UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL
CAMPUS DE TRÊS LAGOAS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL
PROFMAT

DIEGO SAMPAIO SANTIAGO

CONGRUÊNCIA MODULAR: UMA PROPOSTA PARA O ENSINO FUNDAMENTAL

Três Lagoas – MS
2021

UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL
CAMPUS DE TRÊS LAGOAS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL
PROFMAT

DIEGO SAMPAIO SANTIAGO

CONGRUÊNCIA MODULAR: UMA PROPOSTA PARA O ENSINO FUNDAMENTAL

Dissertação apresentada à Universidade Federal de Mato Grosso do Sul no Campus de Três Lagoas, como parte das exigências para obtenção do título de mestre em Matemática.

Prof. Dr. Antonio Carlos Tamarozzi

Três Lagoas – MS
2021

UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL
CAMPUS DE TRÊS LAGOAS
PROFMAT

CONGRUÊNCIA MODULAR: UMA PROPOSTA PARA O ENSINO FUNDAMENTAL

por

DIEGO SAMPAIO SANTIAGO

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT da Universidade Federal de Mato Grosso do Sul, Campus de Três Lagoas, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Banca Examinadora:

Prof. Dr. Antônio Carlos Tamarozzi
UFMS /CPTL

Prof. Dr. Fernando Pereira de Souza
UFMS /CPTL

Prof. Dr. José Ivan da Silva Ramos
UFAC

AGRADECIMENTOS

Agradeço primeiramente a Deus, sei que sem ele nada seria possível.

Agradeço a minha esposa Natália, que esteve, está e sempre estará ao meu lado, na tristeza e principalmente nos momentos de felicidade.

Agradeço aos meus pais, Maria Ângela e Valdir, que me proporcionaram toda a condição para que eu estudasse.

Agradeço a minha irmã Viviane, meu cunhado Fabrício e meus sobrinhos Maria Clara e Daniel, que estiveram ao meu lado oferecendo um colo, uma ajuda e até um momento de descontração.

Agradeço aos meus colegas de PROFMAT, principalmente ao Anderson, Camila, Fernanda e Cecília, dividimos várias angústias e também alegrias durante todo esse período.

Agradeço a todos os professores do programa, em especial, ao meu orientador, Antonio Carlos Tamarozzi, que sempre esteve presente quando precisei, um professor-amigo ou um amigo-professor que vou levar no meu coração.

Por fim, agradeço aos meus alunos que contribuíram demais para a realização desse projeto.

Dedico esse trabalho a minha Mãe, Maria Ângela, falecida em 2011, uma mãe exemplar que sempre prezou pela educação dos filhos e mostrando que a educação pode mudar as pessoas.

RESUMO

Neste trabalho desenvolvemos um projeto que avalia a possibilidade do ensino de congruência modular para alunos do Ensino Fundamental. Descrevemos uma experiência aplicada a alunos do 9º ano de uma escola na cidade de Birigui, estado de São Paulo. O projeto foi desenvolvido ao longo de seis encontros, onde foi passado o conteúdo abordado. Embora tenham sido estudados os fundamentos básicos da Teoria do Números, o projeto centralizou-se em cálculos operacionais com congruências e as aplicações consequentes. As facilidades operacionais proporcionadas pelas congruências modulares despertaram o interesse dos alunos nas resoluções dos problemas e aplicações, de modo que podem constituir temas interessantes para projetos de ensino, como feiras e treinamentos para olimpíadas de Matemática.

Palavras-chave: Divisibilidade; Aritmética dos Restos; Teoria dos Números; Congruência Modular.

ABSTRACT

In this work we developed a project that assesses the possibility of teaching modular congruence to elementary school students. We describe an experience applied to 9th grade students at a school in the city of Birigui, state of São Paulo. The project was developed over six meetings, where the content was discussed. Although the basic foundations of Number Theory have been studied, the project has focused on operational calculations with congruencies and the consequent applications. The operational facilities provided by the modular congruences aroused the students' interest in solving problems and applications, so that they can be interesting topics for teaching projects, such as fairs and training for Mathematics Olympics.

Keywords: Divisibility; Remains Arithmetic; Number Theory; Modular Congruence.

Lista de Ilustrações

Sumário

INTRODUÇÃO

Alunos da educação básica, no Brasil, estão aptos a aprenderem os conceitos da Teoria dos Números? Muitos podem considerar esta pergunta uma ousadia, levando em conta que tal conteúdo normalmente é estudado a partir dos nossos cursos de graduação em Matemática. Por outro lado, a Teoria dos Números está fortemente é ligada à divisão Euclidiana, que por sua vez é encontrada na Base Nacional Comum Curricular (BNCC), a partir do sexto ano do ensino fundamental. Logo, a aprendizagem da Aritmética dos Restos não estaria longe dos domínios de quem já pratica a divisibilidade.

O ensino da Teoria dos Números e, por consequência, a congruência modular, é interessante do ponto de vista escolar, uma vez que encontramos sua aplicabilidade em temas que surgem no cotidiano, como código de barras, sistemas de identificação, criptografia, entre outros.

Além disto, segundo D'Ambrósio (2007),

> É importante a adoção de uma nova postura educacional, a busca de um novo paradigma de educação que substitua o já desgastado ensino aprendizagem. É necessário que ele se empenhe no mundo que cerca os alunos, na sua realidade aproveitando cada oportunidade a fim de sugerir atividades para que o desenvolvimento do ensino aprendizado da matemática seja efetivo e prazeroso, e que no final de cada aula o educador tenha aplicado a matéria com qualidade e que tenha conseguido ensinar ao aluno de forma clara.

Dessa forma, considerando as facilidades operacionais que a utilização de congruências modulares proporciona, no trato com números inteiros, pretendemos discutir a viabilidade de inserir no currículo do ensino fundamental, uma introdução desse assunto e as técnicas interessantes de cálculos que ele possibilita.

O interesse nessa metodologia surgiu ao longo do ano de 2019, quando foi exercido o trabalho de coordenador e de lecionar aulas de Álgebra e Teoria dos Números em um Polo de Treinamento da Olimpíada Brasileira de Matemática das Escolas Públicas e Privadas (OBMEP) para alunos de 8º e 9º ano. O material disponibilizado pelo IMPA (Instituto de Matemática Pura e Aplicada) traz para estudo as disciplinas citadas, além de Geometria e Combinatória e, em discussão com os demais ministrantes dos cursos, comentamos como o ensino fundamental aborda os conteúdos de Geometria, Combinatória e Álgebra e sobre limitações em se tratando da Teoria dos Números. Como professor dessa turma de alunos medalhistas da OBMEP, foi possível observar o interesse e o desenvolvimento da turma no conteúdo de congruências modulares e questionei: Como seria ministrar aulas desse conteúdo em uma turma comum do

ensino fundamental? Com efeito, além dessa experiência positiva, corrobora nessa linha de pensamento o que preconiza os Parâmetros Curriculares Nacionais (PCN) em relação ao ensino de Matemática, BRASIL (2017, p. 267): “Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo.”

O presente trabalho objetiva, portanto, contribuir para essa discussão, apresentando uma experiência aplicada aos alunos do ensino fundamental. A proposta de intervenção pedagógica intitulada “Ensinando congruência Modular para alunos de 9º ano” foi aplicada em uma escola de Birigui, no qual sou o professor de matemática da turma.

Devido a medidas de isolamento social, decretadas pelo estado de pandemia, o contato com os alunos participantes foi *on-line*, sendo feitos os contatos em seis aulas. A ideia é verificar como eles reagem aprendendo a matéria nova, suas dificuldades, seus aprendizados e como esse conhecimento pode contribuir em sua formação Matemática.

A proposta inicial era trabalhar com os alunos os seguintes tópicos relacionados a Aritmética:

- Introdução à divisibilidade;
- O algoritmo de Euclides;
- Menor Múltiplo Comum e Maior Divisor Comum;
- Números Primos e Compostos;
- Congruência Modular;
- Equações Diofantinas.

O Estudo em questão iria auxiliá-los a compreender e explorar as seguintes habilidades encontradas dentro da BNCC:

> (EF06MA05) Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos “é múltiplo de”, “é divisor de”, “é fator de”, e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000.
> (EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor. BRASIL (2017, p. 301).
> (EF07MA01) Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos.
> (EF07MA04) Resolver e elaborar problemas que envolvam operações com números inteiros. BRASIL (2017, p. 307).
> (EF08MA06) Resolver e elaborar problemas que envolvam cálculo do valor numérico de expressões algébricas, utilizando as propriedades das operações. BRASIL (2017, p. 313).
> (EF09MA09) Compreender os processos de fatoração de expressões algébricas, com base em suas relações com os produtos notáveis, para resolver e elaborar problemas

> que possam ser representados por equações polinomiais do 2º grau. (BRASIL, 2017, p. 317).

Porém, com menos aulas disponibilizadas para aplicações, foi feita uma readequação do projeto inicial, onde buscamos alinhar os discentes aos conceitos matemáticos já vistos, em seguida, introduzimos a divisibilidade e teoremas que envolvessem exercícios relacionadas ao resto da divisão e, por fim, a apresentação da congruência, suas propriedades e alguns exemplos de aplicações.

A estrutura desta dissertação foi dividida da seguinte forma:

No primeiro capítulo foi abordado a origem da Matemática e da Teoria dos Números, os primeiros estudos da aritmética dos restos e, em seguida, apresentamos as contribuições que grandes matemáticos deram para o crescimento dessa área.

No segundo capítulo apresenta a aritmética dos restos, o conceito de divisibilidade, a congruência modular, que é o objeto de trabalho desse estudo e as equações diofantinas, completando a teoria que envolve a aritmética básica.

O último capítulo foi dedicado a relatar e descrever o histórico da intervenção junto aos alunos de 9º Ano do Ensino Fundamental, a opinião dos alunos, comentários dos resultados e perspectivas futuras.

1 A ORIGEM DA MATEMÁTICA

Nesse capítulo é tratado uma breve história da Matemática, uma ciência que está sendo construída há muito tempo, seu surgimento através das diversas civilizações antigas, até os momentos atuais. Na primeira parte desse capítulo é apresentado essa construção, em seguida, será mostrado os grandes matemáticos que ao longo dos tempos ajudaram a construir a Teoria dos Números. Maiores e informações e detalhes adicionais à este capítulo poderão ser consultados as seguintes referências (BOYER, 1996), (HEFEZ, 2016), (LIMA, 2006).

1.1 A ORIGEM DA RAINHA DAS CIÊNCIAS

A Matemática, como conhecemos atualmente, é resultado de anos de desenvolvimento, desde os povos antigos do Egito e da Mesopotâmia, onde tem-se os primeiros registros de escritas numéricas, passando por uma imensa contribuição na Grécia antiga, recebendo mais informações da China, Arábia e da Índia e dos grandes Matemáticos Europeus dos séculos XVII, XVIII e XIX. Por isso, como diria Carl Friedrich Gauss, "A Matemática é a rainha das ciências", por isso, vemos nela toda elegância, formalismo e busca por padrões e regularidades que o mundo nos apresenta. Com toda essa apresentação, fica difícil não pensar que ela é uma ciência cujos estudos possuem um nível alto de ser ensinado, estudado e aplicado.

A história costumeiramente é dividida em eras ou períodos, porém, quando tratamos desses espaços de tempo, não podemos defini-lo de maneira que terminou um e começou o outro, pois, cada território no planeta foi saindo de um período e entrando no outro, no seu ritmo, sempre de maneira gradual. Um exemplo é a idade da pedra, seguida da idade do metal. Há registros de países na Ásia em que a transição aconteceu mais cedo do que em países da Europa.

Com a história da Matemática não foi diferente, pois, os povos primitivos viviam em tribos e caçavam juntos. No final, havia a contagem da quantidade de caça e a partilha entre eles, logo, o conceito de contagem e divisão já estava presente desde esse período. Assim, o pensamento matemático estava intrínseco na população, cabendo a evolução da espécie o dever de organizar os pensamentos e desenvolver essa ciência.

> Além disso, há muitas perguntas não respondidas com relação à origem da matemática. Supõe-se usualmente que surgiu em resposta às necessidades práticas, mas estudos antropológicos sugerem a possibilidade de uma outra origem. Foi

> sugerido que a arte de contar surgiu em conexão de rituais religiosos primitivos e que o aspecto ordinal precedeu o conceito quantitativo. Em ritos cerimoniais representado mitos da criação era necessário chamar os participantes à cena segundo uma ordem específica, e talvez a contagem tenha sido inventada para resolver esse problema. Se são corretas as teorias que dão origem ritual a contagem, o conceito de número ordinal pode ter precedido o de número cardinal. Além disso uma tal origem indicaria a possibilidade de que o contar tinha uma origem única, espalhando-se subsequentemente a outras partes da terra. Esse ponto de vista, embora esteja longe de ser provado, estaria em harmonia com a divisão ritual dos inteiros em ímpares e pares, os primeiros considerados como masculinos e os últimos, como femininos. Tais distinções eram conhecidas em civilizações em todos os cantos da terra, e mitos relativos a números masculinos e femininos se mostraram notavelmente persistentes. (BOYER, 1996, p. 04).

Com as descobertas arqueológicas, em relação a registros que mostram que os povos antigos já executavam a contagem com marcas em ossos ou paredes, vemos que foi através das necessidades que o sistema de números foi ganhando *upgrades* necessários como resposta ao que estava por vir.

Paralelamente ao conceito de contagem que os povos estavam criando, sentiu-se a necessidade da criação da ordenação, utilizando objetos e grafias para representação concreta de determinados objetos e animais, ocasionando passos novos para a evolução humana.

Mas, de todos os povos antigos que se tem notícia sobre escritas de contagem e ordenação, os Hindus foram os que tiveram papel mais importante para o avanço da utilização de um sistema de numeração, pois eles que trouxeram o sistema que é utilizado universalmente hoje em dia. É vindo dos mesmos a utilização de um símbolo para representar “nada”, o número zero, e com isso, ganhamos um número que colaborou bastante para criação dos sistemas de posicionamento da base dez, criando as casas das unidades, dezenas, centenas, milhares e assim sucessivamente.

Além da literatura colocada no início do capítulo, temos que citar (COSTA e SANTOS, 2008), (CARAÇA, 2003), (COSTA, 1996) que tratam a história dos sistemas numéricos desde as primeiras civilizações até os dias atuais. Não vamos nos alongar nesse sentido, uma vez que não é objeto do trabalho aqui apresentado, porém, fica a recomendação da leitura desses materiais, para todos que buscam conhecer como foi estabelecido nosso sistema numérico atual.

1.2 OS GRANDES MATEMÁTICOS

Para falarmos de Teoria dos Números, precisamos saber sua origem e toda sua evolução, ou seja, buscar na história da Matemática onde se inicia a Teoria dos Números, sua construção ao longo dos anos, passando pelos matemáticos que estudaram e fizeram grandes

descobertas em suas áreas e porque a pergunta inicial que aparece no primeiro parágrafo da introdução desse trabalho faz tanto sentido nos tempos atuais.

