Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Aritmética Modular:
Aplicações no Ensino Médio

Marco Antonio de Oliveira Barros

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Trabalho financiado pela Capes

Cuiabá - MT

Fevereiro de 2014

Aritmética Modular:
Aplicações no Ensino Médio

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Marco Antonio de Oliveira Barros e aprovada pela comissão julgadora.

Cuiabá, 22 de abril de 2014.

Prof. Dr. Martinho da Costa Araújo
Orientador

Banca examinadora:

Prof. Dr.
Prof. Dr.
Prof. Dr.

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

B277a Barros, Marco Antonio de Oliveira.
Aritmética Modular : Aplicações no Ensino Médio / Marco Antonio de Oliveira Barros. -- 2014
90 f. : il. ; 30 cm.

Orientador: Martinho da Costa Araújo.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2014.
Inclui bibliografia.

1. Aritmética Modular. 2. Congruência Modular. 3. Ensino Médio. 4. Classes Residuais. 5. Criptografia. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Dissertação de Mestrado defendida em ___ de _____ de _____ e aprovada pela banca examinadora composta pelos Professores Doutores

---

Prof. Dr. Nome completo do orientador

Prof. Dr. Nome completo do membro externo

Prof. Dr. Nome completo do membro interno

Aos meus pais, minha esposa Andréa, meus filhos e a toda minha família que, com muito apoio e compreensão, não mediram esforços para que eu concluísse mais essa etapa da minha vida.

Agradecimentos

Gostaria de agradecer aos meus pais, Hildebrando (in memorian) e Erotildes, aos quais devo toda a minha formação , por me ensinarem a importância do estudo em nossa vida.

Não posso deixar de agradecer aos meus familiares, por compreenderem a minha ausência em várias ocasiões devido aos compromissos do mestrado, em especial, à minha esposa Andrea, pelo incentivo, carinho e apoio em todos os momentos e aos meus filhos, Matheus e Lucas, presentes de Deus em minha vida.

Agradeço também aos colegas de mestrado, companheiros de muitas horas de estudo, pelas valiosas sugestões e contribuições, em particular, ao Luiz Fernando, Jessé, Ricardo, Nivaldo, Gilliard e Waldemir, que se tornaram grandes amigos durante o curso.

Devo agradecer ainda ao meu orientador, Prof. Dr. Martinho da Costa Araújo, pelo apoio a realização deste trabalho, bem como, a todos os mestres que contribuíram com o aperfeiçoamento da nossa formação matemática.

Finalmente, agradeço à Deus por colocar todas essas pessoas no meu caminho e dessa forma, proporcionar a realização deste trabalho, que faz parte da conclusão de mais uma etapa da minha vida.

A Matemática apresenta invenções tão sutis que poderão servir não só para satisfazer aos curiosos como, também para auxiliar as artes e poupar trabalho aos homens.

Descartes

Resumo

Este trabalho pretende mostrar que a Aritmética Modular é um tema atual e que pode ser introduzido no Ensino Médio, por meio de uma proposta de ensino do tema com ênfase na resolução de exercícios contextualizados. Para isso, apresenta inicialmente uma fundamentação teórica sobre o assunto, introduz a Congruência Modular e algumas de suas propriedades apresentando a aplicação desse conceito na resolução de exercícios envolvendo vários assuntos da matemática retirados de vestibulares, olimpíadas de matemática e livros didáticos atuais. Faz uma pequena introdução às Classes Residuais e apresenta ainda uma aplicação das Congruências Modulares na Criptografia, bem como, um relato da aplicação da proposta para uma turma do Ensino Médio do IFMT, Campus Bela Vista.

Palavras chave: Aritmética Modular, Congruência Modular, ensino médio, exercícios contextualizados, Classes Residuais, Criptografia.

Abstract

This work intends to show that Modular Arithmetic is a current theme and it may be introduced in high school through a teaching proposal of theme emphasizing on solving contextualized exercises. For that, initially it presents a theoretical background on the subject, introduces the Modular Congruence and some of its properties showing the application of this concept in solving exercises involving various subjects of mathematics taken from college entrance examination, Olympics of math and current textbooks. It makes a brief introduction to the Residuals Classes and presents an application of Modular Congruence in Cryptography, as well as a report of the proposal application to a high school class at IFMT, Bela Vista Campus.

Keywords: Modular Arithmetic, Modular Congruence, high school, contextualized exercises, Residuals Classes, Cryptography.

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

> "Não há ramo da Matemática, por mais abstrato que seja, que não possa um dia vir a ser aplicado aos fenômenos do mundo real."
>
> (Nicolai Lobachevsky)

A Aritmética Modular envolve o conceito de congruência que é a relação entre dois números que, divididos por um terceiro - chamado módulo de congruência - deixam o mesmo resto. Utilizamos frequentemente os restos das divisões para resolver vários problemas dentro do ensino da Matemática, muitos deles, relacionados ao nosso cotidiano.

Diversos assuntos estão associados ao tema, tais como, criptografia, calendários, códigos de identificação numérica, como código de barras, números dos documentos de identidade, CPF, CNPJ, progressões aritméticas e diversos fenômenos periódicos. Apesar disso, este assunto não está presente nos currículos do Ensino Básico ou do Ensino Médio.

Este trabalho tem como objetivo mostrar que a Aritmética modular é um tema atual que pode ser introduzido no Ensino Médio, apresentar uma proposta de ensino sobre o assunto com ênfase na resolução de problemas contextualizados, utilizando uma linguagem que seja acessível aos alunos do Ensino Médio, além de fazer um relato sobre a aplicação dessa proposta, no $5^{\underline{o}}$ semestre, do Curso de Nível Médio Integrado em Química do IFMT - Campus Bela Vista. Para isso, no capítulo 1 apresentaremos a fundamentação teórica necessária à introdução do assunto, no capítulo 2 abordaremos a proposta de ensino do tema, cujos conteúdos foram organizados em unidades contidas na apostila que foi elaborada paralelamente à realização do curso e no capítulo 3 faremos um relato contendo as observações sobre as aulas ministradas nesse curso.

Existe um farto material sobre o tema, principalmente nos livros sobre teoria dos números, mas, como a proposta da realização desse trabalho surgiu do interesse despertado pelo assunto na disciplina de Aritmética, durante o mestrado no PROFMAT, grande parte

do referencial teórico utilizado neste trabalho tem suporte em Hefez (2011).

Serve, também, de referência para esse trabalho, um artigo interessante do Profº Ilydio Pereira de Sá intitulado "Aritmética Modular e algumas de suas aplicações", no qual o mesmo ressalta que o assunto em questão "é um tema bastante atual e que pode ser trabalhado já nas classes do Ensino Fundamental e é gerador de excelentes oportunidades de contextualização no processo de ensino / aprendizagem de matemática", e ainda, um trabalho de dissertação de Mestrado em Ensino de Ciências na Educação Básica, UNIGRANRIO com o tema "Aritmética Modular e suas Possibilidades na Formação Continuada de Professores de Matemática", Mattos, Sérgio Ricardo Pereira de; Puggian, Cleonice e Lozzano, Abel Rodolfo Garcia; no qual observam que "Embora o estudo da aritmética esteja presente nos currículos do ensino obrigatório em todos os países, há muito tempo, conforme afirma Lins e Gimenes (2006), o mesmo não acontece com a aritmética desenvolvida por Gauss, também conhecida como aritmética modular. No entanto, apesar da aritmética modular não ser uma parte da matemática contemplada nas salas de aulas em todos os níveis, usamos os restos das divisões para resolver diversos problemas no nosso dia a dia".

Para um melhor esclarecimento da nossa proposta, elaboramos duas vídeo-aulas sobre Congruências Modulares, uma contendo a introdução ao assunto e a outra sobre algumas propriedades da mesma, relativas às operações de adição e multiplicação. Ressaltamos ainda que, embora, também, pretenda servir de apoio a professores, este trabalho é direcionado principalmente aos alunos do Ensino Médio, que nessa faixa etária ainda não tem a maturidade ou os pré-requisitos necessários para compreender todas as demonstrações referentes à fundamentação teórica. Por isto, o enfoque principal deste trabalho está na aplicação das definições e propriedades em várias áreas da matemática, através da resolução de exercícios contextualizados, vários deles, encontrados em livros didáticos do ensino médio, em vestibulares e olimpíadas de matemática.

Capítulo 1

Fundamentação Teórica

A Aritmética Modular é uma parte da Teoria dos Números que abrange uma grande quantidade de teoremas e propriedades. Abordaremos neste capítulo, apenas as definições, propriedades e teoremas, que julgamos ser necessários à introdução e desenvolvimento do assunto no Ensino Médio. Todos os resultados apresentados abaixo foram retirados do livro Hefez (2011).

1.1 Princípio da Indução Finita

Um poderoso instrumento envolvendo a demonstração de vários resultados é o Princípio da Indução Finita que enunciaremos a seguir:

Teorema 1 *Seja $a \in \mathbb{N}$ e seja $P(n)$ uma sentença aberta em n. Suponha que*

1. *P(a) é verdade, e que*
2. *$\forall n \geq a$, se $P(n)$ é verdade, então $P(n+1)$ é verdade.*

   Então, $P(n)$ é verdade para todo $n \geq a$.

Demonstração: Seja $V = \{n \in \mathbb{N}; P(n)\}$; ou seja, V é o subconjunto dos elementos de $\mathbb{N}$ para os quais $P(n)$ é verdade.
Considere o conjunto

$$S = \{m \in \mathbb{N}; a + m \in V\},$$

que verifica trivialmente $a + S \subset V$.

Como, pela condição (1), temos $a + 0 = a$, segue-se que $0 \in S$.

Por outro lado, se $m \in S$, então $a+m \in V$ e, por (2), temos $a+m+1 \in V$; logo $m+1 \in S$. Assim, pelo axioma de indução, temos que $S = \mathbb{N}$. Portanto,

$\{m \in \mathbb{N}; m \geq a\} = a + \mathbb{N} \subset V$, o que prova o resultado.

Todos os conceitos que abordaremos a seguir serão trabalhados dentro do conjunto dos números inteiros, dessa forma, o princípio da indução poderá ser enunciado da seguinte forma:

Teorema 2 *Suponhamos que sejam dados um inteiro a e uma afirmação $P(n)$ dependendo de $n \in \mathbb{Z}$, $n \neq a$ e que podemos provar as seguintes propriedades:*

1. *$P(a)$ é verdadeira*
2. *Para cada inteiro $k \geq a$, se $P(k)$ for verdadeira, então $P(k+1)$ também é verdadeira. Então, $P(n)$ é verdadeira para todo $n \in \mathbb{Z}$.*

1.2 Divisibilidade

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

Exemplo 1.2.1 $2|6$, pois $6 = 3.2$

Se a não divide b , utilizamos a notação $a \not| b$, significando que não existe $k \in \mathbb{Z}$ tal que $b = k.a$.

Exemplo 1.2.2 $4 \not| 7$

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

Proposição 1 *Sejam $a, b, c \in \mathbb{Z}$. Então $1|a$, $a|a$ e $a|0$.*

Demonstração: Isto decorre das igualdades $a = a.1$, $a = 1.a$ e $0 = 0.a$.

Proposição 2 *Sejam $a, b, c \in \mathbb{Z}$. Se $a|b$ e $b|c$, então $a|c$.*

Demonstração: $a|b$ e $b|c$ implica que existem $m, n \in \mathbb{Z}$, tais que $b = m.a$ e $c = n.b$. Substituindo o valor de b da primeira equação na outra, obtemos:
$c = n.b = n.m.a = (m.n).a$; o que nos mostra que $a|c$.

Proposição 3 *Sejam $a, b, c, d \in \mathbb{Z}$. Se $a|b$ e $c|d$, então $a.c|b.d$.*

Demonstração: $a|b$ e $c|d$, implica que existem $m, n \in \mathbb{Z}$ tais que $b = m.a$ e $d = n.c$. Então, $b.d = m.a.n.c = (m.n).a.c$, o que nos mostra que $a.c|b.d$

Proposição 4 *Sejam $a, b, c \in \mathbb{Z}$, tais que $a|(b \pm c)$. Então, $a|b$ se e somente se $a|c$.*

Demonstração: Suponhamos que $a|(b + c)$. Logo, existe $k \in \mathbb{Z}$ tal que $b + c = k.a$. Então, se $a|b$, temos que existe $m \in \mathbb{Z}$, tal que $b = m.a$. Juntando as duas igualdades acima, temos $k.a + c = m.a$; então temos que $c = m.a - k.a$, o que nos mostra que $a|c$. De maneira análoga demonstramos a implicação contrária.

Desta forma, se $a|(b - c)$ e $a|b$, temos que $a| - c$, o que implica que $a|c$.

Proposição 5 *Se $a, b, c \in \mathbb{Z}$ são tais que $a|b$ e $a|c$, então $a|(x.b+y.c)$, para todo $x, y \in \mathbb{Z}$.*

Demonstração: $a|b$ e $a|c$ implicam que existem $m, n \in \mathbb{Z}$ tais que $b = m.a$ e $c = n.a$. Logo, $x.b + y.c = x.m.a + y.n.a = (x.m + y.n).a$; então, temos que $a|(x.b + y.c)$.

Proposição 6 *Dados $a, b \in \mathbb{N}$. Se $a|b$ então $a \leq b$*

Demonstração: Se $a|b$, existe $k \in \mathbb{Z}$ tal que $b = k.a$. Como $a, b > 0$, segue-se que $k \in \mathbb{N}$. Como $1 \leq k$, segue-se que $1.a \leq k.a \Rightarrow a \leq b$.

1.3 Divisão Euclidiana

Teorema 3 *Sejam a e b dois números inteiros com $a \neq 0$. Existem dois únicos números inteiros q e r , tais que:*

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

Demonstração: Considere o conjunto $S = \{x = b - ay; y \in \mathbb{Z}\} \cap \{\mathbb{N} \cup \{0\}\}$.

Existência: Pela Propriedade Arquimediana, existe $n \in \mathbb{Z}$ tal que $n.(-a) > -b$, logo $b - na > 0$, o que mostra que S não é vazio. O conjunto S é limitado inferiormente por 0, logo, pelo princípio da boa ordenação, temos que S possui um menor elemento r.

Suponhamos então que $r = b - aq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |a|$. Suponhamos por absurdo que $r \geq |a|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |a| + s$, logo $0 \leq s < r$. Mas isto contradiz o fato de r ser o menor elemento de S, pois $a = b - (q \pm 1)$, $a \in S$, com $s < r$.

Unicidade: Suponha que $b = a.q + r = a.q' + r$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |a|$ e $0 \leq r' < |a|$, assim temos que $-|a| < -r \leq r - r' < |a|$. Logo,$|r - r'| < |a|$. Por outro lado, $a(q - q') = r - r'$, o que implica que $|a||q - q'| = |r - r'| < |a|$, o que só é possível se $q = q'$ e consequentemente, $r = r'$.

No teorema acima, os números q e r são chamados, respectivamente, de quociente e de resto da divisão de b por a.

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

Exemplo 1.3.1 Dado um número inteiro $n \in \mathbb{Z}$ qualquer, temos duas possibilidades:

1. o resto da divisão de n por 2 é 0, isto é, existe $q \in \mathbb{N}$ tal que $n = 2q$; ou
2. o resto da divisão de n por 2 é 1, ou seja, existe $q \in \mathbb{N}$tal que $n = 2q + 1$.

Portanto, os números inteiros se dividem em duas classes, a dos números da forma $2q$ para algum $q \in \mathbb{N}$, chamados de números pares, e a dos números da forma $2q + 1$, chamados de números ímpares.

Exemplo 1.3.2 Mais geralmente, fixado um número natural $m > 2$, pode-se sempre escrever um número qualquer n, de modo único, na forma $n = mk + r$, onde $k, r \in \mathbb{Z}$ e $0 \leq r < m$.

Por exemplo, todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $3k, 3k + 1$, ou $3k + 2$.

Ou ainda, todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $4k, 4k + 1, 4k + 2$, ou $4k + 3$.

1.4 Máximo Divisor Comum (MDC)

Definição 1 *Dados dois números inteiros a e b, não simultaneamente nulos, diremos que $d \in \mathbb{Z}$ é um divisor comum de a e b se $d|a$ e $d|b$.*

Um número natural d é um máximo divisor comum de a e b, não simultaneamente nulos, se possuir as seguintes propriedades:

1. d é um divisor comum de a e b.

2. d é divisível por todo divisor comum de a e b.

Denotamos o máximo divisor comum de a e b por (a, b).

Exemplo 1.4.1 Considere os conjuntos dos divisores naturais de 12 e 18:
$D(12) = \{1; 2; 3; 4; 6; 12\}$
$D(18) = \{1; 2; 3; 6; 9; 18\}$

Observe que os divisores naturais comuns de 12 e 18 são 1, 2, 3 e 6. O máximo divisor comum entre 12 e 18 é 6, pois 1|6, 2|6, 3|6 e 6|6.

1.5 Mínimo Múltiplo Comum (MMC)

Definição 2 *Um número inteiro é um múltiplo comum de dois números naturais dados se ele é simultaneamente múltiplo de ambos os números.*

Um número natural m é um mínimo múltiplo comum dos números inteiros a e b, ambos não nulos, se possuírem as seguintes propriedades:

1. m é um múltiplo comum de a e b.

2. Se c é um múltiplo comum de a e b, então $m|c$.

Denotamos o mínimo múltiplo de a e b por $[a, b]$.

Exemplo 1.5.1 Considere os múltiplos naturais não nulos de 12 e 18:

$M(12) = \{12; 24; 36; 48; 60; 72; 84; 96; 108; ...\}$

$M(18) = \{18; 36; 54; 72; 90; 108; 126...\}$

Observe que os múltiplos de 12 formam uma progressão aritmética infinita de razão 12 e os de 18 forma uma progressão aritmética infinita de razão 18.

O conjunto dos múltiplos comuns de 12 e 18 é infinito e formam uma progressão aritmética de razão igual a 36, ou seja, $\{36; 72; 108; 144; ...\}$. O mínimo múltiplo entre 12 e 18 é 36, pois, 36|36, 36|72, 36|108, 36|144,...

1.6 Números Primos

Definição 3 *Um número natural maior que 1 é chamado de número primo, quando apresenta apenas dois divisores naturais ou seja, 1 e ele próprio.*

Dados dois números primos p e q e um número $a \in \mathbb{Z}$, decorrem da definição acima os seguintes fatos:

1. Se $p|q$ então $p = q$.

   Como q é primo e $p|q$, temos $p = 1$ ou $p = q$. Dessa forma, como p é primo, temos $p > 1$, logo $p = q$.

2. Se $p \not| q$ então $(p, a) = 1$.

   De fato, se $(p, a) = d$, então $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$. Como $p \not| q$, temos $d \neq p$, portanto, $d = 1$.

