por* 2*, pois o último algarismo é* 9 *que não é divisível por* 2.

Critério de divisibilidade por 3

Um número é divisível por três quando a soma de seus algarismos absolutos for também divisível por três.

Dado $n = a_n a_{n-1}...a_0 = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10a_1 + a_0$. Como $10 \equiv 1 \pmod 3$, temos então que $n \equiv a_n + a_{n-1} + ... + a_0 \pmod 3$. Portanto um número é divisível por 3 quando a soma de seus algarismos for um número divisível por 3.

Exemplo 1.6 *O número* 111.111 *é divisível por* 3*, pois* $1+1+1+1+1+1 = 6$ *que é divisível por* 3*. O número* 2347 *não é divisível por* 3*, pois* $2+3+4+7 = 16$ *que não é divisível por* 3.

Critério de divisibilidade por 4

Um número é divisível por 4 *quando seus dois últimos algarismos formar um número divisível por* 4.

Dado $n = a_n a_{n-1}...a_0 = 10^n a_n + 10^{n-1}a_{n-1} + ... + 10a_1 + a_0 = 100(10^{n-2}a_n + \ldots + 10^1 a_3 + a_2) + 10a_1 + a_0$, como $100 \equiv 0 \pmod 4$, temos então que $n \equiv 10a_1 + a_0 \pmod 4$. Portanto $10a_1 + a_0$ que representa os dois últimos algarismos de n precisa ser múltiplo de 4, ou seja da forma $10a_1 + a_0 = 4k$, onde $k \in \mathbb{Z}$, para que o número n seja divisível por 4.

Exemplo 1.7 *O número* 1024 *é divisível por* 4*, pois os dois últimos algarismo são* 24*, que é divisível por* 4*. Já o número* 2.345.689 *não é divisível por* 4*, pois os dois últimos algarismos é* 89 *que não é divisível por* 4*.*

Critério de divisibilidade por 5

Um número natural é divisível por 5 *quando ele termina em* 0 *ou* 5*.*

Dado $n = a_n a_{n-1}...a_0 = 10^n a_n + 10^{n-1}a_{n-1} + ... + 10a_1 + a_0$. Como $10 \equiv 0 \pmod 5$, temos então que $n \equiv a_0 \pmod 5$. Portanto para que n seja divisível por 5, n_0 tem que terminar em 0 ou 5.

Exemplo 1.8 *Os números* 45.890 *e* 23.455 *são divisíveis por* 5 *e* 56.784 *não é divisível por* 5*, pois termina em* 4*.*

Critério de divisibilidade por 6

Um número é divisível por 6 *quando for divisível por* 2 *e também por* 3*.*

Exemplo 1.9 *O número* 1.236 *é divisível por* 2*, pois é par, e é divisível por 3 pois* $1 + 2 + 3 + 6 = 12$*, logo é divisível por* 6*. Já o número* 111.111 *é divisível por* 3*, pois* $1 + 1 + 1 + 1 + 1 + 1 = 6$*, mas é ímpar e não é divisível por* 2*. Logo não é divisível por* 6*.*

Mas também podemos usar a congruência modular para demonstrar.

Seja o número $n = a_n a_{n-1}...a_0 = 10^n a_n + 10^{n-1}a_{n-1} + ... + 10a_1 + a_0$

Então:

- $10^0 \equiv 1 \pmod 6$

- $10^1 \equiv 4 \pmod 6$ ou $10^1 \equiv -2 \pmod 6$
- $10^2 \equiv 4 \pmod 6$ ou $10^2 \equiv -2 \pmod 6$
- $10^3 \equiv 4 \pmod 6$ ou $10^3 \equiv -2 \pmod 6$
- $10^4 \equiv 4 \pmod 6$ ou $10^4 \equiv -2 \pmod 6$
- $10^5 \equiv 4 \pmod 6$ ou $10^5 \equiv -2 \pmod 6$

...

Ou seja:

- $a_0.10^0 \equiv 1.a_0 \pmod 6$
- $a_1.10^1 \equiv 4.a_1 \pmod 6$ ou $a_1.10^1 \equiv -2.a_1 \pmod 6$
- $a_2.10^2 \equiv 4.a_2 \pmod 6$ ou $a_2.10^2 \equiv -2.a_2 \pmod 6$
- $a_3.10^3 \equiv 4.a_3 \pmod 6$ ou $a_3.10^3 \equiv -2.a_3 \pmod 6$
- $a_4.10^4 \equiv 4.a_4 \pmod 6$ ou $a_4.10^4 \equiv -2.a_4 \pmod 6$
- $a_5.10^5 \equiv 4.a_5 \pmod 6$ ou $a_5.10^5 \equiv -2.a_5 \pmod 6$

...

- $a_n.10^n \equiv 4.a_n \pmod 6$ ou $a_n.10^n \equiv -2.a_n \pmod 6$

Portanto $n = a_n a_{n-1}...a_0 = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10a_1 + a_0$ é divisível por 6 quando o algarismo das unidades somado ao quádruplo da soma dos algarismos de ordem par e subtraindo do dobro da soma dos algarismos de ordem ímpar o for.

Exemplo 1.10 *Verificando se* 24.678 *é divisível por* 6 *por este critério:*

1. *O algarismo da unidade é* 8
2. *Os algarismos da ordem par são* 6 *e* 2
3. *Os algarismos da ordem ímpar são* 7 *e* 4

Logo aplicando o processo, obtemos: $[8 + 4.(6 + 2) - 2.(7 + 4)] = [8 + 4.(8) - 2.(11)] = [8 + 32 - 22] = 18$

Como $18 = 6.3$ *é divisível por 6, temos então que o número* 24.678 *também é divisível por* 6.

Critério de divisibilidade por 8

Um número é divisível por 8*, quando seus 3 últimos algarismos formar um número divisível por* 8*.*

Exemplo 1.11 *O número* 119.888 *é divisível por* 8*, pois os* 3 *últimos algarismos é* 888 *que é divisível por* 8*. Já o número* 2.444 *não é divisível por* 8*, pois* 444 *não é divisível por* 8*.*

Mas também podemos usar a congruência modular para demonstrar.

Seja o número $n = a_n a_{n-1}...a_0 = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10a_1 + a_0$

Então:

- $10^0 \equiv 1 \pmod 8$
- $10^1 \equiv 2 \pmod 8$ ou $10^1 \equiv -6 \pmod 8$
- $10^2 \equiv 4 \pmod 8$ ou $10^2 \equiv -4 \pmod 8$
- $10^3 \equiv 0 \pmod 8$ ou $10^3 \equiv 0 \pmod 8$
- $10^4 \equiv 0 \pmod 8$ ou $10^4 \equiv 0 \pmod 8$
- $10^5 \equiv 0 \pmod 8$ ou $10^5 \equiv 0 \pmod 8$

...

Ou seja:

- $a_0.10^0 \equiv 1.a_0 \pmod 8$
- $a_0.10^1 \equiv 2.a_1 \pmod 8$ ou $a_0 10^1 \equiv -6.a_1 \pmod 8$
- $a_2.10^2 \equiv 4.a_2 \pmod 8$ ou $a_2 10^2 \equiv -4.a_2 \pmod 8$
- $a_3.10^3 \equiv 0.a_3 \pmod 8$ ou $a_3 10^3 \equiv 0.a_3 \pmod 8$
- $a_4.10^4 \equiv 0.a_4 \pmod 8$ ou $a_4 10^4 \equiv 0.a_4 \pmod 8$
- $a_5.10^5 \equiv 0.a_5 \pmod 8$ ou $a_5 10^5 \equiv 0.a_5 \pmod 8$

...

Portanto $n = a_n a_{n-1}...a_0 = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10a_1 + a_0$ é divisível por 8, se uma dessas duas maneiras distintas acontecer:

1. Um número é divisível por 8 quando o algarismo da unidade somado com o dobro do algarismo da dezena e ao quádruplo do algarismo da centena for divisível por 8
2. Um número é divisível por 8 quando o algarismo da unidade subtraído do sêxtuplo do algarismo da dezena e do quádruplo do algarismo da centena for divisível por 8

Exemplo 1.12 *Seja o número* 455.848, *usando o primeiro critério visto aqui temos:*

1. *O algarismo da unidade é* 8
2. *O algarismo da dezena é* 4
3. *O algarismo da centena é* 8

Aplicando o processo teremos:

$8 + 2.4 + 4.8 = 8 + 8 + 32 = 16 + 32 = 48$

Como $48 = 8.6$, *é divisível por 8, temos que o número* 455.848, *também é divisível por 8.*

Critério de divisibilidade por 9

Um número é divisível por 9, *quando a soma de todos os seus algarismos formar um número divisível por* 9.

Dado $n = a_n a_{n-1}...a_0 = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10a_1 + a_0$. Como $10 \equiv 1 \pmod 9$, temos então que $n \equiv a_n + a_{n-1} + ... + a_0 \pmod 9$. Portanto um número é divisível por 9 quando a soma de seus algarismos for um número divisível por 9.

Exemplo 1.13 *O número* 111.111.111 *é divisível por* 9, *pois* $1+1+1+1+1+1+1+1+1 = 9$ *que é divisível por 9. O número* 2347 *não é divisível por* 9, *pois* $2 + 3 + 4 + 7 = 16$ *que não é divisível por* 9.

Critério de divisibilidade por 10

Um número natural é divisível por 10 *quando ele termina em* 0.

Dado $n = a_n a_{n-1}...a_0 = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10a_1 + a_0$. Como $10 \equiv 0 \pmod{10}$, temos então que $n \equiv a_0 \pmod{10}$. Portanto um número é divisível por 10 quando seu último algarismos ou seja a_0 seja 0.

Utilizando o procedimento acima e as propriedades da congruência modular podemos deduzir critérios de divisibilidade para outros números.

1.4 A Congruência Modular no Cotidiano

Nessa seção apresentaremos algumas aplicações interessantes no nosso cotidiano relacionadas ao conceito de congruência modular. Tais aplicações podem ser abordadas tanto no ensino fundamental como no ensino superior.

