Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional

Inserções de Metodologias Diferenciadas no Ensino de Divisibilidade na Educação Básica

Claudio dos Santos

Goiânia

2021

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO (TECA) PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES

E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo das Teses e Dissertações disponibilizado na BDTD/UFG é de responsabilidade exclusiva do autor. Ao encaminhar o produto final, o autor(a) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do material bibliográfico

[**X**] Dissertação [ ] Tese

2. Nome completo do autor

Claudio dos Santos

3. Título do trabalho

Inserções de Metodologias Diferenciadas no Ensino de Divisibilidade na Educação Básica

4. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador)

Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante:
a) consulta ao(à) autor(a) e ao(à) orientador(a);
b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo da tese ou dissertação.
O documento não será disponibilizado durante o período de embargo.
Casos de embargo:
- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

Obs. Este termo deverá ser assinado no SEI pelo orientador e pelo autor.

Claudio dos Santos

Inserções de Metodologias Diferenciadas no Ensino de Divisibilidade na Educação Básica

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.
Área de Concentração: Matemática do Ensino Básico.
Orientadora: Profª. Drª. Ivonildes Ribeiro Martins Dias.

Goiânia

2021

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Santos, Claudio dos
Inserções de Metodologias Diferenciadas no Ensino de Divisibilidade na Educação Básica [manuscrito] / Claudio dos Santos. - 2021.
LXXII, 72 f.

Orientador: Profa. Dra. Ivonildes Ribeiro Martins Dias.
Dissertação (Mestrado) - Universidade Federal de Goiás, , PROFMAT - Programa de Pós-graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RG), Goiânia, 2021.
Bibliografia.
Inclui lista de figuras.

1. Aritmética. 2. Divisibilidade. 3. Álgebra. 4. Congruência. 5. Polinômios. I. Dias, Ivonildes Ribeiro Martins, orient. II. Título.

CDU 51

UNIVERSIDADE FEDERAL DE GOIÁS

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

ATA DE DEFESA DE DISSERTAÇÃO

Ata nº 20 da sessão de Defesa de Dissertação de Claudio dos Santos, que confere o título de Mestre em Matemática, **na área de concentração em Ensino de Matemática.**

Aos dezoito dias do mês de março de dois mil e vinte e um, a partir das 16 **horas**, por meio de videoconferência devido a pandemia covid-19, realizou-se a sessão pública de Defesa de Dissertação intitulada **"Inserções de Metodologias Diferenciadas no Ensino de Divisibilidade na Educação Básica"**. Os trabalhos foram instalados pela Orientadora, Professora Doutora Ivonildes Ribeiro Martins Dias (IME/UFG) com a participação dos demais membros da Banca Examinadora: Professora Doutora Thaynara Arielly de Lima (IME/UFG) e o membro titular externo a Professora Doutora Eunice Candida Pereira Rodrigues (UFMT). Durante a arguição os membros da banca **não fizeram** sugestão de alteração do título do trabalho. A Banca Examinadora reuniu-se em sessão secreta a fim de concluir o julgamento da Dissertação, tendo sido o candidato **aprovado** pelos seus membros. Proclamados os resultados pela Professora Doutora Ivonildes Ribeiro Martins Dias, Presidente da Banca Examinadora, foram encerrados os trabalhos e, para constar, lavrou-se a presente ata que é assinada pelos Membros da Banca Examinadora, aos dezoito dias do mês de março de dois mil e vinte e um.

TÍTULO SUGERIDO PELA BANCA

Inserções de Metodologias Diferenciadas no Ensino de Divisibilidade na Educação Básica

Documento assinado eletronicamente por **Ivonildes Ribeiro Martins Dias**, **Professor do Magistério Superior**, em 10/04/2021, às 13:13, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Thaynara Arielly De Lima**, **Professora do Magistério Superior**, em 13/04/2021, às 14:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Eunice Cândida Pereira Rodrigues**, **Usuário Externo**, em 13/04/2021, às 16:18, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1872095** e o código CRC **1353867D**.

Referência: Processo nº 23070.007951/2021-14 SEI nº 1872095

Claudio dos Santos graduou-se em Licenciatura em Matemática pela Pontifícia Universidade Católica de Goiás em 2012, especializou-se em Docência do Ensino Superior pela Faculdade Brasileira de Educação e Cultura (FABEC-BRASIL) em 2014 , atualmente é professor do Ensino Básico da Rede Adventista de Ensino.

Dedico aos meus filhos, fonte de inspiração e motivação para o meu desenvolvimento.

Agradecimentos

A Deus, o autor e mantenedor da vida pelas muitas oportunidades de estudar e me qualificar.

Aos meus pais por me ensinar que sempre posso ir além, que, com dedicação e esforço posso alcançar objetivos cada vez maiores.

À Prfa. Dra. Ivonildes Ribeiro Martins Dias, pela dedicação e apoio, afim de desenvolver meus horizontes, enxergando possibilidades e vencendo dificuldades, especialmente pela paciência e compreensão em detalhes que outros professores não teriam ao longo do processo de elaboração deste trabalho.

Ao meu colega de graduação, Luan Gomes, pelo incentivo desde a graduação até o ingresso nesse curso de mestrado.

Aos meus colégas de mestrado, turma maravilhosa, pelo apoio, em especial Ricardo Tomé e Alberto Santos dos Reis.

Resumo

Como professor das séries finais do ensino fundamental, tenho observado que dentre as quatro operações básicas, a divisão é a que apresenta maior grau de dificuldade para os alunos. Tendo como motivação diminuir essa dificuldade o presente trabalho aborda a congruência modular como uma maneira de levar o aluno a enxergar a divisão euclidiana sob um aspecto diferente. Considerando que desde os anos iniciais o aluno tem contato com conceitos da aritmética modular, neste trabalho é sugerida uma abordagem diferenciada do processo de divisibilidade. O estudo aborda tópicos de álgebra em nível avançado, para que o professor aprimore seus conhecimentos nesta área, e limitado a propriedades operatórias básicas com o cuidado de não exceder à capacidade de aprendizagem dos alunos desta fase do ensino. Será apresentada uma aplicação da congruência modular em situações do cotidiano, e na resolução de problemas básicos de divisibilidade afim de tornar a aprendizagem mais interessante e atraente para o aluno.

Palavras-chave

Aritmética, Divisibilidade, Álgebra, Congruência, Polinômios.

Abstract

As a teacher in the final grades of elementary school, I have observed that among the four basic operations, the division is the one that presents the greatest degree of difficulty for students. With the motivation to reduce this difficulty, the present work approaches the modular congruence as a way to take the student to see the Euclidean division in a different aspect. Considering that since the early years the student has had contact with concepts of modular arithmetic, in this work it is suggested a differentiated approach to the divisibility process. The study addresses algebra topics at an advanced level, so that the teacher can improve his knowledge in this area, and limited to basic operative properties, taking care not to exceed the learning capacity of students at this stage of teaching. An application of modular congruence will be presented in everyday situations, and in solving basic problems of divisibility in order to make learning more interesting and attractive to the student.

Keywords

Arithmetic, Divisibility, Algebra, Congruence, Polynomials.

Lista de Figuras

Sumário

Introdução

A busca pelo desenvolvimento sempre foi algo inerente ao ser humano, desde o seu surgimento até os dias atuais. A partir do momento em que passou a viver em grupo o desejo de se adaptar, desvendar, melhorar, foi potencializado. Tais impulsos são vistos no desenvolvimento da linguagem como forma de manter a convivência nas comunidades e realizar atividades coletivas. Houve o mesmo senso em relação aos números, que com perseverança e paciência, ao longo dos séculos alcançou desenvolvimento notável. Muitas mentes dedicadas ao seu estudo e em muitos casos, vidas que foram sacrificadas, privadas de conforto e até ceifadas em consequência de suas descobertas (Galileu Galilei para citar um exemplo). No entanto a marcha para o aperfeiçoamento foi implacável, e as transformações sofridas pela matemática de modo geral, e especialmente pela teoria dos números foram marcantes. A teoria dos números, objeto de estudos de tantas civilizações como, Egito, Babilônia, Roma, Índia, entre outras, sofreu um aperfeiçoamento tão significativo que se tornou um dos principais eixos da matemática moderna, a aritmética. Esta trata das operações e das propriedades numéricas.

Neste trabalho aborda-se conceitos relacionados à aritmética, em especial à congruência modular, que trata da divisão de números inteiros considerando em um grau de destaque o resto desta divisão. Tal abordagem permite ao professor a elabolação de aulas e atividades que envolvam o processo de divisibilidade sob esse aspecto. Em seguida é apresentada uma extensão de seus princípios básicos para o conjunto denominado anel dos polinômios com coeficientes reais, como proposta para que o professor aborde, já no ensino médio, tais conceitos nas operações com polinômios.

Abordar uma situação de diferentes formas, desenvolver múltiplas estratégias para solucionar problemas é uma das inúmeras recompensas que recebe o ávido estudante da matemática. A divisibilidade é exposta sob um aspecto diferente dos métodos tradicionais, todavia, utilizando-se de uma ferramenta que compõe os fundamentos da

educação matemática no ensino básico, a congruência modular, que tem como base os conceitos e propriedades da divisão euclidiana, presente na vida dos estudantes desde os primeiros anos de sua vida escolar; mas que tem de maneira geral seu espectro ofuscado pela maneira como é ensinada, pois desde o início do aprendizado seu ensino tem como principal objetivo identificar o quociente da divisão, não considerando as inúmeras possibilidades de desenvolvimento do conhecimento que são oferecidas ao se considerar como elemento de grande importância não o quociente, mas o resto.

As propriedades apresentadas nas aplicações exibidas no capítulo 4 se limitam àquelas que podem ser compreendidas e aplicadas pelos alunos dos anos finais do ensino fundamental, entre o sexto e sétimo anos, e uma transição de algumas propriedades convenientes do conjunto dos números inteiros para o anel dos polinômios com coeficientes reais, que podem ser aplicadas por alunos do ensino médio.

Tendo por fundamento a proposta da base nacional comum curricular (BNCC), que é a de proporcionar ao aluno a oportunidade de produzir e desenvolver o conhecimento, este trabalho propõe ao aluno a oportunidade de ampliar sua visão sobre essa parte da construção e teoria dos números (a divisibilidade), teoria que tem se mostrado fundamental ao desenvolvimento tecnológico sem precedentes experimentado no final do século vinte e início do século vinte e um. Em consonância com Fiorentini:

> "garantir ao futuro cidadão essa forma de pensamento e de leitura do mundo proporcionada pela matemática que é uma das principais finalidades da educação matemática comprometida com a formação da cidadania, tendo em vista que a matemática está visceralmente presente na sociedade tecnológica em que vivemos, podendo ser encontrada sob inúmeras formas em nosso cotidiano, ou seja, a principal razão pela qual ensinamos e aprendemos matemática tem a ver com o modo de vida do homem moderno (FIORENTINI, 1995, p. 32)".

Uma estratégia fundamental para o processo de ensino e aprendizagem da matemática é despertar no aluno o interesse pelo objeto estudado, promover situações que estimulem a curiosidade e desencadeiem um processo que permita a construção de novos conhecimentos, eis o sentido da educação matemática.

O tema escolhido é justificado por apresentar conhecimentos importantes à vida e ao cidadão moderno. São muitas as aplicações da congruência modular, dentre elas podemos destacar os conceitos que envolvem as propriedades das operações; a construção de códigos; nas mudanças de bases numéricas, no estudo de modelagem de fenômenos periódicos em diferentes campos do conhecimento. A congruência modular é vista na

vida cotidiana, como em um relógio de ponteiros, no qual o dia é dividido em dois períodos de 12 horas cada um; nos ciclos do calendário que se repetem em meses, semanas e dias; mais ainda nos códigos numéricos de identificação, como o código de barras, cadastro de pessoas físicas (CPF), nos números de cartões de crédito, etc.

O objetivo geral é apresentar ao professor a proposta de uma abordagem diferente, não convencional e ao mesmo tempo atrativa para os alunos, afim de que seu interesse e motivação sejam despertados para a aprendizagem da matemática. Já os objetivos específicos são: fazer com que o aluno entenda de maneira ampla o processo de divisibilidade; definir e relacionar a congruência modular com a divisibilidade; permitir ao aluno aplicar as propriedades dos números inteiros a outros conjuntos com características semelhantes, no caso os polinômios; proporcionar ao aluno a possibilidade de enxergar a matemática aplicada em seu cotidiano.

No Capítulo 1 são apresentados dados importantes referentes à educação matemática no Brasil, o que apresenta um quadro insatisfatório da proficiência em matemática (também em língua portuguesa e ciências), por parte do estudante brasileiro, no que diz respeito à sua formação profissional e ao exercício de sua cidadania. Apresentamos alguns aspectos importantes que compõe a base do processo ensino-aprendizagem como o contexto social do aluno, o desenvolvimento de habilidades mediante a resolução de problemas, e a formação continuada do professor. Nos Capítulos 2 e 3, aborda-se como fundamentação teórica (apenas os aspectos necessários ao nosso estudo), as estruturas algébricas dos anéis de números inteiros e dos polinômios, dando atenção ao aspecto da divisão euclidiana. No Capítulo 4 é feita uma relação de situações do cotidiano onde a aritmética é aplicada, e exercícios tanto de nível fundamental como de nível médio como motivação ao professor, com o propósito de que ele amplie e aplique essa metodologia em sala de aula. Nas considerações finais faremos uma reflexão sobre os propósitos do trabalho e as mudanças que a proposta fará para a melhora do nivel da educação matemática brasileira.

Capítulo 1

Fatores que influenciam a educação matemática brasileira

O objetivo deste capítulo é trazer alguns elementos que permitem comparações da condição dos estudantes da educação básica brasileira diante do cenário mundial, diante do fato de os alunos brasileiros terem sido classificados com um nível de desenvolvimento inferior, e até insatisfatório em relação a alguns países. Para uma visão mais ampla do quadro apresentado aqui, o leitor poderá obter mais informações em .

A matemática quando vista corretamente pode desenvolver no estudante uma série de habilidades que lhe são úteis em vários aspectos, independentemente da área profissional ou social onde ele esteja inserido. Habilidades como raciocínio lógico, capacidade de enfrentar e resolver problemas, criação de estratégias para solução de problemas em diferentes situações, desenvolvimento do potencial de adaptação e transposição de ideias para diferentes situações, ampliação de conceitos com o objetivo de solucionar problemas ou de desenvolver novos conhecimentos, generalização de teorias afim de se criar algo inédito, são algumas das vertentes da devida compreensão de uma das disciplinas de mais ampla capacidade de desenvolvimento intelectual e cognitívo; sendo tal capacidade sintetizada nas competências relacionadas ao estudo desta disciplina. Segundo a BNCC o estudo da matemática deve:

> "Desenvolver raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo, ... fazer observações sistemáticas de aspectos quantitativos e qualitativos presentes nas práticas sociais e culturais, de modo a investigar, organizar, representar e comunicar informações relevantes, para interpretá-las e avaliá-las critica e eticamente, produzindo argumentos convincentes."(EDUCAÇÃO, 2017, p. 267)

Contudo, a matemática no contexto do sistema tradicional de ensino brasileiro, de modo geral, não tem sido ensinada de maneira a facinar e libertar a mente de seus estudantes como poderia e deveria fazer.

O mais importante estudo sobre educação realizado no mundo, o programa internacional de avaliação de estudantes (Pisa), tendo sua última avaliação realizada em 2018, revelou que o Brasil quando comparado com outros 78 países que participaram da avaliação possui nível de proficiência abaixo do mínimo necessário, tanto para que os alunos exerçam alguma atividade econômica que exija conhecimentos em leitura, matemática e ciências, quanto para o exercício da cidadania. A edição 2018, revela que 68,1% dos estudantes brasileiros, com 15 anos de idade, não possuem nível básico de matemática, o mínimo para o exercício pleno da cidadania. Em ciências, o número chega a 55% e, em leitura, 50%. Os índices estão estagnados desde 2009. Dentre os quesitos em que os alunos brasileiros foram pontuados com baixa proficiência estão, situações de incapacidade na compreensão de textos e na resolução de cálculos e questões científicas simples e rotineiras. Se comparado à média dos países da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), o Brasil apresenta resultados ainda piores nas três áreas avaliadas, conforme a relação abaixo:

- Leitura: OCDE 487 pontos, Brasil 413 pontos;
- Matemática: OCDE 489 pontos, Brasil 384 pontos;
- Ciências: OCDE 489 pontos, Brasil 404 pontos;

Realizado a cada três anos, o Pisa tem o objetivo de mensurar até que ponto os jovens de 15 anos adquiriram conhecimentos e habilidades essenciais para a vida social e econômica. Em 2018, 79 países e 600 mil estudantes participaram do teste, que ocorre desde 2000. Mais de 40% dos jovens que se encontram no nível básico de conhecimento são incapazes de resolver questões simples. Dos 10.961 alunos brasileiros participantes do Pisa, apenas 0,1% apresentou nível máximo de proficiência na área de matemática. Em termos de escolarização, os estudantes brasileiros estão três anos e meio atrás

dos países da OCDE (489), quando o assunto é proficiência em matemática as escolas particulares (473) e federais (469) têm rendimentos bem superiores à média nacional (384), diferentemente das instituições de ensino públicas estaduais (374) e municipais (314), que estão abaixo da média do Brasil.

Como uma das providências a serem tomadas para a melhora do nível do desempenho dos alunos brasileiros está a necessidade de se estabelecer práticas educacionais que objetivem elevar o nível de nossos alunos, a fim de se alcançar um dos objetivos propostos pela Lei de Diretrizes e Bases da educação brasileira, que é o de garantir o pleno desenvolvimento do educando, seu preparo para o exercício da cidadania e sua qualificação para o trabalho (EDUCAÇÃO, 1996).

Diante da atual conjuntura, faz-se necessário a análise de pontos importantes a serem melhorados para se elevar o nível da educação matemática brasileira.

1.1 O contexto social do aluno

Outro aspecto importante a ser considerado é o contexto social do aluno, com o propósito de criar uma ligação entre a sua realidade e o conhecimento transmitido pelo professor. Há a necessidade de se perceber a importância de entender um pouco melhor quem são os alunos em um aspecto mais amplo, de pessoa com sonhos e objetivos de vida, afim de o estimular para que ele se sinta parte do contexto do ensino, e assim seja provocado a construir juntamente com o professor a aula proposta. Gasparin nos lembra que:

> "São jovens que vivenciam a paixão, o sentimento, a emoção, o entusiasmo, o movimento. Anseiam por liberdade para imaginar, conhecer, tudo ver, experimentar, sentir. O pensar e o fazer, o emocional e o intelectual, estão entrelaçados, de maneira que estão inteiros em cada coisa que fazem".(GASPARIN, 2001, p. 8)

O contexto histórico-social do aluno é fator importante como prática metodológica, as Diretrizes Curriculares de Matemática para a Educação Básica, propõem um ensino da matemática que considere o cotidiano e a cultura do aluno e que o leve a apropriar-se do objeto matemático historicamente construído e assim possa agir criticamente e com autonomia nas suas relações sociais.

Explorando a experiência matemática obtida pelo aluno em seu cotidiano, a escola garante uma aprendizagem mais significativa e com melhores resultados, permitindo que ele estabeleça a ligação entre a prática da vida e a teoria apresentada pela escola afim de que problemas sejam resolvidos com as conexões que podem ser estabelecidas entre os diferentes temas matemáticos, e posteriormente destes com outras áreas do conhecimento.