Segundo Boyer,

> Frequentemente, se pensa, erradamente, que *Os elementos* de Euclides só tratam de geometria. (...)três livros (VII, VIII e IX) são dedicados à teoria dos números. A palavra "número" para os gregos sempre se referia ao que chamamos números naturais – os inteiros positivos." (BOYER, 1996, p. 78).

A Humanidade foi evoluindo e diversos conceitos matemáticos foram sendo construídos ao longo do tempo. Porém, como vimos na primeira sessão desse capítulo, vários sistemas numéricos foram arquitetados ao longo de vários períodos e, no subconsciente, trazendo a ideia de conjuntos numéricos, no entanto, a ideia de caracterização formal dos números naturais, até então, usada para expressar objetos e animais concretos em diversas sociedades, foi formulada e enumerada, no final do século XIX, por Giuseppe Peano (1858-1932) que escreveu os axiomas (uma sentença que não é provada e é considerada como um consenso) para definir o conjunto dos números naturais ($\mathbb{N}$) e eles são conhecidos como *Axiomas de Peano*:

a) Todo número natural tem um sucessor, que ainda é um número natural; números diferentes têm sucessores diferentes.
b) Existe um único número natural 1 que não é sucessor de nenhum outro.
c) Se um conjunto de números naturais contém o número 1 e contém também o sucessor de cada um dos seus elementos, então esse conjunto contém todos os números naturais. LIMA (2006, p. 1)

Nota-se que o estudo da Matemática e, por consequência, da Teoria dos Números é antigo, sendo realizado por diversas pessoas, cada um colaborando de alguma forma para o crescimento dessa ciência.

Grandes matemáticos fizeram várias contribuições para a Teoria dos Números.

Começamos por Euclides, por sua contribuição na Matemática de maneira geral, e que forneceu um método simples e eficiente para o cálculo do máximo divisor comum entre dois números inteiros diferentes de zero. O algoritmo criado é um primor, do ponto de vista computacional, e pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios. (HEFEZ, 2016, p. 77).

Diofante de Alexandria, segundo BOYER (1996, p. 121), o maior algebrista grego, escreveu uma coleção de 13 livros sob o título *Arithmética*, onde trouxe vários problemas

utilizando termos presente na Álgebra atual, como notações e símbolos, deixando de lado o uso da Geometria, praticamente vista em todos os escritos dos autores da Grécia antiga.

> Se pensarmos primariamente em termos de notação, Diofante tem boas razões para pretender o título de pai da álgebra, mas em termos de motivação e conceitos a pretensão é menos justificada. (BOYER, 1996, p. 123).

O livro Arithmética, de Diofante de Alexandria, inspirou diversos matemáticos durante vários períodos da história, e foi ele que atraiu um grande matemático parisiense, Pierre de Fermat (1601-1665). As contribuições de Fermat passam por diversas áreas da Matemática. Seja na geometria analítica, seja na análise infinitesimal, entre outras. Para nosso objeto de estudo, Fermat também trouxe contribuições importantes, como, O Pequeno Teorema de Fermat, onde enunciou que se p é primo e a é primo com p, então $a^{p-1} - 1$ é divisível por p.

Fica uma referência ao "Príncipe dos Amadores", apelido dado a Fermat pois nunca teve a Matemática como principal atividade de sua vida, sendo formado em direito e tendo a magistratura como profissão. No decorrer de sua vida, ele enunciou o teorema que para n um inteiro maior que dois, não há valores inteiros positivos x, y e z tais que $x^n + y^n = z^n$. Esse teorema ficou conhecido como "Último" ou "Grande" Teorema de Fermat. Sua prova foi dada depois de mais de 350 anos, por Andrew Willes, um matemático britânico, colocando um ponto final no maior desafio matemático imposto.

> "Escreveu na margem de seu exemplar do Diofante de Bachet que tinha uma prova verdadeiramente maravilhosa desse célebre teorema, que a partir daí se tornou conhecido como "último" ou "grande" teorema de Fermat. Infelizmente, não deu sua prova, descrevendo-a apenas como tal que "essa margem é demasiada estreita para contê-la". Se Fermat tinha realmente uma prova, permaneceu perdida até hoje." (BOYER, 1996, p. 243).

Andrew Willes possuía conceitos avançados em relação à época de Pierre de Fermat, logo, se Fermat realmente possuía uma demonstração, ela seria muito mais simples e elegante, intrigando diversos matemáticos durante gerações.

Um dos muitos matemáticos que tentaram resolver o Último Teorema de Fermat, sem sucesso, foi Leonhard Euler (1707-1783), porém, a sua contribuição para matemática foi gigantesca, levando a crer que Euler tenha sido o mais importante matemático nascido na Suíça, contribuindo em diversos ramos da matemática pura e aplicada, dos mais elementares aos mais avançados. Uma grande Contribuição de Euler foi, no que se refere, a notações, pois muitos símbolos que ele introduziu, são usados atualmente. Pode-se dizer que Euler foi o grande responsável pela maneira que escrevemos na linguagem matemática.

A Teoria dos Números atraiu fortemente Euler, que escreveu várias cartas e artigos sobre o tema, derrubando, inclusive, algumas conjecturas de Fermat e provando seu Pequeno Teorema. Para a matéria mencionada, sua principal contribuição, além da demonstração do Pequeno Teorema, foi a elaboração da "função de Euler":

> Se m é um inteiro positivo maior que um, a função $\varphi(m)$ é definida como o número de inteiros menores que m que são primos com m (mas incluindo o inteiro um em cada caso). (BOYER, 1996, p. 316).

O século XVIII produziu diversos livros didáticos de sucesso, através de vários matemáticos, como o próprio Euler citado anteriormente. Um dos livros que teve mais sucesso foi o *Cours de mathemátique* de Etienne Bézout (1730-1783). Além de uma compilação de várias descobertas de grandes matemáticos, Bézout foi responsável pelo processo de estabelecimento dos sinais dos termos de um determinante e enunciar o teorema que dado dois inteiros positivos a e b, e $d = mdc(a, b)$, então existem inteiros r e s tais que $d = ra + sb$.

O século XIX, considerado por alguns historiadores, a Idade de Ouro da Matemática, trouxe um menino prodígio nascido em 1777 que colocou a Teoria dos Números em outro patamar. Carl Friedrich Gauss (1777-1855), conhecido como o Príncipe da Matemática, é autor do livro *Disquistiones Arithmeticae*, de 1801, uma obra que constitui um dos grandes clássicos da literatura Matemática e fundamental na discussão sobre o conceito de restos e congruência modular.

Gauss foi o primeiro a demonstrar o Teorema Fundamental da Álgebra, enunciado por outros matemáticos, porém sem a prova devida.

> "Gauss teve o poder de mudar os rumos da matemática a partir dos seus trabalhos revolucionários, apresentados com extremo rigor e grande concisão e elegância. Por isso, foi considerado, pelos seus contemporâneos e pelas gerações que se sucederam, um príncipe da rainha das ciências." (HEFEZ, 2016).

Diversos matemáticos contribuíram imensamente para a Matemática se tornar o que é hoje, a rainha das ciências. Fica a recomendação ao leitor para, caso tenha interesse pela descoberta de como caminhou a matemática junto a história das eras, o livro *História da Matemática* de Carl B. Boyer (BOYER, 1996).

2 ARITMÉTICA DOS NÚMEROS INTEIROS

Nesse capítulo é tratado a teoria que envolve os conjuntos, em especial o conjunto dos números inteiros, para depois, trabalhar toda a parte de divisibilidade e os conceitos que envolvem a Teoria dos Números. Para maiores e informações e detalhes adicionais à este capítulo poderão ser consultadas as seguintes referências (ALENCAR-FILHO, 1981), (BERTOLOTO, 2007), (DOMINGUES, 1991), (FEITOSA, 2019), (HEFEZ, 2016), (IEZZI, 2004), (LIMA, 2006), (LIMA, 2019), (SILVA, 2015).

2.1 O CONJUNTO DOS INTEIROS E SUAS PROPRIEDADES

Já ambientados em grande parte da história da Matemática que envolve a Teoria dos Números, bem como o que os principais matemáticos fizeram por esse tema, podemos iniciar o pensamento sobre a definição do conjunto dos números inteiros e suas propriedades, uma vez que a aritmética dos restos é construída a partir dele.

Recebe o nome de conjunto dos números inteiros, simbolizado por $\mathbb{Z}$, o seguinte conjunto:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Segundo Iezzi (2004, p. 42), no conjunto $\mathbb{Z}$, distinguimos três subconjuntos notáveis:

$\mathbb{Z}_+ = \{0, 1, 2, 3, \dots\} = \mathbb{N}$ (chamado de conjunto dos inteiros não negativos);

$\mathbb{Z}_- = \{0, -1, -2, -3, \dots\}$ (chamado de conjunto dos inteiros não positivos);

$\mathbb{Z}^* = \{\dots, -3, -2, -1,1,2,3, \dots\}$ (chamado de conjunto dos inteiros não nulos).

No conjunto $\mathbb{Z}$ são definidos duas operações fundamentais, a adição e a multiplicação.

Observemos que ocorre o fechamento dos subconjuntos $\mathbb{Z}_+$ e $\mathbb{Z}_-$para estas operações, o que permite definir a seguinte relação de ordem "$<$ " em $\mathbb{Z}$:

$$\text{“}a, b \in \mathbb{Z},\ a < b \Leftrightarrow b - a \in \mathbb{N}\text{ "}$$

A respeito desta relação de ordem admitiremos a seguinte propriedade

Tricotomia em $\mathbb{Z}$***:*** *Para quaisquer* $a, b \in \mathbb{Z}$*, uma, e apenas uma, das seguintes possibilidades é verificada,*

$i)\ a = b,$

$ii)\ a < b,$

$iii)\ b < a.$

Para quaisquer $a, b \in \mathbb{Z}$ são validas as seguintes propriedades:

[A.1] associativa da adição

$$(a + b) + c = a + (b + c).$$

[A.2] comutativa da adição

$$a + b = b + a.$$

[A.3] elemento neutro da adição $\exists\ 0 \in \mathbb{Z}$*, tal que*

$$\exists\ 0 \in \mathbb{Z}, \textit{ tal que } a + 0 = a.$$

[A.4] simétrico ou oposto para a adição

$$\exists - a \in \mathbb{Z} \textit{ tal que } a + (-a) = 0.$$

[M.1] associativa da multiplicação

$$(ab)c = a(bc).$$

[M.2] comutativa da multiplicação

$$ab = ba.$$

[M.3] elemento neutro da multiplicação

$$a \cdot 1 = a.$$

[D] distributiva da multiplicação relativamente à adição

$$a(b + c) = ab + ac.$$

Com as propriedades citadas, podemos enunciar algumas proposições que irão auxiliar o desenvolvimento da Teoria dos Números.

Proposição 2.1. *A relação "menor do que" é transitiva:*

$$\forall\ a, b, c \in \mathbb{Z}, a < b \text{ e } b < c \Leftrightarrow a < c.$$

Demonstração: Supondo $a < b$ e $b < c$, temos que $b - a \in \mathbb{N}$ e $c - b \in \mathbb{N}$. Como $\mathbb{N}$ é aditivamente fechado, temos que

$$c - a = (b - a) + (c - b) \in \mathbb{N},$$

Logo $a < c$. ■

Proposição 2.2. *A adição é compatível e cancelativa com respeito à relação "menor do que":*

$$\forall\ a, b, c \in \mathbb{Z}, a < b \Leftrightarrow a + c < b + c.$$

Demonstração: Supondo $a < b$, $b - a \in \mathbb{N}$, como $b - a = (b + c) - (a + c)$ e sabemos que $b - a \in \mathbb{N}$, logo $a + c < b + c$.

Reciprocamente, supondo $a + c < b + c$ temos que $(b + c) - (a + c) \in \mathbb{N}$, mas $(b + c) - (a + c) = b - a \in \mathbb{N}$. Assim $a < b$. ■

Proposição 2.3. *A multiplicação por elemento de* $\mathbb{N}^*$ *é compatível e cancelativa com respeito à relação "menor do que":*

$$\forall\, a, b \in \mathbb{Z}, \forall\, c \in \mathbb{N}^*\ a < b \iff ac < bc.$$

Demonstração: Supondo $a < b$. Então $b - a \in \mathbb{N}$. Assim, como $\mathbb{N}$ é fechado em relação a multiplicação, seja $c \in \mathbb{N}$ temos:

$$bc - ac = (b - a)c \in \mathbb{N},$$

logo, $ac < bc$.

Reciprocamente, supondo $ac < bc$, com $c \in \mathbb{N}^*$. Pela tricotomia temos três possibilidades:

1. $a = b$. Mas isso resultaria em $ac = bc$ o que é falso pois $c \in \mathbb{N}^*$. ;
2. $b < a$. Mas, pela primeira parte dessa demonstração, isso resultaria em $bc < ac$, para $c \in \mathbb{N}$.
3. $a < b$ é a única possibilidade verdadeira. ■

Para prosseguirmos, inicialmente, vamos definir a noção de valor absoluto.

Definição 2.1. *Seja* $a \in \mathbb{Z}$*, definimos:*

$$|a| = \begin{cases} a, se\ a \geq 0 \\ -a, se\ a < 0. \end{cases}$$

Note que para todo $a \in \mathbb{Z}$, tem-se que $|a| \geq 0$ e $|a| = 0$ se, e somente se, $a = 0$.

O número inteiro $|a|$ é chamado de módulo ou valor absoluto de a.

A seguir, vamos enunciar as propriedades básicas do módulo.

Para $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$ temos:

i) $|ab| = |a||b|$;

ii) $|a| \leq n$ se, e somente se, $-n \leq a \leq n$;

iii) $-|a| \leq a \leq |a|$;

iv) a desigualdade triangular:

$\big||a| - |b|\big| \leq |a \pm b| \leq |a| + |b|$.

Até aqui, descrevemos as propriedades e as proposições que envolvem os números inteiros, lembrando que a adição e a multiplicação definidas nos conjuntos racionais e os reais também possuem essas propriedades.

Vamos verificar, agora, uma importante propriedade que encontramos somente no conjunto dos números inteiros, o Princípio da Boa Ordenação, que diz: "Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento."

Este axioma bastante intuitivo é o que diferencia os números inteiros dos racionais e dos reais. É o que faltava para uma boa caracterização dos números inteiros e é o que faltava para conseguirmos enunciar mais alguma proposições e corolários que vão nos ajudar na compreensão desse trabalho.

Proposição 2.5. *Não existe nenhum número inteiro* n *tal que* $0 < n < 1$.

Demonstração: Supondo por absurdo que exista $n \in S$, onde $S = \{x \in \mathbb{Z}; 0 < x < 1\}$, então o conjunto S é não vazio e limitado inferiormente. Portanto, S possui um menor elemento a, com $0 < a < 1$. Nesta última desigualdade, multiplicando por a, obtemos $0 < a^2 < a < 1$, logo $a^2 \in S$ e $a^2 < a$, o que é uma contradição, pois a é o menor elemento de S.

Portanto $S = \emptyset$. ■

Corolário 2.6. *Dado um número inteiro* n *qualquer, não existe nenhum número inteiro* m *tal que* $n < m < n + 1$.