Um número maior do que 1 que não é primo será chamado composto. Portanto, se um número inteiro $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $n_1 \neq 1$ e $n_1 \neq n$. Portanto, existirá um número natural n_2 tal que

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

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

Teorema 4 (Teorema Fundamental da Aritmética) *Qualquer número natural maior do que 1, ou é primo ou pode ser escrito de forma única (desconsiderando a ordem dos fatores) como um produto de números primos (chamados fatores primos).*

Demonstração: Pelo princípio da indução, se $n = 2$, o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos então, que n seja composto. Logo existem números naturais n_1 e n_2 tais que $n = n_1.n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_r$, tais que $n_1 = p_1...p_r$ e $n_2 = q_1...q_r$ portanto, $n = p_1...p_r q_1, ..., q_r$.

Unicidade: Suponha que tenhamos $n = p_1...p_r = q_1...q_r$, onde os p_i e q_j são números primos. Como $p_1 | q_1, ..., q_r$, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, ..., q_r$, podemos supor que seja q_1. Portanto: $p_1...p_r = q_1...q_r$.

Podemos enunciar esse teorema de uma forma mais ampla, da seguinte forma:

Teorema 5 *Dado um número inteiro $n \notin \{0, -1, 1\}$, existem primos $p_1 < p_2 < ... < p_k$ e $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}$, univocamente determinados, tais que:*

$$n = p_1^{\alpha_1} \ . \ p_2^{\alpha_2} \ ... \ p_k^{\alpha_k}.$$

Na decomposição em fatores primos de dois ou mais números naturais, podemos utilizar o mesmo conjunto de primos $p_1, p_2, ..., p_k$ nessa decomposição, utilizando o artifício de acrescentar de forma adequada um expoente igual à zero para determinado primo p.

Exemplo 1.6.1 $45 = 3^2.5$ e $56 = 2^3.7$, podem ser escritos da seguinte forma:

$45 = 2^0.3^2.5.7^0$ e $56 = 2^3.3^0.5^0.7$

Proposição 7 *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.*

Demonstração: Suponhamos, por absurdo, que n não seja divisível por nenhum número primo p tal que $p^2 \leq n$ e que não seja primo. Seja q o menor número primo que divide n; então, $n = q.n_1$, com $q \leq n_1$. Segue daí que $q^2 \leq q.n_1 = n$. Logo, n é divisível por um número primo q tal que $q^2 \leq n$, absurdo.

A fatoração de números naturais em números primos permite determinar o mdc e o mmc de um conjunto qualquer de números.

Teorema 6 *Sejam* $a = \pm p_1^{\alpha_1}...p_n^{\alpha_n}$ *e* $b = \pm p_1^{\beta_1}...p_n^{\beta_n}$. *Se* $\gamma_i = min\{\alpha_i, \beta_i\}$ *e* $\delta_i = máx\{\alpha_i, \beta_i\}$, *então temos que:*

$$(a, b) = p_1^{\gamma_1}...p_n^{\gamma_n} \text{ e } [a, b] = p_1^{\delta_1}...p_n^{\delta_n}$$

Demonstração: Temos que $p_1^{\gamma_1}...p_n^{\gamma_r}$ é um divisor comum de a e b. Seja c um divisor comumde a e b; logo $c = \pm p_1^{\epsilon_1}...p_n^{\epsilon_r}$, onde $\epsilon_i \leq min\{\alpha_i, \beta_i\}$ e, portanto, $c|p_1^{\gamma_1}...p_n^{\gamma_n}$. Do mesmo modo prova-se a asserção sobre o mmc.

Exemplo 1.6.2 Seja $a = 2^3.3^2.5.7$ e $b = 2^4.3^0.5^2$, então:

$(a, b) = 2^3.3^0.5 = 40$ e $[a, b] = 2^4.3^2.5^2.7 = 25200$.

1.7 Pequeno Teorema de Fermat

Para demonstrar esse teorema, necessitaremos do seguinte lema:

Lema 1 *Seja* p *um número primo e* $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. *Os números binomiais* $\binom{p}{i}$, *onde* $0 < i < p$, *são todos divisíveis por* p.

Demonstração: O resultado vale trivialmente para $i = 1$. Portanto, podemos supor que $1 < i < p$. Neste caso, $i!|p.(p-1)...(p-i+1)$. Como $(i!, p) = 1$, temos que $i!|(p-1)...(p-i+1)$, e o resultado se segue, pois...

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

Teorema 7 (Pequeno Teorema de Fermat) *Dado um número primo* p, *tem-se que* $p|(a^p - a)$, *para todo* $a \in \mathbb{Z}$.

Demonstração: O resultado vale para $a = 0$, pois $p|0$.

Supondo o resultado válido para a, vamos demonstrá-lo para $a + 1$. Utilizando a fórmula do binômio de Newton, temos:

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

Como, pela hipótese da indução $p|(a^p - a)$ e pelo lema anterior, $p|\binom{p}{1}a^{(p-1)} ... + \binom{p}{p-1}a$, temos $p|(a^p - a)$, para todo $a \in \mathbb{Z}$.

Corolário 1 *Se p é um número primo e a é um número inteiro não divisível por p, então $p|(a^{p-1} - 1)$.*

Demonstração: Pelo Pequeno Teorema de Fermat, temos $p|(a.a^{p-1} - 1)$ e como $(a, p) = 1$, segue-se que $p|(a^{p-1} - 1)$.

1.8 Congruência Modular

Definição 4 *Seja m um número natural diferente de zero. Dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Denota-se esta relação da seguinte forma: $a \equiv b \ mod \ m$ (lê-se a é congruente a b módulo m).*

Exemplo 1.7.1 O número 9 é congruente ao número 16, módulo 7, pois ambos deixam resto 2, ao serem divididos por 7. Representamos essa congruência do exemplo por $9 \equiv 16 \ mod \ 7$.

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

Exemplo 1.7.2 Dividindo 163 por 7 obtivemos quociente 23 e resto 2, logo:
$163 \equiv 2 \ mod \ 7$, pois, 2=7.0+2, ou seja dividindo 2 por 7, obtemos quociente 0 e resto 2.

Proposição 8 *Uma maneira equivalente de dizer que $a \equiv b \ mod \ m$, é afirmar que $m|(b - a)$, ou seja, a diferença $(b - a)$ é um múltiplo de m.*

Demonstração: Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$

Supondo que $a \equiv b \ mod \ m$. Sejam $a = m.q + r$ e $b = m.q' + r$, com $r < m$, as divisões euclidianas de a e b por m. Logo:

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

Reciprocamente, supondo que $m|(b - a)$. Sejam $a = m.q + r$ com $r < m$ e $b = m.q' + r$ com $r' < m$, as divisões euclidianas de a e b por m. Logo:

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

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

Exemplo 1.7.3 $10 \equiv 26 \ mod \ 7 \Leftrightarrow 8|(26 - 10)$, ou seja, $8|16$

Proposição 9 *Decorre imediatamente da definição que a congruência modular define uma equivalência, pois atende às propriedades reflexiva, simétrica e transitiva, ou seja:*

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

Demonstração:

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

2. Se $a \equiv b \ mod \ m$, temos que $m|(b - a)$, ou seja, existe $k \in \mathbb{Z}$ tal que $b - a = k.m$.

   Multiplicando esta igualdade por (-1), obtemos:

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

3. Se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, temos que $m|(b - a)$ e $m|(c - b)$, ou seja, existem $k, p \in \mathbb{Z}$ tais que $b - a = k.m$ e $c - b = p.m$

   Somando membro a membro as duas igualdades obtemos:
   $(b - a) + (c - b) = k.m + p.m \Rightarrow c - a = (k + p).m \Rightarrow m|(c - a) \Rightarrow a \equiv c \ mod \ m$.

1.9 Propriedades das congruências modulares

Proposição 10 *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.*

1. *Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então, $a + c \equiv b + d \ mod \ m$.*

2. *Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então, $a.c \equiv b.d \ mod \ m$.*

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

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

$$m|(b+d)-(a+c) \Rightarrow a+c \equiv b+d \ mod \ m.$$

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

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

Corolário 2 *Se $a \equiv b \ mod \ m$, então, $a^n \equiv b^n \ mod \ m$, para todo $n \in \mathbb{N}$.*

Demonstração: Seja $P(n)$ a afirmação: se $a \equiv b \ mod \ m$, então, $a^n \equiv b^n \ mod \ m$, para todo $n \in \mathbb{N}$.

Para $n = 1$, temos $a^1 \equiv b^1 \ mod \ m$. (Verdadeiro)

Supondo $P(n)$ verdadeira, temos, pela propriedade 2 que:
$a^n.a \equiv b^n.b \ mod \ m \Rightarrow a^{n+1} \equiv b^{n+1} \ mod \ m \Rightarrow P(n+1)$ é verdadeira. Então, se $a \equiv b \ mod \ m$, então, $a^n \equiv b^n \ mod \ m$, para todo $n \in \mathbb{N}$.

Com a notação de congruência, o Pequeno Teorema de Fermat pode ser enunciado da seguinte forma:

Se p é um número primo e $a \in Z$, então:

$$a^p \equiv a \ mod \ p.$$

Além disso, se $p \nmid a$, então:

$$a^{p-1} \equiv 1 \ mod \ p.$$

1.10 Classes Residuais

Considerando a divisão euclidiana de números inteiros por 2, podemos dividir o conjunto dos números inteiros em dois subconjuntos, a saber:

1. O conjunto dos números inteiros que divididos por 2 deixam resto zero, ou seja:

   $\{x \in \mathbb{Z}; x \equiv 0 \ mod \ 2\} = \{... - 4; -; 0; 2; 4; ...\}$, ou seja, x é par.

2. O conjunto dos números inteiros que divididos por 2 deixam resto 1, ou seja:

   $\{x \in \mathbb{Z}; x \equiv 1 \ mod \ 2\} = \{... - 3; -1; 1; 3; 5; ...\}$, ou seja, x é ímpar.

Considerando a divisão euclidiana dos números inteiros por 3, podemos dividir o conjunto dos números inteiros em três subconjuntos, a saber:

1. O conjunto dos números que divididos por três deixam resto zero, ou seja:

   $\{x \in \mathbb{Z}; x \equiv 0 \ mod \ 3\} = \{... - 3; 0; 3; 6; ...\}$, ou seja, x é múltiplo de 3.

2. O conjunto dos números que divididos por três deixam resto 1, ou seja:

   $\{x \in \mathbb{Z}; x \equiv 1 \ mod \ 3\} = \{... - 2; 1; 4; 7; ...\}$, ou seja, x é múltiplo de 3 mais 1.

3. O conjunto dos números que divididos por três deixam resto 2, ou seja:

   $\{x \in \mathbb{Z}; x \equiv 2 \ mod \ 3\} = \{... - 1; 2; 5; 8; , , , \}$, ou seja, x é múltiplo de 3.

Dessa forma, fixado um número inteiro $m > 1$, podemos repartir o conjunto Z dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos m; isto nos dá a seguinte partição de Z:

$$[0] = \{x \in \mathbb{Z}; x \equiv 0 \ mod \ m\}.$$
$$[1] = \{x \in \mathbb{Z}; x \equiv 1 \ mod \ m\}.$$
$$.$$
$$.$$
$$.$$
$$[m-1] = \{x \in \mathbb{Z}; x \equiv 0 \ mod \ 3\}$$

Observe que $[m] = [0]$, pois $m \equiv 0 \ mod \ m$. Desta forma, podemos obter apenas m subconjuntos distintos da maneira como foi definida acima.

Definição 5 *O conjunto* $[a] = \{x \in \mathbb{Z}; x \equiv a \ mod \ m\}$ *é chamado de classe residual módulo* m *do elemento* a *de* $\mathbb{Z}$. *O conjunto de todas as classes residuais de módulo* m *será representado por* $\mathbb{Z}_m$, *ou seja:*

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

Verificamos anteriormente as seguintes propriedades:
Se $a \equiv a' \ mod \ m$ e $b \equiv b' \ mod \ m$, então, $a + b \equiv a' + b' \ mod \ m$ e $a.b \equiv a'.b' \ mod \ m$.

Observando essas propriedades, definimos em $\mathbb{Z}_m$ as seguintes operações:

1. Adição: $[a] + [b] = [a + b]$
2. Multiplicação: $[a].[b] = [a.b]$

As operações acima possuem as propriedades definidas a seguir.

Para todo $[a], [b], [c] \in \mathbb{Z}_m$, temos:

- $([a] + [b]) + [c] = [a] + ([b] + [c])$ (Associatividade na adição)
- $([a].[b]).[c] = [a].([b].[c])$ (Associatividade na multiplicação)
- $[a] + [b] = [b] + [a]$ (Comutatividade na adição)
- $[a].[b] = [b].[a]$ (Comutatividade na multiplicação)
- $[a] + [0] = [a]$ (Existência de zero)
- $[a].[1] = [a]$ (Existência de unidade)
- $[a] + [-a] = [0]$ (Existência de Simétrico)
- $[a].([b] + [c] = [a].[b] + [a].[c]$ (Distributividade)

Definição 6 *O conjunto* $\mathbb{Z}_m$ *munido das operações de adição e multiplicação definidas com as propriedades acima é chamado de anel das classes residuais em* m.

Definição 7 *Um elemento* $[a] \in \mathbb{Z}_m$ *é invertível, se existir* $[b] \in \mathbb{Z}_m$ *tal que* $[a].[b] = [1]$. *Dizemos, então, que* $[b]$ *é o inverso de* $[a]$.

Exemplo 1.10.1 Em $\mathbb{Z}_5$, [3] é o inverso de [2], pois [2].[3] = [1].

Uma vantagem das classes residuais é transformar a congruência $a \equiv b \ mod \ m$ na igualdade $[a] = [b]$. Dessa forma, elas permitem resolver congruências lineares do tipo $aX \equiv b \ mod \ m$, reduzindo-as, em $\mathbb{Z}_m$, à seguinte equação:

$$[a].\mathbb{Z} = [b].$$

Proposição 11 *$[a] \in \mathbb{Z}_m$ é invertível se, e somente se, $(a, m) = 1$.*

Demonstração: Se $[a]$ é invertível, então existe $[b] \in \mathbb{Z}_m$ tal que $[1] = [a].[b] = [a.b]$. Logo, $ab \equiv 1 \ mod \ m$, ou seja, existe um inteiro k tal que $a.b+k.m = 1$ e consequentemente, $(a, m) = 1$.

Reciprocamente, se $(a, m) = 1$, existem inteiros b e k tais que $a.b + k.m = 1$ e consequentemente, $[1] = [a.b + k.m] = [ab] + [km] = [a].[b] + [0] = [a].[b]$.

Portanto,$[a]$ é invertível.

Definição 8 *Um anel onde todo elemento distinto de* [0] *é invertível, ou seja, onde todo elemento não nulo possui um inverso multiplicativo é chamado de corpo.*

Corolário 2 *$\mathbb{Z}_m$ é um corpo, se e somente se, $[m]$ é primo.*

Demonstração: Suponha por absurdo que $\mathbb{Z}_m$ é um corpo e $[m]$ não é primo, então $m = m_1.m_2$ com $1 < m_1 < m$ e $1 < m_2 < m$. Logo, $[0] = [m] = [m_1].[m_2]$ com $[m_1] \neq 0$ e $[m_2] \equiv 0$, temos uma contradição.

Reciprocamente, suponha $[m]$ primo. Como $(i, m) = 1$ para $i = 1, ..., m - 1$, segue-se que $[1], [2], ..., [m - 1]$ são invertíveis. Logo, $\mathbb{Z}_m$ é um corpo.

Capítulo 2

A aritmética modular e suas aplicações no ensino médio

A Aritmética Modular é um conceito muito importante e que está relacionado com divisibilidade e os restos de uma divisão de números inteiros. Muito se tem escrito sobre o tema em muitos livros sobre teoria de números, mas, apesar de utilizarmos os restos de divisões para resolver problemas em vários partes da matemática, este assunto não se encontra presente nos currículos do ensino médio e, portanto, não encontramos material destinado a alunos dessa fase do ensino.

Neste capítulo apresentaremos uma proposta para o ensino de Aritmética Modular, com ênfase na resolução de exercícios contextualizados de diversos assuntos da matemática tais como: Progressões Aritméticas, Progressões Geométricas, Geometria, Matrizes, Números Complexos, entre outros, com o objetivo de mostrar a aplicação do tema no ensino médio. Muitas dessas questões foram retiradas de livros didáticos para o ensino médio, exames de vestibulares e olimpíadas de matemática, mostrando que a Aritmética Modular é um tema atual, justificando o ensino desse tema nessas séries.

2.1 Introdução

Nessa proposta, os conteúdos foram organizados em unidades de uma apostila elaborada paralelamente ao desenvolvimento de um curso ministrado para uma turma do 5^{o} semestre do Curso de Nível Médio Integrado em Química do IFMT - Campus Bela Vista.

Nos assuntos abordados em cada unidade, nas demonstrações de diversos teoremas e propriedades, procuramos utilizar a linguagem formal como as mesmas foram apresentadas na fundamentação teórica do capítulo anterior. Mas, grande parte dos alunos do Ensino Médio, para os quais é direcionado este material, não tem a maturidade ou os pré-requisitos necessários para compreender toda essa fundamentação teórica da forma como foi apresentada. Por isto, associamos a toda essa teoria, exemplos numéricos e problemas contextualizados, para que os alunos consigam compreende-la melhor e dar um significado prático para a mesma.

Apresentaremos então a proposta da forma como a mesma foi trabalhada no curso, ou seja, por unidades.

As unidades 1, 2 e 3, apresentam pré-requisitos necessários à introdução do assunto. Nas unidades 4,5 e 6 encontra-se a parte principal deste trabalho que é o estudo das Congruências Modulares e algumas de suas propriedades. Na unidade 7 apresentamos uma aplicação da congruência modular na Criptografia. Cada unidade, com exceção da unidade 1, contém uma lista de exercícios propostos ao final (Anexo I).

2.2 Unidade 1 - Princípio da Indução Finita

Antes de iniciarmos o estudo da Aritmética Modular propriamente dita, é necessário introduzir alguns assuntos indispensáveis à compreensão das unidades que serão trabalhadas e que auxiliarão nas demonstrações de algumas propriedades e na resolução de exercícios. Dessa forma apresentamos nessa unidade o Princípio da Indução Finita, porque várias demonstrações de teoremas e propriedades necessitam do mesmo, mas não com a pretensão de que o aluno saiba utilizá-lo com destreza, pois necessitaríamos de mais tempo e, além disso, este não é o objetivo principal deste trabalho.

Porém, para que o aluno comece a relacionar os assuntos trabalhados neste curso com aqueles que já estudou no ensino médio, utilizamos o exemplo abaixo para a aplicação do Princípio da Indução Finita.

Exemplo 2.2.1 Determinar uma fórmula para a soma dos n primeiros naturais, ou seja:

$$S(n) = 1 + 2 + 3 + 4 + ... + n.$$

Sabemos pelos nossos estudos de Progressões Aritméticas que podemos resolver este problema utilizando a fórmula da soma dos termos de uma Progressão Aritmética finita, ou seja:

$$S_n = (a_1 + a_n).\frac{n}{2}$$

Dessa forma temos:

$$S_n = \frac{(1+n).n}{2}.$$

Segundo conta a história, esta fórmula foi desenvolvida pelo famoso matemático alemão Carl Friederich Gauss, quando ainda garoto; quando o professor de sua turma mandou que seus alunos efetuassem a soma de todos os números naturais de 1 a 100, no intuito de ocupá-los com uma atividade longa e dessa forma aquietá-los. Teve uma grande surpresa com a rapidez da resposta encontrada por Gauss.