1.2 A resolução de problemas

A resolução de problemas como motivação inicial para a apresentação e desenvolvimento de conceitos matemáticos tem sido apontada como uma estratégia de grande valor, despertando um interesse inicial por parte do aluno, induzindo seu envolvimento com o problema proposto e permitindo que ele se sinta desafiado e por sua própria experiência e habilidades desenvolva estratégias de resolução. A própria História da Matemática mostra que ela foi construída como resposta a perguntas provenientes de diferentes origens e contextos, motivadas por problemas de ordem prática (divisão de terras, cálculo de quantidade de produtos), por problemas vinculados a outras ciências como a *física, astronomia*, entre outras, bem como por problemas relacionados a investigações internas à própria *Matemática*.

1.3 A formação continuada do professor

A preparação do professor para enfrentar os questionamentos dos alunos também é um aspecto a ser considerado com o objetivo de melhorar o sistema de ensino. Tendo em vista o alto desenvolvimento tecnológico e as rápidas mudanças sociais e culturais que marcaram o final do século XX e início do século XXI, devemos considerar que a formação do professor, além de ser um requisito exigido por lei, deve ser continuada e contextualizada, considerando-se que a quantidade e diversidade de informações adquiridas pelo aluno são grandes. Esse amplo e rápido desenvolvimento do aluno acaba por de certo modo forçar o professor a se reorganizar, e atualizar tanto sua maneira de enxergar o seu corpo discente, quanto a sua forma de lecionar em um ambiente educacional altamente dinâmico, onde novas maneiras de aprender e ensinar chegam constantemente ao alcance da sociedade.

As deficiências no ensino da matemática brasileira possuem raízes em vários segmentos, este trabalho visa apresentar uma proposta de intervenção pedagógica que alcance os tópicos acima abordados. Obviamente não há aqui a pretenção de apresentar uma única ferramenta para a solução do problema, mas uma alternativa ao ensino que traga em seu escopo os aspectos mencionados, ou seja, mostrar que a matemática está presente no contexto social do aluno, trazer uma visão diferenciada do ensino para o professor aperfeiçoando assim sua atuação em sala de aula, proporcionar ao estudante uma visão mais ampla da matemática através do estudo da divisão euclidiana, afim de que se crie novas abordagens dos problemas a serem resolvidos, ampliando o sentido da operação de divisão de números inteiros, incentivando um olhar diferente, pois de modo geral os alunos são ensinados a observarem apenas o quociente de uma divisão euclidiana, porém, acreditamos que a análise de todo o processo de divisão e em especial o resto pode dar maior sentido e ampliar a visão do aluno sobre o universo dos números. Uma outra condição a ser atingida pelo estudo é a de extender propriedades dos números inteiros para o conjunto dos polinômios, que são elementos importantes no estudo da matemática, afim de oferecer novas ferramentas para a execução de operações e resolução de problemas que os envolvam. Acreditamos que a nível prático esse é um aspecto inicial para o processo de reversão do quadro insatisfatório da educação matemática atual.

Capítulo 2

O desenvolvimento das estruturas algébricas dos anéis

Considerando o elevado grau de organização e estruturação da matemática moderna, seria de bom alvitre, abordarmos inicialmente um pouco de sua história ao longo dos séculos, a fim de entender um pouco melhor seu processo de desenvolvimento. Para um estudo mais detalhado da história da matemática aconselho o leitor a pesquisar em (BOYER, 1974) que foi utilizada como referência desta seção.

2.1 Conhecendo um pouco da história da álgebra

As origens da matemática remontam a tempos antigos, as noções mais primitivas dos conceitos de números, grandezas e formas podem ser encontradas nos primeiros registros da humanidade, e vislumbres de conceitos matemáticos podem ser vistos em formas de vida que podem ter suas origens milhões de anos antes de os seres humanos povoarem a Terra. O desenvolvimento dos vários ramos da matemática percorreu um longo caminho, caminho esse que não pretendemos refazer aqui devido aos objetivos específicos deste trabalho, porém, intenciono dar através de uma abordagem sucinta maior sentido ao que iremos estudar, dando a oportunidade ao leitor de conhecer um pouco do contexto histórico dos desafios e dificuldades encontrados no caminho, e o

alto nível de comprometimento e dedicação das mentes que se ocuparam por anos à árdua tarefa de desvendar o até então desconhecido universo da aritmética e álgebra, tornando assim, o estudo deste trabalho mais interessante e completo.

Nações como Babilônia e Egito podem ser apontadas como originadoras dos conceitos de números e de expressões álgebricas, tais conceitos surgiram a partir de questões práticas cotidianas como, medições de áreas de regiões agrícolas para a cobrança de impostos, e a divisão de bens de consumo como pães, cevada e trigo. Porém à medida que as civilizações se desenvolviam e se organizavam, a necessidade de desenvolvimento da matemática se fazia cada vez mais presente. Assim, ao longo dos séculos outras nações se juntaram contribuindo para o desenvolvimento da matemática como conhecemos hoje.

Nesse percurso destacamos algumas contribuições dadas por civilizações como: Mesopotâmia (equações quadráticas e cúbicas), Grécia (números figurativos e proporções), em especial com Euclides (Teoria dos números e Os elementos), China e Índia (representação do zero, triângulo aritmético, divisão com resto), Arábia (números arábes, problemas algébricos) em especial al-Khowarizmi com o estudo das equações lineares e quadráticas, podendo ser reconhecido como o pai da álgebra, Europa na idade média (sequência de Fibonacci, Teoria dos números). Contudo, o desenvolvimento e estruturação da matemática se deu em um ritmo sem precedentes a partir do século XIX.

> "O século dezenove pode ser considerado como o século de maior desenvolvimento da matemática de todos os tempos, excetuando-se apenas a Grécia antiga no seu período mais produtivo, merecendo o título de idade áurea da matemática, por desenvolver propriedades e generalizações no campo da álgebra, com quantidade e qualidade sem precedentes, o que tornou a matemática a ferramenta poderosa que possuímos".(BOYER, 1974)

Podemos mencionar alguns nomes de destaque como George Peacock (1791 - 1858) um dos fundadores da *Analytical Society*, escola de estudos no *Trinity College*, Cambridge. Com o objetivo de reformar o ensino da matemática e a notação do cálculo, Peacock não produziu novos conhecimentos matemáticos mas seu trabalho foi marcado por implementar a ideia de reformular, estruturar e formalizar a álgebra na Inglaterra. Tendo como motivação a geometria de Euclides que continha tal estruturação formal.

Um apoio para as ideias de Peacock foi Augustus De Morgan (1806-1871) que juntos criaram o que ficou conhecida por *escola inglesa* de matemática. De Morgan nascera

na Índia, estudou e se graduou na Inglaterra, mas por motivos religiosos não conseguiu lugar de destaque em Cambridge ou Oxford. Porém, por ser um jovem de grande talento, aos vinte e dois anos tornou-se professor da recém criada Universidade de Londres. Apesar de possuir uma visão altamente filosófica sobre a matemática e seus símbolos, De Morgan acreditava que as propriedades da álgebra dos números inteiros (apesar da grande controvérsia existente na Ingraterra sobre os números negativos) poderia ser transferida para outro conjunto, o dos números complexos, que de maneira simplória ele acreditava seriam os dois únicos conjuntos possíveis na álgebra. Nesse ponto um outro nome se torna importante, Willian Rowan Hamilton (1805 - 1865), Hamilton ficou órfão sendo ainda menino, tendo sua tutela sob a responsabilidade de um tio. Possuia habilidade intelectual incomum, aos cinco anos de idade já lia grego, hebraico e latim, e aos dez anos já conhecia várias línguas orientais. Apesar de seu talento para a linguística, Hamilton nutria um interesse especial pela matemática, e bastou um econtro inusitado com um calculista da época para fazê-lo se decidir por ela.

Hamilton entrou no Trinity College Dublin, e ainda jovem, aos vinte e dois anos foi nomeado Royal astronomer na Irlanda, diretor do observatório de Dunsink e professor de astronomia. Hamilton acreditava na relação entre tempo e espaço, em uma ligação indissolúvel entre eles, quase que como uma antecipação das ideias de Einstein sobre a teoria da relatividade geral, porém, sua grande contribuição à álgebra se daria por extender propriedades. Seu problema motivador foi a multiplicação de números complexos representados por pares ordenados que ele acreditava ser entidades orientadas no plano. Quando procurou efetuar a operação no espaço, *n uplas* com n maior que dois encontrou dificuldades, pois a comutatividade da multiplicação de inteiros não lhe permitia concluir a operação com os complexos. Tal problema lhe exigiu mais de uma década de estudos até que em um parque, passeando com sua esposa, porém com os pensamentos imersos no universo matemático Hamilton percebeu que poderia desconsiderar a comutatividade da multiplicação, à semelhança do que fez Lobachevsk afim de criar uma nova geometria desconsiderando o postulado das paralelas. Hamilton deu origem às propriedades dos quatérnios. Assim Hamilton percebeu a liberdade que a matemática possui de criar álgebras fundamentadas e significativas sem a necessidade de se prender ao rigor primitivo de seus fundamentos. Deu então início ao desenvolvimento de uma nova era da álgebra, ampla e estruturada que proporcionou o grande desenvolvimento da matemática atual.

2.2 Uma abordagem sobre os anéis

Um anel é uma estrutura algébrica composta por três elementos: Um conjunto não vazio e duas operações, adição e multiplicação. Essas operações não são necessariamente a adição e multiplicação de números que conhecemos desde o início de nossos estudos na educação básica. Poderíamos, por exemplo, considerar o conjunto de todas as funções contínuas com domínio em um intervalo real, nossa adição aqui seria soma de funções e a multiplicação, multiplicação de funções. Porém nesse capítulo restringiremos nosso estudo aos conjuntos numéricos e as operações de adição e multiplicação serão as usuais de tais conjuntos. As informações aqui apresentadas tem como referências (GARCIA; LEQUAIN, 2001),(HERNSTEIN, 1970), (DOMINGUES; IEZZI, 2003) (BOYER, 1974).

Definição 2.2.1. *Dado um conjunto A não vazio, uma operação em A é uma função $* : A \times A \mapsto A$. A imagem desta função $*((x, y))$ aplicada em um par ordenado (x, y) pela função é denominado usualmente por $x * y$*

Definição 2.2.2. *Um conjunto não vazio A é dito um anel associativo se em A estão definidas duas operações, indicadas por $+$ e $\cdot$ respectivamente, tais que para todos a, b e c em A:*

1) $a + b$ está em A.

2) $a + b = b + a$.

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

4) Existência do elemento 0 em A, tal que $a + 0 = a$.

5) Existe o elemento $-a$ em A, tal que $a + (-a) = 0$.

6) $a \cdot b$ está em A.

7) $a \cdot (b + c) = a \cdot c + a \cdot b$ e $(b + c) \cdot a = a \cdot c + a \cdot b$.

8) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

   Denotaremos um anel por $(A, +, \cdot)$, ou quando não houver perigo de confusão, apenas por A. Além disso, para simplificação da escrita, a operação $a \cdot b$ será denotada por ab.

A propriedade (4) garante a existência de um elemento neutro para a adição. É imediato verificar que esse elemento é único e será chamado de zero e denotado por 0. De fato, se 0 e $0'$ são dois elementos neutros para a adição, temos $0 = 0+0' = 0$ onde na primeira igualdade usamos o fato de que $0'$ é elemento neutro, e na segunda, o fato de que 0 é elemento neutro.

Dado um elemento $x \in A$, a propriedade (5) garante a existência de um simétrico para x com respeito à adição, podemos verificar que esse simétrico é único. De fato, se y e y' são simétricos de x, então tem-se que, $y = y + 0 = y + (x + y')$ pois y' é simétrico de x. Assim, $y = (y + x) + y' = 0 + y'$, logo $y = y'$.

O elemento neutro da adição 0 possui a seguinte propriedade: $\forall x \in A$, tem-se que, $0 \cdot x = 0$. De fato, basta observar que $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, somando o simétrico $-(0 \cdot x)$ a ambos os membros teremos $0 = 0 \cdot x$

Se além das propriedades (1) a (8) citadas anteriormente, o anel possuir o elemento neutro da multiplicação, isto é,

9) Existe $e \in A$ tal que $\forall\ x \in$ A, $e \cdot x = x$ e $x \cdot e = x$, tal elemento será chamado unidade de elemento unidade de A, e A será chamado de *anel com unidade* ou *anel unitário*. O elemento neutro da multiplicação é único e ele será chamado de um e denotado por 1.

Se A possuir a seguinte propriedade:

10) Comutatividade de multiplicação $a \cdot b = b \cdot a\ \forall a, b \in A$, então, A será um anel comutativo ou abeliano.

Apresentaremos a seguir alguns tipos particulares de anéis importantes.

Exemplo 2.2.3. *O conjunto das matrizes de ordem 2 com coeficientes nos inteiros e com as operações usuais de soma e multiplicação de matrizes,* $(M_2(\mathbb{Z}), +, \cdot)$ *formam um anel com unidade*

$$1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

porém não comutativo, denominado anel das matrizes de ordem 2.

Exemplo 2.2.4. *O conjunto dos números inteiros com as operações usuais de soma e multiplicação de inteiros forma um anel comutativo denominado anel dos inteiros.*

Além disso, o conjunto dos números racionais com as operações usuais de soma e multiplicação formam um anel comutativo denominado anel dos racionais. $(\mathbb{Z}\ ,\ +\ ,\ \cdot)$ *e* $(\mathbb{Q}\ ,\ +\ ,\ \cdot)$*, ambos com unidade.*

Definição 2.2.5. *Seja A um anel comutativo com elemento unidade. Se para esse anel é válida a lei do cancelamento do produto, ou seja, se uma igualdade do tipo:*

$$a \cdot b = 0$$

em que a e $b \in A$, só for possível para

$$a = 0 \text{ ou } b = 0$$

então se diz que A é um anel de integridade ou domínio de integridade.

A contrapositiva dessa afirmação é a seguinte: Se $a \neq 0$ e $b \neq 0$ então, $a \cdot b \neq 0$. Alguns anéis de integridade são: $(\mathbb{Z}\ ,\ +\ ,\ \cdot)$, $(\mathbb{Q}\ ,\ +\ ,\ \cdot)$, $(\mathbb{R}\ ,\ +\ ,\ \cdot)$ e $(\mathbb{C}\ ,\ +\ ,\ \cdot)$

Definição 2.2.6. *Seja A um anel unitário, $a \in A$ é chamado inversível se existir $b \in A$ tal que $a \cdot b = b \cdot a = 1$, neste caso b é dito o inverso de a, e o denotaremos $b = a^{-1}$.*

Definição 2.2.7. *Chamamos de corpo a todo anel comutativo, com identidade A, onde todo $x \in A$ com $x \neq 0$ existe $x^{-1} \in A$, ou seja, um corpo é um anel comutativo com unidade, onde todo elemento não nulo é inversível.*

2.3 Ideais

Sejam A um anel e B um subconjunto não vazio de A. Diremos que B é um *subanel* de A, se:

1) Dados quaisquer $a, b, \in B; a - b \in B$; onde $a - b = a + (-b)$,

2) Dados quaisquer $a, b \in B$, $a \cdot b \in B$.

Podemos observar que a definição de subanel é equivalente a afirmar que o conjunto B, munido das operações de A restritas a B, é um anel. Ou seja, um subanel é um anel dentro de outro anel.

Podemos mencionar alguns subanéis: $\mathbb{Z}$ é um subanel de $\mathbb{Q}$; $\mathbb{Q}$ é um subanel de $\mathbb{R}$; $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$, pois se tomarmos $2m$ e $2n \in \mathbb{Z}$ teremos, $2m-2n = 2\cdot(m-n) \in 2\mathbb{Z}$; o conjunto dos números ímpares $\{2k + 1,\ k \in \mathbb{Z}\}$, não é um subanel de $\mathbb{Z}$. De fato, note que 1, 3 $\in B$, mas 3 - 1 = 2 $\notin$ B .

Definição 2.3.1. *Seja A um anel comutativo, um subconjunto não vazio B de A será chamado um ideal de A, se, para quaisquer x e $y \in B$ e para qualquer $a \in A$, verificarem-se as seguintes relações:*

1) $x - y \in B$;

2) $a \cdot x \in B$.

Observe que todo ideal é um subanel de A. Além disso, se A é um anel, então $\{0\}$ e o próprio A são ideais de A . São chamados de *ideais triviais* do anel.

Exemplo 2.3.2. *No anel dos inteiros $\mathbb{Z}$, são ideais os subconjuntos $n\mathbb{Z} = \{0, \pm n, \pm 2n, ...\}$, qualquer que seja o inteiro n. De fato:*

Se x e $y \in n\mathbb{Z}$, então $x = rn$ e $y = sn$ para convenientes inteiros r e s. Logo $x - y = rn - sn = (r - s)n$, em que $r - s$ é inteiro. De onde, $x - y \in n\mathbb{Z}$.

Sejam $a \in \mathbb{Z}$ e $x \in n\mathbb{Z}$; então $x = nq(q \in \mathbb{Z})$ e, portanto, $ax = a(nq) = (aq)n$, em que aq é inteiro, o que mostra que $ax \in n\mathbb{Z}$.

Proposição 1. *Considere I um ideal de A. Se I contém algum elemento inversível de A, então $I = A$.*

Demonstração. Temos que $I \subset A$, pois é um ideal de A, devemos então mostrar que $A \subset I$.

Tomando $x \in I$ um elemento inversível de A. Dado qualquer $a \in A$, $a \cdot x^{-1} \in A$, como I é um ideal, $(a \cdot x^{-1}) \cdot x \in I$, logo, $a \cdot (x \cdot x^{-1}) \in I$,então $a \in I$. Portanto, $A \subset I$. □

Definição 2.3.3. *Um ideal M de A com $M \neq A$ é chamado de ideal maximal se para todo ideal I tal que $M \subsetneq I \subset A$, temos que $I = A$.*

Exemplo 2.3.4. *Seja o anel $A = \mathbb{Z}$ e o ideal $I = 2\mathbb{Z}$, se J for um ideal diferente de I e que contém I, então, contém algum número ímpar da forma $x = 2n + 1, n \in \mathbb{Z}$ em J. Como $2n$ é um elemento de I, temos que $1 = (x - 2n)$ está em J, o que pela proposição 2.3.1 nos leva à conclusão de que $J = A$. Portanto, I é ideal maximal.*

2.4 Relações de Equivalência

O conceito de relações e classes de equivalência será fundamental para o nosso trabalho, pois trará propriedades importantes das relações entre conjuntos, por esse motivo

nesta seção faremos uma abordagem desse tema com algumas definições e propriedades importantes. Trabalharemos com a noção intuitiva de conjuntos numéricos e as propriedades básicas de suas operações, que posteriormente serão estendidas para outros conjuntos que assumem características similares. As referências que fundamentam a elaboração dessa seção estão em e .

Dentro do contexto da matemática os motivos das relações são geralmente denominados de operações, e os subgrupos como subconjuntos ou conjunto das partes. As definições a serguir apresentam com mais rigor tais ideias.

Definição 2.4.1. *Seja um conjunto A, será denominado conjunto das partes de A, e denotado por $P(A)$, o conjunto $P(A)$, tal que os seus elementos são todos os subconjuntos de A.*

Exemplo 2.4.2. .

1) Se $A = \{a, b\}$, então $P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \}$;

2) Se $A = \{1, 2, 3\}$, então $P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$;

3) Se $A = \emptyset$, então $P(A) = \{\emptyset\}$, pois o único subconjunto de A é o $\emptyset$.