Demonstração: Supondo por absurdo que exista $m \in \mathbb{Z}$ tal que $n < m < n + 1$, subtraindo n nessa desigualdade temos, $0 < m - n < 1$, o que contradiz a proposição 2.5. ■

Corolário 2.7. *Sejam* $a, b \in \mathbb{Z}$. *Se* $ab = 1$, *então* $a = b = \pm 1$.

Demonstração: Notemos inicialmente que $a \neq 0$ e $b \neq 0$, pois do contrário $ab = 0$. Assim nos resta duas possibilidades, $a > 0$ ou $a < 0$.

Supondo $a > 0$. Como $ab = 1$, temos que $b > 0$. Segue da proposição 2.5 que $a \geq 1$ e $b \geq 1$. Logo, $1 = ab \geq b \geq 1$, o que implica $b = 1$. Como $ab = 1$, temos que $a = 1$.

Para o caso em que $a < 0$, vamos adaptar a proposição 2.5 para o seguinte, não existe nenhum número inteiro n tal que $-1 < n < 0$.

Agora supondo $a < 0$. Como $ab = 1 > 0$, temos que $b < 0$. Segue da adaptação da proposição 2.5 que $a \leq -1$ e $b \leq -1$. Logo, $1 = ab \geq b \leq -1$, o que implica $b = -1$. Como $ab = 1$, temos que $a = -1$. ■

Corolário 2.8. *Se* $a, b \in \mathbb{Z}$ *com* $b \neq 0$*, então* $|ab| \geq |a|$.

Demonstração: De fato, como $b \neq 0$, pela proposição 2.5, temos que $|b| \geq 1$.

Logo, $|ab| = |a||b| \geq |a|$. ■

Corolário 2.9. *Propriedade Arquimediana:*

Sejam $a, b \in \mathbb{Z}$ *com* $b \neq 0$*. Então existe* $n \in \mathbb{Z}$ *tal que* $nb > a$.

Demonstração: Como $|b| \neq 0$, da proposição 2.5, temos que $|b| \geq 1$, assim, multiplicando $|a| + 1$ na desigualdade, resulta em $|b|(|a| + 1) \geq |a| + 1 \geq |a| \geq a$.

O resultado desejado segue-se tomando na desigualdade anterior $n = |a| + 1$, se $b > 0$ e $n = -(|a| + 1)$, se $b < 0$. ■

2.2 DIVISIBILIDADE NOS NÚMEROS INTEIROS

A aritmética dos restos se baseia na possibilidade de dividirmos um número inteiro por outro. Expressamos essa possibilidade através da relação de divisibilidade.

> "Quando não existir uma relação de divisibilidade entre dois números inteiros, veremos que, ainda assim, será possível efetuar uma 'divisão com resto pequeno', chamada de divisão euclidiana." (HEFEZ, 2016, p. 40).

A divisão euclidiana é responsável por diversas propriedades dos inteiros e que veremos ao longo desse trabalho.

Para iniciar o estudo sobre a divisibilidade, devemos ter a noção do conceito de divisor.

Definição 2.2. *Dizemos que o inteiro* a *é divisor do inteiro* b *e denotamos* $a|b$ *, quando existe um inteiro* c *tal que* $ca = b$.

$$a|b \iff (\exists\, c \in \mathbb{Z} \mid ca = b)$$

Quando a *é divisor de* b*, dizemos que "*b *é divisível por* a*" ou "*b *é múltiplo de* a*".*

Vamos estabelecer algumas propriedades da divisibilidade.

Proposição 2.10. *Sejam* a, b *e* $c \in \mathbb{Z}$*. Temos que*

i) $1|a,\ a|a$ *e* $a|0$*;*

ii) *Se* $a|1$, *então* $a = \pm 1$;

iii) *Se* $a|b$ *e* $c|d$, *então* $ac|bd$;

iv) *Se* $a|b$ *e* $b|a$, *então* $a = \pm b$;

v) *Se* $a|b$, *com* $b \neq 0, então\ |a| \leq |b|$;

vi) $0|a \iff a = 0$;

vii) a *divide* b *se, e somente se,* $|a|$ *divide* $|b|$;

viii) *Se* $a|b$ *e* $b|c$, *então* $a|c$;

ix) *Se* $a|b$ *e* $a|c$, *então* $a|(bx + cy)$, $\forall\ x, y\ \in\ \mathbb{Z}$;

x) *Se* $a|(b \pm c)$, *então* $a|b \iff a|c$.

Demonstração:

i) Usaremos a propriedade [M.3] dos números inteiros, $a = a \cdot 1$ e como a definição de divisibilidade exige a existência de $c \in \mathbb{Z}$ tal que $a = c \cdot 1$, fazendo $c = a$ obtemos o desejado, logo $1|a$.

Usaremos ainda a propriedade [M.3] juntamente com a propriedade [M.2] dos números inteiros para mostrar que $a|a$. Assim, $a = a \cdot 1 = 1 \cdot a$ e fazendo $c = 1$ concluímos pela definição de divisibilidade que $a|a$.

Para $a|0$, como $0 = 0 \cdot a$ e fazendo $c = 0$ obtemos o desejado.

ii) Se $a|1$, então existe $x \in \mathbb{Z}$, tal que $1 = xa$. Logo, existem duas possibilidade sobre x e a tornarem a multiplicação verdadeira:

1. $x = 1$ e $a = 1$, e assim $1 \cdot 1 = 1$;
2. $x = -1$ e $a = -1$, e assim $(-1)(-1) = 1$.

Portanto $a = \pm 1$.

iii) Se $a|b$ e $c|d$ então existem $x, y \in \mathbb{Z}$ tais que: $b = xa$ e $d = yc$. Agora multiplicando b e d obtemos $bd = xayc$ e fazendo $xy = z \in \mathbb{Z}$ obtemos $bd = zac$, que pela definição de divisibilidade mostra que $ac|bd$.

iv) Se $a|b$ e $b|a$, então existem $x, y \in \mathbb{Z}$ tais que $b = xa$ e $a = yb$.

Logo, $a = a(xy)$, o que implica em $xy = 1 \Rightarrow y|1$. Assim, pelo item ii) da proposição 2.10, $y = \pm 1$. Portanto, $a = \pm b$.

v) Se $a|b$ e $b \neq 0$, então existe $x \in \mathbb{Z}$ tal que $b = xa$ e $x \neq 0$, e temos ainda que $|b| = |x||a|$. Como $x \neq 0$, segue-se que $|x| \geq 1$ e, portanto $|a| \leq |b|$.

vi) $(\Longrightarrow)$

$$0|a \Rightarrow a = 0,$$

Se $0|a$, temos, pela definição de divisibilidade, que $a = c \cdot 0$ para algum $c \in \mathbb{Z}$, logo, concluímos que $a = 0$.

($\Leftarrow$)

$a = 0 \Rightarrow 0|a$.

Se $a = 0$ basta mostrar que $0|0$, o que já fizemos no item i) já que $a|0$, então vale $a = 0$.

vii) $a|b \implies |a|$ divide $|b|$.

Se $a|b$ então existe $c \in \mathbb{Z}$ tal que $b = c \cdot a$, aplicando o módulo a ambos os membros da igualdade obtemos $|b| = |c \cdot a| = |c||a|$, agora fazendo $|c| = d \in \mathbb{Z}$ (como $c \in \mathbb{Z}$ então $|c| \in \mathbb{Z}$) temos que $|b| = d|a|$, que pela definição de divisibilidade nos mostra que $|a|$ divide $|b|$.

Reciprocamente, se $|a|$ divide $|b|$ então existe $c \in \mathbb{Z}$ tal que $|b| = c|a|$. O que nos dá duas possibilidades:

1. $b = c|a|$ onde $b = c \cdot a$ ou $b = c(-a)$. Para $b = c \cdot a$, pela definição de divisibilidade $a|b$. Para $b = c(-a)$, podemos reescrever da seguinte forma $b = -ca$, onde $-c \in \mathbb{Z}$, o que resulta em $a|b$ pela definição de divisibilidade.
2. $-b = c|a|$ onde $-b = c \cdot a$ ou $-b = c(-a)$. Para $-b = c \cdot a$ podemos reescrever da seguinte forma, $b = -ca$, onde $-c \in \mathbb{Z}$, e pela definição de divisibilidade $a|b$. Analogamente $-b = -ca$ pode ser escrito na forma $b = c \cdot a$, logo $a|b$.

viii) Se $a|b$ e $b|c$ então existem $x, y \in \mathbb{Z}$ tais que $b = xa$ e $c = yb$. Substituindo o valor de b na expressão de c, obtemos:

$$c = yb = yxa = (yx)a = za, \text{ com } z \in \mathbb{Z}.$$

Portanto, $a|c$.

ix) Se $a|b$ e $a|c$ então existem $m, n \in \mathbb{Z}$ tais que $b = ma$ e $c = na$. Agora vamos escrever $bx + cy$ usando as igualdades acima, $bx + cy = max + nay$ que pode ser reescrito como $bx + cy = a(mx + ny)$. Portanto $a|(bx + cy)$.

x) Vamos iniciar a demonstração para $a|(b + c)$ então $a|b \Leftrightarrow a|c$.

Se $a|(b + c)$ então existe $x \in \mathbb{Z}$ tal que $(b + c) = xa$, por outro lado, se $a|b$ existe $y \in \mathbb{Z}$ tal que $b = ya$. Juntando essas duas informações, temos, $ya + c = xa$ assim $c = (x - y)a$ com $(x - y) \in \mathbb{Z}$, logo $a|c$.

Reciprocamente, se $a|c$ então existe $m \in \mathbb{Z}$ tal que $c = ma$ e como $a|(b + c)$ existe também $x \in \mathbb{Z}$ tal que $b + c = xa$. Juntando essas informações, temos, $b + ma = xa$, logo $b = (x - m)a$ com $(x - m) \in \mathbb{Z}$, portanto $a|b$.

Agora, demonstraremos $a|(b-c)$ então $a|b \Leftrightarrow a|c$.

Como $a|(b-c)$ então existe $x \in \mathbb{Z}$ tal que $(b-c) = xa$, por outro lado, se $a|b$ existe $y \in \mathbb{Z}$ tal que $b = ya$. Juntando essas duas informações, temos, $ya - c = xa$ assim $c = (y-x)a$ com $(y-x) \in \mathbb{Z}$, logo $a|c$.

Reciprocamente, se $a|c$ então existe $m \in \mathbb{Z}$ tal que $c = ma$ e como $a|(b-c)$ existe também $x \in \mathbb{Z}$ tal que $b - c = xa$. Juntando essas informações, temos, $b - ma = xa$, logo $b = (x+m)a$ com $(x+m) \in \mathbb{Z}$, portanto $a|b$. ■

Em se tratando da divisão de um número inteiro a por um número inteiro $b \neq 0$, Euclides, nos livros *Elementos*, utiliza, sem enunciar explicitamente, o fato de que é sempre possível efetuar esta divisão com resto. Esse resultado é importante para o desenvolvimento de nosso trabalho e essa afirmação foi enunciada abaixo, na forma de teorema:

Teorema 2.1. (Algoritmo da Divisão) *Para quaisquer inteiros a e b, com $b \neq 0$, existe um único par de inteiros (q, r) tais que $a = bq + r$ e $0 \leq r < |a|$. Os números q e r são chamados de quociente e resto, respectivamente, da divisão de a por b.*

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

Pelo corolário 2.9 (Propriedade Arquimediana), existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$, o que mostra que S é não 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 $r = a - bq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1)b \in S$, com $s < r$.

Mostraremos agora a unicidade.

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

Relacionado ao resto da divisão que introduzimos, agora vamos estudar algumas propriedades.

Teorema 2.2. (Teorema dos Restos) *Se b_1 e b_2 deixam restos r_1 e r_2 na divisão por a, respectivamente, então:*

i) $b_1 + b_2$ *deixa o mesmo resto que* $r_1 + r_2$ *na divisão por* a*;*

ii) $b_1 b_2$ *deixa o mesmo resto que* $r_1 r_2$ *na divisão por* a*.*

Demonstração:

i) Por hipótese, existem q_1, q_2 e q tais que $b_1 = aq_1 + r_1$, $b_2 = aq_2 + r_2$ e $r_1 + r_2 = aq + r$, então:

$b_1 + b_2 = aq_1 + r_1 + aq_2 + r_2 = a(q_1 + q_2) + r_1 + r_2 = a(q_1 + q_2) + aq + r = a(q_1 + q_2 + q) + r$.

Como $0 < r < |a|$, $b_1 + b_2$ deixa o resto r quando dividido por a.

ii) Por hipótese, existem q_1, q_2 e q tais que $b_1 = aq_1 + r_1$, $b_2 = aq_2 + r_2$ e $r_1 r_2 = aq + r$, logo:

$b_1 b_2 = (aq_1 + r_1)(aq_2 + r_2) = aq_1 aq_2 + aq_1 r_2 + r_1 aq_2 + r_1 r_2 = a(aq_1 q_2 + q_1 r_2 + r_1 q_2) + aq + r = a(q_1 + q_2 + q) + r$.

Como $0 < r < |a|$, $b_1 b_2$ deixa o resto r quando dividido por a. ■

Vamos introduzir alguns conceitos que Euclides já tinha enunciado em seu livro *Elementos*.

Definição 2.3. (Máximo Divisor Comum) *Sejam* a *e* b *inteiros diferentes de zero. O máximo divisor comum, resumidamente* mdc*, entre* a *e* b *é o número* d *que satisfaz as seguintes condições:*

i) d *é um divisor comum de* a *e* b*, isto é,* $d|a$ *e* $d|b$*;*

ii) d *é o maior inteiro positivo com a propriedade (i).*

Neste caso, denotamos o mdc *entre* a *e* b *por* $d = mdc(a, b)$ *ou por* $d = (a, b)$*. Se* $(a, b) = 1$*, então dizemos que* a *e* b *são primos entre si.*

Proposição 2.11. (Relação de Bézout) *Sejam* a *e* b *inteiros positivos e* $d = mdc(a, b)$*, então existem inteiros* r *e* s *tais que* $d = ra + sb$*.*

Demonstração: Consideremos o conjunto $S = \{ax + by; x, y \in \mathbb{Z}\} \cap \mathbb{N}$.

S é um conjunto de números inteiros positivos. Logo podemos determinar o menor elemento de S, isto é, existe $d_1 \in S$ tal que $d_1 \leq x$ para todo $x \in S$.

Temos $d_1 \in S$, logo $d_1 = ar + bs$ para alguns $r, s \in \mathbb{Z}$ e nosso objetivo é mostrar que $d_1 = mdc(a, b)$.

Mostraremos que $d_1|a$. Caso isto não ocorresse, d_1 deixaria um resto $t > 0$ ao dividir a, isto é $a = qd_1 + t$ com $0 < t < d_1$.

Assim, $t = a - qd_1 = a - q(ar + bs) = a(1 - qr) + b(= sq)$.

Vemos, portanto, que $t \in S$, mas tal fato contradiz a definição de d_1 visto que $t < d_1$(lembrando que d_1 é o menor número de S). Esta contradição garante que $d_1|a$.

Da mesma forma, podemos mostrar que $d_1|b$.