Utilizamos esta fórmula em vários exercícios envolvendo Progressões Aritméticas, sem nunca questionarmos a referida demonstração. No referido exemplo, será que a fórmula encontrada é válida mesmo para qualquer valor que atribuirmos para n?

Para eliminar essa dúvida, utilizamos o princípio da indução para demonstrar a validade da fórmula para qualquer $n \in \mathbb{N}$. Dessa forma, considere a seguinte sentença:

$$P(n) : 1 + 2 + 3 + 4 + ... + n = \frac{(1+n).n}{2}$$

Observe que:

$$P(1) : \ 1 = \frac{(1+1).1}{2}.$$

Logo P(1) é verdadeiro.

Queremos mostrar que se $P(n)$ é válida, então:

$$P(n+1) : 1 + 2 + 3 + 4 + ... + n + (n+1) = \frac{(n+2)(n+1)}{2} \text{ também é válida.}$$

Supondo $P(n)$ verdadeira para algum $n \in \mathbb{N}$, vamos adicionar $n+1$ aos dois membros da igualdade $1+2+3+4+...+n = \dfrac{(1+n).n}{2}$, ou seja:

$$1+2+3+4+...+n+(n+1) = \frac{(1+n).n}{2} + (n+1)$$

$$1+2+3+4+...+n+(n+1) = \frac{(1+n).n + 2(n+1)}{2}$$

$$1+2+3+4+...+n+(n+1) = \frac{(n+1).(n+2)}{2}$$

Temos então $P(n+1)$ verdadeira, logo, pelo Principio de Indução a fórmula $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

2.3 Unidade 2 - Divisibilidade e Divisão Euclidiana

O conceito de Divisibilidade é abordado no ensino médio, porém, nesta unidade é apresentado ao aluno de uma forma diferente. Além de apresentar algumas propriedades importantes, pretendemos que o aluno conheça e se familiarize com notações que serão utilizadas durante o curso. É muito comum ele confundir a notação $a|b$ (a divide b) com uma fração.

Aproveitamos também para mostrar mais uma aplicação do Princípio da Indução Finita, no exemplo abaixo:

Exemplo 2.3.1 Demonstre por indução que o resto da divisão de 10^n por 9 sempre é igual a 1 para todo $n \in \mathbb{N}$.

Demonstrar a afirmação acima equivale a provar que $9|10^n - 1$. Vamos demonstrar por indução.

Observe que para $n = 1$, a afirmação é verdadeira, pois $9|10^1 - 1 \Rightarrow 9|9$.

Supondo verdadeiro que $9|10^n - 1$, devemos mostrar que $9|10^{n+1} - 1$. Note que: $10^{n+1} - 1 = 10^n.10 - 1 = (9.10^n) + (10^n - 1)$.

Como $9|9.10^n$ e pela hipótese de indução $9|10^n - 1$, temos $9|10^{n+1} - 1$. Logo, o resto da divisão de 10^n por 9 sempre é igual a 1 para todo $n \in \mathbb{N}$.

A Aritmética Modular também é chamada de Aritmética dos Restos, dessa forma, é obrigatório apresentar o Teorema da Divisão Euclidiana, que também é estudado no ensino médio. Nesta unidade começamos a apresentar alguns problemas contextualizados e a enfatizar a questão dos restos na divisão de dois números inteiros.

Exemplo 2.3.2 Dividindo um número natural a por outro número natural b, encontramos quociente 4 e resto 5. Dividindo $a + 4$ por $b - 1$, obtemos quociente 5 e resto 6. Determine o valor de a+b.

De acordo com o teorema da divisão euclidiana, temos:

$a = 4b + 5$ (I)

$a + 4 = 5(b - 1) + 6$ (II)

Substituindo (I) em (II):

$4b + 5 + 4 = 5b - 5 + 6 \Rightarrow 4b + 9 = 5b + 1 \Rightarrow b = 8$

Substituindo em (I), temos:

$a = 4.8 + 5 \Rightarrow a = 37$

Logo: $a + b = 37 + 8 = 45$.

Exemplo 2.3.3 Qual o maior número natural n que dividido por 11 deixa quociente igual ao resto?

De acordo com o teorema da divisão euclidiana, temos:

$$n = 11q + r, \text{ mas como } q = r \Rightarrow n = 11r + r \Rightarrow n = 12r.$$

Os possíveis restos da divisão por 11 são 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 e 10. Mas, como procuramos o maior valor de n, então, $r = 10$, logo:

$$n = 12.10 = 120.$$

De fato, dividindo 120 por 11, encontramos quociente 10 e resto 10.

2.4 Unidade 3 - Números Primos, Máximo Divisor Comum e Mínimo Múltiplo Comum

Um dos conjuntos mais interessantes dentro do conjunto dos números naturais, é o conjunto dos números primos que estão associados a diversos problemas que até hoje desafiam os matemáticos.

Nesta unidade recordaremos o conceito de números primos, que é muito importante em várias propriedades e diversos teoremas estudados na Aritmética Modular, como por exemplo, o Pequeno Teorema de Fermat, cuja demonstração será apresentada no final desta unidade.

Apresentaremos também o Teorema Fundamental da Aritmética, conhecido pelos alunos como a decomposição em fatores primos, aproveitando para recordar os conceitos de Mínimo Múltiplo Comum (MMC) e Máximo Divisor Comum (MDC) entre dois números naturais, que podem ser calculados utilizando essa decomposição, bem como, introduzir as notações utilizadas para esses conceitos, ou seja:

- Máximo Divisor Comum entre a e b: (a, b).
- Mínimo Múltiplo Comum entre a e b: $[a, b]$.

Continuando com o objetivo de nossa proposta, apresentaremos mais problemas contextualizados, também com a finalidade de fixar as novas notações introduzidas.

Exemplo 2.4.1 Para levar os alunos de certa escola a um museu pretende-se formar grupos que tenham quantidades iguais de alunos e de modo que, em cada grupo, todos sejam do mesmo sexo. Se nessa escola estudam 1350 rapazes e 1224 garotas e cada grupo deverá ser acompanhado de um único professor, determine:
a) o número máximo de alunos em cada grupo.

Note que procuramos um número que divida simultaneamente 1350 e1224, e este deve ser o maior possível, pois desejamos o máximo de alunos em cada grupo. Logo, estamos procurando $(1350, 1224)$. Dessa forma, temos:
$1350 = 2.3^3.5^2$ e $1224 = 2^3.3^2.17$

Então, $(1350, 1224) = 2.3^2 = 18$. Logo, cada grupo deve ter 18 alunos.

b) O número de professores que acompanharão esses grupos.

Dividindo 1350 por 18 obtemos 75 grupos de rapazes e dividindo 1224 por 18, obtemos 68 grupos de garotas. Logo, serão necessários $75 + 68 = 143$ professores para acompanhar esses grupos.

Exemplo 2.4.2 As cidades de Cuiabá, Rondonópolis e Poconé realizam festas periódicas. Cuiabá realiza festas de 9 em 9 meses; Rondonópolis , de 12 em 12 meses e Poconé de 15 em 15 meses. Se em janeiro de 2008, as três cidades realizaram essas festas nesse mês, qual o próximo ano em que isto ocorrerá novamente, ou seja, quando as festas das três cidades ocorrerão novamente em um mesmo mês?

Observe que após a realização das festas em janeiro de 2008, as próximas festas em Cuiabá ocorrerão em períodos múltiplos de 9, em Rondonópolis, em períodos múltiplos de 12 e em Poconé, em períodos múltiplos de 15, ou seja:
Cuiabá: 9, 18, 27, 36, ...
Rondonópolis: 12, 24, 36, 48, ...
Poconé: 15, 30, 45,60, ...

Note que no 36^{o} mês ocorrerá as festas da cidade de Cuiabá e Rondonópolis, porém não acontecerá a festa em Poconé.

Então, estamos procurando um mês que seja múltiplo de 9, 12 e 15 simultaneamente e deve ser o menor possível, pois queremos o próximo mês em que acontecerão as três festas, ou seja, estamos procurando [9,12,15].

Dessa forma:
$9 = 3^2$, $12 = 2^2.3$ e $15 = 3.5$

Logo, $[9, 12, 15] = 2^2.3^2.5 = 180$. Como 180 meses correspondem a exatos 15 anos, as festas dessas três cidades ocorrerão num mesmo mês novamente, em janeiro de 2023.

Para apresentar o Pequeno Teorema de Fermat, que no estudo das congruências modulares será utilizado para facilitar a resolução de alguns problemas, antes de enunciá-lo e fazer a sua demonstração, utilizaremos os exemplos particulares a seguir:

Exemplo 2.4.3 Demonstre por indução que $2|a^2 - a$, para todo $a \in \mathbb{Z}$.

Basta demonstrar o resultado para $a \geq 0$.

Para $a = 0$ temos $2|0^2 - 0$, pois $2|0$.

Supondo tal resultado válido para a, vamos demonstrá-lo para $a + 1$. Temos:

$$(a+1)^2 - (a+1) = a^2 + 2a + 1 - a - 1 = a^2 - a + 2a.$$

Como pela hipótese de indução $2|a^2 - a$ e $2|2a$, temos $2|a^2 - a$, para todo $a \in \mathbb{Z}$

Exemplo 2.4.4 Demonstre por indução que $3|a^3 - a$, para todo $a \in \mathbb{Z}$.

Para $a = 0$ temos $3|0^2 - 0$, pois $3|0$

Supondo tal resultado válido para a, vamos demonstrá-lo para $a + 1$. Temos:

$$(a+1)^3 - (a+1) = a^3 + 3a^2 + 3a + 1 - a - 1 = a^3 - a + 3.(a^2 + a).$$

Como pela hipótese de indução $3|a^3 - a$ e $3|3.(a^2 + a)$, temos $3|a^3 - a$, para todo $a \in \mathbb{Z}$.

Da mesma forma que demonstramos as afirmações acima podemos demonstrar, por exemplo, que $5|a^5 - a$, $7|a^7 - a$ ou $11|a^{11} - a$, para todo $a \in \mathbb{Z}$.

Observe que 2, 3, 5, 7, 11 são números primos. O grande matemático Pierre de Fermat generalizou estes resultados, enunciando o pequeno teorema que leva o seu nome.

2.5 Unidade 4 - Congruência Modular

Após revisar conceitos e propriedades importantes para o estudo da Aritmética Modular, como Divisibilidade, Divisão Euclidiana e Números Primos, apresentar notações específicas para alguns conceitos e operações, bem como introduzir alguns assuntos que não são estudados no ensino médio, como o Pequeno Teorema de Fermat, chegamos então, a parte principal deste trabalho, ou seja, o estudo das congruências modulares.

Para introduzirmos o conceito de congruência modular, considere o seguinte exemplo:

Exemplo 2.5.1 A copa do mundo de futebol será realizada no Brasil no ano de 2014. O jogo de abertura ocorrerá no dia 12 de junho. Supondo que não haja um calendário em mãos e sabendo que o dia 1º de janeiro de 2014 será uma quarta feira, determine em que dia da semana ocorrerá o jogo de abertura.

Tabela 2.1: Número de dias de cada mês

JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ
31	28	31	30	31	30	31	31	30	31	30	31

Para determinar quantos dias temos do início do ano até o dia 12 de junho de 2013, devemos efetuar a seguinte soma:

$31 + 28 + 31 + 30 + 31 + 12 = 163$

Logo, o dia 12 de junho é o 163º dia do ano de 2014.

Vamos construir uma tabela com os primeiros dias de Janeiro:

Tabela 2.2: Primeiros dias de Janeiro

QUA	QUI	SEX	SAB	DOM	SEG	TER
1	2	3	4	5	6	7
8	9	10	11	12	13	14
14	16	17	18	19	20	21
22	23	24	25	26	27	28

Observe que:

- Na Terça: 7; 14; 21;28;... São múltiplos de 7, ou seja, quando divididos por 7 deixam resto igual a 0 ($7.n$, com $n \in \mathbb{N}$).
- Na Quarta: 1; 8; 15;22;... São múltiplos de 7, mais 1, ou seja, quando divididos por 7 deixam resto igual a 1($7.n + 1$, com $n \in \mathbb{N}$).
- Na Quinta: 2; 9; 16;23;... São múltiplos de 7, mais 2, ou seja, quando divididos por 7 deixam resto igual a 2 ($7.n + 2$, com $n \in \mathbb{N}$).
- Na Sexta: 3; 10; 17;24;... São múltiplos de 7, mais 3, ou seja, quando divididos por 7 deixam resto igual a 3($7.n + 3$, com $n \in \mathbb{N}$).
- No Sábado: 4; 11; 18;25;... São múltiplos de 7, mais 4, ou seja, quando divididos por 7 deixam resto igual a 4 ($7.n + 1$, com $n \in \mathbb{N}$).

- No Domingo: 5; 12; 19;26;... São múltiplos de 7, mais 5, ou seja, quando divididos por 7 deixam resto igual a 5($7.n + 5$, com $n \in \mathbb{N}$).

- Na segunda: 6; 13; 20;27;... São múltiplos de 7, mais 6, ou seja, quando divididos por 7 deixam resto igual a 6 ($7.n + 6$, com $n \in \mathbb{N}$).

Dessa forma, para descobrirmos em qual dia da semana ocorrerá o jogo de abertura da copa basta dividir 163 por 7 e verificarmos qual é o resto dessa divisão.

Efetuando a divisão de 163 por 7, obtemos quociente 23 e resto 2, ou seja:
$163 = 7.23 + 2$

Portanto, o dia 12 de Junho será uma Quinta feira.

O grande matemático alemão, Carl Friederich Gauss, percebeu que utilizávamos com muita frequência frases do tipo "a e b quando divididos por m deixam o mesmo resto"e que essa relação tinha comportamento semelhante à igualdade. Gauss introduziu uma notação específica para esse fato e denominou-a de Congruência Modular.

Definição 4: *Seja m um número natural diferente de zero. Dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Denota-se esta relação da seguinte forma: $a \equiv b \ mod \ m$.*

Em outras palavras, uma congruência é a relação entre dois números inteiros que, divididos por um terceiro número natural - chamado módulo de congruência - deixam o mesmo resto.

Por exemplo, no problema anterior, observamos na quinta feira, que o número 9 é congruente ao número 16, módulo 7, pois ambos deixam resto 2, ao serem divididos por 7. Representamos essa congruência do exemplo por $9 \equiv 16 \ mod \ 7$.

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

Por exemplo, na divisão de 163 por 7 obtivemos quociente 23 e resto 2, logo: $163 \equiv 2 \ mod \ 7$, pois, 2=7.0+2, ou seja dividindo 2 por 7, obtemos quociente 0 e resto 2.

Observe também, que no exemplo dado, as sequências de números em cada dia, obedecem uma Progressão Aritmética de razão igual a 7. A congruência modular e suas propriedades auxiliam a resolução de vários problemas que envolvem esse tipo de sequência, como veremos em alguns dos exemplos a seguir.

Exemplo 2.5.2 (OBMEP - Olimpíadas de Matemática) - A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?

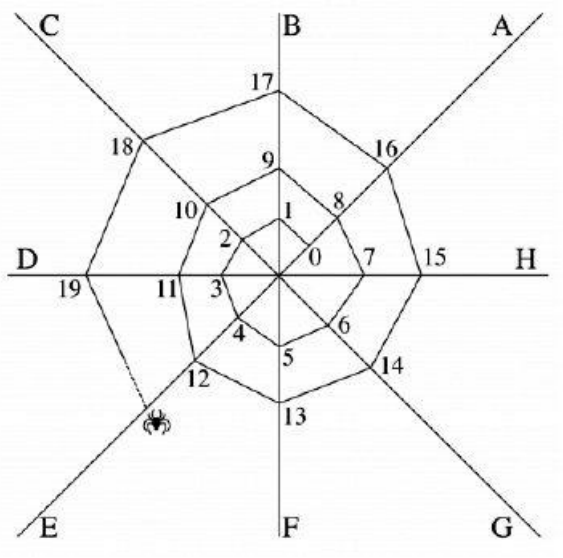

Figura 2.1: Teia da Aranha

Verifique que em cada fio, os números formam uma Progressão Aritmética de razão igual a 8. Agora que conhecemos a definição de congruência, basta construir apenas primeira linha na tabela abaixo:

Tabela 2.3: Número de congruência dos fios

FIOS	A	B	C	D	E	F	G	H
	0	1	2	3	4	5	6	7

Dividindo 118 por 8, obtemos quociente 14 e resto 6, ou seja:
$118 \equiv 6 \ mod \ 8$, portanto, o número 118 estará sobre o fio G.

Exemplo 2.5.3 (FUVEST) Sabendo que os anos bissextos são múltiplos de 4 e que o primeiro dia de 2007 foi segunda-feira, o próximo a começar também em uma segunda feira será:

a) 2012

b) 2011

c) 2014

d) 2018

e) 2024

Como vimos no exemplo 1, temos um caso de congruência no módulo 7. Vamos construir a tabela da primeira semana de um ano qualquer.

Tabela 2.4: Primeiros dias do ano

PRIMEIRO DIA	SEGUNDO DIA	TERCEIRO DIA	QUARTO DIA	QUINTO DIA	SEXTO DIA	SÉTIMO DIA
1	2	3	4	5	6	7

Observe que $365 \equiv 1 \ mod\ 7$. Isto significa que num ano não bissexto, o último dia do ano, ou seja, o 365^{o} dia ocorre num mesmo dia da semana que o primeiro dia desse ano. Dessa forma, o primeiro dia do próximo ano, avança um dia da semana em relação ao primeiro dia do ano anterior.

Por exemplo: 2007 não é um ano bissexto e se iniciou numa segunda feira, portanto, o último dia de 2007 também será uma segunda feira, dessa forma, o primeiro dia de 2008 será uma terça feira.

Já um ano bissexto, possui 366 dias. Observe que $366 \equiv 2 \ mod\ 7$. Isto significa que num ano bissexto, o último dia do ano, ou seja, o 366^{o} dia ocorre num mesmo dia que o segundo dia desse ano. Dessa forma, o primeiro dia do próximo ano, avança dois dias da semana em relação ao primeiro dia do ano anterior.

Por exemplo: 2008 é um ano bissexto, e como já observamos, o primeiro dia desse ano é uma terça feira, logo, o último dia desse ano será uma quarta feira. Dessa forma, o primeiro dia de 2009 será uma quinta feira.