Definição 2.4.3. *Dados dois conjuntos A e B não vazios, o produto cartesiano de A por B será o conjunto de todos os pares ordenados (a, b) tais que $a \in A$ e $b \in B$, $A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}$.*

Exemplo 2.4.4. *Se $A = \{a, b\}$ e $B = \{c, d, e\}$ então,*
$A \times B = \{(a, c), (a, d), (a, e), (b, c), (b, d), (b, e)\}$
$B \times A = \{(c, a), (c, b), (d, a), (d, b), (e, a), (e, b)\}$

Definição 2.4.5. *Uma relação binária R em um conjunto A é qualquer subconjunto do produto cartesiano $A \times A$, isto é, $R \subset A \times A$.*

Do mesmo modo, dados dois conjuntos A e B com, $A \neq B$, uma relação R entre os conjuntos A e B, será qualquer subconjunto de $A \times B$.

Exemplo 2.4.6. *Se $A = \{a, b, c\}$, tem-se que $A \times A = \{(a, a), (a, b), (a, c),$ $(b, a), (b, b), (b, c), (c, a); (c, b); (c, c)\}$, então $R = \{(a, a), (b, a), (c, b), (c, a)\}$ é uma relação em A.*

No contexto deste trabalho, denotaremos que o elemento $x \in A$ está relacionado com o elemento $y \in A$ por xRy, ou o equivalente a dizer que o par $(x, y) \in R$.

Seja R uma relação em A diremos que R é:

1) *Reflexiva:* Se a se relaciona com a. aRa, $\forall a \in A$;

2) *Simétrica:* Para $a, b \in A$, se a se relaciona com b, tem-se a relação de b com a. aRb, implica bRa;

3) *Transitiva:* Para a, b e $c \in A$, se a se relaciona com b e, b se relaciona com c, tem-se que a se relaciona com c. aRb e bRc, implica aRc;

4) *Antissimétrica:* Para $a, b \in A$, se a se relaciona com b, e b se relaciona com a, tem-se que a é igual a b. aRb e bRa, implica $a = b$.

Uma relação binária R sobre um determinado conjunto A, pode ser caracterizada pelas propriedades acima citadas que ela possuir.

Definição 2.4.7. *Seja R uma relação sobre A. R é dita uma relação de ordem sempre que for simultâneamente, reflexiva, antissimétrica e transitiva.*

Exemplo 2.4.8. *Seja R a relação menor que $(\leq)$ sobre o conjunto dos números inteiros, então R é:*

1) Reflexiva, pois, $\forall x \in \mathbb{Z}$, tem-se que $x \leq x$;

2) Antissimétrica, pois, $\forall x$ e $y \in \mathbb{Z}$, tem-se que, se $x \leq y$ teremos $y \geq x$ nesse caso xRy e yRx se,e somente se, $x = y$;

3) Transitiva, pois, $\forall x, y$ e $z \in \mathbb{Z}$ tem-se que, se $x \leq y$ e $y \leq z$, então $x \leq z$.

Observe que a relação R é uma relação de ordem sobre o conjunto dos números inteiros.

Definição 2.4.9. *Seja R uma relação sobre A. R é dita uma relação de equivalência sempre que for simultâneamente, reflexiva, simétrica e transitiva.*

Exemplo 2.4.10. *Seja T o conjunto de todos os triângulos de um plano. Considere a relação de semelhança de triângulos $S = \{(x, y) \in T \times T; x \sim y\}$, então S é:*

1) Reflexiva, pois, qualquer triângulo é semelhante a si mesmo, logo $\forall x \in T$, tem-se que $x \sim x$;

2) Simétrica, pois, se um triângulo x é semelhante a um triângulo y, tem-se que y é semelhante a x, ou seja, $\forall x, y \in T$, tem-se que $x \sim y$ implica $y \sim x$;

3) Transitiva, pois, tomados três triângulos, x, y e z, se, x é semelhante a y e y é semelhante a z, tem-se que x é semelhante a z, ou seja, $\forall x, y, z \in T$, tem-se que $x \sim y$ e $y \sim z$ implica $x \sim z$.

Observe que S é uma relação de equivalência sobre o conjunto T.

Definição 2.4.11. *Seja R uma relação de equivalência em um conjunto A e a um elemento arbitrário qualquer de A. Denomina-se classe de equivalência de a pela relação R, ao conjunto $\overline{a} = \{x \in A \mid xRa\}$. Ou seja, $\overline{a}$ é o conjunto formado por todos os elementos de A que estão relacionados com a.*

Exemplo 2.4.12. *Seja $\mathbb{Z}$ o conjunto dos números inteiros e consideremos R a relação de divisão destes inteiros por 4 deixando resto 0 e 1, ou seja, $R = \{x \in \mathbb{Z} | x = 4k$ e $x = 4k + 1, k \in \mathbb{Z}\}$. Vamos determinar o conjunto de todos os elementos de R.*

Os números que deixam resto 0 são todos os múltiplos de 4, ou seja, os números da forma $4k$, $k \in \mathbb{Z}$. Logo $\overline{0} = \{..., -12, -8, -4, 0, 4, 8, 12, ...\}$.

Os números que deixam resto 1 são todos os múltiplos de 4 mais 1, ou seja, os números da forma $4k + 1$, $k\mathbb{Z}$. Logo $\overline{1} = \{..., -11, -7, -3, 1, 5, 9, 13,$
$...\}$.

O teorema a seguir mostra que as classes de equivalência de dois elementos de um conjunto A são idênticas ou disjuntas, além disso fornece a confirmação de que todo elemento de uma classe de equivalência $\overline{a}$ possui a mesma classe de equivalência de a, ou o equivalente a dizer que $\overline{a}$ pode ser representado por $\overline{x}$, para todo $x \in \overline{a}$.

Teorema 2.4.13. *Seja R uma relação de equivalência sobre um conjunto A, se, a e b são elementos quaisquer de A, então as declarações a seguir são equivalentes:*

1) $a \in \overline{a}$;

2) $\overline{a} = \overline{b} \Leftrightarrow aRb$;

3) $\overline{a} \neq \overline{b} \Leftrightarrow \overline{a} \cap \overline{b} = \emptyset$

Demonstração. 1) $\overline{a} = \{x \in A | xRa\}$ Como R é uma relação de equivalência, aRa (pela propriedade reflexiva), logo $a \in \overline{a}$.

2) Seja $x \in \bar{a}$, então xRa, como por hipótese aRb, segue da propriedade transitiva que xRb, assim $x \in \overline{b}$ e $\bar{a} \subset \overline{b}$.

   Por outro lado se, $b \in \overline{b}$. Por hipótese, aRb sendo R uma relação de equivalência, temos que bRa, portanto $b \in \overline{a}$. Logo, $\overline{b} \subset \overline{a}$.

3) Se, $\overline{a} \neq \overline{b}$, onde $\overline{a} = \{x \in A | xRa\}$ e $\overline{b} = \{y \in A | yRb\}$. Suponhamos por contradição que exista $c \in \overline{a} \cap \overline{b}$, ou seja, $c \in \overline{a}$ e $c \in \overline{b}$. Sendo assim, cRa e cRb, o que pela propriedade transitiva nos garante que aRb. Assim por (ii) temos que $\overline{a} = \overline{b}$, o que gera uma contradição com a hipótese. Portanto, $\overline{a} \cap \overline{b} = \emptyset$

   Reciprocamente suponha, $\overline{a} \cap \overline{b} = \emptyset$. Suponhamos aRb o que por (ii) garante que $\overline{a} = \overline{b}$, ou seja, $a \in \overline{b}$. É certo que $a \in \overline{a}$, sendo assim, a está em $\overline{a}$ e a está em $\overline{b}$ o que contradiz a hipótese de que $\overline{a} \cap \overline{b} = \emptyset$. Portanto $\overline{a} \neq \overline{b}$.

□

Exemplo 2.4.14. *Seja uma relação R sobre o conjunto dos números inteiros, dada por aRb sempre que o resto da divisão de a e b por 2 forem iguais, ou seja, $(5, 21)$ pertence a R, $(6, 14)$ pertence a R, mas $(7, 12)$ não pertence a R.*

Vamos verificar que R é uma relação de equivalência. De fato,

1) R é reflexiva, pois, $\forall x \in \mathbb{Z}$, tem-se que a divisão de x por 2 deixa resto r e é evidente que $r = r$, logo, xRx.

2) R é simétrica, tomando $x, y \in \mathbb{Z}$, se xRy, então x e y deixam o mesmo resto na divisão por 2, logo yRx.

3) R é transitiva, sejam $x, y, z \in \mathbb{Z}$, se xRy, então x e y deixam o mesmo resto t na divisão por 2, e se yRz, tem-se que y e z deixam o mesmo resto s na divisão por 2. Como t e s são os restos de y na divisão por 2, concluímos que $t = s$, portanto, xRz.

Como os restos da divisão de um número inteiro por 2 são 0 e 1, podemos representar as classes de equivalência da seguinte forma:
$\overline{0} = \{..., -4, -2, 0, 2, 4, ...\} = \overline{-2} = \overline{4}$,

$\overline{1} = \{..., -3, -1, 1, 3, 5, ...\} = \overline{-1} = \overline{5}$,
ou seja, a classe de equivalência pode ser representada por qualquer elemento do conjunto.

2.5 Anéis Quocientes

Nessa seção abordaremos de maneira simplificada os conceitos básicos de anel quociente, definindo as operações de adição e multiplicação que são características dos anéis. Omitiremos as expressões classes laterais à direita e à esquerda, considerando que trataremos de anéis comutativos. Deixamos para o leitor interessado em maiores detalhes as referências em e .

Definimos uma relação de equivalência dentro de um anel A por: Para $\forall a, b \in A$ temos que aRb se $a - b \in I$, onde I é um ideal (fixo) de A. Assim, tem-se que R é uma relação de equivalência e a classe de equivalência de um elemento de A é denotada por $\bar{a} = a + I$. Quando consideramos uma relação de equivalência ($\sim$) sobre um conjunto A podemos definir o conjunto quociente $A/\sim$ que é o conjunto de todas as classes de equivalência dos elementos de A; Assim, $A/\sim = \{\bar{a} : a \in A\}$. Dependendo da relação de equivalência podemos definir uma estrutura de anel dentro desse conjunto, neste caso o conjunto quociente será denominado de anel quociente.

Sabendo que no conjunto quociente dois elementos são iguais, se pertencem à mesma classe de equivalência, ou seja, se $a, b \in A$ tem-se que $a = b$, se a e $b \in \overline{x}$ onde $\overline{x}$ é uma classe de equivalência do anel A, para provar que A/I é um anel vamos verificar que valem as propriedades que definem um anel.
Sejam $a, b, c \in A$ e I o ideal em A, denotaremos por $X = a + I$ e $Y = b + I$ e $Z = c + I$.

Adição

Definimos a adição da seguinte forma: $(a + I) + (b + I) = (a + b) + I$.

A1) *Comutatividade da soma*
Sejam $X + Y = (a + I) + (b + I) = (a + b) + I$ e $Y + X = (b + I) + (a + I) = (b + a) + I = (a + b) + I$.

A2) *Associatividade.*
$X + (Y + Z) = (a + I) + [(b + I) + (c + I)] = (a + I) + [(b + c) + I] = (a + b + c) + I$.

$(X+Y)+Z = [(a+I)+(b+I)]+(c+I) = [(a+b)+I]+(c+I) = (a+b+c)+I.$

A3) *Elemento neutro*
Considere $e = 0+I$, onde 0 é o elemento neutro de A, $X+e = (a+I)+(0+I) = (a+0)+I = a+I = X$.

A4) *Simétrico*
Considere $X = a+I$, onde $a \in A$, como A é um anel segue que existe o simétrico de a, $-a \in A$. Afirmamos que $-X = -a+I$ é o simétrico de X. De fato, temos que $X+(-X) = (a+I)+(-a+I) = a+(-a)+I = 0+I = e$

Afim de verificar as demais propriedades precisamos definir a operação de multiplicação. Para tal podemos proceder de maneira natural propondo que, $(a+I)(b+I) = (ab+I)$. No entanto, precisamos ter certeza de que isto tem significado. Em outras palavras temos que provar que se $a+I = a'+I$ e $b+I = b'+I$, então, com relação à nossa definição de multiplicação, $(a+I)(b+I) = (a'+I)(b'+I)$. De modo equivalente, precisa ser estabelecido que $ab+I = a'b'+I$. Com essa finalidade observamos primeiramente que, como $a+I = a'+I$, $a = a'+u_1$ onde, $u_1 \in I$; analogamente, $b = b'+u_2$ onde $u_2 \in I$. Mas então $ab = (a'+u_1)(b'+u_2) = a'b'+u_1b'+a'u_2+u_1u_2$; como I é um ideal de A, $u_1b' \in I, a'u_2 \in I$ e $u_1u_2 \in I$. Consequentemente, $u_1b'+a'u_2+u_1u_2 = u_3 \in I$. Mas então, $ab = a'b'+u_3$, donde deduzimos que $ab+I = a'b'+u_3+I$. O resultado de tudo isso é que $ab+I = a'b'+I$. Uma vez definida a multiplicação podemos verificar as demais propriedades afim de mostrar que A/I é um anel.

M1) *Distributividade à direita*
$(X+Y)Z = ((a+I)+(b+I))(c+I) = ((a+b)+I)(c+I) = (a+b)c+I = ac+bc+I = (ac+I)+(bc+I) = (a+I)(c+I)+(b+I)(c+I) = XZ+YZ$

M2) *Distributividade à esquerda*
$Z(X+Y) = (c+I)((a+I)+(b+I)) = (c+I)((a+b)+I) = c(a+b)+I = ca+cb+I = ac+bc+I = (ac+I)+(bc+I) = (a+I)(c+I)+(b+I)(c+I) = XZ+YZ.$

M3) *Associatividade da multiplicação*
$X(YZ) = (a+I)((b+I)(c+I)) = (a+I)(bc+I) = abc+I$
$(XY)Z = ((a+I)(b+I))(c+I) = (ab+I)(c+I) = abc+I$

A/I é agora um anel. Evidentemente, se A é comutativo, então A/I também o é, pois $(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I)$. (A recíproca porém não é verdadeira). Além disso, A possui o elemento unidade 1, então A/I possui um elemento unidade $1+I$.

Assim, estamos em condições de definir o conceito de anel quocinte como é visto na definição abaixo.

Definição 2.5.1. *Sejam A um anel comutativo e, I um ideal de A. Definimos o anel quociente de A por I, dadas as operações de adição e multiplicação acima demonstradas e definidas como, $\forall a, b \in A, x \in I$;*

Adição $(a+x)+(b+x) = (a+b)+x$.

Multiplicação $(a+x)\cdot(b+x) = (a\cdot b)+x$.

$A/I = \{a+x | a \in A \text{ e } x \in I\}$ *ou o equivalente* $A/I = \{\overline{a} \mid a \in A\}$ *onde,* $\overline{a} = a+x$

Exemplo 2.5.2. *Considere $A = \mathbb{Z}$ e $I = 5\mathbb{Z}$. Vamos construir o anel quociente $A/I = \mathbb{Z}/5\mathbb{Z}$.*

Consideremos o anel $5\mathbb{Z}$ como $\{5k \text{ |k} \in \mathbb{Z}\}$, temos que $\mathbb{Z}/5\mathbb{Z} = \{a+5k, a \in \mathbb{Z}\}$ tomando,

$a = 0$ tem-se $0+5k = \{..., -10, -5, 0, 5, 10, ...\} = I$

$a = 1$ tem-se $1+5k = \{..., -9, -4, 1, 6, 11, ...\}$

$a = 2$ tem-se $2+5k = \{..., -8, -3, 2, 7, 12, ...\}$

$a = 3$ tem-se $3+5k = \{..., -7, -2, 3, 8, 13, ...\}$

$a = 4$ tem-se $4+5k = \{..., -6, -1, 4, 9, 14, ...\}$

$a = 5$ tem-se $5+5k = \{..., -10, -5, 0, 5, 10, ...\} = I$

Note que, quando $k = 0$ e $k = 5$, os elementos se repetem, então os valores de a seguem um ciclo de $a = 0$ até $a = 4$, portanto o anel quociente é tal que,

$\mathbb{Z}/5\mathbb{Z}$ =$\{0 + 5k, 1 + 5k, 2 + 5k, 3 + 5k, 4 + 5k\}$ ou ainda, $\mathbb{Z}/5\mathbb{Z}$ =$\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

dessa forma $5\mathbb{Z}$ representa o anel dos números inteiros módulo 5, ou em símbolos, $\mathbb{Z}_5$.

2.6 Congruência Modular

Antes de iniciarmos esta seção, enunciaremos suscintamente o conceito de divisão euclidiana no conjunto $\mathbb{Z}$ dos números inteiros. Dados dois números inteiros positivos a

e b $a < b$, existe um único par (q, r) de números inteiros não negativos de forma que, $b = a \cdot q + r$, $0 \leq r <\mid a \mid$, onde os números b, a, q e r são chamados de *dividendo*, *divisor*, *quociente* e *resto*, respectivamente, da divisão de b por a. Tomando como exemplos os inteiros 9 e 4, temos que $9 = 4 \cdot 2 + 1$ onde, os números $9, 4, 2$ e 1 são o dividendo, divisor, quociente e o resto respectivamente. Assim, podemos abordar o tema da congruência modular como veremos a seguir.

Dado um número natural m. Dizemos que dois inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m forem iguais, ou o equivalente, a é congruênte a b módulo m se, $m|a - b$, $(mdividea - b)$ e escrevemos da seguinte forma:

$$a \equiv b \bmod m$$

A congruência módulo m é muito útil em problemas de divisibilidade no conjunto dos inteiros por ser uma relação de equivalência. Podendo-se estabelecer as seguintes propriedades fundamentais.

Proposição 2. *Sejam $m \in \mathbb{N}, a, b, c, d \in \mathbb{Z}$, dada a congruência modular $a \equiv b$ mod m, valem as seguintes propriedades:*

1) Reflexiva;
2) Simétrica;
3) Transitiva;
4) Soma e subtração membro a membro;
5) Produto membro a membro;
6) Lei do cancelamento;
7) Potência com expoente natural.

.

Demonstração.

1) Tem-se que, $m \mid a - a$ logo, $a \equiv a \bmod m$.
2) Sabendo que $m \mid a - b = -(b - a)$ segue que $a \equiv b \bmod m$ e $b \equiv a \bmod m$.

3) Se $m \mid a-b$ e $m \mid b-c$, então $m \mid (a-b)+(b-c)$ o que implica $m \mid a-c$ logo, se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$.

4) Suponha que $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $m \mid a-b$ e $m \mid c-d$ logo,$m \mid (a+c)-(b+d)$ portanto, $a \pm c \equiv b \pm d \bmod m$. O caso da subtração segue analogamente.

5) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, temos que $m \mid (b-a)+(d-c)$ isso implica $m \mid d(b-a)+a(d-c)$ logo, $m \mid ac-bd$ portanto, $ac \equiv bd \bmod m$.

6) Suponhamos que $ac \equiv bc \bmod m$ e $mdc(c,m)=1$ então, $m \mid ac-bc=c(a-b)$ logo, $m \mid a-b$ portanto, $a \equiv b \bmod m$.

7) Demonstraremos esta propriedade por indução matemática.

Suponha que $a \equiv b \bmod m$, tem-se que para o menor n natural é válida a congruência $a^1 \equiv b^1 \bmod m$. Suponhamos que é verdadeira a congruência $a^n \equiv b^n \bmod m$. Mostraremos que é válida para, $a^{n+1} \equiv b^{n+1} \bmod m$. Pelo item v temos que $a^1 \cdot a^n \equiv b^1 \cdot b^n \bmod m$. Portanto, $a^{n+1} \equiv b^{n+1} \bmod m$. □

2.7 Os anéis $\mathbf{Z}_n$

Nesta seção é feita a apresentação do anel dos inteiros módulo n, ou $\mathbb{Z}_n$, que são anéis quocientes dos inteiros módulo um natural n.Para um estudo mais detalhado ver (JANESCH; TANEJA, 2011).