Assim, $d_1 \in D(a) \cap D(b)$. Como d é o maior divisor comum de a e b resulta em $d_1 \leq d$. ■

Teorema 2.3 *Sejam a, b inteiros positivos. Então $d = mdc(a, b)$ se, e somente se, d satisfaz as seguintes condições:*

i) $d > 0$*;*

ii) $d|a$ *e* $d|b$*;*

iii) Para todo inteiro d' com $d'|a$ e $d'|b$ tem-se que $d'|d$.

Demonstração:

i) Da definição 2.3, garantimos que d satisfaz o item (i).

ii) Da definição 2.3, garantimos que d satisfaz o item (ii).

iii) Considerando $d' \in \mathbb{Z}$ satisfazendo $d'|a$ e $d'|b$. Pelo item ix) da proposição 2.10, temos que $d'|(ax + by)$ para todo $x, y \in \mathbb{Z}$. Agora uma vez que $d = mdc(a, b)$, pela proposição 2.11, existem $r, s \in \mathbb{Z}$ tais que $d = ar + bs$. Como vimos $d'|(ar + bs)$ e então $d'|d$. ■

Lema 2.1. (Euclides) *Sejam $x, y, a \in \mathbb{Z}$. Se existe $(x, y - ax)$, então, (x, y) existe e $(x, y) = (x, y - ax)$.*

Demonstração: Seja $d = (x, y - ax)$. Como $d|(y - ax)$, segue que d divide $b = b - ax + ax$. Logo, d é um divisor comum de a e b. Supondo agora que n seja um divisor comum de x e y. Logo, n é um divisor comum de $y - ax$ e, portanto, $n|d$. Assim $d = (x, y)$. ■

Logo, para calcular o mdc entre 123 e 164, basta utilizarmos o Lema 2.1, temos:

$$mdc(123, 164) = mdc(123, 123 + 41) = mdc\,(123, 41) = mdc\,(41 + 82, 41)$$
$$= mdc(41, 82) = mdc(\,41, 41) = 41.$$

Um conceito importante refere-se a dois inteiros primos entre si , cuja definição podemos enunciar da seguinte forma:

Definição 2.4. *Dizemos que dois inteiros p e q são primos entre si ou que dois inteiros p e q são relativamente primos, se $mdc(p,q) = 1$.*

Observemos que a fração $\frac{p}{q}$ é irredutível se p e q são relativamente primos. E ainda, decorre dos resultados que:

Corolário 2.12. *Dados $a, b \in \mathbb{Z}$, não ambos nulos, tem-se que*

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

Demonstração: Pelo teorema 2.3, temos que:

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

o que prova o resultado. ■

Proposição 2.13. *Dois números a e b são primos entre si se, e somente se, existem $n, m \in \mathbb{Z}$ de maneira que $an + bm = 1$.*

Demonstração: Supondo que a e b são primos entre si, pela definição 2.4. temos que $mdc(a,b) = 1$. Pela relação de Bèzout (proposição 2.11.), temos que existem números inteiros m e n tais que $an + bm = mdc(a,b) = 1$, logo a primeira parte está demonstrada.

Supondo que existem $n, m \in \mathbb{Z}$ de maneira que $an + bm = 1$. Se $d = mdc(a,b)$ temos que $d|(ma + nb)$, como $an + bm = 1$ por hipótese, temos que $d|1$, logo $d = 1$. O que conclui a segunda parte da demonstração. ■

O próximo resultado tem uma grande importância para o desenvolvimento da Teoria dos Números.

Teorema 2.4. (Lema de Gauss) *Sejam a, b e c números inteiros. Se $a|bc$ e $(a,b) = 1$, então $a|c$.*

Demonstração: Se $a|bc$, então existe $e \in \mathbb{Z}$ tal que $bc = ae$.

Se $mdc(a,b) = 1$, então pela Proposição 2.12. temos que existem $n, m \in \mathbb{Z}$ tais que

$$an + bm = 1. \qquad \text{(I)}$$

Multiplicando por c ambos os lados de (I), temos que:

$$anc + bmc = c. \quad \text{(II)}$$

Substituindo bc por ae em (II), temos que:

$c = anc + mae = a(nc + me)$ e, portanto $a|c$. ■

A divisibilidade nos trouxe até agora a construção do máximo divisor comum, porém, para continuar nosso estudo, podemos usar outra ideia essencial para a Teoria dos Números: O mínimo múltiplo comum (mmc).

Definição 2.5. *Os inteiros $a_1, a_2, \dots, a_n$, todos diferentes de zero, possuem múltiplo comum b se $a_i|b$ para $i = 1,2, \dots, n$ (note que $a_1 a_2 \dots a_n$ é um múltiplo comum). O menor múltiplo comum positivo para tal conjunto dos inteiros é chamado de mínimo múltiplo comum e será denotado por $mmc(a_1, a_2, \dots, a_n)$.*

Uma consequência dessa definição é a seguinte proposição:

Proposição 2.13. *Se a e b são não nulos, então $mmc(a, b) \cdot mdc(a, b) = |ab|$.*

Demonstração: Se $a = 0$ ou $b = 0$, a prova está satisfeita. É também fácil verificar que a igualdade é verificada para a e b se, e somente se, ela é verificada para $\pm a$ e $\pm b$. Então, sem perda de generalidade, podemos supor $a, b \in \mathbb{N}$. Tomando $m = \frac{ab}{(a,b)}$.

Como,

$$m = a\frac{b}{(a,b)} = b\frac{a}{(a,b)},$$

Temos que $a|m$ e $b|m$. Portanto, m é um múltiplo comum de a e b.

Seja c um múltiplo comum de a e b; logo $c = na = n'b$. Segue que

$$n\frac{a}{(a,b)} = n'\frac{b}{(a,b)}.$$

Pelo Corolário 2.12., $\frac{a}{(a,b)}$ e $\frac{b}{(a,b)}$ são primos entre si, segue-se, do Teorema 2.4., que $\frac{ab}{(a,b)}$ divide n', e portanto, $m = \frac{a}{(a,b)}b$ divide $n'b$ que, é igual a c. ■

2.3 NÚMEROS PRIMOS

Um importante conjunto de números para trabalharmos dentro da Teoria dos Números é o conjunto dos números primos, podemos definir um número primo da seguinte forma:

Definição 2.6. *Um inteiro* $p > 1$ *é chamado número primo se não possui um divisor* d *satisfazendo* $1 < d < p$. *Se um inteiro* $a > 1$ *não é primo, ele é chamado de número composto. Um inteiro* m *é chamado de composto se* $|m|$ *não é primo.*

O seguinte teorema é o alicerce dos fundamentos dos números inteiros:

Teorema 2.5. *Todo inteiro* n, *maior que* 1, *pode ser expresso como um produto de números primos.*

Demonstração: Com efeito, se n é primo, nada há que demonstrar, e se n é composto, então, n possui um divisor primo p_1 em sua decomposição e é do tipo:

$$n = p_1 n_1, \text{ com } 1 < n_1 < n. \quad \text{(I)}$$

Se n_1 é primo, então a igualdade (I) representa n como produto de fatores primos, e se, ao invés, n_1 é composto, então n_1 possui um divisor primo p_2, isto é, $n_1 = p_2 n_2$, e temos:

$$n = p_1 p_2 n_2, \text{ com } 1 < n_2 < n_1. \quad \text{(II)}$$

Se n_2 é primo, então a igualdade (II) representa n como produto de fatores primos, e se, ao invés, n_2 é composto, então n_2 possui um divisor primo p_3, isto é, $n_2 = p_3 n_3$, e temos:

$$n = p_1 p_2 p_3 n_3, \text{ com } 1 < n_3 < n_2. \quad \text{(III)}$$

E assim por diante.

Assim sendo, temos a sequência decrescente:

$$n > n_1 > n_2 > n_3 \cdots > 1,$$

e como só existe um número finito de inteiros positivos menores que n e maiores que 1, existe necessariamente um n_k que é um primo p_k $(n_k = p_k)$ e por conseguinte teremos:

$$n = p_1 p_2 p_3 \cdots p_k,$$

igualdade que representa o inteiro positivo $n > 1$ como produto de fatores primos. ■

Também devido a Euclides, no Livro IX dos $Elementos$, temos o seguinte resultado

Teorema 2.6. *Existem infinitos números primos.*

Demonstração: Suponha que exista apenas um número finito de números primos $p_1, p_2, \dots, p_r$. Considere o número natural

$$n = p_1 p_2 \dots p_r + 1$$

Temos pelo Teorema 2.5. que o número n possui um fator primo p que deve ser um dos $p_1, p_2, \dots, p_r$ e consequentemente, divide o produto $p_1 p_2 \dots p_r$. Mas, pelo item ix) da proposição 2.10., isto implica que p divide 1, o que é um absurdo matemático.

Portanto, existem infinitos números primos. ■

Utilizando o resultado de Bèzout, podemos demonstrar um importante resultado , conhecido como o Teorema Fundamental da Aritmética:

Teorema 2.7. (Teorema Fundamental da Aritmética) *A fatoração de qualquer inteiro* $n > 1$*, em fatores primos, é única a menos da ordem dos fatores.*

Demonstração: Usaremos a segunda forma do Princípio de 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 $p_1, p_2, p_3, \cdots, p_r$ e $q_1, q_2, q_3, \cdots, q_s$, tais que $n_1 = p_1 p_2 p_3 \cdots p_r$ e $n_2 = q_1 q_2 q_3 \cdots q_s$.

Portanto, $n = p_1 \cdots p_r q_1 \cdots q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha que tenhamos $n = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_i e os q_j são números primos. Como $p_1 | q_1 q_2 q_3 \cdots q_s$, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, q_2, q_3, \cdots, q_s$, podemos supor que seja q_1. Portanto,

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares. ■

2.4 CONGRUÊNCIAS

Nesta seção tratamos o objeto principal da abordagem deste trabalho.

Definição 2.7. *Dizemos que os inteiros a e b são congruentes módulo m se eles deixam o mesmo resto quando divididos por m. Nesse caso, denotaremos por $a \equiv b \ (mod\ m)$.*

Proposição 2.14. *Dados $a, b, n \in \mathbb{Z}$ com $n \in \mathbb{N}^*$, então:*

$$a \equiv b \ (mod\ n) \Leftrightarrow n|(b-a).$$

Demonstração: Provemos inicialmente que $a \equiv b \ (mod\ n) \Rightarrow n|(b-a)$.

Partindo de $a \equiv b \ (mod\ n)$, sabemos que a e b têm o mesmo resto r quando dividimos por n.

Isto significa que existem $q_1, q_2 \in \mathbb{Z}$ tais que $a = q_1 n + r$ e $b = q_2 n + r$.

Assim, $r = a - q_1 n$ e como $b = q_2 n + r$ obtemos

$$b = q_2 n + (a - q_1 n) \Rightarrow b - a = n(q_2 - q_1) \Rightarrow\ n|(b-a).$$

Provaremos agora que $n|(b-a) \Rightarrow a \equiv b \ (mod\ n)$.

Como $n|(b-a)$ temos $b - a = qn$ onde $q \in \mathbb{Z}$. Seja r o resto da divisão de a por n, então existe $q_1 \in \mathbb{Z}$ tal que $a = q_1 n + r$ onde $0 \leq r < n$.

Substituindo na igualdade $b = a + qn$, obteremos

$$b = q_1 n + r + qn \Rightarrow b = (q_1 + q)n + r.$$

Uma vez que $0 \leq r < n$ vemos $q_1 + q$ e r cumprem a condição de quociente e resto na divisão de b por n. E como quociente e resto são únicos neste processo, resulta que r também é o resto na divisão de b por n.

Portanto a e b tem o mesmo resto r na divisão por n como desejamos provar. ■

Teorema 2.8. *Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então:*

i) $a + c \equiv b + d \ (mod\ m)$;

ii) $a - c \equiv b - d \ (mod\ m)$;

iii) $ka \equiv kb \ (mod\ m) \ \forall\ k\ \in\ \mathbb{Z}$;

iv) $ac \equiv bd \ (mod\ m)$;

v) $a^k \equiv b^k \ (mod\ m)$.

Demonstração:

i) Como $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, pela proposição 2.14., temos respectivamente $m|(a-b)$ e $m|(c-d)$. Assim, resulta do item ix) da proposição 2.10. que $m|(a-b)+(c-d)$, ou ainda $m|(a+c)-(b+d)$.

Pela proposição 2.14., temos que $m|(a+c)-(b+d) \Rightarrow\ a+c \equiv b+d\ (mod\ m)$.

ii) Como $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, pela proposição 2.14., temos respectivamente $m|(a-b)$ e $m|(d-c)$. Assim, resulta do item ix) da proposição 2.10. que $m|(a-b)+(d-c)$, ou ainda $m|(a-c)-(b-d)$.

Pela proposição 2.14., temos que $m|(a-c)-(b-d) \Rightarrow\ a-c \equiv b-d\ (mod\ m)$.

iii) Como $a \equiv b\ (mod\ m)$, pela proposição 2.14., temos respectivamente $m|(a-b)$. Temos ainda, pelo item i) da proposição 2.10. que $1|k$. Assim, resulta do item iii) da proposição 2.10. que $1 \cdot m|k(a-b)$, ou ainda $m|(ka-kb)$.

Pela proposição 2.14., temos que $m|(ka-kb) \Rightarrow\ ka \equiv kb\ (mod\ m)$.

iv) Notemos que $ac-bd = d(a-b)+a(c-d)$ e como $m|(a-b)$ e $m|(c-d)$ pelo item ix) da proposição 2.10., $m|d(a-b)+a(c-d)$ o que é equivalente a dizer que $m|(ac-bd)$. Logo, $ac \equiv bd\ (mod\ m)$.

v) Vamos provar esse item utilizando indução matemática.

Seja $P = \{a^k \equiv b^k\ (mod\ m); k \in \mathbb{N}$ e $a, b \in \mathbb{Z}\}$.

1. Vamos mostrar que $1 \in P$.

   Por hipótese, temos que $a \equiv b\ (mod\ m)$, e para $n = 1$, temos $a^1 \equiv b^1 (mod\ m)$, que torna $a \equiv b\ (mod\ m)$. Portanto $1 \in P$;

2. Agora supondo que um certo $n \in P$ vamos provar que $n+1 \in P$.

   Se $n \in P$ então $a^n \equiv b^n\ (mod\ m)$ e por hipótese $a \equiv b\ (mod\ m)$. Agora, utilizando o item iv) desse teorema, vamos multiplicar as congruências e obteremos o que segue,

$$a^n \equiv b^n\ (mod\ m) \text{ e } a \equiv b\ (mod\ m)$$
$$a^n a \equiv b^n b\ (mod\ m)$$
$$a^{n+1} \equiv b^{n+1}\ (mod\ m).$$

O que prova que $n+1 \in P$, logo $a^k \equiv b^k\ (mod\ m)$. ■

Fermat nos fornece um importante resultado relacionado a congruência modular, mas antes de enunciá-lo e demonstrá-lo, precisamos do seguinte lema:

Lema 2.2. *Seja p um número primo. Os números $\binom{p}{i}$, onde $0 < i < p$ são todos divisíveis por p.*

Demonstração: O resultado vale trivialmente para $i = 1$. Podemos, então, supor $1 < i < p$. Nesse caso, $i!\,|p(p-1)\cdots(p-i+1)$. Como $(i!, p) = 1$, decorre que $i!\,|(p-1)\cdots(p-i+1)$, e o resultado se segue, pois

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

Os chineses conheciam que se, p é um número primo, então $p|2^p - 2$, pelo menos, 500 anos antes de Cristo, porém, coube a Pierre de Fermat generalizar o resultado transformando-o no conhecimento Pequeno Teorema de Fermat.