Considere que N seja o número de dias de um ano não bissexto e M o número de dias de um ano bissexto. Temos que $N \equiv 1 \ mod\ 7$ e $M \equiv 2 \ mod\ 7$. Temos:

Tabela 2.5: Início de cada ano

Ano	Congruência	Último dia	Próximo ano	Início do próximo ano
2007	$N \equiv 1 \ mod\ 7$	Segunda feira	2008	Terça feira
2008	$M \equiv 2 \ mod\ 7$	**Terça feira**	**2009**	**Quinta feira**
2009	$N \equiv 1 \ mod\ 7$	Quinta feira	2010	Sexta feira
2010	$N \equiv 1 \ mod\ 7$	Sexta feira	2011	Sábado
2011	$N \equiv 1 \ mod\ 7$	Sábado	2012	Domingo
2012	$M \equiv 2 \ mod\ 7$	**Domingo**	**2013**	**Terça feira**
2013	$N \equiv 1 \ mod\ 7$	Terça feira	2014	Quarta feira
2014	$N \equiv 1 \ mod\ 7$	Quarta feira	2015	Quinta feira
2015	$N \equiv 1 \ mod\ 7$	Quinta feira	2016	Sexta feira
2016	$M \equiv 2 \ mod\ 7$	**Sexta feira**	**2017**	**Domingo**
2017	$N \equiv 1 \ mod\ 7$	Domingo	2018	Segunda feira

Portanto, o próximo ano a começar numa segunda feira será 2018.

Exemplo 2.5.4 (OBMEP - 2012) Cinco cartas, inicialmente dispostas como na figura, serão embaralhadas. Em cada embaralhamento, a primeira carta passa a ser a segunda, a segunda passa a ser a quarta, a terceira passa a ser a primeira, a quarta passa a ser a quinta e a quinta passa a ser a terceira. Qual será a primeira carta após 2012 embaralhamentos?

Figura 2.2: Cartas I

Vamos verificar o que acontece após alguns embaralhamentos, seguindo as instruções do enunciado:

1. Posição Inicial: **A 2 3 4 5**
2. 1º Embaralhamento: 3 A 5 2 4
3. 2º Embaralhamento: 5 3 4 A 2
4. 3º Embaralhamento: 4 5 2 3 A
5. 4º Embaralhamento: 2 4 A 5 3
6. 5º Embaralhamento: **A 2 3 4 5** (Posição Inicial).

Observe que a cada 5 embaralhamento a sequência se repetirá. Temos um caso de congruência módulo 5. Dessa forma, se N é o número de embaralhamentos, então:

- Se $N \equiv 0 \ mod \ 5$, a primeira carta será A.
- Se $N \equiv 1 \ mod \ 5$, a primeira carta será 3.
- Se $N \equiv 2 \ mod \ 5$, a primeira carta será 5.
- Se $N \equiv 3 \ mod \ 5$, a primeira carta será 4.
- Se $N \equiv 4 \ mod \ 5$, a primeira carta será 2.

Então, é fácil verificar que $2012 \equiv 2 \ mod \ 5$, logo, após 2012 embaralhamentos, a primeira carta da sequencia será o 5 de paus.

No exemplo abaixo, temos uma aplicação da congruência modular numa matriz.

Exemplo 2.5.5 (FUVEST) Os números inteiros positivos são dispostos em "quadrados"da seguinte maneira:

1	2	3	10	11	12	19	...	...
4	5	6	13	14	15	...	...	...
7	8	9	16	17	18	...	...	...

O número 500 se encontra em um desses "quadrados". Determine em qual "quadrado"ele está, e também em qual linha e coluna.

Observe que cada "quadrado"é uma matriz de ordem 3x3, ou seja:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Note que cada elemento a_{11} de um "quadrado"é um múltiplo de 9 mais 1, ou seja, $a_{11} \equiv 1 \ mod \ 9$; cada elemento a_{12} é múltiplo de 9 mais 2, ou seja, $a_{12} \equiv 2 \ mod \ 9$ e assim sucessivamente. Dessa forma, temos:
$a_{11} \equiv 1 \ mod \ 9$, $a_{12} \equiv 2 \ mod \ 9$, $a_{13} \equiv 3 \ mod \ 9$, $a_{21} \equiv 4 \ mod \ 9$, $a_{22} \equiv 5 \ mod \ 9$, $a_{23} \equiv 6 \ mod \ 9$, $a_{31} \equiv 7 \ mod \ 9$, $a_{32} \equiv 8 \ mod \ 9$ e $a_{33} \equiv 0 \ mod \ 9$.

Assim, dividindo 500 por 9, obtemos quociente 55 e resto 5, ou seja, $500 \equiv 5 \equiv a_{22} \ mod \ 9$, logo, o número 500 está na $2^{\underline{a}}$ linha, $2^{\underline{a}}$ coluna do $56^{\underline{o}}$ "quadrado".

Uma maneira equivalente de dizer que $a \equiv b \ mod \ m$, é afirmar que $m|(b-a)$, ou seja, a diferença $(b-a)$ é um múltiplo de m.

A questão abaixo foi retirada da prova do ENEM - 2013 e adaptada para exemplificar uma aplicação da observação acima.

Exemplo 2.5.6 (ENEM 2013 - Adaptada) O ciclo de atividade magnética do Sol tem um período de 11 anos. O início do primeiro ciclo registrado se deu no começo de 1755 e se estendeu até o final de 1765. Desde então, todos os ciclos de atividade magnética do Sol têm sido registrados.

Disponível em: http://g1.globo.com. Acesso em: 27 fev. 2013

De acordo com os dados acima, é correto afirmar que um determinado ciclo de atividade magnética do Sol teve início no ano de:

a) 1842

b) 1854

c) 1906

d) 1958

e) 2013

Tabela 2.6: Primeiro ciclo solar

Ano	1755	1756	1757	1758	1759	1760	1761	1762	1763	1764	1765
	1766	...									

Observe na tabela acima que os anos em que se iniciam os ciclos solares formaram uma Progressão Aritmética de razão 11. Estamos procurando um ano entre as alternativas que seja congruente a 1755 no módulo 11. Testando as possíveis alternativas, temos:

a) $1842 - 1755 = 87$ não é múltiplo de 11.

b) $1854 - 1755 = 99 = 9.11$ é múltiplo de 11.

Ou seja:

$11|(1854 - 1755) \Rightarrow 1854 \equiv 1755 \ mod \ 11$, logo um ciclo solar tem início em 1854.

Para resolvermos a questão original do ENEM, observe na tabela que:

$1766 - 1755 = 11$, ou seja, **1 . 11** e o ano de 1766 é o início do **2º ciclo solar**. No

exemplo anterior: $1854 - 1755 = 99$, ou seja, **9 . 11**, então, o ano de 1854 é o início do **10º ciclo solar**.

Exemplo 2.5.7 (ENEM 2013 - Adaptada) O ciclo de atividade magnética do Sol tem um período de 11 anos. O início do primeiro ciclo registrado se deu no começo de 1755 e se estendeu até o final de 1765. Desde então, todos os ciclos de atividade magnética do Sol têm sido registrados.

Disponível em: http://g1.globo.com. Acesso em: 27 fev. 2013

No ano de 2101, o sol estará no ciclo de atividade magnética de número:

a) 32

b) 34

c) 33

d) 36

e) 31

Tabela 2.7: Anos dos Ciclos Solares

Ano	1755	1756	1757	1758	1759	1760	1761	1762	1763	1764	1765
	1766	1767	1768	1769	1770	1771	1772	1773	1774	1775	1776
	...	...	...	...	...	...	...	...	...	...	...
Restos	6	7	8	9	10	0	1	2	3	4	5

Observe que o ano de 2101 é múltiplo de 11, ou seja, $2101 = 191.11$, logo $2101 \equiv 0 \ mod \ 11$.

Observe também que não é necessário efetuar todas as divisões euclidianas de cada ano por 11 para achar os restos. Como os anos são consecutivos, basta achar o resto da divisão do ano de inicio do primeiro ciclo e os demais são consecutivos até o resto 10. O próximo é múltiplo de 11, ou seja:

$1760 \equiv 0 \ mod \ 11$.

Temos, então:

$2101 - 1760 = 341 = 31.11$.

Portanto:

2101 é o 6º ano do 32º ciclo solar.

2.6 Unidade 5 - Propriedades das Congruências Modulares

A Congruência Modular é compatível com as operações de adição e multiplicação dentro do conjunto dos números inteiros. Este fato torna essa relação uma ferramenta muito útil e poderosa. Nesta unidade apresentamos exemplos de problemas que envolvem Geometria, Progressões Aritméticas, Progressões Geométricas entre outros assuntos, nos quais a aplicação de algumas propriedades e do Pequeno Teorema de Fermat facilitam a resolução dos mesmos.

Propriedades das congruências modulares

Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.

1. Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então, $a + c \equiv b + d \ mod \ m$.

Exemplo 2.6.1

$27 \equiv 32 \ mod \ 5$ (27 e 32 quando divididos por 5 deixam resto igual a 2)

$13 \equiv 282 \ mod \ 5$ (13 e 28 quando divididos por 5 deixam resto igual a 3)

Então:

$27 + 13 \equiv 32 + 28 \ mod \ 5 \Rightarrow 40 \equiv 60 \ mod \ 5$ (40 e 60 divididos por 5 deixam resto igual a zero).

2. Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $a.c \equiv b.d \ mod \ m$

Exemplo 2.6.2

$5 \equiv 8 \ mod \ 3$ (5 e 8 divididos por 3 deixam resto 2)

$7 \equiv 10 \ mod \ 3$ (7 e 10 divididos por 3 deixam resto 1)

Então:

$5.7 \equiv 8.10 \ mod \ 5 \Rightarrow 35 \equiv 80 \ mod \ 5$ (35 e 80 divididos por 3 deixam resto 2).

3. Se $a \equiv b \ mod \ m$, então $a^n \equiv b^n \ mod \ m$, para todo $n \in \mathbb{N}$.

Exemplo 2.6.3

$7 \equiv 12 \ mod \ 5$ (7 e 12 divididos por 5 deixam resto 2)

$7^2 \equiv 12^2 \ mod \ 5 \Rightarrow 49 \equiv 14 \ mod \ 5$ (49 e 144 divididos por 5 deixam resto 4).

Aplicaremos essas propriedades nos exemplos abaixo:

Exemplo 2.6.4 A televisão de Marco consegue sintonizar apenas os canais de 1 até 41. Se Marco começa sintonizando o canal 15 e aperta o botão que avança o canal 2005 vezes, em que canal estará sintonizado ao parar?

Note que ao chegar ao canal 41, na próxima vez que Marco apertar ao botão, ele retornará ao canal 1. Isto se repete a cada 41 apertos no botão de controle. Então, podemos aplicar as propriedades da congruência no módulo 41.

Observe que $2005 \equiv 37 \ mod \ 41$ e $15 \equiv 15 \ mod \ 41$.

Se Marcos tivesse iniciado no canal 1, após 2005 vezes a televisão estaria sintonizada no canal 37, porém como ele iniciou no canal 15, aplicando a propriedade da soma temos:

$$15 + 2005 \equiv 15 + 37 \equiv 52 \equiv 11 \ mod \ 41.$$

Logo, iniciando do canal 15 e apertando 2005 vezes o botão, ao final, a televisão ficará sintonizada no canal 11.

Exemplo 2.6.5 A tabela apresentada a seguir mostra uma sequência de números naturais agrupados em 6 linhas horizontais (A, B, C, D, E, F) e seguindo a uma determinada ordenação.

Tabela 2.8: Sequência de Números I

A	0	6	12	18	24	30	36	42	48	54	60
B	1	7	13	19	25	31	37	43	49	55	...
C	2	8	14	20	26	32	38	44	50	56	...
D	3	9	15	21	27	33	39	45	51	57	...
E	4	10	16	22	28	34	40	46	52	58	...
F	5	11	17	23	29	35	41	47	53	59	...

Em qual linha se encontra o resultado do produto 662.1805?

Note que:

- Se a é um número pertencente a linha A, então $a \equiv 0 \ mod \ 6$.
- Se b é um número pertencente a linha B, então $b \equiv 1 \ mod \ 6$.
- Se c é um número pertencente a linha C, então $c \equiv 2 \ mod \ 6$.
- Se d é um número pertencente a linha D, então $d \equiv 3 \ mod \ 6$.
- Se e é um número pertencente a linha E, então $e \equiv 4 \ mod \ 6$.
- Se f é um número pertencente a linha F, então $f \equiv 5 \ mod \ 6$.

Observe que $662 \equiv 2 \ mod \ 6$ e $1805 \equiv 5 \ mod \ 6$. Logo:

$$662.1805 \equiv 2.5 \equiv 10 \equiv 4 \ mod \ 6.$$

Portanto, o resultado desse produto estará na linha E.

Exemplo 2.6.6 O Bozó é um jogo que utiliza cinco dados na forma de cubos, numerados de 1 a 6, que são colocados em um copo e arremessados à mesa para contagem de pontos, obtidos através de vários tipos de sequências. Lucas possui vários blocos de madeira na forma de cubos de arestas com medidas superiores a 100 cm e deseja recortar esses blocos, de forma a se obter o máximo de cubos menores (dados) com arestas iguais a 2 cm, que serão utilizados na montagem de conjuntos constituídos de um copo e cinco desses dados, para serem posteriormente comercializados. Supondo que não haja perda de material na fabricação desses dados, pergunta-se:
a) Se Lucas utilizar um bloco de madeira de arestas iguais a 106 cm, quantos dados sobram após a montagem de conjuntos completos?

Para se obter o máximo de dados, cada aresta deve ser recortada em 53 pedaços de 2 cm. Dessa forma, o número de dados obtidos de cada bloco, será igual a:

$$53.53.53 = 53^3.$$

Observe que $53 \equiv 3 \ mod \ 5$, então $53^3 \equiv 3^3 \equiv 27 \equiv 2 \ mod \ 5$, portanto, sobrarão 2 dados.

b) Após recortar um bloco e em seguida montar o máximo de conjuntos completos, Lucas verifica que sobraram 3 dados. Qual o valor da menor medida possível para a aresta desse bloco?

Seja X, o número de pedaços de cada aresta, então, X^3 é o número de dados obtidos. Neste caso, devemos ter $X \equiv 0 \ mod \ 5$,ou $X \equiv 1 \ mod \ 5$, ou $X \equiv 2 \ mod \ 5$, ou $X \equiv 3 \ mod \ 5$ ou $X \equiv 4 \ mod \ 5$, Assim:

- $X \equiv 0 \ mod \ 5 \Rightarrow X^3 \equiv 0^3 \ mod \ 5 \Rightarrow X \equiv 0 \ mod \ 5$.
- $X \equiv 1 \ mod \ 5 \Rightarrow X^3 \equiv 1^3 \ mod \ 5 \Rightarrow X \equiv 1 \ mod \ 5$.
- $X \equiv 2 \ mod \ 5 \Rightarrow X^3 \equiv 2^3 \ mod \ 5 \Rightarrow X \equiv 8 \ mod \ 5 \Rightarrow X \equiv 3 \ mod \ 5$.
- $X \equiv 3 \ mod \ 5 \Rightarrow X^3 \equiv 3^3 \ mod \ 5 \Rightarrow X \equiv 27 \ mod \ 5 \Rightarrow X \equiv 2 \ mod \ 5$.
- $X \equiv 4 \ mod \ 5 \Rightarrow X^3 \equiv 4^3 \ mod \ 5 \Rightarrow X \equiv 64 \ mod \ 5 \Rightarrow X \equiv 4 \ mod \ 5$.

Então, num bloco de 100 cm, cada aresta será dividida em 50 pedaços, como 50 é múltiplo de 5, temos $50 \equiv 0 \ mod \ 5$, dessa forma o menor número de pedaços desejado, é 52, pois $52 \equiv 2 \ mod \ 5$. Dessa forma a medida da menor aresta possível é:

$$52 \times 2 \ cm = 104 \ cm.$$

Exemplo 2.6.7 Um número a dividido por 11 deixa resto 2 e b é um número que dividido pelo mesmo divisor deixa resto 3. Calcule o menor número que se deve subtrair de $a^3 + b^2$ para se obter um múltiplo de 11.

Pelo enunciado, temos $a \equiv 2 \ mod \ 11$ e $b \equiv 3 \ mod \ 11$. Aplicando a propriedade das potências, temos:
$a \equiv 2 \ mod \ 11 \Rightarrow a^3 \equiv 2^3 \ mod \ 11 \Rightarrow a^3 \equiv 8 \ mod \ 11$.
$b \equiv 3 \ mod \ 11 \Rightarrow b^2 \equiv 3^2 \ mod \ 11 \Rightarrow b^2 \equiv 9 \ mod \ 11$.

Aplicando a propriedade da soma temos:

$$a^3 + b^2 \equiv 8 + 9 \equiv 17 \equiv 6 \ mod \ 11.$$

Ou seja, $a^3 + b^2$ deixa resto 6 quando dividido por 11, logo, devemos subtrair 6 para obtermos um múltiplo de 11.

Exemplo 2.6.8 Considere a seguinte progressão aritmética: (10, 17, 24, 31, 38,...). Verifique se os números abaixo são termos que pertencem a essa Progressão Aritmética (P.A).
a) 773
b) $51^{19} + 1$

Calculando o termo geral da Progressão Aritmética, temos:

$$a_n = a_1 + (n-1).r$$
$$a_n = 10 + (n-1).7$$
$$a_n = 7n + 3$$

Dessa forma, é fácil perceber que 773 é um termo dessa P.A., pois, $773 = 7.110 + 3$. Mas, para o próximo item, esta verificação não é tão simples.

Todo termo dessa progressão é um múltiplo de 7 mais 3, e como já vimos, isto significa que $a_n \equiv 3 \ mod \ 7$. Assim, para ser um termo dessa P.A., devemos ter $51^{19} + 1 \equiv 3 \ mod \ 7$. Vejamos:

Observe que $51 \equiv 2 \ mod \ 7 \Rightarrow 51^{19} + 1 \equiv 2^{19} + 1 \ mod \ 7$.

Observe ainda que $2^3 = 8 \equiv 1 \ mod \ 7$, então:

$$2^{19} + 1 \equiv (2^3)^6.2 + 1 \equiv 1^6.2 + 1 \equiv 2 + 1 \equiv 3 \ mod \ 7.$$

Portanto, $51^{19} + 1 \equiv 3 \ mod \ 7$, logo, é um termo dessa Progressão Aritmética.

Com a notação de congruência, o Pequeno Teorema de Fermat pode ser enunciado da seguinte forma:

Se p é um número primo e $a \in \mathbb{Z}$, então:

$$a^p \equiv a \ mod \ p$$

Além disso, se $p \nmid a$, então:

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

Nos exemplos abaixo, a aplicação do Pequeno Teorma de Fermat facilita a resolução dos problemas propostos. Os dois problemas envolvem Progressões Geométricas, mas o segundo necessita também de conceitos da Geometria Plana para sua resolução.

Exemplo 2.6.9 Segundo a história, o rei ofereceu uma recompensa ao sábio que desenvolveu o jogo de xadrez no seu reino. A recompensa pedida foi que cada casa do tabuleiro fosse preenchida com sementes de trigo, mas dobrando a cada casa. No caso, seria uma PG de primeiro termo 1 e razão igual a 2. Logo o rei desistiu da recompensa e nomeou o sábio como seu conselheiro repleto de honrarias. Isto porque, se a recompensa fosse realmente cumprida, ao final das 64 casas do tabuleiro, a quantidade de grãos de trigo seria imensa, impossível de ser paga.