Considerando a relação de congruência $a \equiv b \bmod$ n em $\mathbb{Z}$, define-se como classe de equivalência de a o conjunto

$$\overline{a} = \{b \in \mathbb{Z}; b \equiv a \bmod n\}.$$

Dado $b \in \mathbb{Z}$;

$$b \in \overline{a} \Leftrightarrow b \equiv a \bmod n$$

$$\Leftrightarrow n \mid (b-a)$$

$$\Leftrightarrow nx \mid (b-a), \text{ para algum } x \in \mathbb{Z}$$

$$\Leftrightarrow b = a + nx,\ x \in \mathbb{Z}.$$

Portanto $\overline{a} = \{a+nx; x \in \mathbb{Z}\}$, isto é $\overline{a}$ é o conjunto dos múltiplos de n somados com a. Sendo assim,

$$\overline{a} = a + n\mathbb{Z} = a + nx,\ x \in \mathbb{Z}.$$

Lema 2.7.1. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, $n \geq 2$ as seguintes afirmações são equivalentes:*

1) $\overline{a} = \overline{b}$.

2) $a \equiv b \ mod\ n$.

Demonstração. $1 \Rightarrow 2$. Pela propriedade reflexiva, $a \equiv a \mod n$, então $a \in \overline{a} = \overline{b}$. Segue que $a \in \overline{b}$, e pela definição de $\overline{b}$ tem-se que $a \equiv b \mod n$.

$2 \Rightarrow 1$. Para demonstrar esta parte devemos mostrar que os conjuntos $\overline{a}$ e $\overline{b}$ são iguais. Para isso provaremos que $\overline{a} \subseteq b$. A inclusão contrária segue de forma análoga.

Seja $x \in \overline{a}$ então, $x \equiv a \mod n$. Por hipótese, $a \equiv b \mod n$, e pela propriedade transitiva, segue que $x \equiv b \mod n$. Portanto, $x \in \overline{b}$. □

Proposição 3. *Para cada $n \in \mathbb{N}, n \geq 2$ temos que $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots \overline{n-1}\}$ é um conjunto com exatamente n elementos.*

Demonstração. Sendo $\mathbb{Z}_n$ o anel quociente de $\mathbb{Z}$ por n tem-se que; $\{\overline{0}, \overline{1}, \cdots \overline{n-1}\} \subseteq \mathbb{Z}_n$. Temos que mostrar a inclusão contrária, para isso, tome $\overline{a} \in \mathbb{Z}_{\ltimes}$ como a é um número inteiro e n é um número natural maior ou igual a 2, podemos dividir a por n obtendo um quociente q inteiro e um resto r natural. Assim,

$$a = nq + r, 0 \leq r < n.$$

Logo,

$$a - r = nq$$

o que implica,

$$a \equiv r \mod n.$$

Pelo lema 2.7.1 tem-se que, $\overline{a} = \overline{r}$. Sabe-se que $r \in \{0, 1, \cdots n-1\}$ logo, $\overline{a} = \overline{r} = \{\overline{0}, \overline{1}, \cdots \overline{n-1}\}$.

Para mostrar que $\mathbb{Z}_n$ possui exatamente n elementos, devemos mostrar que os elementos de $\{\overline{0}, \overline{1}, \cdots \overline{n-1}\}$ são distintos dois a dois. Suponha que isto não é verdade, ou seja, existem x e y pertencentes a $\{0, 1, \cdots n-1\}$ com $x \neq y$ e $\overline{x} = \overline{y}$. Sem perda de generalidade podemos assumir que $x < y$. Como $\overline{x} = \overline{y}$ temos que $x \equiv y \mod n$ logo, $n \mid y - x$ o que é impossível pois $0 < y - x < n$. Portanto, $x = y$ e os elementos de $\{\overline{0}, \overline{1}, \cdots \overline{n-1}\}$ são distintos dois a dois. □

Para mostrar que $\mathbb{Z}_n$ é um anel devemos definir as operações de adição e multiplicação, considerando que os elementos de $\mathbb{Z}_n$ são classes de equivalência, devem ser definidas de forma que seus resultados não dependam da escolha dos elementos de cada classe. Sendo assim,

1) $\overline{a} + \overline{b} = \overline{a+b}$

2) $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Proposição 4. *As operações* 1 *e* 2 *estão bem definidas isto é,* $a, b, x, y \in \mathbb{Z}, \overline{a} = \overline{x}$ *e* $\overline{b} = \overline{y}$ *implica* $\overline{a} + \overline{b} = \overline{x} + \overline{y}$ *e* $\overline{a} \cdot \overline{b} = \overline{x} \cdot \overline{y}$.

Demonstração. Pela proposição 2.6.1 temos que: $a \equiv x \bmod n$ e $b \equiv y \bmod n$ então, $a + b \equiv x + y \bmod n$ e $a \cdot b \equiv x \cdot y \bmod n$.

Pelo lema 2.7.1 segue que: $\overline{a+b} = \overline{x+y}$ e $\overline{a \cdot b} = \overline{x \cdot y}$.
Assim, $\overline{a} + \overline{b} = \overline{x} + \overline{y}$ □

Proposição 5. $(\mathbb{Z}_n, +, \cdot)$ *é anel comutativo com unidade.*

Demonstração. Sejam $a, b, c \in \mathbb{Z}_n$

1) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$.
   $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$, na segunda igualdade usamos a comutatividade dos inteiros.

2) $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$.
   $\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{(b+c)} = \overline{a + (b+c)} = \overline{(a+b) + c} = \overline{(a+b)} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}$.

3) Elemento neutro.
   Dado $\overline{a} \in \mathbb{Z}_n$, tem-se que $a \in \mathbb{Z}$. Sabe-se também que $0 \in \mathbb{Z}$ e $0 + a = a + 0 = a$.
   Então, $\overline{a} = \overline{a+0} = \overline{a} + \overline{0}$ e $\overline{a} = \overline{0+a} = \overline{0} + \overline{a}$,
   isto é, $\overline{0}$ é o elemento neutro de $\mathbb{Z}_n$.

4) Elemento simétrico.
   Dado $\overline{a} \in \mathbb{Z}_n$, tem-se que $a \in \mathbb{Z}$. Sabe-se também que $-a \in \mathbb{Z}$ e $a + (-a) = (-a) + a = 0$. Então, $\overline{0} = \overline{(-a) + a} = \overline{(-a)} + \overline{a}$ e $\overline{0} = \overline{a - a} = \overline{a + (-a)}$ isto é, $\overline{(-a)}$ é o simétrico de $\overline{a}$.

5) $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.
   $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{(b \cdot c)} = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = \overline{(a \cdot b)} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.

6) $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$ e $(\overline{a} + \overline{b}) \cdot \overline{c} = \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c}$.
$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{(b + c)} = \overline{a \cdot (b + c)} = \overline{a \cdot b + a \cdot c} = \overline{a \cdot b} + \overline{a \cdot c} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.
A outra igualdade é análoga.

7) $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$.
$\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{b \cdot a} = \overline{b} \cdot \overline{a}$.

8) Unidade.
Dado $\overline{a} \in \mathbb{Z}_n$, temos que $a \in \mathbb{Z}$. Como $1 \in \mathbb{Z}$ e $a \cdot 1 = 1 \cdot a = a$ tem-se que,
$\overline{a} = \overline{1 \cdot a} = \overline{1} \cdot \overline{a}$ e $\overline{a} = \overline{a1} = \overline{a} \cdot \overline{1}$.
Portanto, $\overline{1}$ é a unidade em $\mathbb{Z}_n$.

Assim mostramos que $\mathbb{Z}_n$ é um anel com unidade.

□

Apresentamos uma suscinta abordagem da aritmética modular no conjunto dos números inteiros, tendo em vista nosso objetivo de apresentar uma proposta junto aos professores da educação básica, passaremos no próximo capítulo para o estudo dos polinômios que será de grande valor para o enriquecimento da experiência de professores e alunos na sala de aula.

Capítulo 3

Anel de polinômios

3.1 Nota histórica

Como vimos anteriormente, o início do século XIX foi marcado pelo rápido e amplo desenvolvimento da álgebra. Nomes importantes como Hamilton e Peacock contribuíram para essa revolução das estruturas algébricas. No entanto ainda nos séculos I e II da nossa era, o matemático grego Diofanto já havia introduzido, mesmo que sem grandes avanços posteriores, símbolos para indicar uma variável e suas potências dentro de uma equação algébrica. Mais tarde, no início do século XVI, houve outro avanço significativo com a descoberta de fórmulas de resolução para equações do terceiro e quarto grau, no entanto, os raciocínios utilizados eram em grande parte verbais e ainda vinculados à geometria. Porém essa visão seria radicalmente transformada com a contribuição do francês François Viète, que em 1591 introduziu a linguagem de fórmulas, o que tornou possível pela primeira vez na história escrever genericamente uma expressão algébrica como uma equação do segundo grau, mas, a linguagem de Viète ainda não era precisa e clara, então não atingiu maiores progressos. Alguns anos depois René Decartes também daria sua contribuição nesse sentido, apesar de não expressar grande preocupação com enunciados e formalismos teóricos, Decartes introduziu a notação algébrica que utilizamos hoje, representando as variáveis pelas letras x, y, z e as constantes por a, b, c, etc, bem como a notação de potência que conhecemos.

Tais contribuições foram fundamentais para a elaboração dos conceitos de polinômios e suas propriedades, bem como para o sucesso das profundas transformações e

estruturação algébrica ocorrida durante o século XIX.

Nos tópicos deste Capítulo é feita uma abordagem mais detalhada e aprofundada, com o propósito de enriquecer o conhecimento do professor. (DOMINGUES; IEZZI, 2003), (BOYER, 1974)

3.2 Construindo o anel

A construção feita neste capítulo tem por referência (GARCIA; LEQUAIN, 2001).

Dado um anel A, dizemos que a sequência $(a_0, a_1, \cdots, a_n, \cdots)$ é um polinômio numa variável em A, onde $a_i \in A$ e $a_i \neq 0$ para um número finito de índices. Denotaremos por $P[X]$ o conjunto dos polinômios na variável x em A.

Definição 3.2.1. *Dois polinômios são iguais se, e somente se, seus termos correspondentes forem iguais, ou seja* $p = (a_0, a_1, a_2, \cdots)$ *é igual a* $q = (b_0, b_1, b_2, \cdots)$ *se,* $a_i = b_i$ $\forall i \geq 0$.

Definição 3.2.2. *A adição de polinômios será denotada por* $\oplus$ *e defnida da seguinte forma:*

$(a_0, a_1, \cdots) \oplus (b_0, b_1, \cdots) = (a_o + b_0, a_1 + b_1, \cdots)$

Definição 3.2.3. *A multiplicação de polinômios será denotada por* $\odot$ *e definida da seguinte forma:*

$(a_0, a_1, \cdots) \odot (b_0, b_1, \cdots) = (c_o, c_1, \cdots)$.

Onde,

$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0$$
$$\vdots$$
$$c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0$$
$$\vdots$$

Seja o anel $(A, +, \cdot)$ comutativo com unidade 1_A, mostraremos que o conjunto $P[X]$ com as operações $\oplus$ e $\odot$ anteriormente definidas, também é um anel comutativo com unidade, provaremos que $P[X]$ satisfaz todas as propriedades de anel demonstradas a seguir. Para tanto, dados os polinômios $f = (a_0, a_1, a_2, \cdots), g = (b_0, b_1, b_2, \cdots)$ e $h = (c_0, c_1, c_2, \cdots)$ pertencentes a $P[X]$:

A1) Fechado para adição. Pela definição da operação de adição de polinômios, temos que $f \oplus g = (a_0 + b_0, a_1 + b_1, \cdots)$, devemos mostrar que existe um índice k, tal que $a_i + b_i = 0_A$ para todo $i > k$, pois $a_i + b_i \in (A, +, \cdot)$, então existe um índice j, tal que $a_i = 0_A$ para todo $i > j$ e um índice l, tal que $b_i = 0$ para todo $i > l$, se tomarmos $k = max\{j, l\}$, devemos ter $a_i + b_i = 0_A + 0_A = 0_A$, para todo $i > k$.

A2) Associatividade
$(f \oplus g) \oplus h = ((a_0, a_1, a_2, \cdots) \oplus (b_0, b_1, b_2, \cdots)) \oplus$
$(c_0, c_1, c_2, \cdots) = (a_0 + b_0, a_1 + b_1, \cdots) \oplus (c_0, c_1, c_2, \cdots) = ((a_0 + b_0) + c_0, (a_1 + b_1) + c_1, \cdots) = (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1), \cdots) = (a_0, a_1, a_2, \cdots) \oplus ((b_0, b_1, b_2, \cdots) \oplus (c_0, c_1, c_2, \cdots)) = f \oplus (g \oplus h)$.

A3) Comutatividade
$f \oplus g = (a_0, a_1, a_2, \cdots) \oplus (b_0, b_1, b_2, \cdots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots) = (b_0 + a_0, b_1 + a_1, b_2 + a_2, \cdots) = (b_0, b_1, b_2, \cdots) \oplus (a_0, a_1, a_2, \cdots) = g \oplus f$.

A4) Existência do elemento neutro da adição
Seja $e \in P$ tal que, $e = (0_A, 0_A, \cdots)$ temos que: $f \oplus e = e \oplus f = f$ para todo $f \in P$. De fato, $f \oplus e = (a_0, a_1, a_2, \cdots) \oplus (0_A, 0_A, 0_A, \cdots) = (a_0 + 0_A, a_1 + 0_A, a_2 + 0_A, \cdots) = (a_0, a_1, a_2, \cdots) = f$.

Temos por A_3 que $f \oplus e = e \oplus f$. Assim o polinômio $e = (0_A, 0_A, 0_A, \cdots)$ é o elemento neutro da adição e também chamado de polinômio nulo.

A5) Existência do elemento simétrico da adição. Tomando, $-a_i \forall i \geq 0$ como o elemento simétrico de $a_i \in A$ temos o polinômio $x = (-a_0, -a_1, -a_2, \cdots)$, fazendo $f \oplus x = (a_0, a_1, a_2, \cdots) \oplus (-a_0, -a_1, -a_2, \cdots) = (a_0 + (-a_0), a_1 + (-a_1), a_2 + (-a_2), \cdots) = 0_A, 0_A, 0_A, \cdots) = e$. Portanto, $x = -f$.

M1) Fechado para a multiplicação. Pela definição de multiplicação de polinômios, temos que $f \odot g = (d_0, d_1, d_2, \cdots)$ onde, $d_n = \sum_{i=0}^{n} a_i b_{n-i}$ então devemos mostrar que existe um índice k, tal que $d_n = 0_A$ para todo $n > k$. Pela definição de polinômio sabemos que existe um índice j, tal que $a_i = 0_A$, para todo $i > j$ e um índice l, tal que $b_i = 0_A$ para todo $i > l$, se tomarmos $k = j + l$ teremos, $d_n = a_0 \cdot b_n + a_1 \cdot b_{n-1} + a_2 \cdot b_{n-2} + \cdots + a_{(j+1)} \cdot b_{n-(j+1)} + \cdots + a_{n-1} \cdot b_1 + a_n + b_0$, como os coeficientes a_i com índice maior ou igual a $j + 1$ são iguais a 0_A e como $n > k = j + l$, assim $n - (j + 1) \geqslant j + l + 1 - (j + 1) = l$ então os

coeficientes b_i com índice maior do que $i > n - (j+1)$ são iguais a 0_A, logo $d_n = a_0 \cdot b_n + a_1 \cdot b_{n-1} + a_2 \cdot b_{n-2} + \cdots + a_{(j+1)} \cdot b_{n-(j+1)} + \cdots + a_{n-1} \cdot b_1 + a_n + b_0 = 0_A$ para todo $n > k$.

Assim precisamos mostrar que os polinômios p e q são iguais, o que pela igualdade de polinômios implica em $p_n = q_n \ \forall n \geqslant 0$. De fato,
$p_n = \sum_{i+j=n} d_i \cdot c_j = \sum_{i+j=n} (\sum_{\alpha+\beta=i} a_\alpha \cdot b_\beta) \cdot c_j = \sum_{\alpha+\beta+j=n} (a_\alpha \cdot b_\beta) \cdot c_j = \sum_{\alpha+\beta+j=n} a_\alpha \cdot (b_\beta \cdot c_j) = \sum_{\alpha+\gamma=n} a_\alpha \cdot (\sum_{\beta+j=\gamma} b_\beta \cdot c_j) = \sum_{\alpha+\gamma=n} a_\alpha \cdot z_\gamma = q_n$. Portanto os polinômios são iguais.

Portanto devemos mostrar que os polinômios r e s são iguais, ou seja, $r_n = s_n \in n \geqslant 0$. De fato,
$r_n = \sum_{i+j=n} a_i \cdot (b_j + c_j) = \sum_{i+j=n} (a_i \cdot b_j) + (a_i \cdot c_j) = \sum_{i+j=n} (a_i \cdot b_j) + \sum_{i+j=n} a_i \cdot c_j = d_n + t_n = s_n$. Logo, os polinômios r e s são iguais. Analogamente se demonstra que, $(f \oplus g) \odot h = (f \odot h) \oplus (g \odot h)$.

Satisfazendo todas as propriedades acima temos que $P[X]$ é de fato um anel. Resta mostrar que é comutativo e com unidade.

Portanto devemos mostrar que os polinômios f e w são iguais, ou seja, $f_n = w_n \in n \geqslant 0$
Como $k_i = 0_A$ para todo $i \geqslant 1$ e $k_0 = 1$, temos que:
$w_n = \sum_{i=0}^{n} a_i \cdot w_{n-i} = a_0 \cdot 0_A + a_1 \cdot 0_A + a_2 \cdot 0_A + \cdots + a_n \cdot 1_A = a_n$.
Portanto os polinômios f e w são iguais, e o polinômio $k = (1_A, 0_A, 0_A, \cdots)$ é o elemento neutro da multiplicação.
Concluímos que $P[X]$ é um anel comutativo com unidade.

Denotaremos o anel dos polinômios por $A[X]$ e o chamaremos de anel dos polinômios sobre o anel A na variável X.

A fim de simplificar a escrita e tornar mais práticas as operações e manipulações com os polinômios, faremos algumas convenções: Utilizaremos o símbolo X para designar o elemento $(0, 1, 0, 0, \cdots)$, empregaremos o termo a_i para representar o elemento $(a_i, 0, 0, 0, \cdots)$, assim o símbolo a_i irá representar duas coisas distintas, o termo a_i do anel A e o elemento $(a_i, 0, 0, 0, \cdots)$ do anel dos polinômios $A[X]$. Também, ao invés de escrevermos $\oplus$ e $\odot$ escreveremos $+$ e $\cdot$ para representar respectivamente a adição e a

multiplicação tanto em A quanto em $A[X]$, isso não causará confusão pois as operações no anel dos polinômios são as operações usuais de adição e multiplicação. Com essas convenções o polinômio $(a_0, a_1, a_2, \cdots)$ será igual à soma $a_o + a_1x + a_2x^2 + \cdots + a_nx^n$, então,

$$P = \{\sum_{i=0}^{n} a_i xi \mid n \in \mathbb{N} \text{ e } a_i \in A\}$$

Sempre que $0 \leq i \leq n$, os elementos a_i são denominados de *coeficientes*, as parcelas a_ix^i serão os *termos*, o termo a_iX^i é chamado *monômio* de grau i e quando n for o maior expoente de X, diremos que o polinômio possui grau n, o coeficiente a_0 é chamado *termo constante*, não definiremos o grau do polinômio $q(x) = 0\ \forall q(x) \in A[X]$.
Convencionando que:

1) Para todo n natural chamamos $q(x) = 0+0x+...+0x^n$ de *polinômio identicamente nulo* e denotaremos por $q(x) = 0$.