Teorema 2.9. (Teorema de Fermat) *Seja p um primo. Se p não divide a então*

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

Além disso, para todo inteiro a, $a^p \equiv a\ (mod\ p)$.

Demonstração: Se $p = 2$, o resultado é obvio já que $a^2 - a = a(a-1)$ é par. Suponhamos p ímpar. Nesse caso, claramente mostra o resultado para $a \geq 0$. Vamos provar o resultado por indução sobre a.

O resultado vale claramente para $a = 0$ pois $p|0$.

Supondo o resultado válido para a, iremos prová-lo para $a + 1$. Pela fórmula do Binômio de Newton,

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

Como, pelo Lema 2.2 e pela hipótese de indução, o segundo membro da igualdade (I) é divisível por p, o resultado se segue. ■

Lema 2.3. *Se $mdc(a, m) = 1$ então existe um inteiro x tal que*

$$ax \equiv 1\ (mod\ m)$$

Tal x é único módulo m. Se $mdc(a, m) > 1$ então não existe tal x.

Demonstração: Pela relação de Bèzout (proposição 2.11.), existem inteiros x e y tais que $ax + my = 1$.

Analisando essa congruência módulo m, obtemos $ax \equiv 1\ (mod\ m)$. Se y é outro inteiro que satisfaz a congruência, temos $ax \equiv ay\ (mod\ m)$, pelo item iii) do Teorema 2.8., $x \equiv y\ (mod\ m)$. Se $d = mdc(a, m) > 1$, não podemos ter $d|m$ e $m|(ax-1)$ pois $d \nmid (ax-1)$. ■

Definição 2.8. *Um conjunto S é chamado de sistema completo de resíduos módulo n, denotado abreviadamente por scr, se para cada $0 \leq i \leq n-1$, existe um elemento $s \in S$ tal que $i \equiv s \pmod n$. Para qualquer a, o conjunto $\{a, a+1, a+2, \dots, a+(n-1)\}$ é um exemplo de scr.*

2.5 EQUAÇÕES DIOFANTINAS

O proposito desta seção é mostrar uma importante aplicação da aritmética dos restos, as equações diofantinas lineares. Em diversas provas de conhecimento básico, como a Olimpíada Brasileira de Escolas Públicas e Privadas (OBMEP), podem ser encontrados problemas cujas soluções recaem sobre as equações diofantinas lineares de duas variáveis, contudo, a legislação brasileira sobre o currículo do ensino fundamental não contempla esse assunto. O que vamos enunciar na sequência são resultados importantes para o estudo desse tipo de equação.

Definição 2.9. *Uma equação diofantina de duas variáveis é dita linear se ela é da forma $ax + by = c$ onde a, b e $c \in \mathbb{Z}$ com a e b não nulos.*

Proposição 2.15. *Uma equação diofantina $ax + by = c$, em que $a \neq 0$ ou $b \neq 0$, admite solução se, e somente se, $d = mdc(a, b)$ divide c.*

Demonstração: ($\Longrightarrow$) Vamos mostrar que dada uma solução dá equação diofantina, então, $d|c$.

Considere x_0, y_0 soluções da equação. Assim,

$$ax_0 + by_0 = c.$$

Seja $d = mdc(a, b)$, então $d|a$ e $d|b$, logo, a e b podem ser reescritos como $a = k_1 d$ e $b = k_2 d$, com $k_1, k_2 \in \mathbb{Z}$. Substituindo os valores de a e b na equação acima, temos que:

$$c = ax_0 + by_0 = k_1 dx_0 + k_2 dy_0 = d(k_1 x_0 + k_2 y_0) = dq$$

Portanto, $d|c$.

($\Longleftarrow$) Considere $d = mdc(a, b)$. Pela relação de Bèzout (proposição 2.11.), existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$.

Por hipótese temos que $d|c$, isto é, existe $t \in \mathbb{Z}$ tal que $c = dt$. Segue então que

$$c = dt = (ax_0 + by_0)t = a(x_0 t) + b(y_0 t),$$

com $x_0 t, y_0 t$ solução da equação $ax + by = c$. ■

Proposição 2.16. *Seja* (x_0, y_0) *uma solução particular da equação diofantina* $ax + by = c$*, com* $a \neq 0$ *e* $b \neq 0$*. Então essa equação admite infinitas soluções e o conjunto dessas soluções é:* $S = \left\{\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right)\ t \in \mathbb{Z}\right\}$ *sendo* $d = mdc(a, b)$.

Demonstração: Consideremos (x', y') uma solução da equação $ax + by = c$. Então, $ax' + by' = c = ax_0 + by_0$, onde podemos reescrevê-la da seguinte forma

$$a(x' - x_0) = b(y_0 - y'). \quad \text{(I)}$$

Seja $d = mdc(a, b)$. Logo $a = dr$ e $b = ds$, com $r, s \in \mathbb{Z}$ e $mdc(r, s) = 1$. Então,

$$r(x' - x_0) = s(y_0 - y'). \quad \text{(II)}$$

Pela equação (II), temos que $r | s(y_0 - y')$. Como $mdc(r, s) = 1$, necessariamente $r | (y_0 - y')$, ou seja, existe t inteiro tal que $y_0 - y' = rt$. Assim,

$$y' = y_0 - rt = y_0 - \frac{a}{d}t. \quad \text{III)}$$

Então, para encontrarmos a forma das soluções x_0, basta substituirmos o valor de y' na equação (I). Temos que

$$a(x' - x_0) = b\left(y_0 - \left(y_0 - \frac{a}{d}t\right)\right).$$

Isso implica na seguinte equação $a(x' - x_0) = b\left(\frac{a}{d}t\right)$.

Segue que $a(x' - x_0) = \frac{ba}{d}t$ que desenvolvendo, chegamos a $x' - x_0 = \frac{b}{d}t$.

Logo, $x' = x_0 + \frac{b}{d}t$.

Por outro lado, o par $\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right)$ é solução da equação dada, para todo $t \in \mathbb{Z}$.

De fato, substituindo esses valores na equação, temos

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) \\ &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t \\ &= ax_0 + by_0 = c. \end{aligned}$$

■

A proposição anterior traz para nosso estudo que uma equação diofantina pode ter infinitas soluções no conjunto dos inteiros. Uma consequência dessa proposição é foi expresso a seguir, onde nos dá uma solução particular para a equação diofantina.

Proposição 2.17. *Seja* (x_0, y_0) *uma solução da equação diofantina* $ax + by = c$*, com* $mdc(a, b) = 1$*. Então, as soluções* x, y *em* $\mathbb{Z}$ *são* $x = x_0 + tb$*,* $y = y_0 - ta$*;* $t \in \mathbb{Z}$.

Demonstração: Seja x_0, y_0 uma solução de $ax + by = c$, logo,

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

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

Como $mdc(a, b) = 1$, segue que $b|(x - x_0)$. Logo, $x - x_0 = tb, t \in \mathbb{Z}$.

Substituindo a expressão $x - x_0 = tb$ em $a(x - x_0) = b(y_0 - y)$, temos que

$$atb = b(y_0 - y)$$

$$at = y_0 - y$$

$$y = y_0 - ta.$$

O que demonstra que as soluções são do tipo exibido. ■

2.6 CRITÉRIOS DE DIVISIBILIDADE

Uma das aplicações da congruência modular é de construir critérios de divisibilidade de um número inteiro por outro número inteiro. Antes de enunciarmos alguns critérios de divisibilidade, precisamos do um resultado que possibilita representar todo número em um determinado sistema numérico de base maior ou igual que dois.

Nosso sistema atual é na base 10, isto é, todo inteiro positivo a, pode ser escrito na forma

$$a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n + 10^n,$$

onde os coeficientes $a_i \in \mathbb{N}$ são tais que $0 \leq a_i \leq 9$ e são chamados algarismos do número a.

De modo geral para uma base b qualquer, podemos enunciar:

Teorema 2.10. *Sejam dados os números inteiros a e b, com $a > 0$ e $b > 1$. Existem números inteiros $n \geq 0$ e $0 \leq r_0, r_1, \cdots, r_n < b$, com $r_n \neq 0$, univocamente determinados, tais que*

$$a = r_0 + r_1 b + r_2 b^2 + \cdots + r_n b^n.$$

Demonstração: Vamos demonstrar o teorema por Indução Completa sobre a. Se $0 < a < b$, basta tomar $n = 0$ e $r_0 = a$. A unicidade da escrita é clara nesse caso.

Suponhamos o resultado válido para todo natural menor do que a, onde $a \geq b$. Vamos prová-lo para a. Pela divisão Euclidiana, existem q e r, únicos, tais que

$$a = bq + r, \text{ com } 0 \leq r < b. \quad \text{(I)}$$

Como $0 < q < a$, pela hipótese de indução, segue-se que existem números inteiros $n' \geq 0$ e $0 \leq r_1, \cdots, r_{n'+1} < b$, com $r_{n'+1} \neq 0$, univocamente determinados, tais que

$$q = r_1 + r_2 b + \cdots + r_{n'} b^{n'}. \quad \text{(II)}$$

Segue dê (I) e (II) que:

$$a = bq + r = b\left(r_1 + r_2 b + \cdots + r_{n'+1} b^{n'}\right) + r.$$

De onde o resultado segue-se pondo $r_0 = r$ e $n = n' + 1$. ■

Com a representação de um número na sua base bem definida, e trabalhando com a base 10, podemos definir alguns critérios de divisibilidade utilizando congruências.

Proposição 2.18. *(Critério de divisibilidade por 2) Um número a é divisível por 2 se o algarismo da unidade for par.*

Demonstração: Pelo Teorema 2.10., podemos escrever a como

$$a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n.$$

Desenvolvendo a congruência modular desse número em $mod\ 2$, temos

$$a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n \equiv a_0\ mod\ 2$$

Pois $10 \equiv 0\ mod\ 2$.

Logo, pela hipótese a_0 é par, ou seja, $a_0 \equiv 0\ mod\ 2$.

Portanto,

$$a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n \equiv 0\ mod\ 2$$

$$a \equiv 0\ mod\ 2.$$ ■

Proposição 2.19. *(Critério de divisibilidade por 3) Um número a é divisível por 3 se a soma dos seus algarismos é divisível por 3.*

Demonstração: Pelo Teorema 2.6.1 podemos escrever a como

$$a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n.$$

Desenvolvendo a congruência modular desse número em $mod\ 3$, temos

$a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n \equiv (a_0 + a_1 + a_2 + \cdots + a_n)\ mod\ 3$,

pois,

$$10 \equiv 1\ mod\ 3$$

$$10^2 \equiv 1\ mod\ 3$$

$$\vdots$$

$$10^n \equiv 1\ mod\ 3.$$

Logo,

$$a \equiv (a_0 + a_1 + a_2 + \cdots + a_n)\ mod\ 3.$$

Portanto,

$$3|a \Leftrightarrow 3|(a_0 + a_1 + a_2 + \cdots + a_n).$$ ■

Proposição 2.20. *(Critério de divisibilidade por 5) Um número a é divisível por 5 se o algarismo da unidade for 0 ou 5.*

Demonstração: Pelo Teorema 2.10. podemos escrever a como

$$a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n.$$

Desenvolvendo a congruência modular desse número em $mod\ 5$, temos

$$a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n \equiv a_0\ mod\ 5.$$

Pois $10 \equiv 0\ mod\ 5$.

Logo, pela hipótese a_0 é 0 ou 5, ou seja, $a_0 \equiv 0\ mod\ 5$.

Portanto,

$$a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n \equiv 0\ mod\ 5$$

$$a \equiv 0\ mod\ 5.$$ ■

Para demonstrar o critério de divisibilidade por 7, precisamos enunciar os seguintes resultados:

Teorema 2.11. Seja $d \in \mathbb{Z}$. *Se* $mdc(d, 10) = 1$, *então existe um número* $u \in \mathbb{Z}$ *tal que* $10 \cdot u \equiv 1\ (mod\ d)$. *Tal número* u *é chamado o inverso de* 10 *módulo* d *e escrevemos* $u \equiv 10^{-1}\ (mod\ d)$.

Demonstração: De $mdc(d, 10) = 1$, segue da relação de Bèzout (proposição 2.11) que existem k e $u \in \mathbb{Z}$ tal que

$$1 = k \cdot d + u \cdot 10 \Rightarrow (-k) \cdot d = 10 \cdot u - 1 \Rightarrow d|10 \cdot u - 1 \Rightarrow 10 \cdot u \equiv 1\ (mod\ d).$$ ■

Corolário 2.21. Se $u \equiv 10^{-1}\ (mod\ d)$, *escrevemos* $a = a_0 + a_1 10 + \cdots + a_n 10^n$ *e* $a' = (a_1 10 + \cdots + a_{n-1} 10^{n-1}) + u \cdot (a_0)$. *Temos que* a *é divisível por* d *se, e somente se,* a' *é divisível por* d.

Demonstração: Seja $a = a_0 + a_1 10 + \cdots + a_n 10^n$ tal que $d|a$. Logo:

$$a_0 + a_1 10 + \cdots + a_n 10^n \equiv 0\ mod\ d$$

$$\Leftrightarrow 10 \cdot (a_1 10 + \cdots + a_n 10^n) + (a_0) \equiv 0\ mod\ d$$

$$\Leftrightarrow 10 \cdot u \cdot (a_1 10 + \cdots + a_n 10^n) + u \cdot (a_0) \equiv 0 \; mod \; d$$
$$\Leftrightarrow (a_1 10 + \cdots + a_n 10^n) + u \cdot (a_0) \equiv 0 \; mod \; d. \qquad \blacksquare$$

Proposição 2.22. *(Critério de divisibilidade por 7) Dado um número a, quando multiplicamos o algarismo da unidade de a por 2 e subtraímos o resultado pelo número obtido do número inicial suprimido o algarismo da unidade, se o resultado for múltiplo de 7, o número original será múltiplo de 7. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 7.*

Demonstração: Como $mdc\ (7,10) = 1$, segue-se pelo Teorema 2.11. que existe $u \in \mathbb{Z}$, onde $u = -2$, pois $10 \cdot (-2) \equiv 1 \; mod \; 7 \Rightarrow -20 \equiv 1 \; mod \; 7 \Rightarrow 7 | -20 - 1 = -21$.