1.4.1 Congruência Modular no Calendário

Figura 1 – Calendário de 2020

Fonte: Google imagens

Vamos supor que você saiba em qual dia da semana caiu o dia 1º de janeiro de um determinado ano. Em 2006, por exemplo, foi um domingo. Imaginemos que você deseja saber quando cairá um outro dia qualquer (vale para qualquer ano). É só montar uma tabela para essa primeira semana, que no caso será:

- Domingo $\rightarrow 1$, sabemos que $1 \equiv 1 \pmod 7$
- Segunda $\rightarrow 2$, sabemos que $2 \equiv 2 \pmod 7$
- Terça $\rightarrow 3$, sabemos que $3 \equiv 3 \pmod 7$
- Quarta$\rightarrow 4$, sabemos que $4 \equiv 4 \pmod 7$
- Quinta $\rightarrow 5$, sabemos que $5 \equiv 5 \pmod 7$
- Sexta $\rightarrow 6$, sabemos que $6 \equiv 6 \mod 7$

- Sábado $\rightarrow$ 7, sabemos que $7 \equiv 0 \mod 7$
- Domingo $\rightarrow$ 8 , sabemos que $8 \equiv 1 \pmod 7$
- Segunda $\rightarrow$ 9, sabemos que $9 \equiv 2 \pmod 7$
- Terça $\rightarrow$ 10, sabemos que $10 \equiv 3 \pmod 7$

$\vdots$

Verificamos aqui que estamos novamente diante de um caso de congruência, que nesse caso é $\pmod 7$. Digamos que estivéssemos interessados em descobrir em que dia da semana caiu o dia 5 de julho de 2006 (e não temos um calendário em mãos, é claro). Primeiro precisamos saber quantos dias existem de 1 de janeiro até 5 de julho. Vejamos:

Janeiro = 31 dias

Fevereiro= 28 dias (2006 não é bissexto)

Março = 31 dias

Abril = 30 dias

Maio = 31 dias

Junho = 30 dias

Julho = 5 dias

Total= 186 dias. Agora, é como se tivéssemos uma fila de 186 dias e estamos desejando saber, na congruência de (mod 7) (7 dias da semana) qual o correspondente ao 186. Se dividirmos 186 por 7, teremos: quociente 26 e resto 4. Logo, o $186 \equiv 4 \pmod 7$. Como o dia 4 de janeiro de 2006 foi uma quarta-feira, o $186^{\underline{o}}$ desse mesmo ano também o será e, é claro, que todas as demais quarta-feiras deste ano serão ocupados por números congruentes ao 4 módulo 7.

1.4.2 Congruência Modular no CPF-Cadastro de Pessoas Físicas

Nessa seção mostraremos como são calculados os dois dígitos de controle do CPF através dos 9 dígitos anteriores usando-se a aritmética modular.

Uso de congruência na verificação do CPF: temos que verificar os dois dígitos de controle do CPF de uma pessoa: O CPF de uma pessoa registrada no Brasil, é constituído de 11

Figura 2 – Cadastro de pessoa física-CPF

Fonte: Google imagens

dígitos, sendo um primeiro grupo com 9 algarismos e um segundo grupo, com mais dois algarismos, dígitos de controle ou de verificação. Para determinar esses dois dígitos de controle é aplicada a congruência modular. No caso do CPF, o décimo dígito (que é o primeiro dígito verificador) é o resultado de uma congruência, módulo 11 de um número obtido por uma operação dos primeiros nove algarismos.

Se $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ é a sequência formada pelos 9 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e somar os produtos obtidos. O dígito que está faltando, que vamos representar por a_{10} deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número $S - a_{10}$ deve ser múltiplo de 11, ou seja, $S - a_{10} \equiv 0 \pmod{11}$. Observemos que o número será o próprio resto da divisão por 11 da soma obtida. Exemplo, se o CPF de uma pessoa tem os seguintes 9 primeiros dígitos: 235 343 104, o primeiro dígito de controle será obtido da seguinte maneira: Escrevemos os nove primeiros e, abaixo deles, a base de multiplicação com os dígitos de 1 a 9. Vejamos:

2	3	5	3	4	3	1	0	4
1	2	3	4	5	6	7	8	9

Efetuando as multiplicações correspondentes, teremos:

$2.1 + 3.2 + 5.3 + 3.4 + 4.5 + 3.6 + 1.7 + 0.8 + 4.9 = 116.$

Dividindo o número 116 por 11, teremos:

resto 6 e quociente 10 ou seja $116 = 11.10 + 6$

Em notação de congruência seria: $116 \equiv 6 \pmod{11}$.

Dessa forma, o primeiro dígito de controle será o algarismo 6.

A determinação do segundo dígito de controle é feita de modo similar, sendo que agora acrescentamos o décimo dígito (que é o que acabamos de calcular) e usamos uma base de multiplicação de 0 a 9.

2	3	5	3	4	3	1	0	4	6
0	1	2	3	4	5	6	7	8	9

Efetuando as multiplicações, teremos:

$$2.0 + 3.1 + 5.2 + 3.3 + 4.4 + 3.5 + 1.6 + 0.7 + 4.8 + 6.9 = 145$$

Dividindo o número 145 por 11, teremos:

resto 2 e quociente 13 ou seja $145 = 13.11 + 2$

Em notação de congruência seria: $145 \equiv 2 \pmod{11}$.

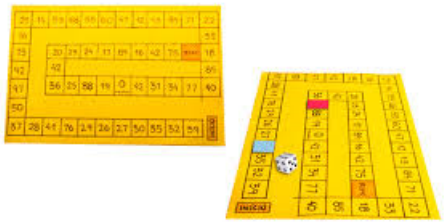
Portanto, o segundo dígito de controle é o 2. Podemos concluir que, no nosso exemplo, o CPF completo seria: 235 343 104-62. Se o resto da divisão fosse 10, ou seja, se o número obtido fosse congruente ao 10, módulo 11, usaríamos, nesse caso, o dígito zero.(SÁ, 2010)

2 Atividades Práticas de Aritmética Modular para o Ensino Médio

Nesse capítulo trazemos propostas de atividades focadas nos ensinos Fundamental e Médio, objetivando tornar os conteúdos matemáticos referente a divisibilidade menos abstratos e mais interessantes aos alunos. Esta abordagem se justifica por vários motivos, dentre eles, contribuir para a formação continuada dos professores que atuam na educação básica e explorar as possibilidades da aritmética modular para o desenvolvimento do raciocínio lógico e pensamento conceitual entre alunos do ensino fundamental e médio. A proposta metodológica aqui é a apresentação do problema antes dos conceitos e das técnicas de como resolvê-lo, permitindo que os alunos assumam uma postura de investigação frente a qualquer situação ou fato que possa ser questionado. As atividades didáticas elaboradas utilizarão o Jogo dos Restos, a Aritmética do Relógio, Congruência Modular no Ciclo Trigonométrico e Congruência Modular Aplicada nos Números Complexos.

2.1 Jogo dos Restos

Figura 3 – Jogo dos Restos



Fonte: Google imagens.

Consiste em formar um caminho de números naturais aleatórios que devem ser divididos por valores de 1 a 6 sorteados em um dado. Por exemplo.

Considere à sequência de número do caminho

$(20, 45, 90, 36, 7, 6, 10, 11, 57)$. O 20 é o número de início do jogo, e o 57 é o número do final do jogo. Pode jogar duas ou mais pessoas.

Regra do jogo

As pessoas começam sorteando um número de 1 a 6 no dado. Exemplo: a primeira pessoa joga o dado e o resultado é 3. Como 20 dividido por 3 tem resto 2, ou seja $20 \equiv 2 \pmod 3$, a pessoa avança duas casas e vai para o próximo número que no exemplo é o número 90, a segunda pessoa tirou um 2 no dado, não avançará pois 20 dividido por 2 tem resto zero

ou seja $20 \equiv 0 \pmod 2$. Ganhará o jogo quem chegar exatamente no número 57 primeiro. Caso a quantidade de avanços passar do número 57 é só parar sobre o número 57.

2.1.1 Sequência didática

Área de conhecimento: Matemática

Público alvo: Alunos do 1º ano do Ensino Médio

Conteúdo: Divisibilidade, números compostos, números primos e congruência modular

Recurso: Papel A4, piloto, quadro branco, jogo e dados

Tempo previsto: Dividimos em 4 momentos de 2 aulas de 50 minutos cada

Competência Específica

Perceber a necessidade de conhecer a diferença entre números primos e compostos e o conceito de congruência modular.

Habilidades

- EF06MA05: Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por $2, 3, 4, 5, 6, 8, 9, 10, 100$ e 1000.
- EF06MA06: Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.

Primeiro Momento:

1. O professor deverá falar do jogo dos restos e ensinar as regras do jogo para a turma.
2. O professor deverá entregar uma atividade impressa conforme (ANEXO 1) com o jogo dos restos para cada dupla. Para jogar serão utilizados sementes diferentes como por exemplo de feijões e milhos. O primeiro jogador joga o dado e o número da face é 6, como o primeiro número do caminho é 20 o aluno deverá dividir o 20 por 6 e determinar o resto que é dois. O resto será o valor da quantidade de casas que ele avançará no jogo. Logo o aluno avançará 2 casas. O segundo jogador joga

o dado e o número da face é 2, como o primeiro número do caminho é 20 o aluno deverá dividir o 20 por 2 e determinar o resto que é zero. Logo o aluno não avançará no jogo. Cada aluno deverá em cada jogada anotar as divisões na folha impressa.

3. O professor deverá mostrar na lousa a notação de congruência modular e pedir para que cada aluno anote os resultados das divisões de duas maneiras: a tradicional e também em notação de congruência modular.

4. Abrir um diálogo para saber o que eles aprenderam com o jogo. Espera-se que o alunos percebam que quando o número do caminho é múltiplo do número da face do dado, ele não avança no jogo. E quando o número do caminho não é divisível pelo número da face do dado ele avança no jogo de acordo o valor do resto da divisão.

Segundo Momento:

1. O professor deverá definir o que é uma congruência modular conforme o capítulo 1.

2. O professor deverá entregar uma lista de exercícios conforme (ANEXO 2) com divisões de números inteiros para cada aluno e pedir para eles escreverem as divisões na forma de congruência modular.

3. Abrir um diálogo para saber se houve dificuldades na resolução da lista de exercícios e fazer a correção da lista de exercícios.

Terceiro Momento:

1. O professor deverá mostrar as propriedades da congruência modular conforme o capítulo 2.

2. O professor deverá entregar uma lista de exercícios com os conteúdos ensinados para os alunos resolverem de maneira individual.

3. Abrir um diálogo para saber se houve dificuldades na resolução da lista de exercícios.

4. Fazer a correção da lista de exercícios.

Quarto Momento:

1. O professor deverá entregar uma lista de exercícios que contemple os conteúdos revisados através do uso de congruência modular para os alunos resolverem de maneira individual.

2. Abrir um diálogo para saber se houve dificuldades na resolução da lista de exercícios e fazer a correção da lista de exercícios.

Instituição:

Aluno(a): ANEXO 1

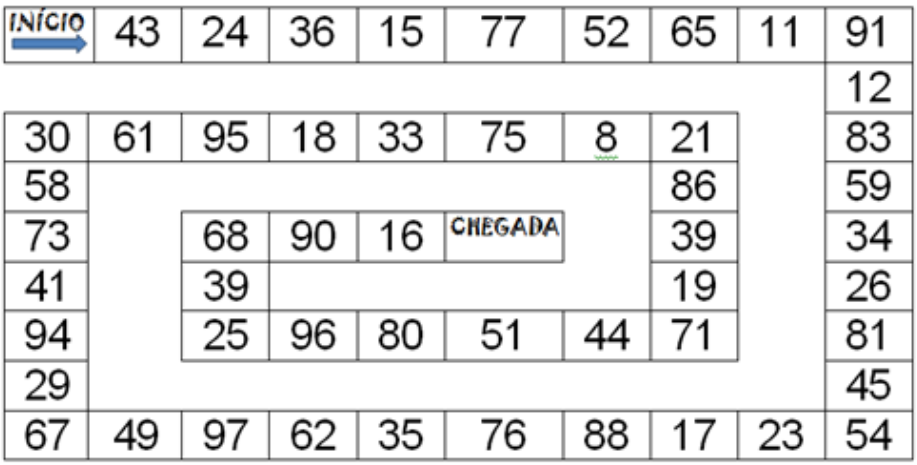
Prof(a): **Data:**

Conteúdo: congruência modular

Atividade

Jogo dos Restos

Utilizem dado, caroços de feijões e milhos para jogarem.