2) Denotaremos por *polinômio constante* sempre que $q(x) = a_0$.

3) Não escreveremos o termo a_ix^i quando $a_i = 0$.

Para qualquer polinômio $q(x)$ se existir um maior n natural tal que $a_nx^n \neq 0$, então definimos o grau de $q(x)$ como sendo n e denotaremos por $Grau(q(x))$, e o coeficiente a_n será chamado de coeficiente *líder*. Por exemplo $a_0 + a_1x + a_2x^2 + a_3x^3$ possui grau 3, e a_3 é o coeficiente líder, observe também que $a_i = 0$ para todo $i > 3$ tais termos existem porém não são escritos. Os polinômios de grau zero, são do tipo $Q(X) = a$ com $a \neq 0$ e são chamados polinômios constantes.
Será denominado *mônico* todo polinômio cujo coeficiente líder for igual a 1.

Com as operações de adição e multiplicação definidas e as convenções acima introduzidas estamos em condições de mostrar algumas propriedades de tais operações no anel dos polinômios.

Teorema 3.2.4. *Sejam os polinômios não nulos* $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ *e* $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ *pertencentes a* $A[X]$*, tais que a adição* $(p + q)(x)$ *é diferente do polinômio nulo. Então*

$$Grau(p + q)(x)) \leq max\{Grau(p(x)), Grau(q(x))\}$$

Demonstração. Suponhamos que $a_n \neq 0_A$ e $b_m \neq 0_A$, assim temos $Grau(p(x)) = n$ e $Grau(q(x)) = m$, com isso temos que considerar quatro casos:

1) $n = m$ e $a_n + b_n \neq 0_A$.

   Então $(p+q)(X) = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n$ onde $a_n+b_n \neq 0_A$ é o coefciente líder da adição $(p+q)(x)$ e o grau da adição é $Grau(p+q)(x) = n = m$.

2) $n = m$ e $a_n + b_n = 0_A$.

   Então $(p+q)(x) = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_k+b_k)x^k+(a_n+b_n)x^n = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_k+b_k)x^k$.

   Se $a_k + b_k \neq 0_A$, então será o coefciente líder da adição $(p+q)(x)$ e o grau da adição $Grau(p+q)(x) = k < n = m$.

   Se $a_k + b_k = 0_A$, então repetindo o argumento, quantas vezes forem necessárias, concluímos que existe um índice i tal que $a_i + b_i \neq 0_A$, pois a adição $(p+q)(x)$ é diferente do polinômio nulo por hipótese, então $a_i + b_i$ será o coefciente líder da adição $(p+q)(x)$ e o grau da adição será $Grau(p+q)(x) = i < k < n = m$.

3) $n \neq m$ e $n < m$.

   Então $(p+q)(x) = (a_0+b_0)+(a_1+b_1)x+\cdots+(0_A+b_m)x^m$, pois $a_i = 0_A$ para todos $i > n$.

   Então $0_A + b_m = b_m \neq 0_A$ é o coefciente líder da adição $(p+q)(x)$ e o grau da adição é $Grau(p+q)(x) = m$

4) $n \neq m$ e $m < n$. 34 Então $(p+q)(x) = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+0_A)x^n$, pois $b_i = 0_A$ para todos $i > m$.

   Então $a_n + 0_A = a_n \neq 0_A$ é o coefciente líder da adição $(p+q)(X)$ e o grau da adição será $Grau(p+q)(x) = n$.

   Portanto, em qualquer caso temos que

$$Grau(p+q)(x)) \leq max\{Grau(\mathrm{p(x)}), Grau(\mathrm{q(x)})\}.$$

□

Teorema 3.2.5. *Seja A um anel comutativo com unidade 1_A. Então $A[X]$ é um anel comutativo com unidade. Além disso, se A é um domínio de integridade, então $A[X]$ é um domínio de integridade.*

Demonstração. Considerando as propriedades $A_1, A_2, A_3, A_4, A_5, M_1, M_2,$
$M_3, M_4, M_5, M_6,$ anteriormente descritas, temos demonstrada a primeira parte do teorema. Basta então mostrarmos a última parte, para isso suponhamos que $q(x)$ e $d(x) \in A[X]$ não nulos, tais que $Grau(q(x)) = n$ e $Grau(d(x)) = m$. Vimos na demonstração da propriedade $M1$ do fechamento da multiplicação, que para todos os coefcientes de índice $i > n+m$ o coefciente é igual a 0_A, ou seja, $c_i = 0_A$, assim o maior índice possível para o coefciente c_i ser diferente de 0_A é o do índice $n + m$, portanto a maior possibilidade para o maior expoente de x que possui o coefciente diferente do 0_A é $n+m$, desta forma $Grau(q(x)\cdot d(x)) \leq n+m = Grau(q(x)) + Grau(d(x))$. Agora, se A é um domínio de integridade, temos para o coeficiente c_{n+m} a seguinte consequência:

$$c_{n+m} = \sum_{\alpha+\beta=n+m} a_\alpha b_\beta \begin{cases} a_\alpha = 0_A, se \alpha > n \\ b\beta = 0_A, se \beta > m \end{cases}$$

Portanto $c_{n+m} = a_0 \cdot 0_A + a_1 \cdot 0_A + \cdots + a_n \cdot b_m + 0_A \cdot b_{m-1} + \cdots + 0_A \cdot b_0 = a_n \cdot b_m$, como A é um domínio de integridade e $a_n \neq 0_A$ e $b_m \neq 0_A$, então $a_n \cdot b_m \neq 0_A$, assim o coefciente líder da multiplicação $(q(x) \cdot d(x))$ é o $a_n \cdot b_m$ e o grau da multiplicação é $Grau((q(x) \cdot d(x)) = n + m = Grau(q(x)) + Grau(d(x))$. □

Sabemos que no anel dos números inteiros ($\mathbb{Z}$) o elemento unidade é o número um (1). O teorema a seguir define o elemento unidade em $A[X]$.

Teorema 3.2.6. *Sejam A um domínio de integridade e $p(x) \in A[X]$. Então $p(x)$ é uma unidade em $A[X]$ se, e somente se, $p(x)$ é um polinômio constante e a_0 é uma unidade em A. Em particular, se A é um corpo, as unidades em $A[X]$ são os polinômios constantes não nulos.*

Demonstração. .
Suponhamos primeiramente, que $p(x)$ é uma unidade em $A[X]$. Então $p(x) \cdot g(x) = 1_A$ para algum $g(x) \in A[X]$. Pelo teorema 3.2.4, temos que $Grau(p(x)\cdot g(x)) = Grau(p(x)) + Grau(g(x)) = Grau(1_A) = 0$. Como o grau de polinômio é um número inteiro não negativo, temos que $Grau(p(x)) = 0$ e $Grau(g(x)) = 0$, Portanto, $p(x)$ e $g(x)$ são polinômios constantes, sendo $p(x) = a_0$ e $g(x) = b_0$, temos que $p(x)\cdot g(x) = a_0 \cdot b_0 = 1_A$, portanto a_0 é uma unidade em A.

Reciprocamente, suponhamos que $p(x) = a_0$ é um polinômio constante e a_0 é uma unidade em A, assim existe $g(x)$ tal que $g(x) = a_0^{-1}$, onde a_0^{-1} é o inverso multiplicativo

de a_0. Então $p(x) \cdot g(x) = a_0 \cdot a_0^{-1} = 1_A$. Portanto $p(x)$ é uma unidade em $A[X]$. Se A é um corpo, os elementos diferentes do elemento neutro da adição são unidades, então os polinômios constantes não nulos, são unidades em $A[X]$ □

Definição 3.2.7. *Seja $p(x)$ um polinômio em um anel $A[X]$. Se existe $a \in A$ tal que, $p(a) = 0$ (zero de A). Então a é dito raiz de $p(x)$.*

Exemplo 3.2.8. *Considerando $p(x) \in \mathbb{R}[X]$ definido como: $p(x) = X^2 - 1$. Os números reais -1 e 1 são suas raízes pois, $p(-1) = p(1) = 0$.*

Em $A[X]$ define-se que:

1) O polinômio constante $p(x) = a$ para algum a em um domínio de integridade infinito A não possui nenhuma raíz, pois para qualquer $u \in A$ tem-se que $p(u) \neq 0$.

2) O polinômio identicamente nulo $p(x) = 0$ em um domínio de integridade infinito A, possui infinitas raízes, pois para todo elemento $a \in A$ tem-se que $p(a) = 0$.

Teorema 3.2.9. *Se $p(x) \in A[X]$ e $\alpha \in A$ então, $p(\alpha) = 0$ se, e somente se, $\exists$ $q(x) \in A[X]$ tal que $p(x) = (x - \alpha)q(x)$. Por consequência, se grau$(p(x)) = n$, então grau$(q(x)) = n - 1$*

Demonstração. Suponha $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ e $p(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$

Se $p(\alpha) = 0$, então $p(x) = p(x) - p(\alpha) = a_n(x^n - \alpha^n) + a_{n-1}(x^{n-1} - \alpha^{n-1}) + \cdots + a_1(x - \alpha)$. Em todas as parcelas há um elemento da forma $(x^k - \alpha^k)$ para concluirmos basta mostrar que $(x - \alpha)$ divide tais parcelas para $k = 1, 2, 3, \cdots$.

É fácil ver que
$x^2 - \alpha^2 = (x - \alpha)(x + \alpha)$
$x^3 - \alpha^3 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$ suponha que $x^k - \alpha^k = (x - \alpha)(x^{k-1} + \alpha x^{k-2} + \cdots + \alpha^{k-2}x + \alpha^{k-1})$ aplicando a propriedade distributiva tem-se que $x^k - \alpha^k = x^k + \alpha x^{k-1} + \cdots + \alpha^{k-2}x^2 + \alpha^{k-1}x - \alpha x^{k-1} - \cdots - \alpha^{k-1}x - \alpha^k = x^k - \alpha^k$ mostrando que de fato a conjectura é verdadeira.
A recíproca do teorema é imediata pois, se $p(x) = (x - \alpha)q(x)$ tem-se que $p(\alpha) = (\alpha - \alpha)q(\alpha) = 0$ □

Corolário 3.2.10. *Dado um polinômio $p(x)$ em $A[X]$, não nulo e de grau n, então $p(x)$ possui no máximo n raizes.*

Demonstração. Sejam $a_1, a_2, a_3, \cdots, a_k$ raizes distintas de $p(x)$, então pelo teorema 3.2.7 tem-se que $p(x) = (x - a_1) \cdot q_1(x)$, como $p(a_2) = 0$, pois a_2 é raiz e $a_1 \neq a_2$, temos que $q_1(a_2) = 0$, logo a_2 é raiz de $q_1(x)$ e novamente pelo teorema 3.2.7 tem-se que $p(x) = (x - a_1) \cdot (x - a_2) \cdot q_2(x)$. Repetindo o raciocínio para a_3 segue que, $a_3 - a_1 \neq 0$, $a_3 - a_2 \neq 0$, logo devemos ter $q_2(3) = 0$, sendo a_3 raiz de $q_2(x)$ e portanto, $p(x) = (x-a_1)\cdot(x-a_2)\cdot(x-a_3)\cdot q_2(x)$. Procedendo de maneira análoga com $a_4, \cdots, a_k$ concluiremos que: $p(x) = (x - a_1) \cdot (x - a_2) \cdot (x - a_3) \cdots (x - a_k) \cdot q_k(x)$ de forma que, $Grau q_k(x) \geq 0$. Considerando o grau de $p(x)$, e aplicando a propriedade distributiva em $(x - a_1) \cdot (x - a_2) \cdot (x - a_3) \cdots (x - a_k)$ teremos $n = k + Grau q_k(X)$, sendo que $Grau q_k(x) \geq 0$ segue que $k \leq n$. Portanto, a quantidade de raizes de um polinômio de grau n é menor ou igual a n. □

Corolário 3.2.11. *Dado um polinômio $p(x)$ em um anel A, o único que se anula para todo $a \in A$ é o polinômio identicamente nulo, ou seja, $p(x) = 0$.*

É fácil ver que $p(x) = 0 = a_0+a_1x+a_2x^2+\cdots+a_nx^n$ onde, $a_0 = a_1 = a_2 = \cdots+a_n = 0$. Podemos observar que, se $a_0 \neq 0$ então $p(x)$ é constante e não se anula em nenhum ponto. Se algum $a_i \neq 0$ para $i > 0$, então $p(x)$ possui grau i e pelo corolário 3.2.8 possui no máximo i raizes.

3.3 Algorítmo da divisão de polinômios

Com as propriedades já definidas, tanto para o anel dos números inteiros, como também para o anel dos polinômios, especialmente os conceitos de divisão euclidiana dos números inteiros onde os números inteiros b e a com $b > a$ podem ser escritos como $b = a \cdot q + r$, $0 \leq r < a$, sendo que q e r são únicos e correspondem ao quociente e o resto da divisão euclidiana de b por a. Com todas as similaridades existentes entre os polinômios e os números inteiros, podemos falar em uma divisão euclidiana de polinômios. Os fundamentos desta teoria foram extraídos de (GARCIA; LEQUAIN, 2001).

Considerando o fato de que os polinômios formam um anel, devemos ter uma operação de divisão que se assemelha à divisão euclidiana dos números inteiros,ou seja, a divisão de um polinômio $p(x)$ por um polinômio não nulo $q(x)$ nos fornece como quociente o polinômio $d(x)$, e como resto o polinômio $r(x)$, ou seja $p(x) = q(x) \cdot d(x) + r(x)$. Sabendo também que dois polinômios são iguais se, e somente se, os coeficientes das

respectivas potências da variável forem iguais, e que ao dividirmos um polinômio $p(x)$ de grau n por $(x-\alpha)$, onde α é uma das raízes do divisor, o polinômio resultante $q(x)$ terá grau $n-1$, pode-se estabelecer uma relação entre polinômios conhecida como o método dos coeficientes a determinar. Vejamos como isso pode ser feito.

Dado o polinômio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ dividí-lo por $(x-\alpha)$ é obter $q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0$ tal que $p(x) = (x-\alpha)\cdot q(x) + r$. Devemos ter então,
$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x-\alpha)\cdot(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0) + r$
aplicando a propriedade distributiva, tem-se $b_{n-1}x^n + b_{n-2}x^{n-1} + \cdots + b_1 x^2 + b_0 x - \alpha b_{n-1}x^{n-1} - \alpha b_{n-2}x^{n-2} - \cdots - \alpha b_1 x - \alpha b_0$ de modo que para cada termo de mesmo expoente em $p(x)$ ocorre a seguinte igualdade de coeficientes:

$a_n x^n = b_{n-1}x^n \Rightarrow b_{n-1} = a_n$
$a_{n-1}x^{n-1} = b_{n-2}x^{n-1} - \alpha b_{n-1}x^{n-1} \Rightarrow b_{n-2} - \alpha b_{n-1} = a_{n-1} \Rightarrow b_{n-2} = a_{n-1} + \alpha b_{n-1}$
$a_{n-2}x^{n-2} = b_{n-3}x^{n-2} - \alpha b_{n-2}x^{n-2} \Rightarrow b_{n-3} - \alpha b_{n-2} = a_{n-2} \Rightarrow b_{n-3} = a_{n-2} + \alpha b_{n-2}$
$\vdots$
$a_0 = -\alpha b_0 + r \Rightarrow r = a_0 + \alpha b_0.$

Nos exemplos abaixo apresentaremos algumas situações em que variações do resultado acima podem ser utilizadas.

Pode-se realizar divisões por polinômios do tipo $x-a$ de uma maneira simples e rápida. Tal procedimento é conhecido por dispositivo prático de Briot-Ruffini.

Exemplo 3.3.1. *Vamos dividir* $p(x) = 3x^3 - 5x^2 + x - 2$ *por* $h(x) = x - 2$

No algorítmo abaixo: $3, -5, 1$ e -2 são os coeficientes de $p(x)$, 2 é a raíz de $h(x)$. Para realizarmos a divisão, repetimos o primeiro coeficiente, multiplicamos a raíz de $h(x)$ por ele e em seguida somamos ao segundo coeficiente, o resultado aparece abaixo da linha, esse resultado será multiplicado pela raíz de $h(x)$ e somado ao terceiro coeficiente e o processo segue até o último coeficiente.

[x=2,stage=8, tutorlimit=8,tutor=true]3x^3 − 5x^2 + x − 2

Os valores $3, 1, 3$ são os coeficientes do quociente $q(x)$ e 4 é o resto. Pelo algorítmo temos:

$$q(x) = 3x^2 + x + 3 \text{ e } r = 4$$

logo,

$$p(x) = h(x)q(x) + r \text{ ou seja, } 3x^3 - 5x^2 + x - 2 = (x-2)(3x^2 + x + 3) + 4$$

Outra consequência importante do resultado acima é o de que o resto da divisão de um polinômio $p(x)$ por $x - a$ é $p(a)$, sabendo que,

$$p(x) = (x - a)q(x) + r$$

fazendo $x = a$ tem-se:

$$p(a) = (a - a)q(a) + r = 0 \cdot q(a) + r = r \Rightarrow r = p(a)$$

Exemplo 3.3.2. *Vamos calcular o resto da divisão de* $p(x) = 2x^3 - x^2 + 5x - 3$ *por* $h(x) = x - 4$

$$p(4) = 2(4)^3 - (4)^2 + 5(4) - 3 = 128 - 16 + 20 - 3 = 129$$

Logo, o resto desta divisão é 129.

Teorema 3.3.3. *Seja* $A[x]$ *o anel dos polinômios e* $f(x), g(x) \in A[x]$*, com* $g(x) \neq 0$*, então existem* $q(x), r(x) \in A[x]$*, únicos tais que;*

$$f(x) = q(x) \cdot g(x) + r(x)$$

onde $r(x) = 0_P$ *ou* $Grau(r(x)) < Grau(g(x))$.

Demonstração. **Existência.**

Se $f(x) = 0_A$ ou $Grau(f(x)) < Grau(g(x))$, então a prova está terminada com $q(x) = 0_A$ e $r(x) = f(x)$, porque $f(x) = 0_A \cdot g(x) + f(x)$.

Se $f(x) \neq 0_A$ e $Grau(g(x)) \leq Grau(f(x))$, então a demonstração da existência será por indução completa [1] sobre o grau de $f(x)$. Seja $Grau(f(x)) = n$, suponhamos $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ com $a_n \neq 0_A$ e $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ com $b_m \neq 0_A$ e $m \leq n$.

Se $Grau(f(x)) = 0$, então $Grau(g(x)) = 0$. Portanto $f(x) = a_0$ e $g(x) = b_0$ com $a_0, b_0 \neq 0_f$,como A é um anel, b_0 é uma unidade, ou seja, possui inverso multiplicativo, assim $a_0 = b \cdot (b^{-1}a_0) + 0$, então o teorema é verdadeiro para $n = 0$, com $q(x) = b^{-1}a_0$ e $r(x) = 0_A$.

Suponhamos que o teorema é verdadeiro para polinômios com grau menor do que $n = Grau(f(x))$, devemos mostrar que o teorema é verdadeiro para polinômios com grau n. Como $b_m \neq 0_A$, b_m é uma unidade, assim multiplicamos o polinômio $g(x)$ por

[1] Para uma melhor compreensão deste princípio, ver [15] p. 24.