Portanto, sendo $a = a_0 + a_1 10 + \cdots + a_n 10^n$, segue do Corolário 2.21. que:

$$(a_1 10 + \cdots + a_n 10^n) - 2 \cdot (a_0) \equiv 0 \; mod \; 7. \qquad \blacksquare$$

Proposição 2.23. *(Critério de divisibilidade por 11) Um número $a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n$ é divisível por 11 se $(a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)$ for divisível por 11.*

Demonstração: Desenvolvendo a congruência modular desse número em $mod\ 11$, temos:

$$a_0 \equiv a_0 \; mod \; 11;$$
$$a_1 10 \equiv -a_1 \; mod \; 11;$$
$$a_2 10^2 \equiv a_2 \; mod \; 11;$$
$$a_3 10^3 \equiv -a_3 \; mod \; 11;$$
$$\cdots$$

Somando os membros destas congruências acima temos:

$$a \equiv (a_0 - a_1 + a_2 - a_3 + \cdots) \; mod \; 11.$$

Portanto,

$$11 | a \;\; \Leftrightarrow \;\; 11 \mid \; (a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots) \; . \qquad \blacksquare$$

Vimos que podemos utilizar a congruência para definir critérios de divisibilidade de um número inteiro por outro.

Agora, a proposição a seguir traz uma nova maneira de encontrar um critério de divisibilidade para números compostos.

Proposição 2.24. *Sejam* a, b *e* $c \in \mathbb{Z}^*$ *tais que* $mdc(a,b) = 1$ *e* $a|c$ *e* $b|c$*. Então* $ab|c$*.*

Demonstração: Da relação de Bèzout para a e b segue que, existem $r, s \in \mathbb{Z}$ tal que

$$ar + bs = 1.$$

Desta forma, $c = car + cbs$, assim (I)

$$a|c \Rightarrow c = ka, k \in \mathbb{Z}, \quad \text{(II)}$$

$$b|c \Rightarrow c = lb, l \in \mathbb{Z}, \quad \text{(III)}$$

Substituindo, as equações (II) e (III) na equação (I), temos:

$$c = lb \cdot ar + ka \cdot bs = ab(lr + ks) \Rightarrow ab|c. \qquad \blacksquare$$

Corolário 2.25. (Critério de divisibilidade por 6) Um número é divisível por 6 se for divisível por 2 e por 3.

Demonstração: Seja a um número qualquer tal que $2|a$ e $3|a$.

Temos que $mdc(2,3) = 1$, logo, pela proposição 2.24. temos que $2 \cdot 3|a \Rightarrow 6|a$. $\blacksquare$

3 INTERVENÇÃO COM OS ALUNOS

Os resultados do capítulo anterior constituem uma síntese importante para a formação do professor que pretende trabalhar esse conteúdo. Além da construção teórica feita no capítulo 2, foi possível observar, no projeto de treinamento que foi realizado em 2019, como na aplicação em 2020, que os alunos preferem os resultados operacionais práticos.

A princípio, a ideia original do projeto era aplicar a proposta em turmas de 9º ano com as quais eu trabalhava, tanto em colégios públicos quanto particulares, para verificar se haveria diferenças entre esses segmentos, bem como avaliar como os discentes receberiam esse conteúdo novo, pensando na formação de cada um ao término do ensino fundamental. Porém, devido às condições impostas pela pandemia, os alunos, ao longo do ano, ficaram desestimulados com o ensino remoto, sendo isso observado nos encontros de minhas turmas, houve um número maior de ausências de alunos das escolas públicas.

Desta forma optamos por elaborar a proposta de intervenção pedagógica "Ensinando Congruência Modular para alunos de 9º ano" que foi aplicada em uma escola privada na cidade de Birigui, estado de São Paulo, no qual sou um dos professores de Matemática. Foi utilizado o período normal das aulas, realizando entre os meses de outubro e novembro de 2020.

A plataforma utilizada pelo colégio é o Google Meet, uma vez que a escola conta com uma parceria com o Google For Education, assim, as aulas da intervenção pedagógica também se utilizaram dessa plataforma. A sala contava com 38 alunos, sendo 20 meninas e 18 meninos, porém, problemas de diversas ordens surgiram durante o processo:

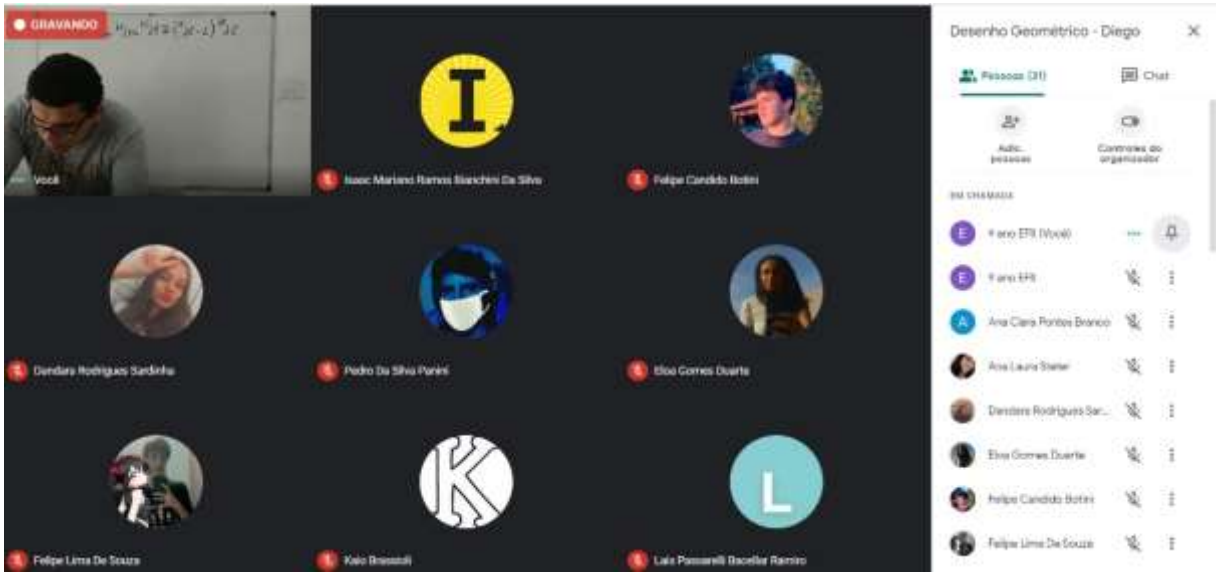
- A participação era irregular, em todas as disciplinas, tendo a devolutiva de apenas dez alunos no aplicativo Google ClassRoom para o projeto de intervenção pedagógica;

- Outro problema visto durante todo o ano letivo, inclusive durante o projeto de interação pedagógica foi que nem todos os alunos tentaram fazer os exercícios propostos. Quase todos os alunos entravam na plataforma, contudo, não faziam nenhum tipo de interação.

- Um grupo de alunos afirma que tem dificuldade com Matemática desde o ensino fundamental I, fazendo-os pensar que não é possível aprendê-la.

- Outro comentário durante a aula foi que não precisara de Matemática porque deseja fazer um curso relacionado à área de humanas, quando terminar o ensino básico. Foi informado para esse aluno e os demais que Matemática aparece em diversas situações do nosso cotidiano, não sendo objeto apenas de ensino escolar.

Figura 3.1. Alunos presentes na aula



Fonte: Próprio autor

A proposta de abordagem neste projeto é sobre um conteúdo que já se encontra presente na matriz curricular do ensino básico que é a divisibilidade. Contudo, vamos desenvolver alguns conhecimentos necessários para superar os problemas propostos. Lembrando que a divisibilidade é uma matéria presente no 6º ano do ensino fundamental e se insere em diversas situações do nosso dia a dia.

Alguns alunos têm dificuldade de relacionar as experiências do mundo real com a Matemática vista em sala de aula, dificuldade que, em alguns casos, convertem-se até em certo medo ao tratar os conteúdos da disciplina de Matemática. Podemos dizer que falta o letramento matemático em alguns alunos.

> Letramento matemático é a capacidade de formular, empregar e interpretar a Matemática em uma série de contextos, o que inclui raciocinar matematicamente e utilizar conceitos, procedimentos, fatos e ferramentas matemáticos para descrever, explicar e prever fenômenos. Isso ajuda os indivíduos a reconhecer o papel que a Matemática desempenha no mundo e faz com que cidadãos construtivos, engajados e reflexivos possam fazer julgamentos bem fundamentados e tomar as decisões necessárias. (BRASIL, 2020, p.100).

E segundo o relatório elaborado pelo Ministério da Educação referente ao PISA 2018, podemos citar que:

> A maioria dos estudantes brasileiros que participaram do Pisa 2018 se encontra no Nível 1 ou abaixo dele (68,1%). Todos os países e economias participantes do Pisa têm estudantes que se encontram nesses níveis, mas as maiores proporções de estudantes

> nessa situação são encontradas nos países com menor desempenho. (BRASIL, 2020, p.114).

Logo, precisamos urgentemente rever o desenvolvimento das habilidades envolvendo a Matemática para o ensino fundamental, uma vez que a expectativa colocada pela Base Nacional Comum Curricular (BNCC) não está sendo atingida de maneira satisfatória.

> Com referência ao Ensino Fundamental – Anos Finais, a expectativa é a de que os alunos resolvam problemas com números naturais, inteiros e racionais, envolvendo as operações fundamentais, com seus diferentes significados, e utilizando estratégias diversas, com compreensão dos processos neles envolvidos. Para que aprofundem a noção de número, é importante colocá-los diante de problemas, sobretudo os geométricos, nos quais os números racionais não são suficientes para resolvê-los, de modo que eles reconheçam a necessidade de outros números: os irracionais. Os alunos devem dominar também o cálculo de porcentagem, porcentagem de porcentagem, juros, descontos e acréscimos, incluindo o uso de tecnologias digitais. No tocante a esse tema, espera-se que saibam reconhecer, comparar e ordenar números reais, com apoio da relação desses números com pontos na reta numérica. (BRASIL, 2017, p. 269).

Ao longo da caminhada do aluno durante o ensino fundamental, verificamos a dificuldade com as quatro operações básicas: Adição, Subtração, Multiplicação e Divisão. Em especial, esse trabalho, foi uma forma de verificar o dinamismo no ensino da Matemática, ou seja, que é possível aprender de uma nova maneira as operações e aguçar o raciocínio lógico do aluno.

> As características da contextualização do ensino, especialmente no caso da Matemática, estão vinculadas às concepções de como o sujeito constrói seu conhecimento. Quando se acredita que a apresentação dos conteúdos matemáticos deve ocorrer com base na gradação da dificuldade que intrinsecamente apresentam, isto é, do simples ao complexo, têm-se no horizonte determinada possibilidade de contextualização, caracterizada pela ultrapassagem de um a outro nível de compreensão. Ou seja, o desafio de galgar um a um os degraus formados pela dificuldade crescente é, nesse caso, o elemento estruturador do contexto de ensino. (SPINELLI, 2011, p.13).

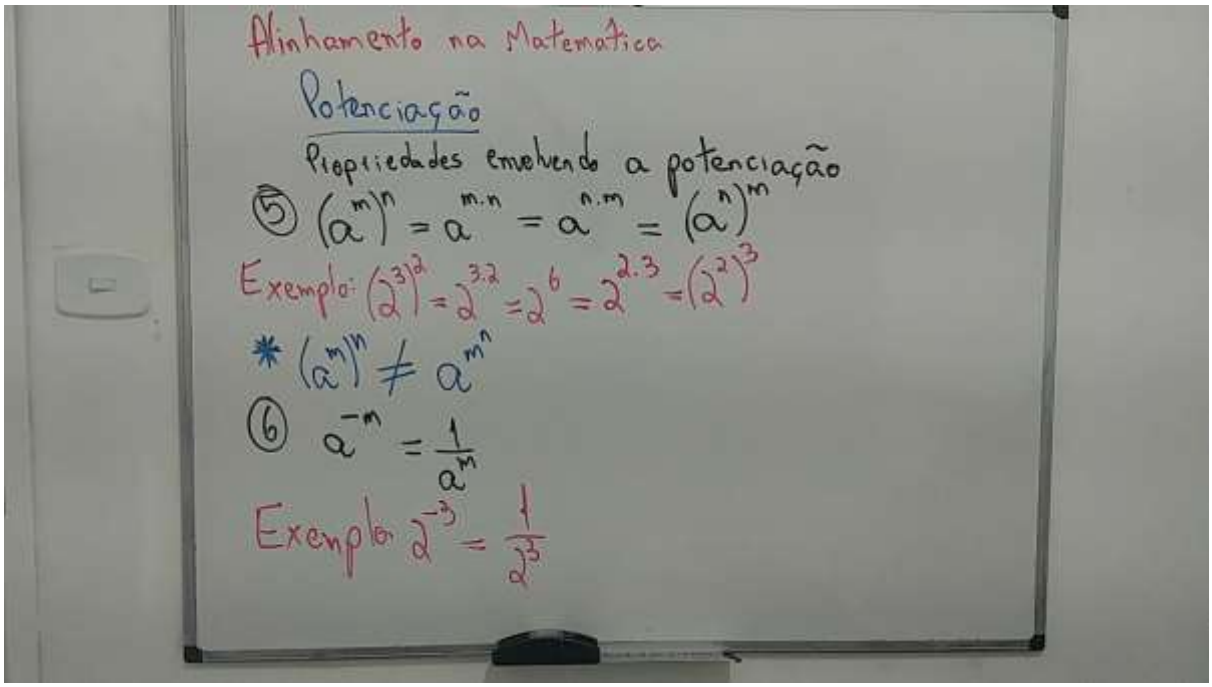
A parte aplicada de nosso projeto foi distribuída em seis aulas de 45 minutos cada, contemplando, inicialmente, um alinhamento de conteúdos básicos de Matemática, necessários para as operações com a congruência modular. Na sequência, foram relembrados conceitos de divisibilidade conhecidos por eles em outros anos, agora, porém com o emprego de notações mais apuradas. Nas aulas subsequentes introduzimos o conteúdo de congruência e desenvolvemos exercícios com situações-problema, vistos também em Olímpiadas de Conhecimento, como a OBMEP (Olímpiada Brasileira de Matemática das Escolas Públicas e Privadas). O material utilizado nas aulas é o que se encontra nos ANEXOS 1, 2 e 3 desse trabalho, desenvolvido pelo Instituto de Matemática Pura e Aplicada (IMPA), para os Polos de

Treinamento (POTI) em Matemática, visando às Olimpíadas de Conhecimento Matemático. Porém, foi feito uma adaptação, uma vez que o curso foi pensado em formato de oficina no contraturno escolar e desenvolvido ao longo de um ano, diferente do tempo disponibilizado para a intervenção pedagógica, objeto desse trabalho.

Na primeira aula, conforme o APÊNDICE 1, foi proposto uma revisão sobre os conjuntos numéricos (naturais, inteiros, racionais, irracionais e reais), propriedades de potenciação, notação científica, dizimas periódicas e fatoração. Foi notado dificuldade em vários alunos de retomarem os temas abordados, considerando tratar-se de uma revisão de conteúdos vistos nos anos finais do ensino fundamental.

Foi notado que os alunos que têm facilidade em cálculos e observações para fazer uma raciocínio lógico-matemático se destacaram na aula, enquanto o grupo de alunos que manifestava medo ou aversão à Matemática criaram uma resistência a esse tipo de conteúdo.