Aproveitando essa história, imagine se o rei, vingando-se da brincadeira do seu agora conselheiro, colocasse um calendário (ou algo similar) sobre a mesa e lhe propusesse o seguinte desafio:

Colocando 1 grão de trigo no dia $1^{\underline{o}}$ do ano, 1 grão de trigo no dia 2, 1 grão no dia 3 e assim sucessivamente até o dia 31 e repetindo esse procedimento até que o último grão da quantia que me solicitou seja colocado sobre o calendário, em qual dia do ano seria colocado esse último grão?

Não podemos saber se o conselheiro conseguiria responder a tal desafio, mas com os conceitos e propriedades da congruência modular podemos encontrar a resposta. Como já sabemos, a quantia solicitada pelo sábio é calculada através da fórmula da soma dos termos de uma progressão geométrica finita, ou seja:

$$S_{64} = \frac{a_1(q^n - 1)}{q - 1} = \frac{1.(2^{64} - 1)}{2 - 1} = 2^{64} - 1.$$

Como 31 é primo, pelo Pequeno Teorema de Fermat, temos que $2^{31} \equiv 2 \ mod \ 31$, logo:

$$2^{64} - 1 = (2^{31})^2.2^2 - 1 \equiv 2^2.4 - 1 \equiv 16 - 1 \equiv 15 \ mod \ 31.$$

Logo, o último grão seria colocado no dia 15 de janeiro.

Exemplo 2.6.10 Uma pista circular possui raio igual a 25 metros. Suponha que um móvel está no ponto de partida dessa pista e começa a percorrê-la da seguinte forma: 6 metros na primeira hora, 18 metros na segunda hora, 54 metros na terceira hora e assim sucessivamente, sempre triplicando a distância percorrida a cada hora. Dessa forma, qual a distância aproximada percorrida pelo móvel após passar pelo ponto de partida pela última vez? (Utilize para os cálculos: $\pi = 3,14$).

De acordo com o enunciado, como o raio da pista $r = 25$, o comprimento da pista é igual a:

$$C = 2\pi r = 2.3, 14.25 = 157\ m.$$

O percurso total do móvel é dado pela soma dos termos de uma progressão geométrica de razão igual a 3, ou seja:

$$S_{160} = \frac{a_1(q^n - 1)}{q - 1} = \frac{6.(3^{160} - 1)}{3 - 1} = \frac{6(3^{160} - 1)}{2} = 3.(3^{160} - 1).$$

Note que a cada 157 m, o móvel retorna à posição inicial. Para determinar a distância pedida, devemos calcular o resto da divisão de $3.(3^{160} - 1)$ por 157.

Como 157 é primo, pelo Pequeno Teorema de Fermat, temos que:

$$3^{156} \equiv 1\ mod\ 157.$$

Dessa forma:

$$3.(3^{160} - 1) = 3.(3^{156}.3^4 - 1) \equiv 3.(1.81 - 1) \equiv 3.80 \equiv 240 \equiv 83\ mod\ \ 157.$$

Logo, a distãncia aproximada percorrida pelo móvel nessa pista, após passar pela última vez pelo ponto de partida, é igual a 83 m.

2.7 Unidade 6 - Classes Residuais

Nesta unidade, introduzimos o conceito de classe residual módulo m e apresentamos o conjunto $\mathbb{Z}_m$ formado por todas essas classes. Aproveitamos a definição do anel das classes residuais módulo m, para destacar a importância de determinar o elemento invertível em $\mathbb{Z}_m$.

Para introduzir o conceito de classes residuais, utilizamos a tabela utilizada no exemplo 2 da unidade anterior, ou seja:

Tabela 2.9: Sequencia de Números

A	0	6	12	18	24	30	36	42	48	54	60
B	1	7	13	19	25	31	37	43	49	55	...
C	2	8	14	20	26	32	38	44	50	56	...
D	3	9	15	21	27	33	39	45	51	57	...
E	4	10	16	22	28	34	40	46	52	58	...
F	5	11	17	23	29	35	41	47	53	59	...

a) Somando um número b da linha B com um número e da linha E, em qual linha vai estar o resultado dessa soma?

Como $b \equiv 1 \ mod \ 6$ e $e \equiv 4 \ mod \ 6$, temos $b + e \equiv (1 + 4) \ mod \ 6$, ou seja $b + e \equiv 5 \ mod \ 6$, portanto, o resultado dessa soma vai estar na linha F.

b) Multiplicando um número c da linha C com um número f da linha F, em qual linha vai estar o resultado desse produto?

Observe que $c \equiv 2 \ mod \ 6$ e $f \equiv 5 \ mod \ 6$, logo, $c.f \equiv 2.5 \ mod \ 6$, ou seja:
$c.f \equiv 10 \equiv 4 \ mod \ 6$, portanto, o resultado desse produto vai estar na linha E.

Observe que a tabela apresenta o conjunto dos números naturais divididos em seis subconjuntos, ou seja, cada linha contém elementos que apresentam a mesma propriedade em relação à divisão euclidiana pelo número 6, a saber:

- Na linha A, temos o subconjunto formados pelos números que divididos por 6 deixam resto 0, ou seja $A = \{x \in \mathbb{N} | x \equiv 0 \ mod \ 6\}$.
- Na linha B, temos o subconjunto formados pelos números que divididos por 6 deixam resto 1, ou seja $B = \{x \in \mathbb{N} | x \equiv 1 \ mod \ 6\}$.
- Na linha C, temos o subconjunto formados pelos números que divididos por 6 deixam resto 2, ou seja $C = \{x \in \mathbb{N} | x \equiv 2 \ mod \ 6\}$.
- Na linha D, temos o subconjunto formados pelos números que divididos por 6 deixam resto 3, ou seja $D = \{x \in \mathbb{N} | x \equiv 3 \ mod \ 6\}$.
- Na linha E, temos o subconjunto formados pelos números que divididos por 6 deixam resto 4, ou seja $E = \{x \in \mathbb{N} | x \equiv 4 \ mod \ 6\}$.
- Na linha F, temos o subconjunto formados pelos números que divididos por 6 deixam resto 5, ou seja $F = \{x \in \mathbb{N} | x \equiv 5 \ mod \ 6\}$.

Verificamos também, através das propriedades das congruências modulares, que somando, por exemplo, qualquer elemento do subconjunto B com qualquer elemento do subconjunto E, obteremos um elemento do subconjunto F, ou, em outro exemplo, se multiplicarmos qualquer elemento do subconjunto C por um elemento do subconjunto F obteremos sempre um elemento do subconjunto E.

Da mesma forma, veremos a seguir que o conjunto dos números inteiros também pode ser repartido em m subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos por m e que o conjunto dos números inteiros, assim subdivididos e munidos das operações de adição e multiplicação com algumas de suas propriedades, permitem definir novas aritméticas que encontram inúmeras aplicações em várias partes da matemática e que servem de base para quase todos os procedimentos de cálculo, possuindo muitas aplicações tecnológicas.

Então, fixado um número inteiro $m > 1$, podemos repartir o conjunto $\mathbb{Z}$ dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos por m; isto nos dá a seguinte partição de $\mathbb{Z}$:

$$[0] = \{x \in \mathbb{Z} | x \equiv 0 \ mod \ m\}$$
$$[1] = \{x \in \mathbb{Z} | x \equiv 1 \ mod \ m\}$$
$$\vdots$$
$$[m-1] = \{x \in \mathbb{Z} | x \equiv m-1 \ mod \ m\}.$$

Observe que $[m] = [0]$, pois $m \equiv 0 \ mod \ m$. Desta forma, podemos obter apenas m subconjuntos distintos da maneira como foi definida acima.

O conjunto $[a] = \{x \in \mathbb{Z}; x \equiv a \ mod \ m\}$ é chamado de classe residual módulo m do elemento a de $\mathbb{Z}$. O conjunto de todas as classes residuais de módulo m será representado por $\mathbb{Z}_m$, ou seja:

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

Exemplo 2.7.1 Seja $m = 2$. Então:

$[0] = \{x \in \mathbb{Z}; x \equiv 0 \ mod \ 2\}$

$[1] = \{x \in \mathbb{Z}; x \equiv 1 \ mod \ 2\}$

Logo $\mathbb{Z}_2 = \{[0], [1]\}$.

Neste caso, dizemos que qualquer número par é um representante da classe residual [0] e qualquer número ímpar é representante da classe residual [1].

Exemplo 2.7.2 Seja $m = 3$. Então:

$[0] = \{x \in \mathbb{Z}; x \equiv 0 \ mod \ 3\}$

$[1] = \{x \in \mathbb{Z}; x \equiv 1 \ mod \ 3\}$

$[2] = \{x \in \mathbb{Z}; x \equiv 2 \ mod \ 3\}$

Logo $\mathbb{Z}_3 = \{[0], [1], [2]\}$.

Neste caso, dizemos que qualquer múltiplo de 3 é representante da classe residual [0], enquanto que 1,4,7,10,... são representantes da classe residual [1] e 2,5,8,... são representantes da classe residual [2].

Na tabela apresentada no exemplo inicial, temos:

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}.$$

Após definir o anel das classes residuais da forma como foi apresentada na fundamentação teórica, as tabelas de adição e multiplicação em $\mathbb{Z}_2 = \{[0], [1]\}$, $\mathbb{Z}_3 = \{[0], [1], [2]\}$ e $\mathbb{Z}_4 = \{[0], [1], [1], [3]\}$ ficaram da seguinte forma:

Tabela 2.10: Adição e Multiplicação em $\mathbb{Z}_2$

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

.	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

Tabela 2.11: Adição e Multiplicação em $\mathbb{Z}_3$

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

.	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Tabela 2.12: Adição e Multiplicação em $\mathbb{Z}_4$

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

.	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Neste ponto, solicitamos aos alunos que elaborem as tabelas de adição e multiplicação em $\mathbb{Z}_5$ e $\mathbb{Z}_6$ e respondam as seguintes perguntas:

a) Identifique nas tabelas de multiplicação em $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$ e $\mathbb{Z}_6$; os pares de elementos $[a]$ e $[b]$ de cada conjunto, onde $[a].[b] = [1]$.

O objetivo deste item é apresentar a definição do elemento invertível, ou seja: Um elemento $[a] \in \mathbb{Z}_m$ é invertível, se existir $[b] \in \mathbb{Z}_m$ tal que $[a].[b] = [1]$.

b) Em quais desses conjuntos, todo elemento distinto de [0] é invertível?

O aluno deve perceber, por exemplo, que em $\mathbb{Z}_4$, [0] e [2] não são invertíveis e que $(4, 0) = 4$ e $(4, 2) = 2$. Já [1] e [3] são invertíveis em $\mathbb{Z}_4$ e que $(4, 1) = (4, 3) = 1$. Deve notar também que em $\mathbb{Z}_5$, todo elemento distinto de [0] é invertível, que $(5, 1) = (5, 2) = (5, 3) = (5, 4) = (5, 5) = 1$ e que isto também ocorre em $\mathbb{Z}_2$ e $\mathbb{Z}_3$.

O objetivo desse item é levar o aluno a concluir que $[a] \in \mathbb{Z}_m$ invertível se, e somente se, $(a, m) = 1$ e que $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$ são chamados de corpos, ou seja, são anéis onde todo elemento não nulo possui um inverso multiplicativo.

O aluno deve notar também que 2, 3 e 5 são primos e chegar à conclusão que $\mathbb{Z}_m$ é um corpo, se e somente se, m é primo.

Uma vantagem das classes residuais é transformar a congruência $a \equiv b \ mod \ m$ na igualdade $[a] = [b]$. Dessa forma, elas permitem resolver congruências lineares do tipo $aX \equiv b \ mod \ m$, reduzindo-as, em $[a] \in \mathbb{Z}_m$, à seguinte equação:

$$[a].Z = [b].$$

Podemos notar a importância de determinar o elemento invertível no exemplo abaixo:

Exemplo 2.7.3 N é um múltiplo de 4 que possui três algarismos. Dividindo N por 5 encontramos resto igual a 3. Determine o menor valor de N.

Observe que $N = 4.X$. Dessa forma devemos ter:

$$4.X \equiv 3 \ mod \ 5.$$

Resolver essa congruência equivale a resolver em $\mathbb{Z}_5$ a seguinte equação:

$$[4].Z = [3].$$

Observe que [4] é invertível em $\mathbb{Z}_5$, pois $[4].[4] = [1]$. Logo, basta multiplicar ambos os membros da equação por [4] e obtemos:

$$[4].[4].Z = [4].[3] \Rightarrow [1].Z = [2] \Rightarrow Z = [2]$$

Em $\mathbb{Z}_5$, [2] é o conjunto dos números inteiros que divididos por 5 deixam resto 2, ou seja: $X = 5.t + 2$

Como $N \geq 100 \Rightarrow 4.X \geq 100 \Rightarrow X \geq 25 \Rightarrow 5t + 2 \geq 25 \Rightarrow t \geq 4,6 \Rightarrow t = 5$. Assim:

$$X = 5.5 + 2 \Rightarrow X = 27 \text{ . Logo: } N = 4.27 \Rightarrow N = 108.$$

Na próxima unidade veremos uma aplicação prática desta observação.

2.8 Unidade 7 - Criptografia

Nesta última unidade apresentamos uma aplicação da aritmética modular fazendo uma pequena introdução à criptografia.

Procuramos mostrar através dos exemplos, a relação existente entre esses dois temas, explorando as definições e propriedades da aritmética modular estudadas nas unidades anteriores e relacionando estes exemplos com o conceito de funções estudado no ensino médio.

Introduzimos o tema da seguinte forma:

CRIPTOGRAFIA

A Criptografia (do grego "Kriptos"que significa oculto e "gráphein"que significa escrever) é um conjunto de técnicas que visa esconder (codificar) uma informação de forma que só o emissor da informação e o receptor da mesma consigam decifrá-la. Dessa forma, o objetivo da criptografia é transformar um conjunto de informações legíveis em um emaranhado de caracteres impossíveis de ser compreendidos por quem não possui a "chave"que possibilita recuperar a informação na forma legível.

A utilização da criptografia é tão antiga quanto a necessidade do homem em esconder a informação. Muitos pesquisadores atribuem o uso mais antigo da criptografia conhecido aos hieróglifos usados em monumentos do Antigo Egito (cerca de 4500 anos atrás). Diversas técnicas de ocultar mensagens foram utilizadas pelos gregos e romanos.

Sabe-se que o imperador romano Júlio César (50 A.C.) utilizava um método de criptografia para se comunicar com seus generais. O chamado Codificador de Júlio César que apresentava uma das técnicas mais clássicas de criptografia, é um exemplo de codificação que, simplesmente, substitui as letras do alfabeto avançando três casas (Chave três). O emissor da mensagem trocava cada letra por outra situada a três posições à frente no alfabeto. O receptor, sabendo da chave dessa codificação, aplicava a operação inversa na frase recebida, ou seja, substituía cada letra recebida pela que ficava três posições antes dela no alfabeto.

Observe no quadro abaixo, como cada letra do alfabeto era codificada nesse método:

Tabela 2.13: Codificação Chave 3

Original	A	B	C	D	E	F	G	H	I	J	K	L	M
Codificada	D	E	F	G	H	I	J	K	L	M	N	O	P
Original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Codificada	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Dessa forma, ao codificarmos a palavra **GENERAL**, por exemplo, obteríamos como resultado a palavra **JHQHUDO**.

Observe que para codificar a letra X, retornamos ao início do alfabeto, ou seja, obtemos a letra A.

Para verificarmos a relação com a aritmética modular, vamos substituir cada letra do alfabeto por um número de dois dígitos, de acordo com a tabela abaixo:

Tabela 2.14: Codificação Chave K

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

Observe que representando por X a letra original e por Y a letra que a substituirá no código, é como se tivéssemos uma função, definida pela fórmula $Y = X + 3$.

Note também que essa soma não pode ser maior que 25, pois de acordo com a tabela, não existe letra no alfabeto que corresponda a um número superior a 25. Dessa forma, quando o resultado da soma é superior a 25, voltamos ao início do alfabeto. Por exemplo, na tabela temos $Z = 25$, utilizando a chave 3 de Júlio César, temos $25 + 3 = 28$. Como $28 = 26 + 2$, o número 28 corresponderá a letra C, pois, como já sabemos $28 \equiv 2 \ mod\ 26$.

Neste ponto, solicitamos que os alunos resolvam os exemplos abaixo para perceberem melhor a relação deste assunto com a aritmética modular.

Exemplo 2.8.1 Utilizando a tabela anterior, podemos escolher um número K, de modo que, para criptografarmos uma mensagem somamos o número K ao valor correspondente na tabela da letra que se deseja codificar e depois substituímos pela letra correspondente ao valor dessa soma na tabela. Esse número K será a chave do novo método de criptografia.

Dessa forma, codifique as mensagens utilizando a chave K (Somar K) indicada:
a) ARITMETICA MODULAR (K=05)
b) ARITMETICA MODULAR (K=31)
c) ENSINO FUNDAMENTAL (K=11)
d) ENSINO FUNDAMENTAL (K=37)

Com este exemplo, pretendemos que o aluno faça as seguintes observações e chegue às seguintes conclusões:

Os textos criptografados para os itens a) e b) são idênticos, ou seja, "**FWNXRJX-NHF RTKZQFW**". Isto acontece porque $31 \equiv 5 \ mod\ 26$. O mesmo acontece para os textos criptografados nos itens c) e d), pois $11 \equiv 37 \ mod\ 26$.

Em seguida, o aluno deve utilizar estas observações para resolver o exemplo abaixo.

Exemplo 2.8.2 A mensagem abaixo foi criptografada utilizando a chave 32. Decodifique a mensagem.

LKROF TGZGR

Como $32 \equiv 6 \ mod \ 26$, para encontrarmos a letra original, basta verificarmos o valor da letra codificada na tabela e subtrairmos 6, ou seja:

- $L = 11 \longrightarrow 11 - 6 = 5 \longrightarrow \mathbf{F}$
- $K = 10 \longrightarrow 10 - 6 = 4 \longrightarrow \mathbf{E}$
- $R = 17 \longrightarrow 17 - 6 = 11 \longrightarrow \mathbf{L}$
- $O = 14 \longrightarrow 14 - 6 = 8 \longrightarrow \mathbf{I}$
- $F = 5 \longrightarrow 5 - 6 = -1 \longrightarrow \mathbf{Z}$ Note que: $-1 \equiv 25 \ mod \ 26$
- $T = 19 \longrightarrow 19 - 6 = 13 \longrightarrow \mathbf{N}$
- $G = 6 \longrightarrow 6 - 6 = 0 \longrightarrow \mathbf{A}$
- $Z = 25 \longrightarrow 25 - 6 = 19 \longrightarrow \mathbf{T}$
- $G = 6 \longrightarrow 6 - 6 = 0 \longrightarrow \mathbf{A}$
- $R = 17 \longrightarrow 17 - 6 = 11 \longrightarrow \mathbf{L}$

Após a resolução destes dois exemplos apresentaremos a relação existente na codificação e decodificação desses exemplos de maneira generalizada e aproveitaremos para associar estas relações ao conceito de funções e algumas de suas propriedades.