$a_n b_m^{-1} x^{n-m}$ para obter $a_n b_m^{-1} x^{n-m} \cdot g(x) = a_n b_m^{-1} x^{n-m}(b_m x^m + b_{n-1} x^{m-1} + \cdots + b_1 x + b_0) = a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \cdots + a_n b_m^{-1} b_1 x^{n-m+1} + a_n b_m^{-1} b_0 x^{n-m}$

Como os polinômios $f(x)$ e $a_n b_m^{-1} x^{n-m} \cdot g(x)$ tem o mesmo grau n e o mesmo coeficiente lider a_n, a diferença $f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x)$ é um polinômio de grau menor que n. Por hipótese de indução, existem $q_1(x)$ e $r_1(x)$ em $A[x]$ tais que,

$$f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x) = q_1(x) \cdot g(x) + r_1(x)$$

com $r_1(x) = 0_A$ ou $Grau(r_1(x)) < Grau(g(x))$.Portanto,

$$f(x) = q_1(x) \cdot g(x) + r_1(x) + a_n b_m^{-1} x^{n-m} \cdot g(x)$$

$$f(x) = g(x) \cdot [q_1(x) + a_n b_m^{-1} x^{n-m}] + r_1(x)$$

Se tomarmos $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r(x) = r_1(x)$, temos que o teorema é verdadeiro para os polinômios de grau n. Portanto pelo princípio da indução completa o teorema é verdadeiro para todo polinômio independente de seu grau.

Unicidade. Sejam $q_1(x), q_2(x), r_1(x), r_2(x) \in A[X]$, tais que $f(x) = q_1(x) \cdot g(x) + r_1(x)$ e $f(x) = q_2(x) \cdot g(x) + r_2(x)$, onde $r_1 = 0_A$ ou $Grau(r_1(x)) < Grau(g(x))$, e $r_2 = 0_A$ ou $Grau(r_2(x)) < Grau(g(x))$.Assim

$q_1(x) \cdot g(x) + r_1(x) - q_2(x) \cdot g(x) - r_2(x) = f(x) - f(x) = 0$

$q_1(x) \cdot g(x) - q_2(x) \cdot g(x) = r_2(x) - r_1(x)$

$g(x) \cdot (q_1(x) - q_2(x)) = r_2(x) - r_1(x)$

Se $q_1(x) \neq q_2(x)$, temos $Grau(g(x)) \cdot (q_1(x) - q_2(x))) = Grau(r_2(x) - r_1(x))$, mas como A é domínio de integridade pelo Teorema 2.4.1, temos $Grau(g(x)) \cdot (q_1(x)) - q_2(x))) = Grau(g(x)) + Grau(q_1(x) - q_2(x))$ então, $Grau(r_2(x) - r_1(x)) = Grau(g(x) + Grau(q_1(x) - q_2(x))$. Assim, $Grau(r_2(X) - r_1(x)) \geqslant Grau(g(x))$.

No entanto, $Grau(r_2(x) - r_1(x)) \leqslant max\, Grau(r_1(x)), Grau(r_2(x))$, mas como $Grau(r_1(x)) < Grau(g(x))$ e $Grau(r_2(x)) < Grau(g(x))$,temos que, $Grau(r_2(x) - r_1(x)) \leqslant max\, Grau(r_1(x)), Grau(r$ $Grau(g(x))$

Portanto temos uma contradição. Logo $q_1(x) = q_2(x)$ e temos $g(x) \cdot (q_1(x) - q_2(x)) = r_2(x) - r_1(x) \Rightarrow g(x) \cdot 0_A = r_2(x) - r_1(x) \Rightarrow 0_A = r_2(x) - r_1(x) \Rightarrow r_2(x) = r_1(x)$

Concluímos que existem únicos polinômios $q(x)$ e $r(x)$ tais que $f(x) = q(x)(x) + r(x)$. □

Exemplo 3.3.4. *Sejam os poliômios* $f(x) = x^4 + x^3 - 7x^2 + 9x - 1$ *e* $g(x) = x^2 + 3x - 2$ *vamos realizar a divisão de* $f(x)$ *por* $g(x)$.

[style=D,stage=11] $x^4 + x^3 - 7x^2 + 9x - 1x^2 + 3x - 2$

Observe que $x^2 - 2x + 1$ é o quociente $(q(x))$ e $2x + 1$ é o resto $(r(x))$, então $f(x) = g(x) \cdot q(x) + r(x)$, além disso o grau de $r(x)$ é menor do que o grau de $g(x)$.

3.4 Máximo divisor comum, Mínimo múltiplo comum e divisibilidade

Definição 3.4.1. *Sejam F um corpo e $a(x)$, $b(x) \in F[x]$ com $b(x)$ não nulo. Dizemos que $b(x)$ divide $a(x)$, ou que $b(x)$ é um fator de $a(x)$, e escrevemos $b(x) \mid a(x)$, se $a(x) = h(x) \cdot b(x)$ para algum $h(x) \in F[x]$. Neste caso, diremos que $a(x)$ é múltiplo de $b(x)$.*

Ao aplicarmos o algorítmo da divisão nos polinômios$a(x)$ e $b(x) \in F[x]$ com $b(x)$ não nulo, se o polinômio do resto for o polinômio nulo, então $b(x)$ divide $a(x)$.

Teorema 3.4.2. *Sejam F um corpo e $a(x)$, $b(x) \in F[x]$ com $b(x) \neq 0$. Então valem as seguintes propriedades:*

1) Se $b(x) \mid a(x)$, então $c \cdot b(x) \mid a(x)$, para todo $c \in F$ e $c \neq 0$.

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

3) Se $a(x) \mid b(x)$ e $a(x) \mid c(x)$, então $a(x) \mid (b(x) + c(x))$.

4) Se $a(x) \mid b(x)$, então $a(x) \mid b(x) \cdot c(x)$, para todo $c(x) \in F[x]$.

5) Se $a(x) \mid b(x)$ e $a(x) \mid c(x)$, então $a(x) \mid (b(x) \cdot d(x) + c(x) \cdot e(x))$, para quaisquer $d(x)$ e $e(x) \in F[x]$.

6) Se $a(x) \mid b(x)$ e $b(x) \mid a(x)$, então $a(x) = c \cdot b(x)$,onde c é uma constante de F.

7) Se $b(x) \mid a(x)$, então $Grau(b(x)) \leq Grau(a(x))$.

Demonstração. 1) Se $b(x) \mid a(x)$, então $a(x) = b(x) \cdot h(x)$ para algum $h(x) \in F[x]$. Assim temos: $a(x) = 1_F \cdot b(x) \cdot h(x) = c \cdot c^{-1} \cdot b(x) \cdot h(x) = c \cdot b(x)[c^{-1} \cdot h(x)]$. Portanto, $c \cdot b(x) \mid a(x)$.

2) Se $a(x) \mid b(x)$ e $b(x) \mid c(x)$, então temos:
$b(x) = a(x) \cdot q_1(x)$, para algum $q_1(x) \in F[x]$ e
$c(x) = b(x) \cdot q_2(x)$, para algum $q_2(x) \in F[x]$ assim,
$c(x) = a(x)_1(x) \cdot q_2(x)$ e como $q_1(x), q_2(x) \in F[x]$, temos que $a(x) \mid c(x)$.

3) Se $a(x) \mid b(x)$ e $a(x) \mid c(x)$, então temos:
$b(x) = a(x) \cdot q_1(x)$, para algum $q_1(x) \in F[x]$ e
$c(x) = a(x) \cdot q_2(x)$, para algum $q_2(x) \in F[x]$, assim,
$b(x) + c(x) = a(x) \cdot (q_1(x) + q_2(x))$ com $q_1(x) + q_2(x) \in F[x]$, então $a(x) \mid (b(x) + c(x))$.

4) Se $a(x) \mid b(x)$, então $b(x) = a(x)(x)$ para algum $q(x) \in F[x]$, e para todo $c(x) \in F[x]$ temos: $b(x) \cdot c(x) = a(x) \cdot q(x) \cdot c(x)$ e como $q(x) \cdot c(x) \in F[x]$ então $a(x) \mid b(x) \cdot c(x)$.

5) $a(x) \mid b(x)$ e $a(x) \mid c(x)$, temos pelo item 4 que:
$a(x) \mid b(x) \cdot d(x)$, para algum $d(x) \in F[x]$ e
$a(x) \mid c(x) \cdot e(x)$, para algum $e(x) \in F[x]$, então pelo item 3 temos que;
$a(x) \mid (b(x) \cdot d(x) + c(x) \cdot e(x))$ para quaisquer $d(x), e(x) \in F[x]$.

6) Se $a(x) \mid b(x)$ e $b(x) \mid a(x)$, então temos:
$b(x) = a(x) \cdot q_1(x)$, para algum $q_1(x) \in F[x]$ e
$a(x) = b(x) \cdot q_2(x)$, para algum $q_2(x) \in F[x]$ assim,
$a(x) = a(x) \cdot q_1(x) \cdot q_2(x)$
desta forma $Grau(a(x)) = Grau(a(x)) \cdot q_1(x) \cdot q_2(x)$, sendo $F[x]$ domínio de integridade, temos que $Grau(a(x)) = Grau(a(x)) + Grau(q_1(x)q_2(x))$, com isso $Grau(q_1(x)q_2(x)) = 0$,ou seja $Grau(q_1(x)) + Grau(q_2(X)) = 0$, o que implica $Grau(q_1(x)) = 0$ e $Grau(q_2(x)) = 0$. Portanto, $q_2(x) = c$ é um polinômio constante e $a(x) = c \cdot b(x)$.

7) Suponha $b(x) \mid a(x)$, então $a(x) = b(x) \cdot h(x)$ para algum $h(x) \in F[x]$. Temos que $Grau(a(x)) = Grau(b(x)) + Grau(h(x))$. Uma vez que o grau dos polinômios são números naturais, devemos ter $0 \leq Grau(b(x)) \leq Grau(a(x))$.

□

Definição 3.4.3. *Sejam F um corpo e $a(x), b(x) \in F[x]$, ambos não nulos. O máximo divisor comum (mdc) entre $a(x)$ e $b(x)$ é o polinômio mônico de maior grau que divide*

$a(x)$ e $b(x)$, ou seja:

1) $d(x) \mid a(x)$ e $d(x) \mid b(x)$;

2) $Sec(x) \mid a(x)$ e $c(x) \mid b(x)$, então o $Grau(c(x)) \leq Grau(d(x))$.

Teorema 3.4.4. *Seja F um corpo e $a(x), b(x) \in F[x]$, ambos não nulos. Então, existe um único máximo divisor comum $d(x)$ entre $a(x)$ e $b(x)$. Alem disso, existem polinômios $u(x)$ e $v(x)$, não necessariamente nulos tais que $d(x) = a(x) \cdot u(x) + b(x) \cdot v(x)$.*

Demonstração. **Existência.**

Seja S o conjunto de todas as combinações lineares de $a(x)$ e $b(x)$, isto é,

$$S = a(x) \cdot m(x) + b(x) \cdot n(x); m(x), n(x) \in F[x]$$

observe que S contém polinômios não nulos, ao menos $a(x)$ e $b(x)$ pois, $a(x) = a(x) \cdot 1_F + b(x) \cdot 0_F$ e $b(x) = a(x) \cdot 0_F + b(x) \cdot 1_F$. Assim, o conjunto de todos os graus em S é um conjunto não vazio de inteiros não negativos, que tem um menor elemento, Assim existe um polinômio $w(x)$ de menor grau em S. Se d é o coeficiente líder de $w(x)$, então $t(x) = d^{-1} \cdot w(x)$ é um polinômio mônico de menor grau em S. Pela definição de S temos que:

existem $u(x), v(x) \in F[x]$, tal que $t(x) = a(x)(x) + b(x) \cdot v(x)$.

Vamos mostrar que $t(x)$ é o máximo divisor comum entre $a(x)$ e $b(x)$. Sabemos que existem $q(x)$ e $r(x)$, tal que $a(x) = q(x) \cdot t(x) + r(x)$, com $r(x) = 0_F$ ou $Grau(r(x)) < Grau(t(x))$. Em consequência temos que:

$r(x) = a(x) - q(x) \cdot t(x)$

$r(x) = a(x) - q(x) \cdot [a(x) \cdot u(x) + b(x) \cdot v(x)$

$r(x) = a(x) - q(x) \cdot a(x) \cdot u(x) - q(x) \cdot b(x) \cdot v(x)$

$r(x) = a(x) \cdot [1 - q(x) \cdot u(x)] + [b(x) \cdot [-q(x) \cdot v(x)]$

Assim, $r(x)$ é uma combinação linear de $a(x)$ e $b(x)$, portanto $r(x) \in S$, e como $t(x)$ é o polinômio mônico de menor grau em S não há a possibilidade de $Grau(r(x)) < Grau(t < (x))$, então a única possibilidade é $r(x) = 0_F$. Portanto $a(x) = q(x) \cdot t(x) + r(x) = q(x) \cdot t(x) + 0_F = q(x) \cdot t(x)$, de modo que $q(x) \mid a(x)$. Analogamente se mostra que $t(x) \mid b(x)$. Assim provamos a primeira propriedade: □

1) $t(x) \mid a(x)$ e $t(x) \mid b(x)$

Se $c(x) \mid a(x)$ e $c(x) \mid b(x)$, então por (5) do teorema anterior $c(x) \mid a(x) \cdot u(x) + b(x)(x) = t(x)$, com isso $c(x) \mid t(x)$ e por (7) temos que $Grau(c(x)) \leq Grau(t(x))$. Assim provamos a segunda propriedade:

2) Se $c(x) \mid a(x)$ e $c(x) \mid b(x)$, então $Grau(c(x)) \leq Grau(t \leq (x))$

portanto $t(x)$ é o máximo divisor comum de $a(x)$ e $b(x)$.

Unicidade.

Vamos mostrar que além de $t(x)$ ser o maior divisor comum de $a(x)$ e $b(x)$, ele também é único.

Suponha que $d(x)$ seja um dos máximos divisores comuns de $a(x)$ e $b(x)$. Devemos provar então que $d(x) = t(x)$. Como $d(x)$ é o máximo divisor comum de $a(x)$ e $b(x)$, então existem $f(x), g(x) \in F[x]$ tais que $a(x) = d(x) \cdot f(x)$ e $b(x) = d(x) \cdot g(x)$. Portanto,
$t(x) = a(x) \cdot u(x) + b(x) \cdot v(x)$
$t(x) = [d(x) \cdot f(x)] \cdot u(x) + [d(x) \cdot g(x)] \cdot v(x)$
$t(x) = d(x)[f(x) \cdot u(x) + g(x) \cdot v(x)]$. Logo,
$Grau(t(x)) = Grau(d(x)) + Grau([f(x) \cdot u(x) + g(x) \cdot v(x)])$
como $t(x)$ e $d(x)$ são máximos divisores comuns, temos que: $Grau(t(x)) = Grau(d(x))$ consequentemente,

$$Grau([f(x) \cdot u(x) + g(x) \cdot v(x)]) = 0$$

assim, $f(x) \cdot u(x) + g(x) \cdot v(x) = c$ para alguma constante $c \in F$, o que significa que $t(x) = d(x) \cdot c$. Sendo $d(x)$ e $t(x)$ polinômios mônicos, o coeficiente líder do primeiro membro da igualdade é 1_F e o segundo membro é c, então devemos ter $c = 1_F$. Portanto, $d(x) = t(x) = a(x) \cdot u(x) + b(x) \cdot v(x)$ sendo o único máximo divisor comum de $a(x)$ e $b(x)$.

Definição 3.4.5. *Seja F um corpo e $a(x), b(x) \in F[x]$, ambos não nulos. O mínimo múltiplo comum (mmc) de $a(x)$ e $b(x)$ é o polinômio mônico de menor grau que é múltiplo de $a(x)$ e $b(x)$.*

O polinômio $m(x)$ é o mínimo múltiplo comum entre $a(x)$ e $b(x)$ se satisfaz

1) $a(x) \mid m(x)$ e $b(x) \mid m(x)$;

2) Se $a(x) \mid c(x)$ e $b(x) \mid c(x)$, então o $Grau(m(x)) \leq Grau(c(x))$.

Teorema 3.4.6. *Sejam F um corpo e $a(x); b(x) \in F[X]$, ambos não nulos, com os coeficientes líderes a e b respectivamente, e sendo $q(x)$ o quociente da divisão de $a(x) \cdot b(x)$ pelo $mdc(a(x); b(x))$. Então existe um único mínimo múltiplo comum entre $a(x)$ e $b(x)$, que é*

$$mmc(a(x); b(x)) = q(x) \cdot a^{-1} \cdot b^{-1}.$$

Demonstração. **Existência.**

Denotaremos por $d(x)$ o $mdc(a(x); b(x))$, sendo assim, $d(x) \mid a(x)$ e temos que $d(x) \mid a(x) \cdot b(x)$, assim podemos escrever $a(x) \cdot b(x) = d(x) \cdot q(x)$, como $d(x)$ é mônico e o coeficiente líder de $a(x) \cdot b(x)$ é igual a $a \cdot b$, então o coeficiente líder de $q(x)$ é igual a $a \cdot b$. Assim $q(x) \cdot a^{-1} \cdot b^{-1}$ é mônico.

Para provar que $m(x) = q(x) \cdot a^{-1} \cdot b^{-1}$ é o $mmc(a(x); b(x))$, devemos mostrar que $m(x)$ satisfaz as duas propriedades da definição de mínimo múltiplo comum.

Multiplicando os dois lados da igualdade $m(x) = q(x) \cdot a^{-1} \cdot b^{-1}$ por $d(x)$ temos:

$$d(x) \cdot m(x) = d(x) \cdot q(x) \cdot a^{-1} \cdot b^{-1}$$

$$d(x) \cdot m(x) = a(x) \cdot b(x) \cdot a^{-1} \cdot b^{-1}$$

como $b(x) = d(x) \cdot h(x)$ para algum $h(x) \in F[x]$, temos

$$d(x) \cdot m(x) = a(x) \cdot d(x) \cdot h(x) \cdot a^{-1} \cdot b^{-1}$$

além disso, sendo $F[x]$ um domínio de integridade, segue que:

$$m(x) = a(x) \cdot h(x) \cdot a^{-1} \cdot b^{-1},$$

portanto $a(x) \mid m(x)$. Analogamente se prova que $b(x) \mid m(x)$. Assim provamos a primeira propriedade

1) $a(x) \mid m(x)$ e $b(x) \mid m(x)$.

Seja $c(x) \in F[X]$ tal que $a(x) \mid c(x)$ e $b(x) \mid c(x)$ ou seja, $c(x) = a(x) \cdot f(x)$ para algum $f(x) \in F[X]$, $c(x) = b(x) \cdot g(x)$ para algum $g(x) \in F[X]$. Então, existem $u(x); v(x) \in F[X]$ tais que $d(x) = a(x) \cdot u(x) + b(x) \cdot v(x)$, multiplicando os dois lados da igualdade acima por c(x) temos o seguinte:
$c(x) \cdot d(x) = c(x) \cdot a(x) \cdot u(x) + c(x) \cdot b(x) \cdot v(x)$
$c(x) \cdot d(x) = b(x) \cdot g(x) \cdot a(x) \cdot u(x) + a(x) \cdot f(x) \cdot b(x) \cdot v(x)$

$c(x) \cdot d(x) = a(x) \cdot b(x) \cdot [g(x) \cdot u(x) + f(x) \cdot v(x)]$
$c(x) \cdot d(x) = d(x) \cdot q(x) \cdot [g(x) \cdot u(x) + f(x) \cdot v(x)]$
$c(x) = q(x) \cdot [g(x) \cdot u(x) + f(x) \cdot v(x)]$,
portanto $q(x) \mid c(x)$, e temos que $a^{-1} \cdot b^{-1} \cdot q(x) \mid c(x)$, ou seja, $m(x) \mid c(x)$. Sabemos que $Grau(m(x)) \leq Grau(c(x))$. Assim provamos a segunda propriedade:

2) Se $a(x) \mid c(x)$ e $b(x) \mid c(x)$, então o $Grau(m(x)) \leq Grau(c(x))$.