Figura 3.2. Alinhamento - Revisando propriedades de potenciação



Fonte: Próprio autor

Na segunda e terceira aula, conforme o APÊNDICE 2, foi desenvolvido o conteúdo relacionado à divisibilidade. Iniciamos com o problema seguinte, retirado da prova da OBMEP de 2010, para que os alunos tentassem resolver o problema com os conhecimentos que detinham, para em seguida, ser passada à teoria que envolve a divisibilidade e tentarem fazer novamente o exercício inicial.

O problema proposto:

Ano bissexto – Um ano comum tem 365 dias e um ano bissexto, 366 dias. O ano bissexto, quando o mês de fevereiro tem 29 dias, ocorre a cada quatro anos.

(a) Com frequência dizemos "Um ano comum tem 52 semanas". Será correta essa afirmação? E para um ano bissexto? Justifique suas respostas.

(b) Se um ano comum inicia numa terça-feira, então o ano seguinte iniciará em qual dia da semana?

A resolução esperada:

(a) Uma semana tem sete dias. Na divisão de 365 por 7 encontramos quociente 52 e resto 1. Logo, o ano comum tem 52 semanas e 1 dia. Portanto, a frase correta é "O ano comum tem cinquenta e duas semanas e um dia." Como o ano bissexto tem 366 dias, ele possui 52 semanas e 2 dias. Portanto, o correto é dizer "O ano bissexto tem cinquenta e duas semanas e dois dias."

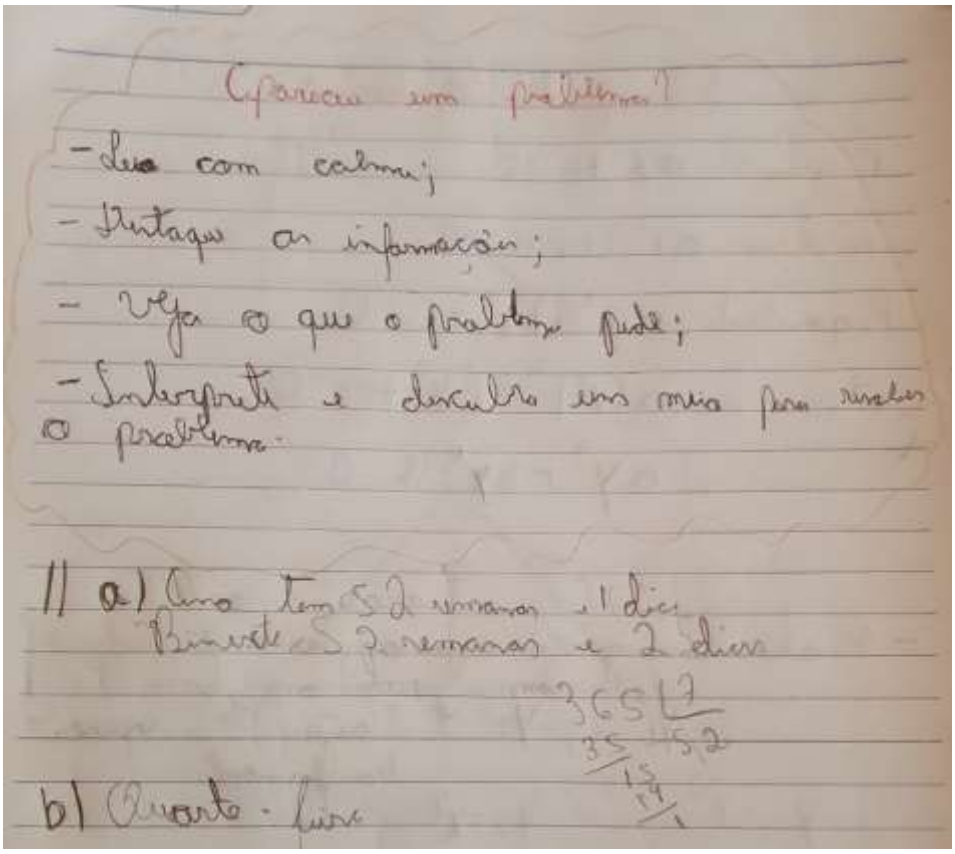
(b) Se um ano comum inicia numa terça-feira, então a sua 52ª semana inicia numa terça e termina numa segunda, ou seja, a 52ª semana é dada por terça – quarta – quinta – sexta – sábado – domingo – segunda. Como esse ano tem 52 semanas e mais 1 dia, o último dia deste ano será uma terça. Logo, o ano seguinte iniciará numa quarta.

O resultado foi que vários alunos tiveram dificuldade de conseguir pensar num raciocínio para desenvolver o problema ou ainda, faziam a divisão, porém, quando encontravam o resultado e viam que no quociente estava o número 52, acreditavam que a frase estava correta sem fazer o devido pensamento referente ao resto.

Com isso, foi possível retomar o tema da divisibilidade, a nomenclatura sobre os elementos que envolvem a divisão e que podemos escrever uma divisão em forma de uma equação.

Nesse tipo de abordagem vemos a dificuldade dos alunos de assimilar conceitos já estudados. Os alunos que mostravam mais habilidades não lembravam os nomes dos elementos que envolviam a divisão: dividendo, divisor, quociente e resto. Foi colocado para os alunos observarem quais números dariam resto 1 para uma divisão por 7. Eles deram a resposta antes de introduzir as próximas aulas.

Figura 3.3. Aluno conseguiu pensar no problema



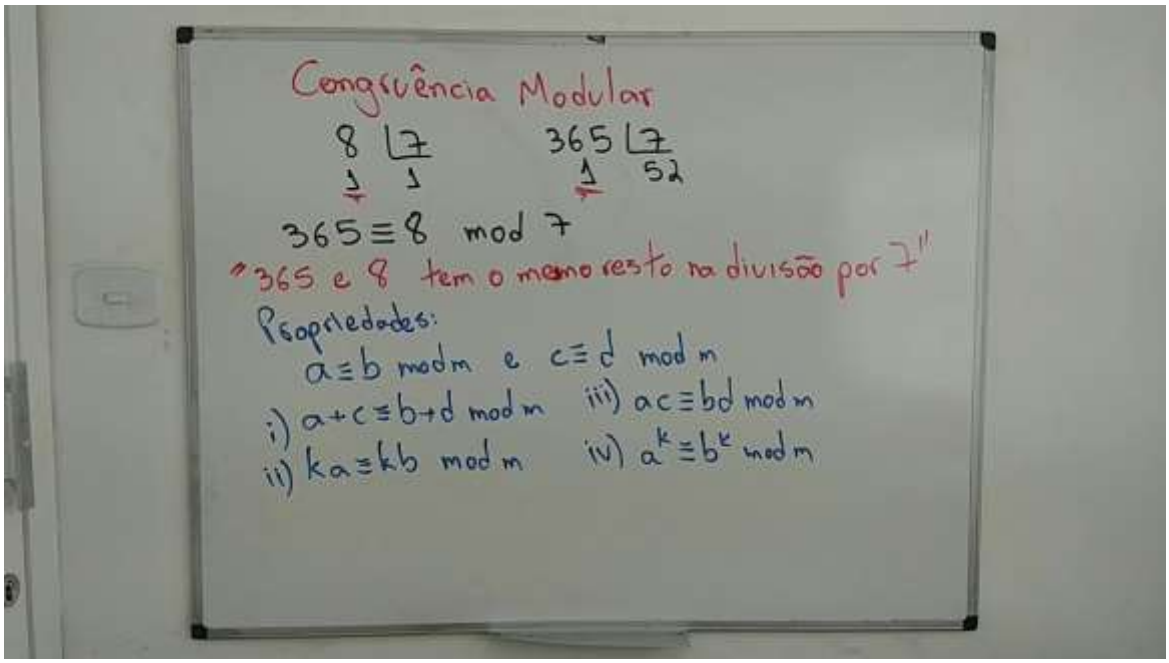
Fonte: Próprio Autor

Na quarta, quinta e sexta aula, conforme APÊNDICE 3, foram apresentados os conteúdos relacionados a congruência modular e explicado que ela poderia nos ajudar a resolver exercícios de diversas formas. Foi perguntado se eles já tinham visto falar sobre esse assunto e somente uma aluna respondeu que viu quando estava estudando para a OBMEP através do próprio sítio eletrônico da Olimpíada, onde existia uma serie de videoaulas que ensinavam o que era e como utilizá-las para resolver problemas.

Com isso, podemos mostrar como a congruência e suas propriedades podem nos ajudar a resolver diversos problemas, muitos desses exercícios que aparecem na OBMEP e em outras atividades culturais relacionadas com os conhecimentos matemáticos.

Foram passados alguns exercícios para treinamento dos alunos e foi perceptível a melhora de alguns deles no quesito de elaboração de estratégias de resolução. Percebeu-se também que congruências podem reduzir, ou mesmo, organizar cálculos.

Figura 3.4. Definição de Congruência Modular e Propriedades



Fonte: Próprio Autor

O objetivo principal deste projeto é o ensino da congruência modular e como os alunos se sentiriam, estudando este conteúdo mais avançado. Como visto no capítulo 2, as congruências podem ser utilizadas no desenvolvimento de critérios de divisibilidade, uma aplicação importante que repercute no dia a dia do estudante, através de cálculos mentais, simplificação de divisões e frações.

Um exemplo de aplicação desse conceito, temos na resolução do seguinte exercício:

Exercício. Qual o resto de $36^{36} + 41^{41}$ na divisão por 77?

Nesse tipo de exercício era necessário que o aluno conhecesse e aplicasse a proposição 2.24., como veremos abaixo:

A resolução esperada para este problema:

Inicialmente devemos perceber que existe uma relação entre os números do problema: $36 + 41 = 77$.

Assim:

$$-36 \equiv 41 \; mod \; 77$$

$$(-36)^{41} \equiv 41^{41} \; mod \; 77$$

$$36^{36}(-36)^{41} \equiv 36^{36}41^{41} \; mod \; 77$$

$$36^{36}[(-36)^5 36^{36}] \equiv 36^{36}41^{41}\ mod\ 77$$

$$36^{36}(1 - 36^5) \equiv 36^{36}41^{41}\ mod\ 77.$$

Nosso próximo passo é encontrar o resto de 36^5 na divisão por 77.

Como

$$36 \equiv 1\ mod\ 7$$

$$36^5 \equiv 1^5\ mod\ 7$$

$$36^5 \equiv 1\ mod\ 7.$$

Além disso,

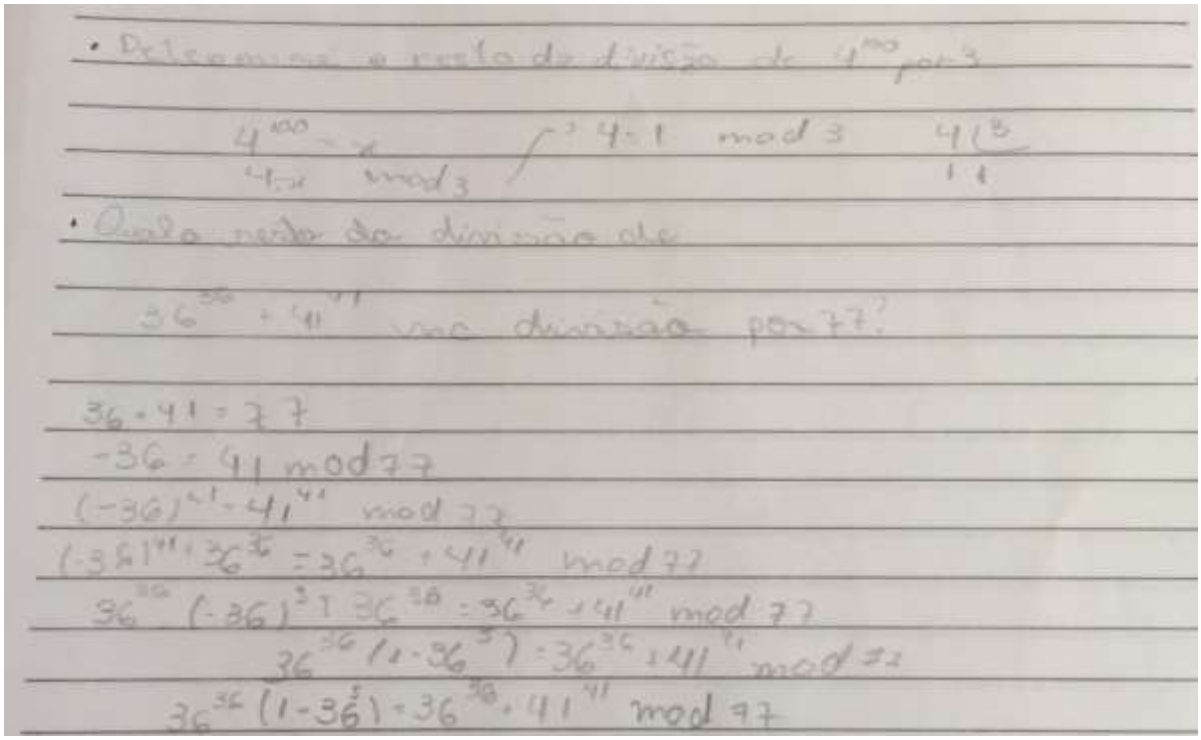
$$36 \equiv 3\ mod\ 11$$

$$36^5 \equiv 3^5 \equiv 1\ mod\ 11.$$

Como $mdc(7,11) = 1$ e ambos dividem $36^5 - 1$, podemos concluir que $7 \cdot 11 | 36^5 - 1$, ou seja, $77 | 36^5 - 1$.

Logo, $36^{36} + 41^{41}$ deixa resto 0 na divisão por 77.

Figura 3.5. Aluna realizando exercícios para encontrar resto de uma divisão



Fonte: Próprio autor

Na finalização das aulas enfatizamos como assuntos atuais têm relação com o conteúdo teórico que eles acabaram de estudar. Neste sentido, apresentamos ideias introdutórias do funcionamento dos sistemas de criptografia e código de barras, evidenciando que mesmo

assuntos puramente teóricos podem ter aplicações tão práticas que podem impactar diretamente o nosso cotidiano.

A avaliação do projeto por parte dos alunos foi satisfatória mediante o interesse de participarem dos trabalhos e confirmando a aprendizagem das principais técnicas desenvolvidas. Inicialmente a receptividade não foi tão boa, mas, conforme os exercícios de fixação foram sendo desenvolvidos, a grande maioria percebeu as simplificações de cálculos proporcionadas pela utilização de congruências. Abaixo descrevemos algumas manifestações recebidas:

"No começo achei um pouco complicado, mas com a boa explicação do professor, isso ajudará a resolver problemas que parecem difíceis, é muito útil."

"Acho interessante estudar isso, mas tive um pouco de dificuldade para entender."

"Acho que aprender congruência modular seria viável."

"aula daora."

"Não entendi mto bem o método."

Uma experiência nova para todos eles, a aritmética dos restos mostra que pode contribuir para maior autonomia e uma tomada de decisão eficiente e que traz uma segurança para resolverem questões que envolvam divisibilidade, dentro e fora da Matemática.