Resultado das divisões do número do caminho pelo número da face do dado escrito na forma tradicional e na forma de congruência modular. Onde R representa o resto e F é o número da face do dado.

Caminho $\equiv$ **R** $(\text{mod } F)$ **Caminho**$\equiv$ **R** $(\text{mod } F)$

Instituição:

Aluno(a): ANEXO 2

Prof(a): **Data:**

Conteúdo: divisibilidade, números primos, compostos e critérios de divisibilidade

Lista de exercícios

1) **Determine o quociente e o resto nas divisões abaixo.**

a) $342.345 \div 16 =$ **b)**$111.111.111 \div 9 =$

2) **Sem efetuar a divisão verifique se os números abaixo são divisíveis por oito.**

a) $1.234.888$ **b)**$3.456.012$

3) **Determine o maior número de** 4 **algarismos que seja divisível por quatro.**

4) **Determine o maior número de** 5 **algarismos que seja divisível por três.**

5) **Verifique se 97 é primo ou composto.**

6) **Qual o resto na divisão euclidiana de** -14 **por** 4 **?**

7) **Quantos divisores têm os números A=** $3^4.7^5.11^8$ **e B=** 1024 **?**

Gabarito do ANEXO 2

Questão 1

a) Quociente 21396 e resto 9

b) Quociente 12345679 e resto 0

Questão 2

a)$888 = 8.111$

b) 012 não é divisível por 8

Questão 3

O maior número de 4 algarismos é o 9999, mas que seja divisível por 4 é o 9996

Questão 4

O maior número de 5 algarismos é o 99999 e também é divisível por 3, pois $99999 = 3.33333$

Questão 5

Devemos dividir o número 97 pela sequência de números primos até o quociente ficar menor que o divisor. Como 97 não divisível por 2,3,5,7,11 e quando dividimos por 11 o quociente é 8 que é menor que 11. Portanto 97 é primo.

Questão 6

$-14 = 4.(-4) + 2$. Portanto o resto é 2.

Questão 7

O número A tem 5.6.8= 240 divisores e o número B tem 11 divisores

2.2 Aritmética do Relógio

Figura 4 – Relógio de Parede

Fonte: Google imagens.

Trata-se de um caso de congruência, módulo 12 (nos relógios analógicos, é claro). Note que 13 horas é congruente a 1 hora, no módulo 12. Ambos divididos por 12, deixam resto 1. 17 horas é congruente a 5 horas, módulo 12. Tanto 17, como 5, divididos por 12, deixam resto 5... e assim, sucessivamente. $1 \equiv 13 \equiv 25 \equiv ....,\mod 12$, $5 \equiv 17 \equiv 29 \equiv ....,\mod 12$. Assim as horas marcadas num relógio analógico constituem também um caso clássico de congruência, nesse caso com módulo 12. (SÁ, 2010)

2.2.1 Sequência didática

Área de conhecimento: Matemática

Público alvo: Alunos do 1º ano do Ensino Médio

Conteúdo: Divisibilidade, medida de tempo e medida de ângulo

Recurso: Relógio de parede, piloto e quadro branco

Tempo previsto: Dividimos em 3 momentos de 2 aulas de 50 minutos cada

Competência Específica

Trabalhar as conversões de grandezas de tempo, ângulo e o conceito de congruência modular.

Habilidades

- EF06MA27: Determinar medidas da abertura de ângulos, por meio de transferidor e/ou tecnologias digitais.
- EF06MA26: Resolver problemas que envolvam a noção de ângulo em diferentes contextos e em situações reais, como ângulo de visão.
- EF06MA24: Resolver e elaborar problemas que envolvam as grandezas comprimento, massa, tempo, temperatura, área (triângulos e retângulos), capacidade e volume (sólidos formados por blocos retangulares), sem uso de fórmulas, inseridos, sempre que possível, em contextos oriundos de situações reais e/ou relacionadas às outras áreas do conhecimento.
- EM13MAT103: Interpretar e compreender o emprego de unidades de medida de diferentes grandezas, inclusive de novas unidades, como as de armazenamento de dados e de distâncias astronômicas e microscópicas, ligadas aos avanços tecnológicos, amplamente divulgadas na sociedade.
- EF06MA05: Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por $2, 3, 4, 5, 6, 8, 9, 10, 100$ e 1000.
- EF06MA06: Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.

Primeiro Momento:

1. O professor deverá perguntar para turma por que no relógio de parede não podemos escrever 23h. Espera-se que eles respondam que 23h seria o mesmo que 11h. O professor deverá perguntar quais relações existem entre os números 23h e 11h , 19h e 7h ou 26h e 2h. Espera-se que eles percebam que a diferença entre eles são múltiplo de 12. O professor deverá definir o que é uma congruência modular através do relógio de parede e pedir para os alunos escrevem alguns pares de horas que são congruentes módulo 12.
2. O professor deverá entregar uma lista de exercícios conforme o ANEXO 3, com exemplos que envolvam divisões de números inteiros e pedir para que os alunos escrevam as divisões na notação de congruência modular.
3. Abrir um diálogo para saber se houve dificuldades na resolução da lista de exercícios e fazer a correção da lista de exercícios.

Segundo Momento:

1. O professor deverá fazer uma breve revisão do conteúdo de divisibilidade, números compostos, números primos, medidas de tempo e medidas de ângulo.
2. O professor deverá entregar uma lista de exercícios conforme o ANEXO 4, com o conteúdo explicado para os alunos resolverem de maneira individual.
3. Abrir um diálogo para saber se houve dificuldades na resolução da lista de exercícios e fazer a correção da lista de exercícios.

Terceiro Momento:

1. O professor deverá mostrar as propriedades da congruência modular.
2. O professor deverá entregar uma lista de exercícios com o conteúdo explicado para os alunos resolverem de maneira individual.
3. Abrir um diálogo para saber se houveram dificuldades na resolução da lista de exercícios e fazer a correção da lista de exercícios.

Instituição:

Aluno(a): ANEXO 3

Prof(a): **Data:**

Conteúdo: divisibilidade, medidas de tempo e medidas de ângulo

Lista de exercícios

1) **Transforme as medidas abaixo.**

a) $3h$ **em** s **b)**12 **dias em h**

2) **Transforme as medidas abaixo.**

a) $30°$ **em minutos** **b)**$120'$ **em graus** **c)**$3600''$ **em graus**

3) **Converta os dias do mês de Julho em segundos.**

4) **Calcule.**

a) $30°\ 12'\ 27'' \div 3 =$ **b)**$48'\ 12'' \div 4 =$

5) **Quantos graus indica os ponteiros dos minutos e horas do relógio abaixo ?**

Resposta:

Gabarito do ANEXO 3

Questão 1

a) 10.800 segundos

b) 288 horas

Questão 2

a)1800'

b) 2 graus

c) 1 grau

Questão 3

2.678.400 segundos

Questão 4

a)$10^\circ\ 4'\ 9''$ b) $12'\ 3''$

Questão 5

120 graus

Instituição:

Aluno(a): ANEXO 4

Prof(a): **Data:**

Conteúdo: divisibilidade, medidas de tempo, medidas de ângulo e congruência modular

Lista de exercícios

1) **Escreva em notação de congruência modular as divisões abaixo.**

a) $28 \div 5$ **b)**$34 \div 6$

2) **Em um relógio de parede quantas horas representa** $26h$ **?**

3) **Escreva** $56h$ **em notação de congruência modular. Considere um relógio de parede.**

4) **Quantos graus indica os ponteiros dos minutos e horas do relógio abaixo ? Escrevendo** 21 **horas em notação de congruência modular módulo** 12 **o que podemos concluir ?**

Respostas:

Gabarito do ANEXO 4

Questão 1

a) $28 \equiv 3 \pmod 5$

b) $34 \equiv 4 \pmod 6$

Questão 2

$26 \equiv 2 \pmod{12}$ ou seja são 2 horas

Questão 3

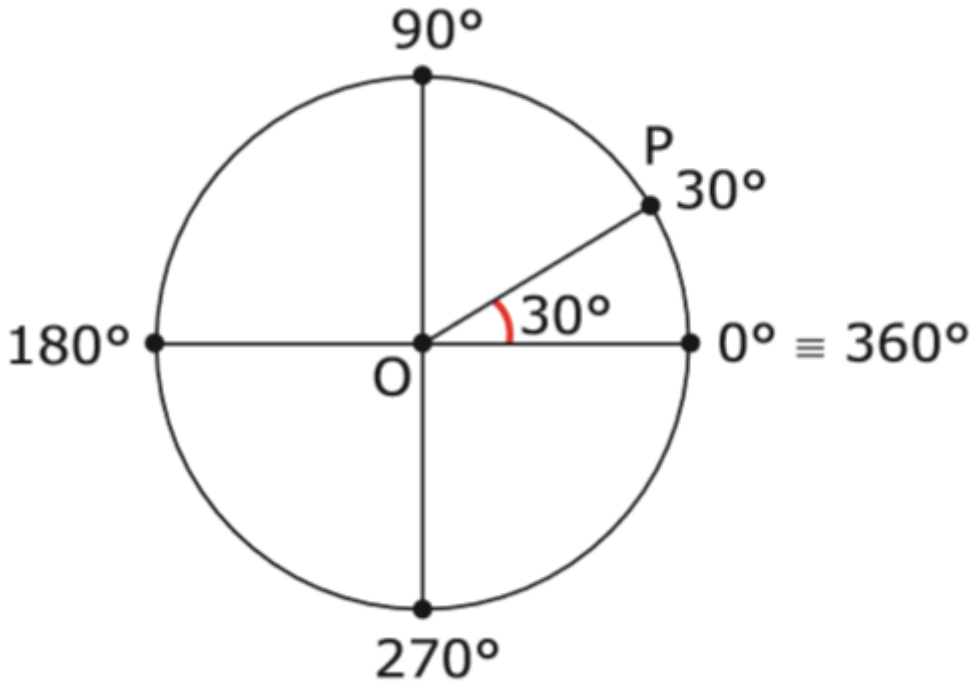
$56 \equiv 8 \pmod{12}$

Questão 4

$270°$ e $21 \equiv 9 \pmod{12}$, podemos concluir que são 9 horas

2.3 Congruência Modular no Ciclo Trigonométrico

Figura 5 – Ciclo Trigonométrico



Fonte: Google imagens

Definição 2.1 *Dois arcos são côngruos quando possuem a mesma origem e a mesma extremidade. Uma regra prática eficiente para determinar se dois arcos são côngruos consiste em verificar se a diferença entre eles é um número divisível ou múltiplo de* $360°$.