Portanto $m(x) = q(x) \cdot a^{-1} \cdot b^{-1}$ é mínimo múltiplo comum de $a(x)$ e $b(x)$.

Unicidade.

Vamos provar que $m(x)$ é o único mínimo múltiplo comum entre $a(x)$ e $b(x)$. Suponhamos que $t(x)$ seja qualquer mínimo múltiplo comum entre $a(x)$ e $b(x)$. Para provar a unicidade, devemos mostrar que $m(x) = t(x)$, na demonstração de existência do $mmc(a(x); b(x))$, demonstramos que $m(x)$ divide todos os múltiplos comuns de $a(x)$ e $b(x)$, em particular $m(x) \mid t(x)$, ou seja, $t(x) = m(x) \cdot f(x)$ para algum $f(x) \in F[X]$. Assim, $Grau(t(x)) = Grau(m(x)) + Grau(f(x))$. Como $t(x)$ e $m(x)$ são mínimos múltiplos comuns, então o $Grau(t(x)) = Grau(m(x))$, consequentemente $Grau(f(x)) = 0$. Assim $f(x) = c$ para alguma constante $c \in F$. Portanto, $t(x) = m(x)c$. Como $m(x)$ e $t(x)$ são polinômios mônicos, o coefciente líder do lado esquerdo da igualdade é 1_F e o do lado direito é c, então devemos ter $c = 1_F$. Portanto $t(x) = m(x) = q(x) \cdot a^{-1} \cdot b^{-1}$ é o único mínimo múltiplo comum de $a(x)$ e de $b(x)$. □

3.5 Irredutibilidade

Como os polinômios apresentam várias propriedades similares às dos números inteiros, vamos introduzir o conceito de irredutibilidade em um corpo de polinômios $F[x]$.

Definição 3.5.1. *Um elemento a em um anel $[A]$ comutativo com unidade, será chamado de associado de um elemento $b \in A$, se $a = b \cdot u$ para alguma unidade $u \in A$.*

Observe que se um elemento a é associado a um elemento b, então b é associado de a, pois se, $a = b \cdot u$, então $b = a \cdot u^{-1}$ e u^{-1} é uma unidade. Por exemplo no anel dos números inteiros $\mathbb{Z}$, os únicos associados de um número inteiro n são n e $-n$, porque somente 1 e -1 são as unidades em $\mathbb{Z}$.

Teorema 3.5.2. *Se F é um corpo e $a(x); b(x) \in F[X]$, então $a(x)$ é associado a $b(x)$ se, e somente se, $a(x) = b(x) \cdot c$ para algum polinômio constante não nulo c.*

Suponha que $a(x)$ é associado a $b(x)$, ou seja, $a(x) = b(x) \cdot u(x)$ onde $u(x)$ é uma unidade de $F[X]$. Pelo Corolário 2.1.17 as unidades em F[X] são os polinômios constantes não nulos, assim a(x) = b(x) c para algum polinômio não nulo c. Reciprocamente, se a(x) = b(x)c para algum polinômio constante não nulo c, então novamente pelo Teorema 2.4.2 sabemos que c é uma unidade em $F[X]$. Portanto $a(x)$ é associado a $b(x)$.

No anel dos números inteiros $\mathbb{Z}$, um número p diferente de zero dito primo, se não for uma unidade, ou seja, $p \neq \pm 1$, e seus únicos divisores são ± 1 (as unidades) e $\pm p$ (os associados de p). Se F é um corpo, então as unidades em $F[X]$ são os polinômios constantes não nulos, assim podemos enunciar a seguinte defnição de polinômio irredutível.

Definição 3.5.3. *Seja F um corpo. Um polinômio não constante $p(x) \in F[X]$ é dito polinômio irredutível se seus únicos divisores são seus associados e os polinômios constantes não nulos (as unidades). Um polinômio não constante que não é irredutível é chamado de redutível.*

Exemplo 3.5.4. *Considere o polinômio $f(x) = 3x + 1$ em $\mathbb{R}$, temos que os divisores de $f(x)$ são de grau 0 ou 1. Os divisores de $f(x)$ de grau 0 são polinômios constantes não nulos. Se $g(x)$ é um divisor de $f(x)$ de grau 1, então, $3x + 1 = g(x) \cdot h(x)$, com isso o $Grau(h(x)) = 0$, de modo que $h(x) = c$, então $g(x) = c^{-1} \cdot (3x + 1)$, assim $g(x)$ é um associado de $f(x)$. Portanto, $f(x)$ é irredutível em $R[X]$.*

Teorema 3.5.5. *Seja F um corpo, então todo polinômio de grau 1 pertencente a $F[X]$ é irredutível em $F[X]$.*

A demonstração segue da generalização do argumento do exemplo 2.4.5.

Teorema 3.5.6. *Seja F um corpo. Um polinômio não nulo $f(x)$ é redutível em $F[X]$ se, e somente se, $f(x)$ pode ser escrito como produto de dois polinômios de grau menor.*

Suponha que $f(x)$ é redutível em $F[X]$, então $f(x)$ tem um divisor $g(x) \in F[X]$ que não é associado a $f(x)$ e não é um polinômio constante não nulo, ou seja, $f(x) = g(x) \cdot h(x)$. Se $g(x)$ ou $h(x)$ tem o mesmo grau de $f(x)$, então um deles tem grau igual 0. Como um polinômio de grau 0 é um polinômio constante não nulo em $F[X]$, isso

signica que $g(x)$ é um polinômio constante não nulo ou um associado de $f(x)$, ou seja, contrário a hipótese. Portanto, tanto $g(x)$ como $h(x)$ tem grau menor que $f(x)$.

Reciprocamente, suponha que $f(x)$ pode ser escrito como produto de dois polinômios de grau menor, ou seja, $f(x) = g(x) \cdot h(x)$, onde $Grau(g(x)) < Grau(f(x))$ e $Grau(h(x)) < Grau(f(x))$, então $Grau(g(x)) \neq 0$ e $Grau(h(x)) \neq 0$, assim $g(x)$ e $h(x)$ são polinômios não constantes não nulos. Se $g(x)$ é um associado de $f(x)$, então temos que $g(x) = f(x) \cdot c$ para algum polinômio constante não nulo c. Portanto,

$$\begin{aligned} 1_F \cdot f(x) &= g(x) \cdot h(x) \\ 1_F \cdot f(x) &= f(x) \cdot c \cdot h(x) \\ 1_F &= c \cdot h(x) \end{aligned}$$

Assim $Grau(1_F) = Grau(c) + Grau(h(x))$, como $Grau(1_F) = Grau(c) = 0$. Com isso $Grau(h(x)) = 0$, o que não pode ocorrer. Logo $g(x)$ não pode ser associado de $f(x)$, de maneira análoga $h(x)$ também não pode ser associado de $f(x)$. Portanto $f(x)$ é redutível em $F[X]$.

Teorema 3.5.7. *Seja F um corpo. Cada polinômio não constante em $F[X]$ é irredutível ou pode ser escrito como produto de polinômios irredutíveis em $F[X]$. Esta escrita é única no seguinte sentido: Se,*

$$f(x) = p_1(x) \cdot p_2(x) \cdots p_r(x) \text{ e } f(x) = q_1(x) \cdot q_2(x) \cdots q_s(x).$$

com cada $p_i(x)$ e $q_i(x)$ irredutível, então $r = s$, ou seja, o número de polinômios irredutíveis é o mesmo. Após, se necessário, os $qi(x)$ serem reordenados temos,

$$p_i(x) \text{ é um associado a } q_i(x)(i = 1; 2; 3; \cdots; r).$$

Demonstração. Vamos provar que $f(x) \in F[X]$ sendo um polinômio não constante é irredutível ou pode ser escrito como produto de polinômios irredutíveis em $F[X]$. Considere $Grau(f(x)) = n$, temos que $n \geq 1$, faremos a demonstração por indução completa sobre n. No caso de $n = 1$, pelo Teorema 2.4.17, $f(x)$ é irredutível, portanto a propriedade é válida. Suponhamos que a propriedade é válida para todo polinômio de grau menor que n, ou seja, nossa hipótese de indução é que qualquer polinômio em $F[X]$ de grau menor que n é irredutível ou pode ser escrito como produto de polinômios irredutíveis em $F[X]$. Se $f(x)$ é irredutível em $F[X]$, nada temos que fazer. Caso contrário, $f(x)$ é redutível em $F[X]$, portanto pelo Teorema 2.4.18, $f(x)$ pode ser escrito com produto de dois polinômios de grau menor, ou seja, $f(x) =$

$g(x) \cdot h(x)$ onde $Grau(g(x)) < n$ e $Grau(h(x)) < n$. Aplicando a hipótese de indução em $g(x)$ e $h(x)$, ou seja, que $g(x)$ ou $h(x)$ é irredutível ou pode ser escrito como produto de polinômios irredutíveis em $F[X]$. Assim $f(x)$ é irredutível ou pode ser escrito como produto de polinômios irredutíveis em $[X]$, então a propriedade é válida para n. Portanto pelo princípio da indução completa a propriedade é válida para todo $n \geq 1$. Vamos provar que esta fatoração é única, a menos da ordem de fatores. Suponhamos que $f(x) = p_1(x) \cdot p_2(x) \cdot \cdot$ e $p_r(x) = q_1(x) \cdot q_2(x) \cdots q_s(x)$ com $p_i(x)$ e $q_j(x)$ irredutíveis. Como $p_1(x) \cdot [p_2(x) \cdots p_r(x)] = q_1(x) \cdot q_2(x) \cdots q_s(x)$, logo $p_1(x) \mid q_1(x) \cdot q_2(x) \cdots q_s(x)$, então $p_1(x) \mid q_j(x)$ para algum j. Reorganizando os $q_j(x)'s$, podemos assumir que$p_1(x) \mid q_1(x)$. Como $q_1(x)$ é irredutível, temos que $p_1(x)$ é um polinômio constante ou um associado de $q_1(x)$. No entanto,$p_1(x)$ é irredutível, e pela defnição de polinômio irredutível não pode ser um polinômio constante. Portanto, $p_1(x)$ é um associado de $q_1(x)$, com $p_1(x) = c_1 \cdot q_1(x)$ para algum polinômio constante c_1. Portanto $q_1(x) \cdot [c_1 \cdot p_2(x) \cdot p_3(x) \cdots p_r(x)] = p_1(x) \cdot p_2(x) \cdots p_r(x) = q_1(x) \cdot q_2(x) \cdots q_s(x)$ podemos cancelar $q_1(x)$, temos

$$p_2(x) \cdot [c_1 \cdot p3(x) \cdots p_r(x)] = q_2(x) \cdot q_3(x) \cdots q_s(x),$$

usando o mesmo argumento com relação $p_2(x)$, teremos

$$p_3(x) \cdot [c1 \cdot c2 \cdot p_4(x) \cdots p_r(x)] = q_3(x) \cdot q_4(x) \cdots q_s(x).$$

Usando o mesmo argumento e eliminando continuamente um polinômio irredutível de cada lado da igualade a cada etapa. Se $r = S$, então esse processo prova a unicidade da escrita. Então para completar a demonstração do teorema, devemos mostrar que $r = s$. Suponhamos por contradição que $r \neq s$, ou seja, $r < s$ ou $r > s$. Primeiro, suponha que $r > s$, após as etapas do processo anterior, todas os $q_j(x)'s$ serão eliminados e teremos o seguinte,

$$c_1 \cdot c2 \cdots c_s \cdot p_{s+1}(x) \cdot p_{s+2}(x) \cdots pr(x) = 1_F.$$

Isto mostra que $p_r(x) \mid 1_F$, pelo Item (7) do Teorema 2.4.9, temos $Grau(p_r(x)) \leq Grau(1_F) = 0$, assim $Grau(p_r(x)) = 0$, mas $p_r(x)$ é irredutível e pela defnição de polinômio irredutível, temos que $Grau(p_r(x) \geq 1$, logo chegamos a uma contradição. Portanto, $r > s$ não pode ocorrer. Analogamente mostra-se que $r < s$ também leva a uma contradição e não pode ocorrer. Portanto, $r = s$ é a única possibilidade. Concluímos então que a fatoração é única. □

3.6 Divisão como relação de equivalência e congruência de polinômios

A divisão de polinômios se assemelha à divisão dos números inteiros, nos permitindo estabelecer uma relação de equivalência, e pelo algorítmo da divisão nos oferece a oportunidade de extender a linguagem de congruência modular para os polinômios. Pelo teorema 2.4.7 sabemos que

$$p(x) = q(x) \cdot d(x) + r(x)$$

onde $r(x) = 0$ ou $Grau(r(x)) < Grau(q(x))$. Em consequência temos que,

$$p(x) - r(x) = q(x) \cdot d(x)$$

logo,

$$q(x) \cdot d(x) \mid p(x) - r(x)$$

ou o equivalente,

$$p(x) - r(x) \equiv 0 \ \mathrm{mod} q(x) \cdot d(x)$$

Portanto a congruência modular pode ser transposta para o corpo dos polinômios.

Vamos mostrar que a divisão de polinômios é uma relação de equivalência.
Dados os polinômios $p(x) = a_o + a_1x + \cdots + a_nx^n$, $q(x) = b_o + b_1x + \cdots + b_nx^n$ e $d(x) = c_o + c_1x + \cdots + c_nx^n$ pertencentes a $A[X]$ onde $p(x), q(x)$ e $d(x)$ são diferentes do polinômio identicamente nulo, a divisão é:
Reflexiva. Pois $d(x) \mid p(x) - p(x) = 0$.
Simétrica. Se $d(x) \mid p(x) - q(x)$ então, $d(x) \mid -(p(x) - q(x)) = q(x) - p(x)$ como os coeficientes são inteiros, sabemos que para quaisquer a, c inteiros, se c divide a, então c divide $-a$.
Transitiva. Se $d(x) \mid p(x) - q(x)$ e $d(x) \mid q(x) - s(x)$ logo, $d(x) \mid p(x) - q(x) + q(x) - s(x) = p(x) - s(x)$, então $d(x) \mid p(x) - s(x)$.
Em consequência do fato de a divisão ser uma relaçao de equivalência podemos definir a equivalência na relação de congruência, ou seja,
Reflexiva: $p(x) \equiv p(x)$ mod$d(x)$.
Simétrica: $p(x) \equiv q(x)$ mod$d(x)$, então $q(x) \equiv p(x)$ mod$d(x)$.
Transitiva: $p(x) \equiv q(x)$ mod$d(x)$ e $q(x) \equiv s(x)$ mod$d(x)$ então, $p(x) \equiv s(x)$ mod$d(x)$.

Podemos definir algumas propriedades operatórias importantes na congruência dos polinômios.

Proposição 6. *Sejam* $p(x), q(x), f(x), g(x), d(x) \in A[x]$ *com* $d(x) \neq 0$.

1) Se $p(x) \equiv q(x)$ *modd*(x) *e* $f(x) \equiv g(x)$ *modd*(x), *então* $p(x) + f(x) \equiv q(x) + g(x)$ *modd*(x).

2) Se $p(x) \equiv q(x)$ *modd*(x) *e* $f(x) \equiv g(x)$ *modd*(x), *então* $p(x) \cdot f(x) \equiv q(x) \cdot g(x)$ *modd*(x).

Demonstração. Suponhamos que $p(x) \equiv q(x)$ mod$d(x)$ e $f(x) \equiv g(x)$ mod$d(x)$. Logo, temos que $d(x) \mid p(x) - q(x)$ e $d(x) \mid f(x) - g(x)$.

1) Basta observar que $d(x) \mid (p(x) - q(x)) + (f(x) - g(x))$ e, assim $d(x) \mid (p(x) + f(x)) - (q(x) + g(x))$. Portanto, $p(x) + f(x) \equiv q(x) + g(x)$ mod$d(x)$.

2) Sabendo que $d(x) \mid g(x) - f(x)$ e $d(x) \mid q(x) - p(x)$ tem-se respectivamente que, $d \mid q(x) \cdot (g(x) - f(x))$ e $d \mid f(x) \cdot (q(x) - p(x))$ mas, $q(x) \cdot (g(x) - f(x)) + f(x) \cdot (q(x) - p(x)) = q(x) \cdot g(x) - f(x) \cdot p(x)$ logo, $d(x) \mid q(x) \cdot g(x) - f(x) \cdot p(x)$. Portanto, $q(x) \cdot g(x) \equiv f(x) \cdot p(x)$ mod $d(x)$.

□

Proposição 7. *Sejam* $p(x), q(x), f(x), d(x) \in A[x]$ *com* $d(x) \neq 0$. *Tem-se que* $p(x) + f(x) \equiv q(x) + f(x)$ *mod* $d(x)$ *se, e somente se,* $p(x) \equiv q(x)$ *mod* $d(x)$.

Demonstração. Se, $p(x) \equiv q(x)$ mod $d(x)$, segue imediatamente da proposição 2.4.1 $i)$ que $p(x) + f(x) \equiv q(x) + f(x)$ mod$d(x)$ pois, $f(x) \equiv f(x)$ mod $d(x)$. Reciprocamente, se $p(x) + f(x) \equiv q(x) + f(x)$ mod$d(x)$, então $d(x) \mid p(x) + f(x) - (q(x) + f(x))$, o que acarreta que $d(x) \mid p(x) - q(x)$ e, consequentemente, $p(x) \equiv q(x)$ mod$d(x)$. □

Capítulo 4

A congruência modular na resolução de problemas da educação básica

Nesse capítulo abordaremos através de exercícios, algumas situações em que o uso da congruência módulo m pode ser apresentado aos alunos da educação básica como uma ferramenta que em muitos casos poderá facilitar a abordagem e resolução de problemas, como também lhes dar uma compreensão mais significativa das estruturas das operações numéricas no conjunto dos números inteiros.

O objetivo dessa abordagem é dar ao professor do ensino básico algumas referências de situações (não apenas de questões) em que é posssível se aplicar os conceitos de congruência modular no contexto da sala de aula, cabendo a cada professor a análise de outras situações que possam ser apresentadas aos alunos afim de que o ensino da matemática se torne mais significativo, dinâmico e atrativo.

Iniciamos nossa lista com algumas situações interessantes do cotidiano, para despertar o interesse por parte dos alunos, mostrando que a congruência modular está presente em seu dia a dia.

4.1 A obtenção do dígito verificador do CPF

As pessoas que faziam anualmente a declaração de imposto de renda no Brasil, a partir de 1965, recebiam juntamente com o Manual de Orientações e formulários, o Cartão de Identificação do Contribuinte (CIC), que era um número de registro criado para controle desse tipo de imposto, porém, o Decreto-lei de 30 de dezembro de 1968 alteraria o Registro de Pessoas Físicas criado em 29 de novembro de 1965, para Cadastro de Pessoas Físicas (CPF). A inscrição no Cadastro de Pessoas Físicas, requerido pelo Ministério da Fazenda a partir desse decreto, se estenderia a todas as pessoas físicas, contribuíntes ou não do imposto de renda. O CPF é um documento emitido pela secretaria da receita federal. A idade mínima exigida para que uma pessoa seja inscrita no cadastro vem diminuindo nos últimos anos. Atualmente, assim que a criança nasce já deve ser registrada. O número do CPF é composto por 11 dígitos, obedecendo à seguinte estrutura: 8 Dígitos base + 1 dígito da região fiscal + 2 Dígitos verificadores.

Os nove primeiros dígitos são a base do cálculo para se determinar o décimo e décimo primeiro dígitos, que são os verificadores, sendo que esses serão um primeiro indicativo de que o documento é legítimo. Diremos que será um indicativo pois esse não é o único critério para se determinar se o número é verdadeiro ou falso, pois além de verificar a parte matemática o número do CPF deve constar no cadastro de registros da receita federal.