Seja X o número correspondente à letra do texto original da mensagem, Y o número da letra que a substituirá no texto cifrado e K o número da chave utilizada. Podemos representar a relação entre X e Y utilizando a congruência modular da seguinte forma:

Na codificação da mensagem temos que:

$$Y \equiv (X + K) \ mod \ 26$$

Na decodificação, temos:

$$(Y - K) \equiv X \ mod \ 26$$

Podemos ainda representar essa relação como uma função bijetora da seguinte forma:

Dado o conjunto $A = \{0; 1; 2; 3; 4...; 24; 25\}$. Seja $f : A \longrightarrow A$, a função que associa a cada número $X \in A$, um número $Y \in A$, tal que $Y \equiv (X + K)\ mod\ 26$, com $k \in \mathbb{Z}$. Esta seria a função de codificação.

A decodificação seria a sua função inversa, ou seja: $g : A \longrightarrow A$ é a função que associa a cada número $Y \in A$, um número $X \in A$ tal que $(Y - K) \equiv X\ mod\ 26$.

Nos exemplos anteriores, utilizamos na codificação a operação de adição, ou seja, para obtermos o número correspondente à letra do texto criptografado, devemos somar K (chave) ao número correspondente à letra da mensagem original.

Se utilizássemos a operação de multiplicação ao invés da adição, o método de criptografia funcionaria para qualquer valor de K multiplicado pelo número correspondente à letra da mensagem original?

Observe que os resultados da multiplicação também não podem ser maiores que 25, então, como temos um caso de congruência no módulo 26, podemos dividir os possíveis valores de K em 26 subconjuntos, como estudamos na unidade anterior. Assim, apresentaremos abaixo, uma parte da tabela com os resultados da multiplicação no módulo 26:

Tabela 2.15: Multiplicação em $\mathbb{Z}_{26}$

.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...	24	25
0	0	0	0 ¨	0	0	0	0	0	0	0	0	0	0	0	0	0	...	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...	24	25
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	...	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	...	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	...	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	...	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	...	14	20
7	0	7	14	21	2	9	16	23	6	11	18	25	6	13	20	1	...	12	19
8	0	...																	
...																			

Na unidade anterior, verificamos que uma determinada classe $[a]$ tem inverso em $\mathbb{Z}_m$, se e somente se, a e m são primos entre si. Nesse caso, em $\mathbb{Z}_{26}$, as classes que possuem inverso são [1], [3], [5], [7], [9], [11], [15], [17], [19], [21], [23] e [25]. Então, a operação de decodificação só é possível se o valor da chave K for um elemento de uma dessas classes.

Exemplo 2.8.3 Uma mensagem foi codificada utilizando a multiplicação de cada valor correspondente das letras originais por 3 (chave 3). Qual a letra original correspondente à letra T no texto criptografado?

Observe na tabela que $T = 19$, então, para descobrirmos a letra original precisamos resolver primeiro uma congruência linear. Seja β o número correspondente à letra original, devemos ter:

$$3.\beta \equiv 19 \ mod \ 26.$$

Como estudamos na unidade anterior, resolver esta congruência, equivale a resolver a equação:

$$[3].Z = [19].$$

Em $\mathbb{Z}_{26}$, o inverso de [3] é [9], pois $[3].[9] = [1]$. Então:

$$[9].[3].Z = [9].[19]$$
$$[1].Z = [15]$$
$$Z = [15].$$

Portanto, no nosso exemplo $\beta = 15$, que corresponde na tabela à letra P.

Seja X o número correspondente a letra do texto original da mensagem, Y o número da letra que a substituirá no texto cifrado e K o número da chave utilizada na multiplicação. Podemos representar a relação entre X e Y utilizando a congruência modular da seguinte forma:

$$Y \equiv K.X \ mod \ 26.$$

Observe na tabela, que se K pertence às classes invertíveis, para cada número correspondente à letra da mensagem original, o resultado da congruência acima é um número distinto pertencente à mesma classe. Associando ao conceito de funções, cada um dos 26 elementos do conjunto está associado a um elemento distinto desse mesmo conjunto, temos, portanto, uma função bijetora, logo, esta função admite uma inversa, o que significa que a decodificação é possível.

Quando K não pertence às classes invertíveis, existem números distintos correspondentes às letras da mensagem original, cujo resultado da congruência são iguais (Para $K = 2$, temos $2 \equiv 2.1$ e $2 \equiv 2.14$). Logo, existem elementos distintos do conjunto associados a um mesmo elemento desse conjunto, ou seja, a função não é injetora, portanto, ela não é bijetora. Neste caso, a função não admite uma inversa, portanto a decodificação da mensagem não é possível.

Os sistemas de criptografia utilizados nos exemplos anteriores e outros similares, em que as letras são "embaralhadas"através de permutações, são muito simples e, portanto, muito fáceis de serem decifrados, porém serviram durante muito tempo para codificar mensagens.

Durante a segunda guerra mundial, os aliados passaram a utilizar computadores para "quebrar"os códigos alemães, italianos e japoneses. Desde então, a Criptografia passou a ser estudada de modo científico e com o desenvolvimento no pós-guerra dos computadores, passou a incorporar complexos algoritmos matemáticos.

Para finalizar esta unidade, apresentamos o exemplo abaixo que encontra-se em Sá (2007).

"Imaginemos um casal, Alice e Bob, que vivem isolados e apenas podem se comunicar através do correio. Eles sabem que o carteiro é um tremendo fofoqueiro e que lê todas as suas cartas. Alice tem uma mensagem para Bob e não quer que ela seja lida. O que ela pode fazer? Ela pensou em lhe enviar um cofre com a mensagem, fechado a cadeado. Mas como lhe fará chegar a chave? Não pode enviar dentro do cofre, pois assim Bob não o poderá abrir. Se enviar a chave em separado, o carteiro pode fazer uma cópia.

Depois de muito pensar, ela tem uma ideia. Envia-lhe o cofre fechado com um cadeado. Sabe que Bob é esperto e acabará por perceber a sua ideia. Com mais uma ida e uma volta do correio, e sem nunca terem trocado chaves, a mensagem chega até Bob, que abre o cofre e a lê. Como é que você acha que resolveram o problema? Pense bem no assunto, tente responder a questão. É simples... depois que você descobrir, é claro.

O "truque"usado foi o seguinte: Bob colocou outro cadeado no cofre e ele tinha a chave desse segundo cadeado. Devolve o cofre a Alice por correio, desta vez fechado com os dois cadeados. Alice remove o seu cadeado, com a chave que possui e reenvia o cofre pelo correio só com o cadeado colocado por Bob. É claro que Bob tem apenas que abrir o cofre, com a sua própria chave e ler a mensagem enviada pela sua amada. O carteiro não tem como saber o conteúdo do cofre".
Este texto foi retirado de Crato (2011).

Na criptografia usam-se chaves que, de certa forma, são análogas à estratégia usada pelos namorados de nossa história.

Esta história talvez tenha servido de inspiração para os três jovens norte-americanos, Whitefield Diffie, Martin Hellman e Ralph Merkle, ao construírem em 1976 um sistema de criptografia em que o segredo da comunicação é assegurado por duas chaves, que os comunicantes não precisam trocar entre si, como aconteceu na historinha do Bob e da Alice. Foi esta invenção que inspirou o sistema de criptografia RSA.

Segundo o esquema que Diffie, Hellman e Merkle propuseram, Alice e Bob começam por acordar em dois números. E estes podem ser públicos, pois mesmo que o carteiro os consiga descobrir não terá como descobrir a chave do processo. Cada um deles escolhe outro número, que mantém secreto. Feitas algumas contas, baseadas em aritmética modular, ambos chegam a um mesmo resultado: um número que mais ninguém conhece e que será a chave de codificação das suas mensagens. O processo que inventaram é relativamente simples, embora muito engenhoso, e será mostrado no quadro abaixo. Tudo se passa de forma parecida com a da história dos dois cadeados. As chaves não são trocadas, mas cada um acaba por poder abrir o cofre, sem que o carteiro, o consiga.

Em Singh (2011) temos um exemplo que retrata bem o processo matemático da aritmética modular, envolvido nessas chaves públicas.

Os comunicantes, como Alice e Bob combinam os números que servem: o primeiro de base para uma potenciação e o segundo para o módulo da congruência. Digamos que tenham optado pelos números **5** e **11**. Estariam então se referindo ao cálculo de 5^x e da congruência no módulo 11. O expoente x seria secreto, à escolha de cada um deles.

Alice escolhe **3** para seu número secreto (expoente da potência).

Alice calcula $5^3 = 125$ e, através de congruência módulo 11, gera o número 4, pois 125 dividido por 11 deixa resto 4.

Alice envia o resultado, 4, para Bob.

Bob escolhe **6** para seu número secreto (novamente o expoente da potência)

Bob calcula $5^6 = 15625$ e, através de congruência módulo 11, gera o número 5, pois 15 625 dividido por 11 deixa resto 5.

Bob envia o resultado, 5, para Alice.

Note que, mesmo que esses dois números que eles enviaram um ao outro, fossem interceptados, as pessoas não teriam como saber a chave final do processo.

Alice pega o resultado de Bob, **5**, e o seu número secreto, **3**, e calcula? $5^3 = 125 \equiv 4$ *mod* 11 (125 dividido por 11 deixa resto 4).

Bob pega o resultado de Alice, **4**, e o seu número secreto, **6**, e calcula $4^6 = 4096 \equiv 4$ *mod* 11 (4096 dividido por 11 também deixa resto 4).

Veja que Alice e Bob encontraram o mesmo número, 4, sem que tivessem informado um ao outro os seus números secretos pessoais. Esse número seria agora usado como chave para a composição das mensagens criptográficas. A congruência, como foi aplicada aqui, funcionou exatamente como a história dos cadeados e do correio.

Tente fazer com outros números secretos, verifique que você sempre irá obter resultados iguais.

Atualmente, muitas transações que envolvem dinheiro são feitas de maneira eletrônica, como compras por cartão de crédito via internet, por exemplo. As informações referentes a essas diversas transações seguem por linhas telefônicas ou redes de alta velocidade, e em ambos os casos, podem ser facilmente interceptadas. O processo de envio de informações e a tentativa de interceptá-los, pelos chamados "hackers", é uma luta que se trava inimterruptamente na *internet*.

Para que essas informações não trafeguem em aberto por esses canais de transmissão, o uso da criptografia é muito importante para que as mesmas sejam codificadas de tal forma que somente os bancos, empresas de cartão de crédito, lojas, etc., que a estão sendo utilizando consigam ler essa informações.

É lógico que o processo matemático e os algoritmos utilizados na criptografia são muito mais complexos do que mostramos neste material, a começar pelos números utilizados, que são números primos muito, mas muito grandes.

Utilizamos exemplos com chaves criptográficas simples, apenas para mostrar a relação que existe entre a aritmética modular e esse tema.

Capítulo 3

Relato sobre o curso

Neste capítulo, faremos um breve relato da aplicação da proposta de ensino de Aritmética Modular realizada no curso para o 5º semestre do Curso de Nível Médio Integrado de Química do IFMT Campus Bela Vista.

Nesse relato, incluímos observações sobre fatos importantes ocorridos durante as aulas ministradas nesse curso, em relação à utilização dos conceitos aprendidos pelos alunos em alguns assuntos anteriormente estudados na disciplina de matemática do Ensino Médio.

3.1 Início do curso

Inicialmente foi encaminhado ao Departamento de Ensino do IFMT Campus Bela Vista um projeto (Anexo II) contendo o tema a ser trabalhado: objetivos e justificativa do curso, desenvolvimento, material necessário e solicitação de uma autorização para ministrar o curso para algumas turmas do curso de Química do IFMT Campus Bela Vista.

Como o curso teve início em outubro, não foi possível ministrar as aulas para todas as turmas previstas, pois já estava em andamento, no campus Bela Vista, outro projeto que visava preparar os alunos para prestarem o ENEM no final daquele mês. Apenas o 5º semestre do curso de Química possuía um horário disponível para aplicação do mesmo.

Para estimular a participação desses alunos, foram feitas avaliações sobre os conteúdos ministrados no curso, paralelamente as avaliações normais do 2º bimestre, ou seja, avaliação mensal e bimestral, sendo que a nota das avaliações do curso, que totalizavam um total de 10 pontos, substituiria a menor das notas referentes às duas avaliações do bimestre. Dessa forma houve a participação de todos os alunos do 5º semestre cuja relação de nomes se encontra no Anexo III.

3.2 Observações sobre as aulas

Na Unidade 1 foi apresentado o Princípio da Indução Finita e apesar de não ser o objetivo do curso prepará-los para utilizar com destreza esta ferramenta, não podemos deixar de observar que a aplicação desse princípio proporcionou uma excelente oportunidade para trabalhar assuntos como produtos notáveis e fatoração de expressões algébricas, pois as demonstrações presentes nessa unidade e que utilizam esse princípio, necessitam de manipulações algébricas que envolvem esses assuntos. Dessa forma pudemos mostrar uma aplicação para assuntos que normalmente os estudantes apresentam dificuldades de aprendizagem.

Nas Unidades 2 e 3 apresentamos os conceitos de Divisibilidade, Divisão Euclidiana, Números Primos, Máximo Divisor Comum e Mínimo Múltiplo Comum, que já haviam sido abordados em séries anteriores, por isto os alunos não apresentaram muita dificuldade em entender a forma como os mesmos foram apresentados, embora inicialmente seja comum a confusão da notação $a|b$ (a divide b) com uma fração, de (a, b) (máximo divisor comum entre a e b) com um par ordenado ou de $[a, b]$ (mínimo múltiplo comum) com um intervalo.

Aproveitamos a demonstração do Pequeno Teorema de Fermat para mostrar uma aplicação do binômio de Newton, que é utilizado na demonstração feita na Unidade 3. Ao final destas três unidades aplicamos a primeira avaliação (Anexo IV) com o objetivo de verificar o aprendizado dos conceitos, das notações e de algumas propriedades estudadas nessas unidades.

Nas unidades seguintes desenvolvemos a parte principal desse trabalho, ou seja, a introdução da Aritmética Modular através da resolução de exercícios contextualizados e observamos fatos interessantes ao trabalharmos conceitos que não são abordados normalmente no ensino médio.

Numa determinada aula do curso, introduzimos o conceito de Congruência Modular e resolvemos alguns exercícios para fixar a notação $a \equiv b \ mod \ m$. Na mesma semana em que ocorreu essa aula, estudávamos num dos conteúdos normais do semestre, o que ocorria com as potências da unidade imaginária dos números complexos, ou seja:

$$\begin{array}{cccc} i^0 = 1 & i^4 = 1 & i^8 = 1 & i^{12} = 1 \\ i^1 = i & i^5 = i & i^9 = i & i^{13} = ... \\ i^2 = -1 & i^6 = -1 & i^{10} = -1 & i^{14} = ... \\ i^3 = -i & i^7 = -i & i^{11} = -i & i^{12} = ... \end{array}$$

Ao verificar que os resultados das potências da unidade se repetiam a cada quatro potências, o aluno Rafael França perguntou se podia utilizar o que estávamos estudando no curso nesse assunto. Respondi que era possível e aproveitei para lançar um desafio, ou seja, como poderíamos utilizar a notação de congruência na tabela observada acima.

Após algumas tentativas e discussões alguns alunos chegaram ao resultado esperado, assim:

Seja i a unidade imaginária e $n \in \mathbb{N}$, temos:

- $n \equiv 0 \ mod \ 4 \Rightarrow i^n = 1$.
- $n \equiv 1 \ mod \ 4 \Rightarrow i^n = i$.
- $n \equiv 2 \ mod \ 4 \Rightarrow i^n = -1$.
- $n \equiv 3 \ mod \ 4 \Rightarrow i^n = -i$.

Note que o aluno, ao assimilar o conceito de congruência, começa a relacioná-lo com outros assuntos.

Ao final da Unidade 4 realizamos a segunda avaliação (Anexo IV) para verificar a assimilação do conceito de congruência modular. Verificamos certa resistência em usar a notação de congruência na resolução de exercícios contextualizados. Numa questão dessa avaliação tínhamos o seguinte problema:

Uma empresa de coleta de lixo dividiu o município de Cuiabá em 171 áreas para realizar pontualmente a coleta de lixo nas residências.

Foi feito um cronograma para a coleta de lixo de acordo com o quadro abaixo.

Tabela 3.1: Cronograma de coleta de lixo

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	...	...	...	...
...						

Determine em que dia da semana, a área de número 166 deve esperar o caminhão de lixo.

Nessa questão, alguns alunos completaram a tabela até chegarem ao número 166, a maioria efetuou a divisão euclidiana por 7, encontrando resto 5 e concluindo que o dia correto seria quinta-feira, porém apenas dois alunos utilizaram a notação $166 \equiv 5 \ mod \ 7$ para justificar a resposta.

Após estudarmos algumas propriedades das congruências modulares em relação às operações de adição e multiplicação na unidade 5, retornamos ao assunto das potências dos números complexos propondo um novo desafio, ou seja, utilizar a propriedade da adição nas congruências modulares para calcular o valor da expressão:

$$\sum_{n=1}^{k} i^n.$$

No estudo dos números complexos já havíamos demonstrado que a soma de quatro potências consecutivas da unidade imaginária i é sempre igual a 0, ou seja:

$$i^n + i^{n+1} + i^{n+2} + i^{n+3} = 0.$$

Observe os exemplos abaixo:

a) $\sum_{n=1}^{8} i^n = (i^1 + i^2 + i^3 + i^4) + (i^5 + i^6 + i^7 + i^8) = 0 + 0 = 0.$
Note que $8 \equiv 0 \ mod \ 4$.

b) $\sum_{n=1}^{9} i^n = i^1 + (i^2 + i^3 + i^4 + i^5) + (i^6 + i^7 + i^8 + i^9) = i + 0 + 0 = i.$
Note que $9 \equiv 1 \ mod \ 4$.

c) $\sum_{n=1}^{10} i^n = i^1 + i^2 + (i^3 + i^4 + i^5 + i^6) + (i^7 + i^8 + i^9 + i^{10}) = -1 + i.$
Note que $10 \equiv 2\ mod\ 4$.

d) $\sum_{n=1}^{11} i^n = i^1 + i^2 + i^3 + (i^4 + i^5 + i^6 + i^7) + (i^8 + i^9 + i^{10} + i^{11}) = -1.$
Note que $11 \equiv 3\ mod\ 4$.

O objetivo desses exemplos era chegar à conclusão que:

- $\sum_{n=1}^{n} i^n = 0$, se $n \equiv 0\ mod\ 4$.
- $\sum_{n=1}^{n} i^n = i$, se $n \equiv 1\ mod\ 4$.
- $\sum_{n=1}^{n} i^n = -1 + i$, se $n \equiv 2\ mod\ 4$.
- $\sum_{n=1}^{n} i^n = -1$, se $n \equiv 3\ mod\ 4$.

Durante as aulas dessa unidade, observamos como a assimilação desse novo conceito pode auxiliar na resolução de problemas tradicionais de uma forma mais simples.