4 CONSIDERAÇÕES FINAIS

A essência deste trabalho foi descrever a intervenção pedagógica aplicada a uma turma de alunos de 9º ano do ensino fundamental, desenvolvendo conceitos básicos da Teoria dos Números, em particular, congruências modulares. As condições de distanciamento social, imposto pelo estado de pandemia, exigiram que os principais contatos com os alunos concentrassem em apenas 6 encontros virtuais, o que limitou a amplitude dos conteúdos abordados, ou, mesmo, suprimiu outros, como máximo divisor comum e menor múltiplo comum.

A despeito dessas dificuldades, a experiência foi positiva, porque, retoma temas anteriores do currículo escolar como a divisibilidade e possibilita contato dos alunos com técnicas matemáticas importantes para a resolução de problemas dentro e fora da Matemática. Estes benefícios já tive oportunidade de observar também na formação Matemática dos meus alunos cursistas do polo de treinamento da OBMEP. De fato, o estudo da aritmética dos restos, no ensino fundamental, é uma maneira interessante para que o aluno contextualize problemas que podem aparecer no cotidiano e amplie a gama de ferramentas para resolvê-los.

Um olhar para um trabalho futuro na direção aqui iniciada e esclarecer ideias matemáticas que estão sendo construídas pelo aluno, especialmente para dar respostas a alguns “porquês” é pensar nas facilidades operacionais proporcionadas pelas congruências modulares e que despertaram o interesse dos alunos nas resoluções dos problemas e aplicações, de modo que podem constituir temas interessantes para projetos de ensino, como feiras e treinamentos para olimpíadas de Matemática.

Com isso, podemos tornar a Matemática uma alavanca importante para democratizar o acesso ao ensino superior, despertar a aptidão para o estudo e o surgimento de vocações para carreiras tecnológicas e científicas.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ALENCAR-FILHO, E. d. **Teoria elementar dos números**. Nobel, 1981.

[2] **Base Nacional Comum Curricular**. Brasília, 2017. Disponível em: <http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf>. Acesso em: 02 nov. 2020.

[3] BERTOLOTO Jr., J. **Álgebra I**. Notas de Aula –Universidade Federal do Mato Grosso do Sul. Três Lagoas, 2007.

[4] BRASIL. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. Brasil no Pisa 2018. Brasília, 2020. Disponível em <http://portal.inep.gov.br/documents/186968/484421/RELAT%C3%93RIO+BRASIL+NO+PISA+2018/3e89677c-221c-4fa4-91ee-08a48818604c?version=1.0> Acesso em: 10 nov. 2020.

[5] BRASIL. **Parâmetros Curriculares Nacionais (PCN)**. Brasília, 2017. Disponível em: <http://portal.mec.gov.br/seb/arquivos/pdf/matematica.pdf>. Acesso em: 21 out. 2020.

[6] BOYER, C. B. **História da Matemática.** 2ª edição. São Paulo, 1996.

[7] D'AMBROSIO, U. **Educação Matemática: Da Teoria à Prática**. Papirus Editora, 2007.

[8] DOMINGUES, H. H. **Fundamentos de aritmética**. Atual Editora Ltda, 1991.

[9] FEITOSA, S. B. Curso de Teoria dos Números – Nível 2. Rio de Janeiro, 2019. Disponível em: https://www.dropbox.com/sh/c658cq0nl8v240f/AACc4-AIlxeqlSSGDErm0RuIa/Aulas%20N%C3%ADvel%202/TNN2?dl=0&subfolder_nav_tracking=1> Acesso em: 16 out. 2020.

[10] HEFEZ, A. **Aritmética**. 2ª edição. Rio de Janeiro, 2016.

[11] IEZZI, G.; MURAKAMI, C. **Fundamentos de Matemática Elementar: Conjuntos, Funções**. 8ª edição, 2005.

[12] LIMA, E. L. **Análise Real volume 1: Funções de Uma variável**. 8ª edição. Rio de Janeiro, 2006.

[13] LIMA, R. V. **Equações Diofantinas**. Trabalho de Conclusão de Curso –Universidade Federal de São João del-Rei. São João del-Rei, 2019.

[14] OBMEP. Banco de questões da OBMEP. Disponível em: <http://www.obmep.org.br/bq/bq2010.pdf>. Acesso em: 10 nov. 2020.

[15] SILVA, L. H. P. **Uma Aplicação da Congruência na Determinação de Critérios de Divisibilidade**. Dissertação de Mestrado – Universidade Federal de Goiás. Goiânia, 2015.

[16] SPINELLI, W. **A construção do Conhecimento entre o abstrair e o contextualizar: O caso do Ensino da Matemática**. Tese Doutorado em Educação – Faculdade de Educação da Universidade de São Paulo. São Paulo, 2011.

APÊNDICE 1

PLANO DE ESTUDO DIÁRIO

Turma: 9º Ano do EF II	**Disciplina: Matemática**
Data: 30/09/2020	**Hora atividade (tempo previsto): 01 aula**
Coordenador(a) Pedagógico(a): XXXXXXX	**Professor: Diego Sampaio Santiago**

REFERÊNCIA: Alinhamento na Matemática – Aula 01

	Orientações
	Com intuito de aproximar os alunos com a matemática, nesse final de bimestre faremos um alinhamento na matemática. Retomaremos conceitos vistos em anos anteriores: - Potenciação e suas propriedades; - Notação Científica e Dízimas Periódicas; - Fatoração.
Dúvidas	Podem ser postadas no Mural do GoogleClassRoom, via ClassApp, ou via Google Meet no horário de aula.
Devolutiva	Via Google ClassRoom

APÊNDICE 2

PLANO DE ESTUDO DIÁRIO

Turma: 9º Ano do EF II	**Disciplina: Matemática**
Data: 02/10/2020	**Hora atividade (tempo previsto): 02 aulas**
Coordenador(a) Pedagógico(a): XXXXXX	**Professor: Diego Sampaio Santiago**

REFERÊNCIA: Experiências Matemáticas – Aula 02 e 03

	Orientações
	Após ter feito um alinhamento na matemática, retomaremos a matéria de divisibilidade visto no 6º ano, porém, com outro olhar utilizando material de treinamento da OBMEP
Dúvidas	Podem ser postadas no Mural do GoogleClassRoom, via ClassApp, ou via Google Meet no horário de aula.
Devolutiva	Via Google ClassRoom

APÊNDICE 3

PLANO DE ESTUDO DIÁRIO

Turma: 9º Ano do EF II	**Disciplina: Matemática**
Data: 07/10/2020	**Hora atividade (tempo previsto): 03 aulas**
Coordenador(a) Pedagógico(a): XXXXXX	**Professor: Diego Sampaio Santiago**

REFERÊNCIA: Experiências Matemáticas – Aula 04, 05 e 06

	Orientações
	Com vários conceitos assimilados em aulas anteriores, passaremos a introduzir um novo tema: Congruência Modular e será pedido a opinião dos alunos a respeito dessa nova matéria
Dúvidas	Podem ser postadas no Mural do GoogleClassRoom, via ClassApp, ou via Google Meet no horário de aula.
Devolutiva	Via Google ClassRoom

ANEXO 1

Módulo de Potenciação e Dízimas Periódicas

Potenciação

(Material Adaptado da aula zero do curso de Teoria dos Números do Treinamento Olímpico Intensivo – POTI)

Propriedades da potenciação

1) $a^0 = 1$
2) $a^1 = a$
3) $a^m . a^n = a^{m+n}$
4) $\frac{a^m}{a^n} = a^{m-n}$
5) $(a^m)^n = a^{m.n}$
6) $a^{-m} = \frac{1}{a^m}$
7) $\left(\frac{a}{b}\right)^m = \frac{a^m}{a^n}$
8) $a^{\frac{m}{n}} = \sqrt[n]{a^m}$

Exercício 1. Calcule o valor das expressões:

a) 3^5

b) $2^2 + 3^2$

c) 5^4

d) $2^3 + 3^3$

e) $\frac{1}{2} . 2^4 . 3$

Exercício 2. Calcule o valor das expressões:

a) $(0{,}01)^3$

b) $100 . \frac{1}{5^2}$

c) $80 . \left(\frac{5}{2}\right)^3$

d) $\frac{1}{3} . (0{,}3)^2$

e) $200 . (0{,}04)^4$

Dízimas Periódicas

$$x \cdot 10^n \; com \; 1 \leq x < 10 \; e \; n \in \mathbb{Z}$$

Exercício 3. Escreva os seguintes números na notação científica:
científica:

a) 45673

b) $0{,}0012345$

c) -555

d) $0{,}09$

Exercício 4. Encontre a fração geratriz de:

a) $0{,}333\ldots$

b) $0{,}121212\ldots$

c) $6{,}5555\ldots.$

d) $-0{,}666\ldots$

Exercício 5. Fatore as expressões:

a) $5a + ba$

b) $am + an$

c) $xa + xb + xc$

d) $ax + a$

e) $ab + bc + abc$

Exercício 6. Simplifique as frações fatorando o denominador e o numerador.

a) $\frac{3a+5b}{6a+10b}$

b) $\frac{3x+3y}{8x+8y}$

c) $\frac{3a^2+5a}{6a+10}$

d) $\frac{a(x+y)+b(x+y)}{(a-b)x+(a-b)y}$

e) $\frac{x^4+x^3}{x^2+x}$

ANEXO 2

Divisibilidade

(Material Adaptado das aulas 01 e 02 do curso de Teoria dos Números do Treinamento Olímpico Intensivo – POTI)

Teorema (Algoritmo da Divisão) Para quaisquer inteiros a e b, com $a \neq 0$, existe um único par de inteiros (q, r) tais que $b = aq + r$ e $0 \leq r < |a|$. Os números q e r são chamados de quociente e resto, respectivamente, da divisão de b por a.

Exemplo: Encontre um número natural N que, ao ser dividido por 10, deixa resto 9, ao ser dividido por 9 deixa resto 8, e ao ser dividido por 8 deixa resto 7.

O que acontece ao somarmos 1 ao nosso número? Ele passa a deixar resto 0 na divisão por 10, 9 e 8. Assim, um possível valor para N é $10 \cdot 9 \cdot 8 - 1$.

Teorema (Teorema dos Restos) Se b_1 e b_2 deixam restos r_1 e r_2 na divisão por a, respectivamente, então:

$b_1 + b_2$ deixa o mesmo resto que $r_1 + r_2$ na divisão por a

$b_1 b_2$ deixa o mesmo resto que $r_1 r_2$ na divisão por a

Observação. Em alguns casos, é preferível que o professor faça uma demonstração do resultado anterior para $a = 3$ ou $a = 5$ apenas com o intuito de deixar os alunos mais confortáveis a respeito do resultado. É preferível que mais tempo seja gasto resolvendo exemplos e problemas. Na seção de congruências, os alunos terão um contato mais apropriado com o enunciado anterior.

Exemplo 1. Qual o resto que o número $1002 \cdot 1003 \cdot 1004$ deixa quando dividido por 7?

Como 1002 deixa resto 1 por 7, o número acima deixa o mesmo resto que $1 \cdot 2 \cdot 3 = 6$ por 7.

Exemplo 2. Qual o resto que o número 4^{5000} deixa quando dividido por 3?

Como 4 deixa resto 1 por 3, 4^{5000} deixa o mesmo resto que $\underbrace{1 \cdot 1 \cdot \ldots \cdot 1}_{5000} = 1$ por 3.

Ano bissexto – Um ano comum tem 365 dias e um ano bissexto, 366 dias. O ano bissexto, quando o mês de fevereiro tem 29 dias, ocorre a cada quatro anos.

(a) Com frequência dizemos “Um ano comum tem 52 semanas”. Será correta essa afirmação? E para um ano bissexto? Justifique suas respostas.

(b) Se um ano comum inicia numa terça-feira, então o ano seguinte iniciará em qual dia da semana?

Resolução: (a) Uma semana tem sete dias. Na divisão de 365 por 7 encontramos quociente 52 e resto 1. Logo, o ano comum tem 52 semanas e 1 dia. Portanto, a frase correta é "O ano comum tem cinquenta e duas semanas e um dia." Como o ano bissexto tem 366 dias, ele possui 52 semanas e 2 dias. Portanto, o correto é dizer "O ano bissexto tem cinquenta e duas semanas e dois dias."

(b) Se um ano comum inicia numa terça-feira, então a sua 52ª semana inicia numa terça e termina numa segunda, ou seja, a 52ª semana é dada por terça – quarta – quinta – sexta – sábado – domingo – segunda. Como esse ano tem 52 semanas e mais 1 dia, o último dia deste ano será uma terça. Logo, o ano seguinte iniciará numa quarta.

O resultado foi que vários alunos tiveram dificuldade de conseguir pensar num raciocínio para desenvolver o problema ou ainda, faziam a divisão, porém, quando encontravam o resultado e viam que no quociente estava o correto, acreditavam que a frase estava correta sem fazer o devido pensamento referente ao resto.

ANEXO 3

Congruências

(Material Adaptado das aulas 04, 05 e 06 do curso de Teoria dos Números do Treinamento Olímpico Intensivo – POTI)

Definição 1 Dizemos que os inteiros a e b são congruentes módulo m se eles deixam o mesmo resto quando divididos por m. Denotaremos por $a \equiv b \ (mod\ m)$.

E podemos estabelecer as seguintes propriedades em relação a congruência:

Teorema 2 Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então:

i) $a + c \equiv b + d \ (mod\ m)$

ii) $a - c \equiv b - d \ (mod\ m)$

iii) $ka \equiv kb \ (mod\ m) \ \forall\ k \in \mathbb{Z}$

iv) $ac \equiv bd \ (mod\ m)$

v) $a^k \equiv b^k \ (mod\ m)$

Exemplo 1. Calcule o resto de $4^{100}\ por\ 3$

Como $4 \equiv 1 \ (mod\ 3)$, temos $4^{100} \equiv 1^{100} = 1 \ (mod\ 3)$

Exemplo 2. Calcule o resto de $4^{100}\ por\ 5$

Como $4 \equiv -1 \ (mod\ 5)$, temos $4^{100} \equiv (-1)^{100} = 1 \ (mod\ 5)$

Exemplo 3. Calcule o resto de $4^{100}\ por\ 7$

Você deve ter percebido que encontrar relações do tipo $a \equiv \pm 1 \ (mod\ m)$ podem simplificar bastante o cálculo de $a^k \ (mod\ m)$. Procuremos alguma relação como essa para 4 e 7. Veja que:

$4^0 \equiv 1 \ (mod\ 7)$, $4^1 \equiv 4 \ (mod\ 7)$ $\ 4^2 \equiv 2 \ (mod\ 7)$, $4^3 \equiv 1 \ (mod\ 7)$.

Assim,

$$4^{99} \equiv (4^3)^{33} \equiv 1^{33} = 1 \ (mod\ 7).$$

Como $4^3 \equiv 1 \ (mod\ 7)$, os restos das potências de 4 na divisão por 7 se repetem periodicamente de 3 em 3 pois $4^{3k+r} \equiv 4^{3k} \cdot 4^r \equiv 4^r \ (mod\ 7)$

Exercício. Qual o resto de $36^{36} + 41^{41}\ na\ divisão\ por\ 77$?