Definição 2.2 *Um grau* $1°$ *equivale a uma das* 360 *partes iguais em que a circunferência pode ser dividida. Um grau, por sua vez, divide-se em* 60 *minutos* $(60')$ *e cada minuto pode ser divido em* 60 *segundos* $(60'')$.

Definição 2.3 *Razão trigonométrica também chamada de relação trigonométrica é o resultado da divisão entre as medidas de dois lados de um triângulo retângulo. As razões trigonométricas são capazes de relacionar os lados com os ângulos de um triângulo retângulo. Exemplo: seno, cosseno, tangente, cotangente , secante e cossecante são razões trigonométricas.*

2.3.1 Sequência didática

Área de conhecimento: Matemática

Público alvo: Alunos do 2^{o} ano do Ensino Médio

Conteúdo: Divisibilidade, medida de ângulo e arcos côngruos

Recurso: piloto e quadro branco

Tempo previsto: Dividimos em 3 momentos de 2 aulas de 50 minutos cada

Competência Específica

Aprender como utilizar congruência modular em arcos côngruos.

Habilidades

- EM13MAT103: Interpretar e compreender o emprego de unidades de medida de diferentes grandezas, inclusive de novas unidades, como as de armazenamento de dados e de distâncias astronômicas e microscópicas, ligadas aos avanços tecnológicos, amplamente divulgadas na sociedade.
- EM13MAT308: Aplicar as relações métricas, incluindo as leis do seno e do cosseno ou as noções de congruência e semelhança, para resolver e elaborar problemas que envolvem triângulos, em variados contextos.

Primeiro Momento:

1. O professor deverá revisar o conteúdo de trigonometria no triângulo retângulo, razões trigonométricas e medidas de ângulo.
2. O professor deverá entregar uma lista de exercícios conforme o ANEXO 5, com os conteúdos revisados para os alunos resolverem de maneira individual.
3. Abrir um diálogo para saber se houve dificuldades na resolução da lista de exercícios.
4. Fazer a correção da lista de exercícios.

Segundo Momento:

1. O professor deverá perguntar para a turma quais as relações que existem entre as medidas dos ângulos de 750 graus e 30 graus, 450 graus e 90 graus. Espera-se que os alunos respondam que a diferença entre esses pares de números são múltiplos de 360.
2. O professor deverá pedir para os alunos darem exemplos de pares de arcos cuja medidas de suas diferenças são múltiplos de $360°$.

3. O professor deverá definir o que é uma congruência modular e o que são arcos côngruos.

4. O professor deverá pedir para os alunos escreverem exemplos de medidas de arcos cuja diferença é múltiplo de 360 graus em notação de congruência modular.

5. O professor deverá entregar lista de exercícios conforme o ANEXO 6, com o conteúdo explicado para os alunos resolverem de maneira individual.

6. Abrir um diálogo para saber se houve dificuldades na resolução da lista de exercícios e fazer a correção da lista de exercícios.

Terceiro Momento:

1. O professor deverá mostrar as propriedades da congruência modular conforme o capítulo 1.

2. O professor deverá mostrar como passar as medidas de arcos no círculo trigonométrico com mais de uma volta para o primeiro quadrante através da congruência modular sem mudar os valores dos cálculos.

3. O professor deverá entregar uma lista de exercícios com os conteúdos revisados para os alunos resolverem de maneira individual.

4. Abrir um diálogo para saber se houve dificuldades na resolução da lista de exercícios e fazer a correção da lista de exercícios.

Instituição:

Aluno(a): ANEXO 5

Prof(a): **Data:**

Conteúdo: razões trigonométricas, medidas de ângulos e congruência modular

Lista de exercícios

1) **Calcule sen** $750°$**.**

2) **Determine o quociente** $\frac{cos390°}{sen450°}$ **.**

3) **Calcule** $sen^2450° + cos^290°$**.**

4) **Calcule** $sen410° - cos400°$**.**

5) **Calcule** $tg750°$**.**

Gabarito do ANEXO 5

Questão 1

$sen750° = sen30° = \frac{1}{2}$, pois $750 \equiv 30 \pmod{360}$

Questão 2

$\frac{cos390°}{sen450°} = \frac{cos30°}{sen90°} = \frac{\sqrt{3}}{2}$

Questão 3

$sen^2450° + cos^290° = sen^290° + cos^290° = 1$

Questão 4

$sen410° - cos400° = sen50° - cos40° = 0$, pois $sen50° = cos40°$

Questão 5

$tg750° = tg30° = \frac{\sqrt{3}}{3}$

Instituição:

Aluno(a): ANEXO 6

Prof(a): **Data:**

Conteúdo: razões trigonométricas, medidas de ângulos e congruência modular

Lista de exercícios

1) **Escreva em notação de congruência modular, módulo** 360 **o ângulo de medida** $750°$**.**

2) **Sabendo que** $cos1110° = x$**. Calcule** $sen1110° + cos1110°$

3) **Determine o valor de** $0 < y < 360°$ **na congruência modular** $y \equiv 390° \pmod{360}$**.**

4) **Determine o valor de** $0 < x < 360°$ **na congruência modular** $750° \equiv x \pmod{360}$**.**

5) **Escreva em notação de congruência modular as divisões abaixo.**

a) $1080° \div 360$ **b)**$720° \div 360$

Gabarito do ANEXO 6

Questão 1

$750° \equiv 30°$ (mod 360°)

Questão 2

$cos1110° = cos30° = x$ e $sen1110° = sen30° = \frac{1}{2}$, logo a resposta é $x + \frac{1}{2}$

Questão 3

$360° \equiv 30°$ (mod 360), portanto $y = 30°$

Questão 4

$750° \equiv 30°$ (mod 360), portanto $x = 30°$

Questão 5

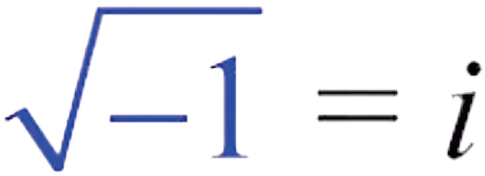
a) $1080° \equiv 0°$ (mod 360)

b) $720° \equiv 0°$ (mod 360)

2.4 Congruência Modular nos Números Complexos

Nessa seção falaremos das potências dos números complexos, mas especificamente das potências de i cujos valores tem um comportamento cíclico quando aumentamos os valores dos expoentes. Mostraremos como aplicar a congruência modular para diminuir o valor do expoente e facilitar os cálculos.

Figura 6 – Unidade imaginária



Fonte: Google imagens

Potências de i

Vamos calcular algumas potências de i:

- $i^0 = 1$
- $i^1 = i$
- $i^2 = -1$
- $i^3 = i^2.i = -1.i = -i$
- $i^4 = i^2.i^2 = (-1).(-1) = 1$
- $i^5 = i^4.i = 1.i = i$
- $i^6 = i^5.i = i.i = i^2 = -1$
- $i^7 = i^6.i = -1.i = -i$
- $i^8 = i^7.i = -i.i = -i^2 = 1$

$\vdots$

Note que os resultados repetem-se de 4 em 4 formando o seguinte conjunto $\{1, i, -1, -i\}$. As potências de i são cíclicas. Então podemos escrever:

- $i^0 = i^4 = i^8 = \cdots = i^{4k} = (i^4)^k = 1^k = 1$
- $i^1 = i^5 = i^9 = \cdots = i^{4k+1} = i^{4k}.i^1 = (i^4)^k.i^1 = 1.i = i$
- $i^2 = i^6 = i^{10} = \cdots = i^{4k+2} = i^{4k}.i^2 = (i^4)^k.i^2 = 1.(-1) = -1$

- $i^3 = i^7 = i^{11} = \cdots = i^{4k+3} = i^{4k}.i^3 = (i^4)^k.i^3 = 1.i^3 = 1.(-i) = -i$

$\vdots$

Ou seja, para calcular potências de i, basta dividir o expoente de i por 4 e considerar apenas i elevado ao resto dessa divisão.

Portanto podemos usar a congruência modular para determinar o resto da divisão de i por 4.

Exemplo 2.1 *Calcule* i^{122}.

Solução:

Temos que dividir 122 por 4.

Como $122 \equiv 2 \pmod 4$, temos que $i^{122} = i^2 = -1$

Solução:

Temos que dividir 403 por 4.

Como $403 \equiv 3 \pmod 4$, temos que $i^{403} = i^3 = i^2.i = -1.i = -i$

2.4.1 Sequência didática

Área de conhecimento: Matemática

Público alvo: Alunos do 3º ano do Ensino Médio

Conteúdo: Divisibilidade, potenciação: propriedades e congruência modular

Recurso: piloto e quadro branco

Tempo previsto: Dividimos em 3 momentos de 2 aulas de 50 minutos cada

Competência Específica

Aprender como utilizar as propriedades das potências para facilitar os cálculos e entender o conceito de congruência modular.

Habilidades

- EF06MA11: Resolver e elaborar problemas com números naturais envolvendo a potenciação.

- EF06MA06: Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.

Primeiro Momento:

1. O professor deverá revisar o conteúdo de potenciação e suas propriedades.
2. O professor deverá entregar uma lista de exercícios conforme o ANEXO 7, com os conteúdos revisados para os alunos resolverem de maneira individual.
3. Abrir um diálogo para saber se houve dificuldades na resolução da lista de exercícios e fazer a correção da lista de exercícios.

Segundo Momento:

1. O professor deverá calcular algumas potências de i até os alunos perceberem que os valores estão se repetindo. Espera-se que os alunos percebam que os valores se repetem de 4 em 4.
2. O professor deverá perguntar para a turma como calcular as potências de i quando o expoente for um número com muitos dígitos. Espera-se que os alunos percebam que basta dividir por 4 o expoente da potência e substituir ele pelo seu resto.
3. O professor deverá definir o que é uma congruência modular conforme o capítulo 1.
4. O professor deverá pedir para os alunos calcularem divisões de números naturais por 4 na forma tradicional e na forma de congruência modular.
5. O professor deverá mostrar como calcular potências de i nos números complexos através da congruência modular.
6. O professor deve entregar uma lista de exercícios conforme ANEXO 8, com o conteúdo explicado para os alunos resolverem de maneira individual.
7. Abrir um diálogo para saber se houve dificuldades na resolução da lista de exercícios e fazer a correção da lista de exercícios.

Terceiro Momento:

1. O professor deverá ensinar as propriedades da congruência modular conforme o capítulo 1.
2. O professor deverá entregar uma lista de exercícios com os conteúdos ensinados e revisados para os alunos resolverem de maneira individual.