Observe o problema proposto em sala:

Exemplo 3.2.1 Considere a seguinte progressão aritmética: (10, 17, 24, 31, 38,...). Verifique se os números abaixo são termos que pertencem a essa Progressão Aritmética (P.A).

a) 773

b) $51^{19} + 1$

Para resolvermos esta questão utilizando a congruência modular necessitávamos calcular o termo geral a_n dessa progressão. No ensino médio, para calcular o termo geral dessa Progressão Aritmética, utilizamos a fórmula do termo geral, ou seja:
$a_n = a_1 + (n-1).r$ $a_n = 10 + (n-1).7$ $a_n = 7n + 3$

Observamos então que qualquer termo dessa progressão é um múltiplo de 7 mais 3, o que equivale a dizer que $a_n \equiv 3\ mod\ 7$.

Neste momento da aula, a aluna Fernanda Dias interrompeu-me fazendo a seguinte observação: "Então, professor, se a razão é 7 basta eu verificar que o primeiro termo é igual a $7 + 3$ e concluir que o termo geral é igual a $7.n + 3$".

Antes de concluir o exercício, aproveitei para discutir com a sala essa observação, propondo o cálculo do termo geral das progressões aritméticas abaixo, da forma como a Fernanda havia proposto:

a) (9, 17, 25, 33, ...)

b) (11, 17, 23, 29, ...)

c) (2, 9, 16, 23, ...)

d) (3, 8, 13, 18, ...)

e) (7, 9, 11, 13, ...)

Nos itens a) e b) não houve dificuldades, ou seja:

a) Na progressão (9, 17, 25, 33, ...) a razão é igual a 8 e temos $9 = 8 + 1$, ou seja $9 = 8.1 + 1$, logo podemos concluir que o termo geral dessa P.A. é $a_n = 8.n + 1$, ou seja, $a_n \equiv 1 \ mod \ 8$.

De fato, temos :

$(9 = 8.1 + 1, 17 = 8.2 + 1, 25 = 8.3 + 1, 33 = 8.4 + 1..., a_n = 8.n + 1)$

b) Da mesma forma, na progressão (11, 17, 23, 29, ...) a razão é igual a 6 e temos $11 = 6 + 5$, ou seja $11 = 6.1 + 5$, logo podemos concluir que o termo geral dessa P.A. é $a_n = 6.n + 5$, ou seja, $a_n \equiv 5 \ mod \ 6$.

Nos itens c) e d), os alunos tiveram um pouco de dificuldade pois nessas sequências o primeiro termo é menor que a razão, mas após algumas discussões, chegaram a seguinte conclusão:

c) Na progressão (2, 9, 16, 23, ...) a razão é igual a 7 e temos $2 = 7 - 5$, ou seja $2 = 7.1 - 5$, logo podemos concluir que o termo geral dessa P.A. é $a_n = 7.n - 5$, ou seja, $a_n \equiv -5 \equiv 2 \ mod \ 7$.

d) Na progressão (3, 8, 13, 18, ...) a razão é igual a 5 e temos $3 = 5 - 2$, ou seja $3 = 5.1 - 2$, logo podemos concluir que o termo geral dessa P.A. é $a_n = 5.n - 2$, ou seja, $a_n \equiv -2 \equiv 3 \ mod \ 5$.

Observe que essas sequências tem a forma é $a_n = b.n + r$, com $b, r \in \mathbb{Z}$, $n \in \mathbb{N}$ e $|r| < b$.

Este fato não ocorre com a sequência do item e), ou seja:

e) Na progressão (8, 11, 14, 17,...) a razão é igual a 3 e temos $8 = 3+5$, ou seja $8 = 3.1+5$, logo podemos concluir que o termo geral dessa P.A. é $a_n = 3.n + 5$.

Neste caso devemos notar que $a_n \equiv 5 \equiv 2 \ mod \ 3$.

A noção de congruência modular e a prática de resolver exercícios utilizando esse conceito, estimula o raciocínio do aluno levando-o a buscar outras soluções mais simples para problemas anteriormente resolvidos a partir de uma fórmula decorada.

Este raciocínio foi utilizado em uma questão pelo aluno Allif na terceira avaliação (Anexo IV) sobre as propriedades das congruências modulares, na seguinte questão:

03- O quadro abaixo representa uma parte de uma tabela que pode continuar sendo preenchida indefinidamente.

A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	...							

Responda:

a) Multiplicando um número que pertence à coluna G com um número que pertence à coluna H, em qual coluna estará o resultado desse produto?

Nesta questão o objetivo era avaliar a propriedade da multiplicação nas congruências modulares, ou seja, esperava-se que o aluno resolvesse a mesma da seguinte forma:

Na coluna G, temos que $g \equiv 7 \ mod \ 9$.

Na coluna H, temos que $h \equiv 8 \ mod \ 9$.

Dessa forma, temos: $g.h \equiv 7.8 \equiv 56 \equiv 2 \ mod \ 9$.

Logo o resultado deste produto estará na coluna B.

Porém, o referido aluno teve o seguinte raciocínio:

Na coluna G, temos $g = 9.n - 2$.

Na coluna H, temos $h = 9.n - 1$.

Dessa forma temos:

$g.h = (9n - 2).(9n - 1) = 81n^2 - 27n + 2 = 9.(9n^2 - 3) + 2 = 9.k + 2$

Logo, $g.h$ pertence à coluna B.

Apesar da resolução deste aluno, nesta avaliação percebemos que a grande maioria já utilizava com mais frequência a notação de congruência e as suas propriedades. A principal dificuldade foi a aplicação das propriedades das potências na obtenção dos restos da divisão de números muito grandes como no exemplo abaixo:

Exemplo 3.2.2 Determine o resto da divisão $51^{19} + 1$ por 7.

O aluno já percebe que $51 \equiv 2 \ mod \ 7$, e portanto:

$$51^{19} + 1 \equiv 2^{19} + 1$$

Porém, muitos não conseguem observar a igualdade: $2^{19} = 2^{3.6+1} = (2^3)^6.2$, para utilizar o fato de que $2^3 \equiv 1 \ mod \ 7$.

Na Unidade 6, onde introduzimos o conceito de classes residuais, utilizamos a estratégia de elaborar exercícios para que o aluno construísse as tabelas de adição e multiplicação em $\mathbb{Z}_m$, observasse os resultados obtidos nessas tabelas e chegasse a uma conclusão sobre as propriedades dentro do anel das congruências módulo m, principalmente sobre o elemento invertível, pois utilizaríamos essa propriedade em um exemplo da próxima unidade.

Ao final da unidade efetuamos a quarta avaliação (Anexo IV), a última na forma de prova individual escrita.

Quando finalmente chegamos à última unidade, os alunos encontravam-se em período de provas bimestrais, então, para não sobrecarregá-los com mais conteúdos e para incentivar a participação nas aulas do curso, elaboramos uma atividade em grupo (Anexo IV) para introduzirmos a criptografia e verificarmos a relação desse assunto com as congruências modulares.

Cada avaliação, incluindo este último trabalho, tinha o valor de 2,0 pontos, totalizando 10 pontos e substituíram uma das duas avaliações normais do semestre, caso a nota fosse superior a uma delas. O resultado dessas avaliações se encontra no Anexo V.

Inicialmente havíamos previsto um total de 20 aulas para o curso, porém com as avaliações necessitamos de um total de 30 aulas para concluir todas as unidades. O universo de alunos para os quais a nossa proposta foi aplicada é muito pequeno para se fazer avaliações e conclusões significativas, o que fizemos aqui é apenas um breve relato dos fatos mais relevantes observados nas aulas ministradas no curso e nas avaliações feitas sobre o tema proposto neste trabalho.

Considerações finais

Este trabalho teve como objetivo mostrar que a Aritmética modular é um tema atual que pode ser introduzido no ensino médio através de uma proposta com ênfase na resolução de exercícios contextualizados.

Para isto, mostramos no desenvolvimento da proposta a resolução de exercícios retirados de vestibulares recentes: ENEM, FUVEST, Olimpíadas Brasileiras de Matemática (OBMEP) e de livros didáticos recém publicados.

Na resolução desses exercícios, abordamos vários assuntos ministrados no ensino médio, tais como Progressões Aritméticas, Progressões Geométricas, Matrizes, Geometria Plana, Geometria Espacial, Números Complexos entre outros. Mostramos que a Aritmética Modular, por meio do conceito de Congruência Modular e suas propriedades, apresenta uma maneira diferente de resolver problemas, simplificando a resolução dos mesmos.

Durante a apresentação da introdução à Criptografia, um assunto que desperta interesse nos alunos por estar relacionado com temas atuais como segurança na *internet*, apresentamos uma aplicação prática do tema, mostrando a relação existente entre esse assunto e a Congruência Modular.

Como produto deste trabalho elaboramos duas vídeo - aulas sobre Congruência Modular e algumas de suas propriedades, com o objetivo de facilitar a compreensão desta proposta (disponível em: http:// marcobazuca.blogspot.com.br). Elaboramos também uma apostila (disponível em: http:// marcobazuca.blogspot.com.br) sobre Aritmética Modular contendo os assuntos trabalhados nessa dissertação e exercícios propostos para o aluno.

Na aplicação dessa proposta num curso ministrado para uma turma do 5º semestre do Curso de Nível Médio Integrado em Química do IFMT Campus Bela Vista, observamos que os alunos não apresentaram dificuldades em assimilar o conceito de con-

gruência e conseguiram relacionar o tema com outros assuntos já estudados no ensino médio, além de apresentar soluções diferentes para problemas tradicionais utilizando esse conceito e suas propriedades.

Nessa proposta podem ser incluídos outros assuntos que apresentam vários problemas contextualizados, tais como, Congruências Lineares, Equações Diofantinas e o Teorema do Resto Chinês, e que não foram abordados neste trabalho devido a duração do curso no qual a proposta foi ministrada.

Finalmente, observamos neste trabalho que a Aritmética Modular é um assunto que motiva a aprendizagem por ser de fácil contextualização, proporciona a elaboração de atividades didáticas desafiadoras, mostra a realização das operações aritméticas de uma forma diferente da tradicionalmente apresentada aos alunos, além de reforçar a importância de alguns conceitos básicos, como a divisibilidade e os números primos. Dessa forma, acredito que a introdução desse assunto no Ensino médio seja de grande auxílio no desenvolvimento do pensamento aritmético e algébrico de nossos alunos.

Referências Bibliográficas

.

HEFEZ, Abramo (2011). *Elementos da Aritmética*, 2ª edição, SBM.

MATTOS, Sergio R. P. de.; PUGGIAN, Cleonice.; LOZANO, Abel R. G (2011). *Aritmética Modular E Suas Possibilidades Na Formação Continuada De Professores De Matemática.* Recife.

SÁ, Ilydio Pereira. *Aritmética Modular e algumas de suas aplicações.* Disponível em http://magiadamatemática.com. Acesso em: 15 jul. 2013

CRATO, N (2011). *Alice e Bob. Expresso / Revista*, 22 de Setembro, pp. 118-120.

SINGH, S (2011). *O Livro dos Códigos.* São Paulo: Record.

LINS, Rômulo, C. δ GIMENEZ, J. (2006). Perspectivas em Aritmética e Álgebra para o século XXI.Campinas, SP: Papirus.

COUTINHO, Severino (2012). *Coleção Programa de iniciação Científica OBMEP.Criptografia* Rio de Janeiro, IMPA.

MALANGA, Umberto C. C (2013). *Nosso trabalho consiste: Livros 1 e 2 Matemática Sistema de Ensino Poliedro Pré Vestibular*, Editora Poliedro.

SÁ, Ilydio, P. (2007). *A magia da matemática.* Rio de Janeiro: Ciência Moderna.

Apêndice: Material adicional

.

A.1 Anexo I - Listas de Exercícios

Unidade 2 - Divisibilidade

1-Mostre que, para todo $n \in N$:

a) $8|3^{2n} + 7$

b) $6|5^{2n+1} + 1$

2- (Unicamp)

a) Qual o quociente e o resto da divisão de 3875 por 17?

b) Qual o menor número natural, maior que 3785 que é múltiplo de 17?

3- Determine o menor número que se deve somar a 8746 para se obter um múltiplo de 11 aumentado de 4 unidades.

4- A soma de dois números inteiros positivos é igual a 56. Dividindo o maior pelo menor, obtêm-se quociente 5 e resto 4. Determine o valor desses números.

5- Sejam a e b dois números inteiros. Dividindo-se a por b obtemos quociente 7 e resto 3. Se aumentarmos o dividendo a de 2 unidades e aumentarmos o divisor b de 1 unidade, obtemos quociente 6 e resto 7. Determine o valor de $a - b$.

6- Determine o maior úmero natural que dividido por 13 deixa o quociente igual ao

dobro do resto.

7-(PUC Campinas) Seja x um número natural que ao ser dividido por 9 deixa resto 5 e ao ser dividido por 3 deixa resto. Sabendo-se que a soma desses quocientes é 9, podemos afirmar corretamente que x é igual a:

a) 28

b) 36

c) 27

d) 33

e) 23

8 - (Unb) Três números naturais a, b e c são tais que $a + b + c = 131$. Na divisão de a por b, o quociente é 1 e o resto é 9, e na divisão de c por b, o quociente é 9 e o resto é 1. Ache a diferença entre o maior e o menor número.

9 - Discuta a paridade:

a) da soma de dois números.

b) da diferença de dois números.

c) do produto de dois números.

d) da potência de um número.

10 - Seja n um número natural. Mostre que um, e apenas um, número de cada terna abaixo é divisível por 3.

a) $n; n + 2; n + 4$

b) $n; n + 10; n + 23$

c) $n; n + 1; 2n + 1$

11- Mostre que todo quadrado perfeito é da forma $4k$ ou $4k + 1$.

12-Mostre, para todo $a \in \mathbb{Z}$, que:

a) $2|a^2 - a$

b) $3|a^3 - a$

c) $5|a^5 - a$

Unidade 3 - Números Primos

1-Decomponha os números abaixo em fatores primos:

a) 392

b) 525

c) 4400

2-Determine:

a) $(124, 250)$

b) $[48, 70]$

03- Sejam os números $a = 2^n.3^2.7$ e $b = 2.3^3$. Se $[a, b] = 1512$, então,o valor de n é:

a) 3

b) 4

c) 5

d) 6

04 - (UFMG MG/2001) O número n é o máximo divisor comum dos números 756 e 2205. Então, a soma dos algarismos de n é igual a:

a) 3

b) 8

c) 9

d) 13

05 - (PUC PR/2003) O produto de 2 números, não primos entre si é 990, então o máximo divisor comum entre eles é:

a) 2

b) 3

c) 5

d) 9

e) 11

06-De uma estação urbana partem ônibus de três linhas diferentes, A, B e C. Os ônibus da linha A partem a cada 10 minutos, os da linha B a cada 12 minutos e os da linha C a cada 18 minutos. Sabe-se que às 08 horas partiram simultaneamente, ônibus dessas três linhas. Qual será o próximo horário que isto ocorrerá novamente?

07- Matheus decidiu contar quanto dinheiro tinha economizado em moedas e verificou que possuía 216 moedas de 1 real, 360 moedas de 50 centavos e 450 moedas de 25 centavos. Resolveu separar as moedas em pacotes contendo a mesma quantidade de moedas e somente moedas de mesmo valor, de tal forma que, o número de pacotes obtidos seja o menor possível. Dessa forma, o valor contido em cada pacote de moedas de 50 centavos, em reais, é igual a:

a) 20

b) 18

c) 10

d) 9

e) 5

08- Uma espécie de cigarra que existe somente no leste dos EUA passa um longo período dentro da terra alimentando-se de seiva de raízes, ressurgindo após 17 anos. Em revoada, os insetos dessa espécie se acasalam e produzem novas ninfas que irão cumprir novo ciclo de 17 anos.

Em 2004, ano bissexto, os EUA presenciaram outra revoada dessas cigarras. O próximo ano bissexto em que ocorrerá uma revoada da futura geração de cigarras será:

a) 2072.

b) 2068.

c) 2076.

d) 2080.

e) 2086.

09- Um funcionário de uma biblioteca deve empacotar 72 livros de História, 180 livros de Português e 288 livros de Matemática, de modo que cada pacote contenha a mesma quantidade de livros e somente livros de uma mesma disciplina. Sabendo que o funcionário colocou a maior quantidade possível de livros dentro de cada pacote, é correto afirmar que:

a) o total de pacotes formados é igual a 12

b) o número de pacotes contendo livros de História é igual a 5

c) o número de pacotes contendo livros de Português é igual a 6

d) o número de livros em cada pacote é igual a 18

e) o número de pacotes contendo livros de Matemática é igual a 8

10 - (FUVEST) No alto de uma torre de uma emissora de televisão, duas luzes "piscam"com frequências diferentes. A primeira "pisca"15 vezes por minuto e a segunda "pisca"10 vezes por minuto. Se num certo instante as luzes piscam simultaneamente, após quantos segundos elas voltaram a piscar simultaneamente?

a) 12

b) 10

c) 20

d) 15

e) 30

11 - (UNESP SP/2005) Uma faixa retangular de tecido deverá ser totalmente recortada em quadrados, todos de mesmo tamanho e sem deixar sobras. Esses quadrados deverão ter o maior tamanho (área) possível. Se as dimensões da faixa são 105 cm de largura por 700 cm de comprimento, o perímetro de cada quadrado, em centímetros, será:

a) 28.

b) 60.

c) 100.

d) 140.

e) 280.

12 - (UFMG MG/2005) No sítio de Paulo, a colheita de laranjas ficou entre 500 e 1 500 unidades. Se essas laranjas fossem colocadas em sacos com 50 unidades cada um, sobrariam 12 laranjas e, se fossem colocadas em sacos com 36 unidades cada um, também sobrariam 12 laranjas. Assim sendo, quantas laranjas sobrariam se elas fossem colocadas em sacos com 35 unidades cada um?

a) 4

b) 6

c) 7

d) 2

Unidade 4 - Congruência Modular

01-Determine se o dia 23/03/10 (82^{o} dia do ano) e o dia 08/10/10 (281^{o} dia do ano) caem no mesmo dia da semana, sabendo que o dia 1^{o} de janeiro de 2010 foi uma sexta feira? (justifique a sua resposta através de cálculos, sabendo que não existe um calendário em mãos)

02 - Assinale a alternativa FALSA abaixo:

a) $22 \equiv 67 \ mod \ 5$

b) $38 \equiv 74 \ mod \ 6$

c) $87 \equiv 115 \ mod \ 7$

d) $61 \equiv 93 \ mod \ 8$

e) $46 \equiv 67 \ mod \ 9$

03- Uma empresa de coleta de lixo dividiu o município de Cuiabá em 171 áreas para realizar pontualmente a coleta de lixo nas residências. Foi feito um cronograma para a coleta de lixo de acordo com o quadro abaixo:

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	...	...	...	...
...						

Determine:

a) Em qual dia da semana, a área de número 166 deve esperar o caminhão de lixo.

b) Em qual dia da semana, a área de número 99 deve esperar o caminhão de lixo.

c) Em quais dias da semana serão atendidas um maior número de áreas?

04-Qual a 1993ª letra da sequência ABCDEDCBABCDEDCBABCDEDCBA ...?

a) A

b) B

c) C

d) D

e) E

05-(ENEM 2013 - Adaptada) O ciclo de atividade magnética do Sol tem um período de 11 anos. O início do primeiro ciclo registrado se deu no começo de 1755 e se estendeu até o final de 1765. Desde então, todos os ciclos de atividade magnética do Sol têm sido registrados.