3. Abrir um diálogo para saber se houve dificuldades na resolução da lista de exercícios e fazer a correção da lista de exercícios.

Instituição:

Aluno(a): ANEXO 7

Prof(a): **Data:**

Conteúdo: Potenciação e suas propriedades

Lista de exercícios

1) **Determine o algarismo da dezena do número** 2^{12}**.**

2) **Aplique as propriedades da potência e calcule.**

a) $\frac{2^{500}}{2^{498}}$ **b)** $3^{-34}.3^{37}$ **c)** $(3^3)^2$

3) **Calcule** $2^{2^2} + 4^{2^2}$**.**

4) **Determine o próximo número da sequência** $(1024, 512, 256, 128, \ldots)$**.**

5) **Sabendo que a base de uma potência é** -7 **e a potência é** $\frac{1}{49}$**. Determine o expoente.**

Gabarito do ANEXO 7

Questão 1

$2^{12} = 4096$, portanto o algarismo da dezena são 9

Questão 2

a) $\frac{2^{500}}{2^{498}} = 2^2 = 4$ **b)** $3^{-34}.3^{37} = 3^3 = 27$ **c)** $(3^3)^2 = 3^6 = 729$

Questão 3

$2^{2^2} + 4^{2^2} = 2^4 + 4^4 = 16 + 256 = 272$

Questão 4

64

Questão 5

$(-7)^x = \frac{1}{49}$, portanto $x = -2$

Instituição:

Aluno(a): ANEXO 8

Prof(a): **Data:**

Conteúdo: Congruência modular e Números complexos: potência de i

Lista de exercícios

1) **Calcule as potências abaixo .**

a) $i^{120} =$ **b)** $(\frac{1}{i})^{-40} =$ **c)** $i^{400n+10} =$

2) **Calcule.**

a) $i^{4001} + i^{32} =$ **b)** $(-i)^0 =$

3) **Calcule a potência** $(2 - 2i)^8$**.**

4) **Calcule** $i^1.i^2.i^3.\ldots.i^{99}.i^{100}$**.**

5) **Calcule** $\sum_{n=1}^{200} i^n$**.**

Gabarito do ANEXO 8

Questão 1

a) $i^{120} = i^0 = 1$ **b)**$(\frac{1}{i})^{-40} = i^{40} = i^0 = 1$ **c)**$i^{400n+10} = i^{10} = i^2 = -1$

Questão 2

a) $i^{4001} + i^{32} = i^1 + i^0 = i + 1$ **b)**$(-i)^0 = 1$

Questão 3

$(2 - 2i)^8 = -8i$

Questão 4

$i^1.i^2.i^3.\ldots.i^{99}.i^{100} = i^{5050} = ir = -1$

Questão 5

$\sum_{n=1}^{200} i^n = i^{20100} = i^0 = 1$

3 Teoremas Importantes e Resolução de Problemas

O assunto abordado neste capítulo é mais voltado para os alunos do ensino superior. Um dos nossos objetivos neste capítulo será apresentar alguns dos principais teoremas que envolvem o conceito da aritmética modular de modo a levar os alunos do ensino superior a ampliar sua compreensão acerca destes resultados e promover o desenvolvimento do pensamento aritmético e algébrico. Para promover esta maior compreensão, falaremos um pouco sobre o autor de cada teorema, além de obviamente enunciar e demonstrar cada teorema. Por fim, serão resolvidos vários exercícios de nível superior, também com o objetivo de promover uma melhor fixação deste assunto.

3.1 Pequeno Teorema de Fermat

Nessa seção traremos um pouco da história do matemático e cientista Pierre de Fermat $(1601, 1665)$, também apresentaremos o Pequeno Teorema de Fermat, que é de grande importância na resolução de problemas que envolvem Congruência Modular com Potenciação. Enunciaremos, demonstraremos e daremos exemplo de aplicação.

Figura 7 – Pierre de Fermat

Fonte: Google imagens

Pierre de Fermat $(1601, 1665)$ foi um matemático e cientista francês, nascido na primeira década do século XVII. Nascido na região de Basca, Fermat teve uma infância rica e com uma educação privilegiada, que foi custeada pelo seu pai, um rico mercador de peles. Iniciou seus estudos no mosteiro franciscano de Grandselve e posteriormente matriculou-se na Universidade de Toulouse, estudando direito e depois matemática. Fermat seguiu sua carreira no funcionalismo público e em 1652 foi promovido a Juiz Supremo da corte criminal do parlamento de Toulouse. Sua carreira na matemática foi pouco di-

vulgada, pois o próprio Fermat não tinha interesse em publicar suas descobertas. O pouco que se conhece é pelas cartas a amigos, anotações pessoais e trabalhos que foram resgatados depois de sua morte. Fermat desenvolveu, independentemente de René Descartes, os princípios matemáticos para usar um sistema de coordenadas para definir as posições de pontos. Trabalhou também intensivamente com o estudo de curvas, onde um de seus avanços consiste em calcular a área sob uma curva de modo muito similar ao cálculo integral. As contribuições de Fermat são de extrema importância para o cálculo geométrico e infinitesimal, obtendo em seus cálculos diversas áreas de figuras geométricas bem como seu centro de massa. Em uma observação escrita por Isaac Newton em um de seus cálculos, citava Pierre de Fermat como referência e inspiração para o desenvolvimento do cálculo. (BOYER; MERZBACH, 2019)

Contudo, o que mais interessava a Fermat, era um ramo da Matemática chamado teoria dos números, com poucas aplicações práticas claras. É nesta teoria dos números que se engloba o seu famoso teorema, conhecido como Último Teorema de Fermat. Este teorema tem um enunciado extremamente simples: Não existe nenhum conjunto de inteiros positivos x, y, z e n com n maior que 2 que satisfaça a equação $x^n + y^n = z^n$. Como o matemático possuía a prática de fazer apenas anotações informais sobre seus estudos, o único indício de uma prova deste teorema é uma observação por ele deixada em 1637 em um de seus livros, "Aritmética", de Diofante: Esta anotação foi descoberta pelo seu filho alguns anos após sua morte, e junto a outros comentários de Fermat, foi publicada numa edição comentada do livro em questão. A partir disso, o teorema virou objeto de estudo de diversos estudiosos ao longo dos anos, que tentaram através de diversas abordagens desenvolver uma demonstração que provasse o teorema. (SIMON, 1998)

E de sua autoria outro teorema importante, o "Pequeno Teorema de Fermat". Apesar da grande importância, a primeira demonstração do chamado "pequeno teorema de Fermat" levou quase cem anos para ser divulgada. Foi publicada apenas em 1736, pelo grande Leonhard Euler.(Túnel do tempo 18 de outubro de 2017).

Teorema 3.1 *(Pequeno Teorema de Fermat - PTF): seja $a \in \mathbb{Z}$, e se p é primo e se o $MDC(p, a) = 1$, então:*

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

Demonstração:

Considere os $(p-1)$ primeiros múltiplos positivos de a, isto é, os inteiros

$$a, 2.a, 3.a, \ldots, (p-1).a$$

Claramente, nenhum desses $(p-1)$ inteiros é divisível por p e, além disso, dois quaisquer deles são incongruentes módulo p, pois, se

$$r.a \equiv s.a \pmod{p}, 1 \leq r < s \leq p-1$$

então, o fator comum a poderia ser cancelado, visto que o MDC$(a, p) = 1$, e teríamos:

$$s \equiv r \pmod{p}, \text{ isto é } p|(s-r)$$

o que é impossível, porque $0 < s - r < p$.

Assim sendo, dois quaisquer dos $(p-1)$ inteiros $a, 2.a, 3.a, \ldots, (p-1).a$ divididos por p deixam restos distintos, e por conseguinte cada um desses $(p-1)$ inteiros é congruente módulo p a um único dos inteiros $1, 2, 3, \ldots, p-1$, naturalmente numa ordem, multiplicando ordenadamente essas $(p-1)$ congruências, teremos:

$$a.2.a.3.a.\ldots.(p-1).a \equiv 1.2.3.\ldots.(p-1) \pmod{p}$$

ou seja,

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

Como o MDC$(p, (p-1)!) = 1$, porque p é primo e p não divide $(p-1)!$, podemos cancelar o fator $(p-1)!$. Portanto

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

■

(OLIVEIRA, 2019)

Exemplo 3.1 *Determine o resto da divisão de* 3^{90} *por* 7.

Solução:

Podemos aplicando o Pequeno Teorema de Fermat, pois o MDC$(3, 7) = 1$ $3^{7-1} = 3^6 \equiv 1 \pmod{7}$ e pelo Teorema 1.2 temos que $(3^6)^{15} \equiv 1^{15} \pmod{7}$ ou seja $3^{90} \equiv 1 \pmod{7}$. Logo o resto é 1.

Corolario 3.1 *Se* p *é um primo , então* $a^p \equiv a \pmod{p}$*, qualquer que seja o inteiro* a*.*

Demonstração:

Se p divide a, então $a \equiv 0 \pmod{p}$ e $a^p \equiv 0 \pmod{p}$, que implica em:

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

Se, ao invés disto, p não dividisse a, então pelo PTF:

$$a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p} \text{ (Teorema 1.2 da seção 1)}$$

■

(OLIVEIRA, 2019)

3.2 Teorema de Wilson

Trataremos nessa seção um pouco sobre a história de Jonh Wilson, autor do teorema que será abordado. Apresentaremos o teorema que é de grande importância na resolução de problemas que envolvem Congruência Modular com Fatorial. O teorema será demonstrado e terá um exemplo resolvido.

Figura 8 – Jonh Wilson

Fonte: Google imagens

Este teorema (4.2) foi enunciado primeiramente por John Wilson (1741-1793), estudante do matemático inglês Edward Waring. Ele anunciou o teorema em 1770, embora nenhum deles tenha conseguido prová-lo. Lagrange deu a primeira prova em 1773. Há uma evidência que Leibniz estava ciente do resultado um século antes, mas nunca o publicou.(FONSECA, 2011)

Teorema 3.2 *(Teorema de Wilson): se p é primo, então*

$$(p-1)! \equiv -1 \pmod{p}$$

.

Demonstração:

O teorema é verdadeiro para $p = 2$ e para $p = 3$, pois:

$$(2-1)! = 1! = 1 \equiv -1 \pmod{2}$$

$$(3-1)! = 2! = 2 \equiv -1 \pmod{3}$$

de modo que vamos supor $p \geq 5$. Consideremos a congruência linear $a.x \equiv 1 \pmod{p}$, onde a é um $(p-1)$ primeiros inteiros positivos $1, 2, 3, ..., p-1$ de modo que o MDC(a,p)= 1.

Nessas condições, existe um único inteiro positivo a', com $1 \leq a' \leq p-1$, tal que

$$a.a' \equiv 1 \pmod{p}$$

Como p é primo, tem-se que $a = a'$ se e somente s $a = 1$, ou $a = p-1$, visto que $a^2 \equiv 1 \pmod{p}$ implica em $(a-1).(a+1) \equiv 0 \pmod{p}$ e, portanto,

$$a - 1 \equiv 0 \pmod{p}, \text{ ou } (a+1) \equiv 0 \pmod{p}$$

isto é, $a = 1$ ou $a = p-1$. ■

Teorema 3.3 *(Teorema de Leibniz): um inteiro $n > 1$ é primo, se e somente se,*

$$\boxed{(n-2)! \equiv 1 \pmod{n}}$$

Demonstração:

($\Rightarrow$) Suponhamos que o inteiro $n > 1$ é primo. Então, pelo Teorema de Wilson:

$$(n-2)! \equiv 1 \pmod{n}$$

obviamente,

$$(n-1)! = (n-1).(n-2)! \equiv -(n-2)! \pmod{n}$$

portanto,

$$(n-2)! \equiv 1 \pmod{n}$$

($\Leftarrow$) Reciprocamente, se $(n-2)! \equiv 1 \pmod{n}$, então:

$$(n-1)! \equiv -(n-2)! \equiv -1 \pmod{n}$$

Logo, pelo recíproco do Teorema de Wilson, o inteiro n é primo. ■

3.3 Teorema de Euler

Falaremos nessa seção um pouco da história de Leonhard Euler, autor do teorema que será abordado. Faremos o enunciado e demonstraremos o teorema que é de grande importância na resolução de problemas que envolve Congruência Modular com Função Totient.

Figura 9 – Leonhard Euler

Fonte: Google imagens

Leonhard Euler (15/04/1707 – 18/07/1783) foi um matemático e físico de origem suíça. Durante sua vida resolveu enorme quantidades de problemas, da navegação de finanças, da acústica à irrigação. A solução de tais problemas, que atendiam aos reclamos do mundo prático, não o entediava, principalmente porque cada novo trabalho inspirava-o para criar uma matemática nova e engenhosa. Era capaz de escrever vários trabalhos em um único dia com os cálculos completos e prontos para serem publicados.

Conseguiu provar o uma conjectura de Fermat relativa aos números primos. Fermat afirmava que o primeiro tipo de número primo sempre era representado pela soma de números ao quadrado enquanto que o segundo jamais o seria. Esta propriedade dos números primos é extremamente simples, porém, ao tentar provar que isto é uma verdade para qualquer número primo, torna-se extremamente difícil. Em 1749, depois de sete anos de trabalho e quase cem anos após a morte de Fermat, conseguiu apresentar essa prova. (FONSECA et al., 2015)

Função Totient: $\phi(n)$

Definição 3.1 *Chama-se função Totient a função aritmética ϕ assim definida para todo inteiro positivo n: $\phi(n)$ = quantidade de inteiros positivos menores que n relativamente primos a n.* □

Em outros termos, $\phi(n)$ é igual ao número de elementos do conjunto

$$\sharp\{x \in Z | 1 \leq x < n, MDC(x,n) = 1\}$$

Observação: $\phi(1) = 1$,pois $MDC(1,1) = 1$.

Exemplo 3.2 $\phi(30) = 8$ *e* $\phi(12) = 4$.

n	1	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	1	2	2	4	2	6	4	6	4

Tabela de $\phi(n)$ para os dez primeiros inteiros positivos.

Cálculo de $\phi(n)$

Teorema 3.4 *Seja p primo, então* $\phi(p) = p - 1$.

Demonstração:

($\Rightarrow$) Se $n > 1$ é primo, então cada um dos inteiros positivos menores que n é primo com n e, portanto $\phi(n) = n - 1$.

($\Leftarrow$) Reciprocamente, se $\phi(n) = n - 1$, com $n > 1$, então n é primo, pois, se n fosse composto, teria pelo menos um divisor d tal que $1 < d < n$, de modo que pelo menos dois inteiros $1, 2, 3, \ldots, n$ não seriam primos com n, d e n, isto é, $\phi(n) \leq n - 2$. Logo, n é primo. ■

Teorema 3.5 *Se p é primo e se k é um inteiro positivo, então*

$$\phi(p^k) = p^k - p^{k-1} = p^k.(1 - \frac{1}{p})$$

Demonstração:

Obviamente, o MDC$(p^k, n) = 1$, se e somente se, p não divide n, e entre 1 e p^k existem p^{k-1} inteiros que não são primos com p^k, que são todos os múltiplos de $p : p, 2.p, 3.p, \ldots, p^2, \ldots, p^3, \ldots, p^k$ segue-se que o conjunto

$$\{p, 2.p, 3.p, \ldots, p^2, \ldots, p^3, \ldots, p^k\}$$

contém exatamente $p^k - p^{k-1}$ inteiros que são relativamente primos a p^k, de modo que pela definição da função $\phi(n)$ de Euler, temos:

$\phi(p^k) = p^k - p^{k-1}$ ■

Teorema 3.6 *(Teorema de Euler): se n é um inteiro positivo e se MDC$(a, n) = 1$, então*

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}}$$

Provaremos, primeiramente, o seguinte:

Lema. Sejam, a e $n > 1$ inteiros tais que o $MDC(a, n) = 1$. Se $a_1, a_2, ..., a_{\phi(n)}$ são inteiros positivos menores que n e que são relativamente primos com n, então cada um dos inteiros $a.a_1$,$a.a_2, ..., a.a_{\phi(n)}$ é congruente módulo n a um dos inteiros $a_1, a_2, ..., a_{\phi(n)}$ (não necessariamente nesta ordem em que aparecem)".

Demonstração do Lema:

Os inteiros $a.a_1$,$a.a_2, ..., a.a_{\phi(n)}$ são mutuamente incongruentes módulo n, pois, se $a.a_i \equiv a.a_j \pmod{n}$, com $1 \leq i \leq j \leq \phi(n)$, com o MDC$(a, n) = 1$, podemos cancelar o fator comum a, o que dá $a_i \equiv a_j \pmod{n} \Leftrightarrow n|(a_j - a_i)$. Isto é impossível, visto que $(a_j - a_i) < n$.

Por outro lado, como o MDC$(a_i, n) = i$, $i = 1, 2, \ldots, \phi(n)$ e o MDC$(a, n) = 1$, segue que o MDC$(a.a_i, n) = 1$. Mas, pelo algoritmo da divisão, $a.a_i = n.q_i + .r_i$, $0 \leq r_i \leq n$, que implica em

$$a.a_i \equiv r_i \pmod{n}, \text{ com } 0 \leq r_i \leq n$$

portanto, MDC$(r_i, n) =$ MDC$(a.a_i, n) = 1$, de modo que r_i é um dos inteiros $a_1, a_2, ..., a_{\phi(n)}$, isto é, cada um dos inteiros $a.a_1$,$a.a_2, ..., a.a_{\phi(n)}$ é congruente módulo n a um único dos inteiros $a_1, a_2, ..., a_{\phi(n)}$, em uma certa ordem.

Agora, provemos por indução sobre n o Teorema de Euler.

O resultado é verdadeiro para $n = 1$, pois $a^{\phi(1)} \equiv 1 \pmod 1$.
Suponhamos, pois, $n > 1$, e sejam $a_1, a_2, ..., a_{\phi(n)}$ os inteiros positivos menores que n e relativamente primos a n.

Como o $MDC(a, n) = 1$, então, pelo Lema acima, os inteiros
$a.a_1, a.a_2, ..., a.a_{\phi(n)}$ são congruentes módulo n aos inteiros $a_1, a_1, ..., a_{\phi(n)}$, em uma ordem:

$$a.a_1 \equiv a_1^*,\ a.a_2 \equiv a_2^*, ..., a.a_{\phi(n)} \equiv a_{\phi(n)}\ ^*$$

onde $a_1{}^*\ a_2{}^*$,..., $a_{\phi(n)}{}^*$ denotam os inteiros $a_1, a_2, ..., a_{\phi(n)}$ em uma certa ordem.

Multiplicando ordenadamente todas essas $\phi(n)$ congruências, obtemos:

$$(a.a_1), (a.a_2).\ ...\ .(a.a_{\phi(n)}) \equiv a_1^*.a_2^*\ .\ ...\ .\ a_{\phi(n)}{}^* \pmod n$$

ou seja,

$$a^{\phi(n)}.(a_1.a_2.....a_{\phi(n)}) \equiv a_1.a_2.....a_{\phi(n)} \pmod n$$

Cada um dos inteiros $a_1, a_2, ..., a_{\phi(n)}$ é relativamente primo a n, de modo que podem ser sucessivamente cancelados, o que dá a congruência de Euler:

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

■

Observe que, se p é um primo, então $\phi(p) = p - 1$ e se o $MDC(a, p) = 1$, então:

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

que é a congruência de Fermat. Assim, o Teorema de Euler é uma generalização do Teorema de Fermat.

Corolario 3.2 *Se $m > 1$, $k \geq 0$, $n \geq 0$ e a um inteiro qualquer são tais que, $MDC(a, m) = 1$ e $k = n \pmod{\phi(m)}$ então , $a^k \equiv a^n \pmod m$.*

Demonstração:

Basta considerar o caso em que $k > 0$. Como $k \equiv n \pmod{\phi(m)}$ existe $q \geq 1$ tal que $k - n = q.\phi(m)$ e, portanto, $a^k = a^{k-n}.a^n = a^{q.\phi(n)}.a^n = (a^{\phi(n)})^q.a^n \equiv a^n \pmod m$. ■
Vejamos agora uma aplicação do Teorema de Euler.

Exemplo 3.3 *Determine o valor de x na congruência $5^8 \equiv x \pmod 6$.*

Solução: Temos que $a = 5$, $n = 6$ e $k = 8$. Como $(5, 6) = 1$ podemos aplicar o Teorema de Euler.

Temos que $\phi(6) = 2$, ou seja $5^{\phi(6)} = 5^2 \equiv 1 \pmod 6$, então $5^2 \equiv 1 \pmod 6$ e que elevando a quarta potência teremos $5^8 \equiv 1 \pmod 6$. Concluímos que $x = 1$.

Congruência Linear

Chamamos de congruência linear em uma variável uma congruência de forma $a.x \equiv b \pmod m$ onde x é uma incógnita.

É fácil de verificar que se x_0 é uma solução, i,e., $a.x_0 \equiv b \pmod m$ e $x_1 \equiv x_0 \pmod m$ então x_1 também tem solução. Isto é óbvio pois $x_1 \equiv x_0 \pmod m$ então $a.x_1 \equiv a.x_0 \pmod m$.

O que acabamos de verificar é que se um membro de uma classe de equivalência é solução então todo membro desta classe é solução. Destas observações surge uma questão natural: no caso de existir alguma solução, quantas soluções incongruentes existem?

Antes de respondermos a esta importante questão, necessitamos provar um teorema que nos dá informações sobre a existência de soluções para uma equação diofantina linear.

Uma equação da forma $a.x + b.y = c$, onde a, b e c são inteiros é chamada **equação diofantina linear**. (o nome vem do matemático grego Diofanto).