Seja N um ano pertencente ao atual ciclo solar. Se $N \equiv 2\ mod\ 11$, então, é correto afirmar que N é:

a)o segundo ano desse ciclo.

b) o terceiro ano desse ciclo

c) o último ano desse ciclo

d) o oitavo ano desse ciclo

e) o nono ano desse ciclo

06-Uma empresa, a fim de cumprir o prazo de entrega de suas mercadorias, colocou seus funcionários em regime de trabalho ininterrupto, estabelecendo três turnos de atividades.

Estima-se que serão necessárias 822 horas de trabalho. Se esse regime iniciou às 08 horas do dia 06/09/2010 (segunda-feira) e o serviço não vai parar nem nos finais de semana, qual o dia da semana e a que horas encerra-se esse regime de trabalho?

07-(UERJ - Adaptada) Em uma boate há luzes vermelhas, verdes e amarelas. Quando a boate começa a funcionar, as lâmpadas são acesas simultaneamente. A partir daí, a cada 5 segundos as lâmpadas vermelhas são apagadas, se estiverem acesas ou, acesas se estiverem apagadas. O mesmo acontece com as lâmpadas verdes a cada 15 segundos e com as amarelas a cada 30 segundos. Se a boate começou a funcionar as 21 h, pode-se afirmar que às 21h 50 min 32 s, estarão acesas:

a) Todas as lâmpadas

b) Lâmpadas de apenas duas cores diferentes.

c) Somente lâmpadas vermelhas

d) Somente lâmpadas verdes

e) Somente lâmpadas vermelhas

08- (FUVEST) Os números inteiros positivos são dispostos em "quadrados"da seguinte maneira:

1	2	3	10	11	12	19	...	...
4	5	6	13	14	15	...	...	...
7	8	9	16	17	18	...	...	...

O número 500 se encontra em um desses "quadrados". Determine em qual "quadrado"está, linha e coluna.

9- [OBMEP (2012), Banco de Questões] Estefânia tem cinco cartas marcadas com as letras A, B, C, D e E, empilhadas nessa ordem de cima para baixo. Ela embaralha as cartas pegando as duas de cima e colocando-as, com a ordem trocada, embaixo da pilha. A figura mostra o que acontece nas duas primeiras vezes em que ela embaralha as cartas. Se Estefânia embaralhar as cartas 74 vezes, qual carta estará no topo da pilha?

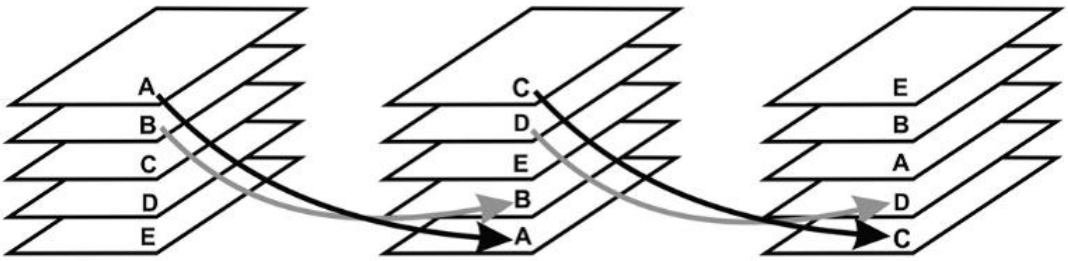

Figura A.1: Cartas II

Se Estefânia embaralhar as cartas 74 vezes, qual carta estará no topo da pilha?

a) A

b) B

c) C

d) D

e) E

Unidade 5 - Propriedades das Congruencias Modulares

01- A tabela apresentada a seguir mostra uma sequência de números naturais agrupados em 9 colunas verticais (A, B, C, D, E, F, G,H,I) e seguindo a uma determinada ordenação.

A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	...							

Responda as perguntas abaixo:

a) Somando dois elementos da coluna G, em qual coluna estará o resultado dessa soma?

b) Multiplicando dois números da coluna E, em qual coluna estará o resultado desse produto?

c) Seja h um elemento da coluna H. Em qual coluna estará o resultado da potencia h^{40}? (Note que $8^2 = 64 \equiv 1 \ mod \ 9$)

d) Em qual coluna se encontra o resultado do produto 9993. 2708?

e) Em qual coluna se encontra o resultado da potencia 65^{60}?

02 - Determine o resto da divisão de:

a) 63^{12} por 5

b) $(121 + 22^{15})^4$ por 7

03 - Seja a sequência (13; 21; 29;...). Qual dos números abaixo é um termo dessa sequência?

a) 590

b) 26^7

c) $91^3 + 2$

d) $13^3 - 1$

04- (ENC-98) O resto da divisão de 12^{12} por 5 é:

a) 0

b) 1

c) 2

d) 3

e) 4

O5 - Determine o resto da divisão da soma dos 100 primeiros termos da progressão aritmética (11, 18, 25, 32, ...) por 7.

06- Considere a sequencia de matrizes:

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \quad \begin{bmatrix} 10 & 11 & 12 \\ 13 & 14 & 15 \\ 16 & 17 & 18 \end{bmatrix} \quad \begin{bmatrix} 19 & ... & ... \\ ... & ... & ... \\ ... & ... & ... \end{bmatrix}$$

Os números abaixo são elementos de uma determinada matriz dessa sequência. Determine a linha e a coluna no qual se encontram localizados nessas matrizes.

a) 1000000085

b) 29^8

c) 908.813

07- Dividindo-se o produto dos 20 primeiros termos da progressão geométrica (7,49,343,..) por 43, encontramos resto igual a:

a) 0

b) 1

c) 17

d) 23

e) 42

(Sugestão: Aplique o pequeno teorema de Fermat)

08- Uma pista circular possui raio igual a 25 metros. Suponha que um móvel está no ponto de partida dessa pista e começa a percorrê-la da seguinte forma: 6 metros na primeira hora, 18 metros na segunda hora, 54 metros na terceira hora e assim sucessivamente até a $160^{\underline{a}}$ hora, sempre triplicando a distância percorrida a cada hora. Dessa forma, qual a distância aproximada percorrida pelo móvel após passar pelo ponto de partida pela última vez? (Utilize para os cálculos: $\pi = 3,14$).

09- Dividindo um número a por 13 encontramos resto igual a 7 e dividindo um número b pelo mesmo divisor encontramos resto 10. Determine o resto da divisão de $a^{26} + b^{12}$.

10-(Colégio Naval - 2003) O resto da divisão de $5^{131} + 7^{131} + 9^{131} + 15^{131}$ por 12 é igual a:

a) 0

b) 2

c) 7

d) 9

e) 11

Unidade 6 - Classes Residuais

01-Complete as tabelas da adição e da multiplicação para $\mathbb{Z}_7$.

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

.	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]							
[1]							
[2]							
[3]							
[4]							
[5]							
[6]							

Responda as questões abaixo:

a) Quais elementos de $\mathbb{Z}_7$ são invertíveis?

b) $\mathbb{Z}_7$ é um corpo?

02- Resolva a congruência linear:

3.$X \equiv 4 \ mod \ 7$

03- Determine dois múltiplos de 3 maiores que 200, que divididos por 7 deixam resto 4.

04- Construa a tabela de multiplicação em $\mathbb{Z}_6$ e diga quais elementos de$\mathbb{Z}_6$ são invertíveis?

05 - Quais elementos de $\mathbb{Z}_{22}$ são invertíveis?

Unidade 7 - Criptografia

01-Utilizando a tabela abaixo codifique as mensagens utilizando a chave K (Somar K) indicada:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	Y	X	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

a) CRIPTOGRAFIA (K=7)

b) ENSINO MÉDIO (K=12)

c) CURSO TECNICO DE NIVEL MEDIO INTEGRADO EM QUIMICA (K=36)

02- A mensagem abaixo foi criptografada utilizando a chave 31 (Somar 31). Decodifique a mensagem.

GTFY KJYXFY

03- Uma mensagem foi codificada utilizando a multiplicação de cada valor correspondente das letras originais por 11 (Chave 11). Qual a letra original correspondente à letra **P** no texto criptografado?

04 - A palavra abaixo foi codificada utilizando a multiplicação de cada valor correspondente das letras originais por 33 (Chave 33). Qual a palavra original?

HPAWEZ

05- Utilizando o método utilizado por Alice e Bob descritos no texto, descubra a chave final do processo nos seguintes casos:

a) Números combinados por Bob e Alice: 7 e 13

Número secreto de Bob: 2

Número secreto de Alice: 5

b) Números combinados por Bob e Alice: 4 e 9

Número secreto de Bob: 3

Número secreto de Alice: 7

A.2 Anexo II - Projeto Inicial do Curso

SERVIÇO PÚBLICO FEDERAL

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO

CAMPUS CUIABÁ-BELA VISTA

Projeto: Aritmética Modular e Suas Aplicações no Ensino Médio

Autor: Profº Marco Antonio de Oliveira Barros

Apresentação:

Este projeto faz parte do trabalho de conclusão de curso do Mestrado Profissional em Matemática na UFMT e pretende levar aos alunos do ensino médio, noções básicas da Aritmética Modular

Justificativa:

A aritmética modular envolve o conceito de congruência que é a relação entre dois números que, divididos por um terceiro - chamado módulo de congruência - deixam o mesmo resto. Por exemplo, o número 16 é congruente ao número 9, módulo 7, pois ambos deixam resto 2, ao serem divididos por 7. Representamos essa congruência do exemplo por $16 \equiv 9 \ mod \ 7$. Utilizamos frequentemente os restos das divisões para resolver vários problemas dentro do ensino da Matemática, muitos deles, relacionados ao nosso cotidiano. Apesar disto, a aritmética modular não está presente nos currículos do Ensino Básico e do Ensino Médio. Alguns trabalhos foram realizados sobre esse assunto em cursos de formação continuadas de professores do ensino Básico, porém, acredito que a Aritmética Modular seria de grande auxílio no desenvolvimento do pensamento aritmético e algébrico de nossos alunos.

Desenvolvimento do Projeto

O curso será ministrado aos alunos do 5º, 6º e 7º semestre do Curso Técnico de Nível Médio Integrado de Química que se inscreverem para o mesmo. As aulas serão ministradas no período vespertino, no horário das 17:30 às 18:30 após o término do período normal de aula, em uma das salas das referidas turmas durante os meses de outubro e novembro, totalizando uma carga horária de 20 horas.

Material Necessário para o Curso:

Cópias das listas de atividades que serão propostas aos alunos semanalmente

Roteiro do Curso:

1. Introdução: Um breve histórico sobre os surgimento da Aritmética Modular de Gauss.
2. Divisibilidade e o Algoritmo da Divisão de Euclides
3. Números primos e o Pequeno Teorema de Fermat
3. A Congruência Modular ($a \equiv b \ mod \ m$)
4. Propriedades das congruências modulares
5. Aplicações práticas da congruência e suas propriedades
7. Resolução de congruências lineares simples
8. Aritmética Modular na criptografia
9. Introdução às classes residuais
10. Conclusão

Considerações Finais:

Ao final do curso será elaborada uma apostila com os conteúdos trabalhados e as atividades realizadas no curso que será apresentada no trabalho de conclusão de mestrado e que deve ficar à disposição dos alunos do Campus IFMT Bela Vista na biblioteca.

A.3 Anexo III - Lista de Alunos

Alunos do 5º semestre do Curso de Nível Médio Integrado em Química

Allif Vinícius da Silva Neves

Carlos Augusto Barbosa D'Aurelio de Castilho

Danilo Barros dos Santos

Fernanda Ferreira Dias

Isabelle Rodrigues Fransosi

Izlia Morais de Paula

Julia Maria Alves de Oliveira Jaques

Jully Wyndy Arguelho Pereira

Kamilla Nicolau

Larissa Correa de Melo

Lidhiane Pessoa Andreotti

Matheus Ormond de Magalhães

Rafael Correa da Silva

Rafael França Vidal

Silvano dos Santos Silva Júnior

Thamara Pedroso Martins e Souza

Thaynara Bertelli Lima

Thaynara da Silva Santos

Valéria Ventura Miranda

Vitor Jorge Nascimento da Fonseca

Yasmin Maria Ferreira da Cruz Silva

A.4 Anexo IV - Avaliações

1ª Avaliação - Conceitos

Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso

Campus Cuiabá - Bela Vista

Nome: **Turma:**

1 -No estudo realizado sobre divisibilidade, a expressão $a|b$ significa:

a) a dividido por b

b) a é múltiplo de b

c) a é maior que b

d) a sobre b

e) a divide b

2- Sejam $a, b, c, k \in \mathbb{Z}$, é FALSO afirmar que:

a) Se $a|b$, então, existe um $k \in \mathbb{Z}$ tal que $b = k.a$

b) $1|a$, qualquer que seja o valor de a

c) Se $a|b$ então, $b|a$

d) Se $a|b$ e $c|d$, então, $a.c|b.d$

e) Se $a|b$ e $b|c$,então, $a|c$

3 - (Teorema da divisão Euclidiana) Sejam a e b dois números inteiros com $a \neq 0$. Existem dois únicos números inteiros q e r, com $0 \leq r < |a|$, tais que:

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

b) $a = r.q + b$

c) $q = b.a + r$

d) $a = b.q + r$

e) $b = r.q + a$

4- Todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas:

a) $3k, 3k + 1, 3k + 2$

b) $k, 2k, 3k$

c) $k+1, 2k+2, 3k+3$

d) $3k, 3k+1, 3k+2$

e) $k+1, k+2, k+3$

5 - Se $a = 2^3.3.5^4.7^2$ e $b = 2^2.3^5.7^2.11$, calcule o valor de (a, b).

2ª Avaliação - Congruência Modular

Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso

Campus Cuiabá - Bela Vista

Nome: **Turma:**

01 - Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$, se $a \equiv b \ mod \ m$, então, podemos afirmar que:

a) $m|a.b$

b) $m|(a+b)$

c) $m|(b-a)$

d) $a|(m+b)$

e) $(b-a)|m$

02 - Assinale a alternativa FALSA abaixo:

a) $22 \equiv 67 \ mod \ 5$

b) $38 \equiv 74 \ mod \ 6$

c) $87 \equiv 115 \ mod \ 7$

d) $61 \equiv 93 \ mod \ 8$

e) $46 \equiv 67 \ mod \ 9$

03- Uma empresa de coleta de lixo dividiu o município de Cuiabá em 171 áreas para realizar pontualmente a coleta de lixo nas residências.

Foi feito um cronograma para a coleta de lixo de acordo com o quadro abaixo:

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	...	...	...	...
...						

Determine em que dia da semana, a área de número 166 deve esperar o caminhão de lixo.

04-(ENEM 2013 - Adaptada) O ciclo de atividade magnética do Sol tem um período de 11 anos. O início do primeiro ciclo registrado se deu no começo de 1755 e se estendeu até o final de 1765. Desde então, todos os ciclos de atividade magnética do Sol têm sido registrados.

Seja N um ano pertencente ao atual ciclo solar. Se $N \equiv 2 \; mod \; 11$, então, é correto afirmar que N é:

a) o segundo ano desse ciclo

b) o terceiro ano desse ciclo

c) o último ano desse ciclo

d) o oitavo ano desse ciclo

e) o nono ano desse ciclo

3ª Avaliação - Propriedades da Congruência Modular

Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso

Campus Cuiabá - Bela Vista

Nome: **Turma:**

01 - Determine o resto da divisão de :

a) 63^{12} por 5

b) $(121 + 22^15)^4$ por 7

02 - Seja a sequência (13; 21; 29;...).Qual dos números abaixo é um termo dessa sequência?

a) 590

b) 26^7

c) $91^3 + 2$

d) $13^3 - 1$

03- O quadro abaixo representa uma parte de uma tabela que pode continuar sendo preenchida indefinidamente.

A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	...							

Responda:

a) Multiplicando um número que pertence a coluna G com um número que pertence a coluna H, em qual coluna estará o resultado desse produto?

b) Escolhe-se 10 números de cada uma das colunas A, B, C e D. O resultado da soma desses 40 números pertence a qual coluna?

4ª Avaliação - Classes Residuais

01-Complete as tabelas da adição e da multiplicação para $\mathbb{Z}_7$.

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

.	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]							
[1]							
[2]							
[3]							
[4]							
[5]							
[6]							

02- Resolva a congruência linear:

3.$X \equiv 4\ mod\ 7$

03- Determine dois múltiplos de 3 maiores que 200, que divididos por 7 deixam resto 4.

04- Quais elementos de $\mathbb{Z}_6$ são invertíveis?

5ª Avaliação - Trabalho sobre Criptografia

01-Utilizando a tabela abaixo codifique as mensagens utilizando a chave K (Somar K) indicada:

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

a) ARITMETICA MODULAR (K=05)

b) ARITMETICA MODULAR (K=31)

c) CURSO TECNICO DE NIVEL MEDIO INTEGRADO EM QUIMICA (K=11)

d) CURSO TECNICO DE NIVEL MEDIO INTEGRADO EM QUIMICA (K=37)

02- O que você observou no exercício acima? Porque isto acontece?

03- De quantas maneiras diferentes podemos criptografar uma mensagem utilizando este método?

04- A mensagem abaixo foi criptografada utilizando a chave 33. Decodifique a mensagem.

IVHZ MLXPHZ

05- Seja X o número correspondente a letra original da mensagem , Y o número da letra que a substituirá no código e K o número da chave utilizada. Como podemos representar a relação entre X e Y utilizando a congruência modular?

A.5 Anexo V - Resultado das Avaliações

Tabela 3.2: Resultado das Avaliações

Aluno	Avaliação I	Avaliação II	Avaliação III	Avaliação IV	Trabalho	Média Final
Allif	1,2	1,5	2,0	1,6	2,0	8,3
Carlos	0,8	1,0	0,0	0,8	2,0	4,6
Danilo	1,6	0,5	1,2	1,2	2,0	6,5
Fernanda	1,6	1,5	1,6	1,6	2,0	8,3
Isabelle	0,4	1,5	1,4	0,8	2,0	6,1
Izlia	1,6	2,0	1,6	0,8	2,0	8,0
Júlia	1,2	1,0	0,8	1,2	2,0	6,2
Jully	0,4	0,5	0,2	0,2	2,0	3,3
Kamilla	0,8	0,5	1,0	0,8	2,0	5,1
Larissa	0,8	2,0	0,8	0,8	2,0	6,4
Lidhiane	0,4	1,0	0,4	1,6	2,6	5,4
Matheus	2,0	1,0	1,8	1,6	2,0	8,4
Rafael C.	1,6	1,5	0,4	1,0	2,0	6,5
Rafael F.	1,6	2,0	1,8	1,2	2,0	8,6
Silvano	1,6	1,0	1,2	1,2	2,0	7,0
Thamara	1,6	1,0	0,8	0,8	2,0	6,2
Thaynara B	1,6	1,5	1,6	1,2	2,0	7,9
Thaynara S.	0,8	0,5	0,4	0,8	2,0	4,5
Valéria	1,2	1,5	0,4	1,2	2,0	6,3
Vitor	0,8	1,6	0,4	1,0	2,0	5,7
Yasmin	1,6	1,5	0,6	1,2	2,0	6,9