Teorema 3.7 *Sejam a e b inteiros e $d = (a, b)$. Se $d \nmid c$ então a equação $a.x + b.y = c$ não tem possui nenhuma solução inteira. Se $d|c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é solução particular, então todas as soluções são dadas por*

$$x = x_0 + (\frac{b}{d})k$$
$$y = y_0 - (\frac{a}{d})k$$

onde k é um inteiro.

Notação: o símbolo (a, b) significa $MDC(a, b)$.

Demonstração:

Se $d \nmid c$, então a equação $a.x + b.y = c$ não possui solução pois, como $d|a$ e $d|b$, d deveria dividir c, o qual é uma combinação linear de a e b.Suponhamos, pois, que $d|c$.Existem inteiros n_0 e m_0, tais que

$$a.n_0 + b.m_0 = d \tag{1}$$

Como $d|c$, existe um inteiro k tal que $c = k.d$. Se multiplicarmos, ambos os membros de (4.1) por k, teremos $a(n_0k) + b(m_0k) = k.d = c$. Isto nos diz que o par (x_0, y_0) com $x_0 = n_0k$ e $y_0 = m_0k$ é uma solução de $a.x + b.y = c$. É fácil a verificação de que os pares da forma

$$x = x_0 + (\frac{b}{d}).k \tag{2}$$

$$y = y_0 - (\frac{a}{d}).k \tag{3}$$

são soluções, uma vez que

$a.x + b.y = a.(x_0 + (\frac{b}{d}).k) + b.(y_0 - (\frac{a}{d}).k) = a.x_0 + \frac{ab}{d}.k + b.y_0 - \frac{ab}{d}.k = a.x_0 + b.y_0 = c$

O que acabamos de mostrar é que, conhecida uma solução particular (x_0, y_0), podemos, a partir dela, gerar infinitas soluções.Precisamos, agora, mostrar que todo solução da equação $a.x + b.y = c$ é da forma (4.2), (4.3). Vamos supor que (x, y) seja uma solução, i.e., $a.x + b.y = c$. Mas, como $a.x_0 + b.y_0 = c$, obtemos, subtraindo membro a membro, que

$$a.x + b.y - a.x_0 - b.y_0 = a.(x - x_0) + b.(y - y_0) = 0,$$

o que implica $a.(x - x_0) = b.(y_0 - y)$. Como $d = (a, b)$ temos,

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

Portanto, dividindo-se os dois membros da última igualdade por d, teremos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \tag{4}$$

Logo, $(\frac{b}{d})|(x - x_0)$ e portanto existe um inteiro k satisfazendo $x - x_0 = k.(\frac{b}{d})$ ou seja $x = x_0 + (\frac{b}{d}).k$. Substituindo-se esse valor de x na equação (4.4) temos $y = y_0 - (\frac{a}{d}).k$, o que conclui a demonstração. ■

Com este teorema à mão podemos dizer quantas são as soluções incongruentes (caso exista alguma) que a congruência linear $a.x \equiv b \pmod{m}$ possui.

Resolução de Congruências Lineares Através do Teorema de Euler

A congruência linear $ax \equiv b \pmod{m}$ no caso em que o MDC$(a, m) = 1$, admite uma única solução módulo m, que se pode facilmente obter usando o Teorema de Euler. Realmente, temos:

$$a^k = a^{k-n}a^n = a^{q.\phi(n)}a^n = (a^{\phi(n)})^q a^n \equiv a^n \pmod{m}$$

portanto,

$$ax \equiv ba^{\phi(m)} \pmod{m}$$

Como MDC$(a, m) = 1$, podemos cancelar o fator comum a, que resulta em:

$$x \equiv ba^{\phi(m)-1} \pmod{m}$$

Exemplo 3.4 *No caso da congruência linear* $3.x \equiv 5 \pmod{8}$*, temos que o MDC*$(3, 8) = 1$*. Logo*

$x \equiv 5.3^{\phi(8)-1} \pmod{8} \equiv 5.3^{4-1} \pmod{8} \equiv 5.27 \pmod{8} \equiv 135 \pmod{8} \equiv 7 \pmod{8}$

Em particular,

$$ax \equiv 1 \pmod{n} \Leftrightarrow x \equiv a^{\phi(n)} \pmod{n}$$

determina um inverso de a módulo n.

Exemplo 3.5 *Queremos determinar o inverso de 7 módulo 11, ou seja, queremos resolver a congruência linear* $7.x \equiv 1 \pmod{11}$

Queremos determinar o menor inteiro positivo de Z_{11} *que satisfaça a equação*

$$x \equiv 7^{\phi(11)-1} \pmod{11} \equiv 7^{10-1} \pmod{11} \equiv 7^9 \pmod{11} \equiv 8 \pmod{11}$$

assim, temos que $x = 8$ *é a menor solução positiva de* Z_{11} *para o problema.*

Teorema 3.8 *(Teorema Chinês dos Restos -TCR) Sejam $m_1, m_2, \ldots, m_k$ inteiros positivos primos entre si dois a dois, isto é, tais que o MDC$(m_i, m_j) = 1$ se $i \neq j$. Nessas condições, o sistema de congruências lineares:*

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

tem única solução módulo $m = m_1.m_2.\ldots.m_k$, dada por:

$$x \equiv a_1.M_1.x_1 + a_2.M_2.x_2 + \ldots + a_k.M_k.x_k \pmod{m}$$

Demonstração:

Para cada $r = 1, 2, 3, \ldots$, seja:

Seja $M_r = \frac{m}{m_r} = \frac{m_1.m_2.\ldots.m_k}{m_r}$. Como os inteiros m_i são todos primos entre si dois a dois, o MDC$(M_r, m_r) = 1$, $\forall\ r = 1, 2, 3, 4 \ldots k$ de modo que a congruência linear $M_r.x \equiv 1 \pmod{M_r}$ tem única solução $x \equiv x_r \pmod{m_r}$.

Posto isso, vamos mostrar que o inteiro $x \equiv a_1.M_1.x_1 + a_2.M_2.x_2 + \ldots + a_k.M_k.x_k \pmod{m}$ é uma solução do sistema considerado.

Com efeito se $i \neq r$, então $m_r | M_i$ e $M_i \equiv 0 \pmod{m_r}$, que implica em:

$$x \equiv a_1.M_1.x_1 + a_2.M_2.x_2 + \ldots + a_k.M_k.x_k \pmod{m}$$

Para demonstrar a unicidade desta solução, suponhamos que x_1 é uma outra solução qualquer do sistema considerado. Então:

$$x \equiv a_r \pmod{m_r} \equiv x_1 \pmod{m_r},\ r = 1, 2, ..., k$$

e, portanto, $m_r | (x - x_1)$, $r = 1, 2, ..., k$.

Mas, o MDC$(m_i, m_j) = 1$ implica em $(m_1.m_2.....m_k)$, isto é, $m | (x - x_1)$ e $x \equiv x_1 \pmod{m}$, com o que termina a demonstração do TCR. ■

Na próxima seção traremos alguns problemas cuja resolução utiliza o Teorema Chinês dos Restos.

3.4 Exercícios Resolvidos

Nesta seção apresentaremos vários exercícios resolvidos através das noções de congruência modular e com o auxílio dos teoremas abordados anteriormente, com o objetivo de promover uma melhor fixação deste assunto.

Problema 3.1 ***Resolva o sistema de congruências lineares:***

$$\begin{cases} x \equiv 8 \pmod 5 \\ x \equiv 5 \pmod 3 \\ x \equiv 11 \pmod 7 \\ x \equiv 2 \pmod 4 \end{cases}$$

Solução:

Devemos aplicar o Teorema 4.8 (TCR)

Os módulos $5, 3, 7$ *e* 4 *das congruências lineares que formam o sistema são primos entre si dois a dois, de modo que pelo TCR este sistema tem única solução módulo* $m = m_1.m_2.m_3.m_4 = 5.3.7.4 = 420$. *Temos então:*

$M_1 = \frac{m}{m_1} = \frac{420}{5} = 84$, $M_2 = \frac{m}{m_2} = \frac{420}{3} = 140$, $M_3 = \frac{m}{m_3} = \frac{420}{7} = 60$, $M_4 = \frac{m}{m_4} = \frac{420}{4} = 105$.

Os inversos x_k *dos* M_k *dados por:*

$$\begin{cases} 84x_1 \equiv 1 \pmod 5 \\ 140x_2 \equiv 1 \pmod 3 \\ 60x_3 \equiv 1 \pmod 7 \\ 105x_4 \equiv 1 \pmod 4 \end{cases}$$

Aplicando o método de Euler nas equações acima obtemos as soluções respectivas: $x_1 = 4$, $x_2 = 2$, $x_3 = 2$ *e* $x_4 = 1$.

Portanto, temos:

$$x \equiv a_1.M_1.x_1 + a_2.M_2.x_2 + \ldots + a_k.M_k.x_k \pmod m$$

$$x \equiv 8.84.4 + 5.140.2 + 11.60.2 + 2.105.1 \pmod{420}$$

$$x \equiv 5618 \pmod{420} \equiv 158 \pmod{420},$$

segue-se que $x = 158$ *é a menor solução positiva módulo* 420*, do sistema de congruências lineares. Qualquer outra solução é da forma:*

$$x \equiv 158 \pmod{420} \Leftrightarrow x = 158 + 420.k, k \in \mathbb{Z}$$

Problema 3.2 ***Calcular o resto da divisão de*** 2^{50} ***por*** 7***.***

Solução:

Como 7 é primo e o $(2, 7) = 1$ podemos aplicar o Pequeno Teorema de Fermat $a^{p-1} \equiv 1 \pmod{p}$ e o teorema 2.3 (3).

Temos que $2^6 \equiv 1 \pmod 7 \Rightarrow (2^6)^8 \equiv 1^8 \pmod 7 \Rightarrow 2^{48} \equiv 1 \pmod 7$ e como $2^2 \equiv 4 \pmod 7$, basta multiplicar as congruências $2^{48} \equiv 1 \pmod 7$ e $2^2 \equiv 4 \pmod 7$.

$2^{48}.2^2 \equiv 1.4 \mod 7 \Rightarrow 2^{50} \equiv 4 \pmod 7$.

Portanto sem precisar calcular 2^{50} descobrimos que o resto da divisão por 7 é 4.

Problema 3.3 ***Calcular o resto da divisão de*** 15! ***por*** 17***.***

Como 17 é primo podemos aplicar o teorema de Leibniz $(n-2)! \equiv 1 \pmod n$.

Temos que $(17-2)! \equiv 1 \pmod{17} \Rightarrow 15! \equiv 1 \pmod{17}$

Portanto sem precisar calcular 15! descobrimos que o resto é 1.

Problema 3.4 ***Calcular o resto da divisão do polinômio*** $P(x) = x^4 - 1$ ***por*** $x^3 + x^2 + x + 1$***.***

Solução:

Podemos associar a divisão euclidiana a notação em módulo e utilizá-la para polinômios.

Temos então que $P(x) = x^4 - 1 \equiv 0 \pmod{x^3 + x^2 + x + 1}$ pois fatorando $x^4 - 1$, tem-se que $x^4 - 1 = (x - 1).(x^3 + x^2 + x + 1)$ ou seja, $x^4 - 1$ deixa resto zero na divisão por $x^3 + x^2 + x + 1$.

Problema 3.5 ***Determine o algarismo da unidade do número*** 9^{9^9}***.***

Solução:

Usando a Definição 2.1

Basta dividir 9^{9^9} por 10 e verificar o resto, que será o algarismo da unidade.

Verificaremos o comportamento das potências de 9.

- $9^0 = 1 \equiv 1 \pmod{10}$
- $9^1 = 9 \equiv 9 \pmod{10}$
- $9^2 = 81 \equiv 1 \pmod{10}$
- $9^3 = 729 \equiv 9 \pmod{10}$

$\vdots$

Podemos concluir que:

$9^n \equiv 1 \pmod{10}$ se n for par

$9^n \equiv 9 \pmod{10}$ se n for ímpar

Como 9^9 é ímpar temos que:

9^{9^9} tem algarismos da unidades 9.

Problema 3.6 ***Mostrar que*** $6^n + 8^n$ ***é divisível por 7 quando, e só quando, n for ímpar.***

Solução:

Usando a Definição 2.1 e o Teorema 2.2(1) e o Teorema 2.2(3).

Temos que $6 \equiv -1 \pmod{7}$ e $8 \equiv 1 \pmod{7}$, de modo que $a = 6^n + 8^n \equiv (-1)^n + 1^n \equiv (-1)^n + 1$ e então temos que $a \equiv 2 \pmod{7}$ se n par, e $a \equiv 0 \pmod{7}$ se n ímpar.

Problema 3.7 ***Mostrar que não existe*** n ***natural tal que*** $2n^2 + n + 1$ ***seja divisível por 3.***

Solução:

Usando a Definição 2.1

Para cada número natural n temos apenas três possibilidades: $n \equiv 0, 1, 2 \mod 3$. Examinemos o que ocorre em cada caso:

- para $n \equiv 0$, temos $2n^2 + n + 1 \equiv 0 + 0 + 1 \equiv 1 \pmod 3$;
- para $n \equiv 1$, temos $2n^2 + n + 1 \equiv 2 + 1 + 1 \equiv 4 \equiv 1 \pmod 3$;
- para $n \equiv 2$, temos $2n^2 + n + 1 \equiv 8 + 2 + 1 \equiv 11 \equiv 2 \pmod 3$;

Assim, como em nenhuma das possibilidades podemos chegara 0 (mod 3), segue nunca ocorre de $2n^2 + n + 1$ ser divisível por 3.

Problema 3.8 ***Mostre que o quadrado de um número inteiro não pode terminar em 2, 3, 7 ou 8.***

Solução:

Usando a Definição 2.1

Pela divisão euclidiana todo número inteiro pode ser escrito em uma das formas: $10n + 1, 10n + 2, 10n + 3, 10n + 4, 10n + 5, 10n + 6, 10n + 7, 10n + 8$ ou $10n + 9$.

Elevando cada um deles ao quadrado e calculando suas classes de resto módulo 10, para se observar o algarismo da unidade teremos:

- $(10n + 1)^2 = 100n^2 + 20n + 1 \equiv 1 \pmod{10}$
- $(10n + 2)^2 = 100n^2 + 40n + 4 \equiv 4 \pmod{10}$
- $(10n + 3)^2 = 100n^2 + 60n + 9 \equiv 9 \pmod{10}$
- $(10n + 4)^2 = 100n^2 + 80n + 16 \equiv 6 \pmod{10}$
- $(10n + 5)^2 = 100n^2 + 100n + 25 \equiv 5 \pmod{10}$
- $(10n + 6)^2 = 100n^2 + 120n + 36 \equiv 6 \pmod{10}$
- $(10n + 7)^2 = 100n^2 + 140n + 49 \equiv 9 \pmod{10}$
- $(10n + 8)^2 = 100n^2 + 160n + 64 \equiv 4 \pmod{10}$
- $(10n + 9)^2 = 100n^2 + 180n + 81 \equiv 1 \pmod{10}$

Podemos ver que o quadrado de um número inteiro termina em $1, 4, 5, 6$ ou 9. Logo não termina nunca em $2, 3, 7$ ou 8.

Problema 3.9 ***Qual o resto da divisão euclidiana de*** $1^5+2^5+3^5+\ldots+99^5+100^5$ ***por*** 4***?***

Solução:

Usando a Definição 2.1 e o Teorema 2.2(1)

Vamos dividir a soma dada em 25 grupos de 4 parcelas e calcular a congruência módulo 4.

$1^5 + 2^5 + 3^5 + \ldots + 99^5 + 100^5 \equiv (1^5 + 2^5 + 3^5 + 0^5) + (1^5 + 2^5 + 3^5 + 0^5) + \ldots (1^5 + 2^5 + 3^5 + 0^5) \pmod 4$.

Divididos 100 por 4 o resultado será 25. Então concluímos que existem 25 grupos de quatro termos na soma acima. Teremos então:

$1^5+2^5+3^5+\ldots+99^5+100^5 \equiv (1^5+2^5+3^5+0^5)+(1^5+2^5+3^5+0^5)+\ldots(1^5+2^5+3^5+0^5) = 25.(1^5 + 2^5 + 3^5 + 0^5) = 25.(1 + 32 + 243 + 0) = 25.276 \equiv 0 \pmod 4$. Logo o resto é 0.

Problema 3.10 ***Determine os dois últimos dígitos verificadores do CPF de número***
$586840419XY$***.***

Solução:

Vamos usar a Definição 2.1

Para calcular o primeiro dígito X, multiplicamos os 9 primeiros dígitos do CPF em uma ordem respectivamente pela base $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, somamos os resultados e dividimos por 11, o resto será o primeiro dígito verificador do CPF, caso o resto seja 10 convencionase usar o 0.

$5.1 + 8.2 + 6.3 + 8.4 + 4.5 + 0.6 + 4.7 + 1.8 + 9.9 = 208 \equiv 10 \pmod{11}$.

Como o resto é 10, pela convenção $X = 0$. Agora que já temos os 10 dígitos do CPF, falta calcular o décimo primeiro dígito.

Para calcular o valor de Y, multiplicamos os 10 primeiros dígitos do CPF em uma ordem respectivamente pela base $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, somamos os resultados e dividimos por 11, o resto será o segundo dígito verificador do CPF, caso o resto seja 10 usaremos o 0.

$5.0 + 8.1 + 6.2 + 8.3 + 4.4 + 0.5 + 4.6 + 1.7 + 9.8 + 0.9 \equiv 9 \pmod{11}$.

Pela regra $Y = 9$.

Portanto os dois últimos dígitos do CPF são respectivamente 0 e 9.

Problema 3.11 *Mostre que 163 e 221 são congruentes módulo* 29.

Solução:

Pela Definição 2.1 e pelo Teorema 2.1

Temos que $163 \equiv 18 \pmod{29}$ e $221 \equiv 18 \pmod{29}$. Como os números 163 e 221 têm o mesmo resto 18 eles são congruentes módulo 18.

Problema 3.12 *Mostre que o conjunto* $\{7, 8, 9, 10\}$ *é um sistema completo de restos módulo* 4.

Solução:

Pela Definição 2.1 e Definição 2.3 temos que:

$7 \equiv 3 \pmod{4}$
$8 \equiv 0 \pmod{4}$
$9 \equiv 1 \pmod{4}$
$10 \equiv 2 \pmod{4}$
Os restos forma o conjunto $\{0, 1, 2, 3\}$, logo o conjunto $\{7, 8, 9, 10\}$ é um sistema completo de resto módulo 4.

4 Considerações Finais

A aritmética modular foi bastante explorada nesse trabalho, buscando a sua aplicação tanto para sistemas de identificação, quanto para calendários, como também em aplicações práticas em sala de aula. Foram apresentadas algumas aplicações de congruência modular, buscando mostrar as mais interessantes como: CPF, calendário, relógio de parede, critérios de divisibilidade e jogo dos restos. Foi associada a congruência modular em assuntos relacionados a trigonometria e aos números complexos que são abordados no ensino médio tornando mais fácil a compreensão dos mesmos. Uma vez mostradas as aplicações mais abrangentes, passou-se a verificar as aplicações na educação básica, utilizadas na escola como forma de reforçar a habilidade com a divisibilidade e estudos de aritmética. Procuramos apresentar propostas de atividade com alunos do ensino médio, onde os mesmos são levados a experimentarem as aplicações da congruência modular nas situações destacadas no desenvolvimento deste trabalho. A intenção é mostrar mais uma ferramenta para ajudar na resolução de problemas, tornando mais fácil sua resolução, promovendo melhores condições para a aprendizagem. Isso chama a atenção para a necessidade de implementar metodologias de ensino que reforcem a aplicação da matemática no dia a dia. Mostrar as aplicações da matemática é importantíssimo para motivar os alunos a estabelecerem processos de investigação nesse campo, bem como de valorização dessa disciplina como conteúdo curricular. Esperamos que esse material traga ganhos e melhorias da capacidade crítica do aluno, possibilitando progresso da habilidade interpretativa. Principalmente, espera-se que este trabalho possa servir como material de pesquisa para professores de matemática da educação básica e superior visando estabelecer novas metodologias em suas aulas sobre aritmética modular.

Referências

BOYER, C. B.; MERZBACH, U. C. **História da matemática**. [S.l.]: Editora Blucher, 2019.

FONSECA, R. V. Teoria dos números. **Belém: UEPA**, 2011.

FONSECA, R. V. et al. Números primos e o teorema fundamental da aritmética: uma investigação entre estudantes de licenciatura em matemática. Pontifícia Universidade Católica de São Paulo, 2015.

GAUSS, C. F. **Disquisitiones arithmeticae, trans. Arthur A. Clarke**. [S.l.]: New Haven: Yale University Press, 1801.

GOLDSTEIN, C.; SCHAPPACHER, N.; SCHWERMER, J. **The shaping of arithmetic after CF Gauss's Disquisitiones Arithmeticae**. [S.l.]: Springer Science & Business Media, 2007.

KONAGESKI, D. M. F. et al. **Experiências concretas na aritmética modular**. Dissertação (Mestrado) — Universidade Tecnológica Federal do Paraná, 2019.

MARTINS, C. J. L. Algoritmo da divisão de euclides: uma nova proposta de ensino de matemática na educação básica. Universidade Estadual Paulista (UNESP), 2015.

OLIVEIRA, F. E. F. d. Sobre várias demonstrações do pequeno teorema de fermat e as inter-relações entre as áreas da matemática. 2019.

SÁ, I. P. de. Aritmética modular e algumas de suas aplicações. 2010.

SIMON, S. Último teorema de fermat. **Editora Record. Rio de Janeiro**, 1998.