O nono algarismo identifica a unidade fiscal onde o CPF foi emitido, seguindo uma tabela pré-definida, como segue abaixo.

Dígito	Região
0	RS
1	DF, GO, MS, MT e TO
2	AC, AM, AP, PA, RO e RR
3	CE, MA e PI
4	AL, PB, PE e RN
5	BA e SE
6	MG
7	ES e RJ
8	SP
9	PR e SC

Tabela de Regiões Fiscais
Fonte: receita.economia.gov.br

O número do CPF é composto da seguinte sequência: $d_1d_2d_3d_4d_5d_6d_7d_8$ $d_9d_{10}d_{11}$, onde a sequência $d_1d_2d_3d_4d_5d_6d_7d_8$ é fornecida pelo sistema da receita federal, o dígito d_9 indica a região fiscal de origem do documento, e os dígitos verificadores, d_{10} e d_{11} são calculados pelo seguinte algorítmo: $d_1 \cdot 1 + d_2 \cdot 2 + d_3 \cdot 3 + d_4 \cdot 4 + d_5 \cdot 5 + d_6 \cdot 6 + d_7 \cdot 7 + d_8 \cdot 8 + d_9 \cdot 9 = X$ e verificada a sua congruência $mod 11$, ou seja, $X \equiv y$ mod 11 sendo que o valor de y será o primeiro dígito verificador.
Para o segundo dígito verificador incluímos $d_{10} = y$ e o algorítmo segue da seguinte forma: $d_1 \cdot 0 + d_2 \cdot 1 + d_3 \cdot 2 + d_4 \cdot 3 + d_5 \cdot 4 + d_6 \cdot 5 + d_7 \cdot 6 + d_8 \cdot 7 + d_9 \cdot 8 + d_{10} \cdot 9 = W$ e novamente verifica-se a congruência $mod 11$, $W \equiv K$ mod 11, onde o valor de K será o segundo dígito verificador. Quando $y = 10$ ou $K = 10$ o algarismo considerado será 0 (zero).

Vamos calcular os dígitos verificadores de um CPF fictício, cujos nove primeiros dígitos são 310232101. Pelo algoritmo acima teremos:

$$3 \cdot 1 + 1 \cdot 2 + 0 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 2 \cdot 6 + 1 \cdot 7 + 0 \cdot 8 + 1 \cdot 9 = 56$$
$$56 \equiv 1 \text{ mod } 11$$

logo o primeiro dígito verificador é 1.
Vamos calcular o segundo dígito verificador

$$3 \cdot 0 + 1 \cdot 1 + 0 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + 2 \cdot 5 + 1 \cdot 6 + 0 \cdot 7 + 1 \cdot 8 + 1 \cdot 9 = 52$$
$$52 \equiv 8 \bmod 11$$

então o segundo dígito verificador é 8, portando o número completo do CPF será 310232101-18.
Como o nono algarísmo é 1, pela tabela das regiões fiscais, nosso CPF fictício foi emitido em uma das unidades federativas DF, GO, MS, MT ou TO.

4.2 Dígito verificador do cartão de crédito

Na década de 1920 alguns comerciantes nos Estados Unidos ofereciam aos seus clientes cartões como cortesia para usarem em compras, sendo que estes cartões eram aceitos apenas pelos comerciantes que os emitiam. O Diners Club aprimorou essa prática, criando cartões que eram aceitos em vários tipos de estabelecimentos, cobrando dos comerciantes uma taxa percentual em cada transação, porém, com a perspectiva de que os portadores dos cartões gastariam mais que os não portadores, pois além de ser um símbolo de status, também havia a comodidade do pagamento de apena uma fatura mensal.

Ao final de seu primeiro ano de operações o Diners Club conquistou 42 mil membros, tornando-se em 1953 o primeiro cartão de débito aceito internacionalmente.

Porém, anos depois, ele ganhou dois concorrentes de peso. O primeiro deles, o BankAmericard, foi aceito em uma infinidade de estabelecimentos. Ele é o que conhecemos hoje como VISA. Neste mesmo ano, o Master Charge também foi criado.

Embora o seu sucesso não fosse tão grande quanto do VISA, conquistou grande clientela e chegou a mudar o nome para MasterCard. Hoje, é a segunda bandeira de cartões mais forte do mundo.

A maioria dos cartões de crédito no Brasil são formados por 16 dígitos, os 6 primeiros se referem à instituição financeira emissora, sendo que o primeiro desses dígitos identifica a bandeira do cartão, se for visa começa com 4, se for mastercard começa com 5 e etc. Os 9 dígitos seguintes são identificadores do cliente e o último é o dígito verificador, que confere junto com o código de segurança, a autenticidade do número do cartão.

O dígito verificador é calculado com uma fórmula conhecida por algoritmo de Luhn, em homenagem ao seu criador, Hans Peter Luhn (1896 - 1964) engenheiro da International Business Machines, IBM.

A verificação do número do cartão de crédito se dá da seguinte maneira:
Sejam $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}$ os dígitos do cartão. Multiplica-se os algarísmos de ordem ímpar por 2 e os de ordem par por 1. Ao se multiplicar os dígitos de ordem ímpar por 2 deve-se considerar a seguinte restrição:

$$2ai = \begin{cases} 2ai, \text{ se } 2a_i < 10 \\ 2a_i - 9, \text{ se } 2a_i \geqslant 10 \end{cases}$$

Soma-se os produtos obtidos e verifica-se a congruência módulo 10, ou seja, $2 \cdot a_1 + 1 \cdot a_2 + 2 \cdot a_3 + 1 \cdot a_4 + 2 \cdot a_5 + 1 \cdot a_6 + 2 \cdot a_7 + 1 \cdot a_8 + 2 \cdot a_9 + 1 \cdot a_{10} + 2 \cdot a_{11} + 1 \cdot a_{12} + 2 \cdot a_{13} + 1 \cdot a_{14} + 2 \cdot a_{15} + 1 \cdot a_{16} \equiv 0 \pmod{10}$.
Vamos utilizar a sequência 4593 6000 0968 9060 como o número fictício de um cartão de crédito e verificar se é autentico através do algorítmo.

$$2{\cdot}4+1{\cdot}5+2{\cdot}9+1{\cdot}3+2{\cdot}6+1{\cdot}0+2{\cdot}0+1{\cdot}0+2{\cdot}0+1{\cdot}9+2{\cdot}6+1{\cdot}8+2{\cdot}9+1{\cdot}0+2{\cdot}6+1{\cdot}0 \equiv 0 \pmod{10}$$

$$8+5+(18-9)+3+(12-9)+0+0+0+0+9+(12-9)+8+(18-9)+0+(12-9)+0 \equiv 0 \pmod{10}$$

$$60 \equiv 0 \pmod{10}.$$

Verificamos que o número do cartão está correto pois a soma dos produtos é congruênte a zero módulo 10.

Do mesmo modo que no caso do CPF, esse não é o único critério utilizado para se verificar a autenticidade do número do cartão de crédito.

4.3 Código de barras

A prática realizada por comerciantes, especialmente supermercados conhecida como balanço era muito comum, até meados do século XX. Consistia em fechar as portas por um dia, com o propósito de fazer a contagem manual de suas mercadorias, por mais de uma vez e por mais de um funcionário. Esta era a forma de se controlar os estoques,

porém este método acarretava prejuízos por perda de vendas neste dia e podia haver erros de contagem.

Surgiu então a necessidade de contabilizar de forma mais eficaz esses produtos. Após vários estudos e tentativas de elaboração de um sistema eficiente, em 1973 um código foi formalmente aceito e utilizado nos Estados Unidos e no Canadá, código esse conhecido por UPC (Universal Product Code). No estado de Ohio em junho de 1974 em um supermercado uma caixa de chicletes foi o primeiro produto a ser passado pelo caixa tendo o código lido por um scanner. O código era composto por 13 dígitos que eram traduzidos por barras brancas e pretas com um padrão pré-estabelecido. Mais tarde o código foi aprimorado de modo a identificar o país de origem do produto.

Desde sua criação, os códigos sofreram algumas alterações, porém não vamos discutir essas mudanças, vamos dar atenção apenas à versão que foi introduzida no Brasil em 1983, e que é utilizada hoje. Essa versão é composta por 13 dígitos e conhecida por EAN (European Article Numbering System). O sistema de código de barras é muito popular em nossos dias. Desde um simples picolé, a um refrigerador são identificados pelos códigos de barras. Nesta seção vamos discutir alguns aspectos dos códigos de barras e sua ligação com a matemática, especialmente com a congruência modular. (**??**)

Quem nunca foi em um supermercado e notou que ao operador passar um produto pelo leitor ótico por mais de uma vez, ele não realizou a leitura, então o operador digíta os algarísmos que estão abaixo das barras fazendo com que o sistema reconheça o produto que está sendo vendido. Vamos utilizar o código de barras da Figura 4.1 tanto para identificar a finalidade dos números quanto para calcular o dígito verificador do código.

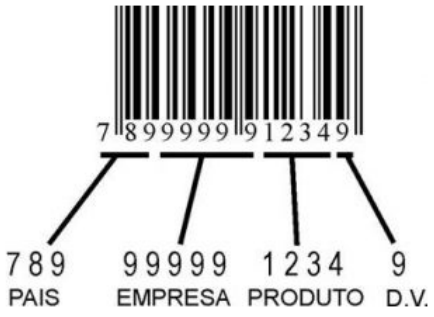

Figura 4.1: Código de barras

Fonte: Fictício

Os três primeiros dígitos identificam o país de cadastro do produto (não necessariamente onde ele foi produzido, mas onde foi registrado), o Brasil utiliza 789, a Argentina por exemplo, usa 779, Portugal, 560, Alemanha, qualquer um entre 400 e 440 e assim por diante. Alguns países como Estados Unidos e Canadá fogem a essa regra pois utilizam apenas 12 dígitos em seus códigos de barras. O segundo bloco de 5 dígitos(em nosso exemplo a sequência é de 5 dígitos, mas ela pode variar de 4 a 7 dígitos), identificam a empresa que fabricou o produto, os códigos identificadores das empresas são fornecidos pela GSI, organização mundial que estabelece parâmetros para comunicação empresarial em 150 países, os próximos quatro dígitos identificam o produto. Fornecem informações específicas do produto, como, quantidade, tipo de embalagem, peso e tamanho. por esse motivo o código estampado em um fardo de suco é diferente do que consta em uma caixa de 1 litro ou uma lata de 350 ml, ou de alguma embalagem menor que componha o fardo. Para completar a sequência do código, é utilizado um digíto que tem a função de "dígito verificador", sua utilidade é mostrar ao computador que fez a leitura do código se os outros dígitos estão corretos. O dígito verificador é calculado conforme o seguinte algorítmo:

Sejam $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}$ os 12 primeiros dígitos de um código de barras, os dígitos de ordem ímpar são multiplicados por 1, e os de ordem par, são multiplicados por 3, a seguir somam-se tais produtos $a_1 \cdot 1 + a_2 \cdot 3 + a_3 \cdot 1 + a_4 \cdot 3 + a_5 \cdot 1 + a_6 \cdot 3 + a_7 \cdot 1 + a_8 \cdot 3 + a_9 \cdot 1 + a_{10} \cdot 3 + a_{11} \cdot 1 + a_{12} \cdot 3$ o dígito verificador que chamaremos aqui de x adicionado à soma acima deve resultar em um número múltiplo de 10, ou seja, $a_1 \cdot 1 + a_2 \cdot 3 + a_3 \cdot 1 + a_4 \cdot 3 + a_5 \cdot 1 + a_6 \cdot 3 + a_7 \cdot 1 + a_8 \cdot 3 + a_9 \cdot 1 + a_{10} \cdot 3 + a_{11} \cdot 1 + a_{12} \cdot 3 + x \equiv 0 \mod 10$. Vamos aplicar o algorítmo ao código da figura 4.1

$$7 \cdot 1 + 8 \cdot 3 + 9 \cdot 1 + 9 \cdot 3 + 9 \cdot 1 + 9 \cdot 3 + 9 \cdot 1 + 9 \cdot 3 + 1 \cdot 1 + 2 \cdot 3 + 3 \cdot 1 + 4 \cdot 3 + x \equiv 0 \mod 10$$

$$161 + x \equiv 0 \mod 10.$$

Portanto, $x = 9$ é o dígito verificador.

4.4 Critérios de divisibilidade

Os critérios de divisibilidade por alguns números são ensinados aos alunos do ensino fundamental e podem ser abordados do ponto de vista da congruência modular, dando

aos estudantes tanto a oportunidade de conhecerem um pouco mais das estruturas dos números inteiros, quanto de instigá-los a desenvolverem tais critérios, privilégio que no método tradicional de ensino lhes é negado, pois o material didático apresenta apenas os resultados afim de que sejam memorizados e aplicados como uma regra na resolução dos problemas de divisibilidade.

A seguir apresentaremos algumas divisibilidades que fazem parte do currículo da segunda fase do ensino fundamental, consideraremos que os alunos tenham um cohecimento prévio de potênciação, ao menos das potências de base 10, e da expansão decimal dos números inteiros, ou seja, um número natural N seja da forma:

$$N = a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1.$$

4.4.1 Divisibilidade por 2

Tomando um número natural na sua forma extendida, ou seja,

$$N = a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1$$

observe que $10^{n-1} \equiv 10^{n-2} \equiv \cdots \equiv 10 \equiv 0 \pmod 2$ multiplicando cada termo por $a_n, a_{n-1}, \cdots, a_2$ e somando membro a membro teremos, $a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 \equiv 0 \pmod 2$, somando a_1 a ambos os membros da congruência temos, $a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1 \equiv a_1 \pmod 2$, o que mostra que N será divisível por 2 se a_1 o for, isso ocorrerá quando a_1 for par.

Exemplo 4.4.1. *Verifique se 1983 é divisível por 2.*

Note que a expansão decima de 1983 é:

$$1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10 + 3$$

aplicando a congruência modular teremos,

$$1983 \equiv 1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10 + 3 \pmod 2,$$

mas sabemos que $10 \equiv 0 \pmod 2$, logo $1983 \equiv 1 \cdot 0 + 9 \cdot 0 + 8 \cdot 0 + 3 \equiv \pmod 2$, como $3 \equiv 1 \pmod 2$, por transitividade segue que $1983 \equiv 1 \pmod 2$. Portanto, 1983 não é divisível por 2.

Observação. Analogamente obtemos as divisibilidades por 5 e por 10.

4.4.2 Divisibilidade por 3

Consideremos o número N na sua expansão decimal,

$$N = a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1$$

observe que $10^{n-1} \equiv 10^{n-2} \equiv \cdots \equiv 10 \equiv 1 \pmod 3$. Multiplicando cada termo por $a_n, a_{n-1}, \cdots, a_2$ e somando membro a membro teremos,

$$a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 \equiv a_n + a_{n-1} + \cdots + a_2 \pmod 3$$

somando a_1,

$$a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1 \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 \pmod 3.$$

Concluímos que N será divisível por 3 quando a soma de seus algarismos o for.

Observação. Visto que 10 deixa o mesmo resto na divisão por 3 e por 9, o critério de divisibilidade por 9 segue em sentido análogo.

Exemplo 4.4.2. *Verifique se 1467 é divisível por 3.*

$$1467 = 1 \cdot 10^3 + 4 \cdot 10^2 + 6 \cdot 10 + 7$$

como

$$10 \equiv 1 \pmod 3$$

aplicando a congruência modular

$$1 \cdot 10^3 + 4 \cdot 10^2 + 6 \cdot 10 + 7 \equiv 1 + 4 + 6 + 7 \equiv 18 \equiv 0 \pmod 3.$$

Portanto 1467 é divisível por 3.

4.4.3 Divisibilidade por 4

Consideremos o número N na sua expansão decimal,

$$N = a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1$$

observe que $10^{n-1} \equiv 10^{n-2} \equiv \cdots \equiv 10^2 \equiv 0 \pmod 4$ multiplicando cada termo por $a_n, a_{n-1}, \cdots, a_3$ e somando membro a membro teremos,

$$a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_3 \cdot 10^2 \equiv 0 \pmod 4$$

somando $a_2 \cdot 10 + a_1$ a ambos os membros

$$a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_3 \cdot 10^2 + a_2 \cdot 10 + a_1 \equiv a_2 \cdot 10 + a_1 \pmod 4.$$

Portanto, para que N seja divisível por 4 é necessário que o número $M = a_2 \cdot 10 + a_1$ seja divisível por 4.

Exemplo 4.4.3. *Verifique se 135478 é divisível por 4.*

$$135478 = 1 \cdot 10^5 + 3 \cdot 10^4 + 5 \cdot 10^3 + 4 \cdot 10^2 + 7 \cdot 10 + 8$$

sabemos que,

$$1 \cdot 10^5 \equiv 3 \cdot 10^4 \equiv 5 \cdot 10^3 \equiv 4 \cdot 10^2 \equiv 0 \pmod 4$$

como

$$7 \cdot 10 + 8 = 78 \equiv 2 \pmod 4.$$

Concluímos que 135478 não é divisível por 4. Além disso sabemos pela congruência que o resto de sua divisão euclidiana por 4 é 2.

Observação. Sabendo que $a_n \cdot 10^{n-1} \equiv a_{n-1} \cdot 10^{n-2} \equiv \cdots \equiv a_4 \cdot 10^3 \equiv 0 \pmod 8$ em sentido análogo obtemos o critério de divisibilidade por 8.

4.4.4 Divisibilidade por 6

Pela propriedade de congruência, $a \equiv b \pmod{\text{k}} \Leftrightarrow a \equiv b \pmod{\text{m}}$ e $a \equiv b \pmod{\text{n}}$ onde $m \cdot n = k$ e $mdc(m, n) = 1$ segue que $N \equiv 0 \pmod 6 \Leftrightarrow N \equiv 0 \pmod 2$ e $N \equiv 0 \pmod 3$.
Para que um múmero natural seja divisível por 6, basta que ele seja divisível por 2 e por 3 simultâneamente.

Exemplo 4.4.4. *Verifique se 2394 é divisível por 6.*

Como $4 \equiv 0 \pmod 2$, sabemos que 2394 é divisível por 2, e $2 + 3 + 9 + 4 = 18 \equiv 0 \pmod 3$, temos que 2394 é divisível por 3. Portanto 2394 é divisível por 6.

4.5 Exercícios de livros didáticos

A seguir apresentaremos um lista de exercícios que apresentam sugestões de situações onde a congruência modular pode ser aplicada. Ficando livre cada professor para ampliar esta lista com novas situações e atividades interessantes que motivem e ensinem seus alunos ainda mais. As referências para os exercícios a seguir estão em (CARVALHO; REIS, 2017) e (RUY; CASTRUCCI, 2015).

Exemplo 4.5.1. *A duração do ano solar (tempo que a Terra leva para dar uma volta completa em torno do Sol) não é exatamente de 365 dias, mas dura aproximadamente 365 dias e 6 horas. Por isso, sobram cerca de 6 horas todos os anos. Para corrigir esse problema, a cada 4 anos acrescenta-se o dia 29 de fevereiro ao calendário. Os anos com um dia a mais são chamados bissextos, e todos são múltiplos de 4. Mas fiquem atentos! Para que os cálculos do calendário tenham êxito, os anos que terminam com 00 só são bissextos se eles forem múltiplos de 400.*

a) Verifique se o ano 1822, que foi o ano da Independência do Brasil foi bissexto.
Podemos escrever: $1822 \equiv 0$ mod4? Se a resposta foi sim, então é bissexto, se a resposta for não, então não será.
Do critério de divisibilidade por 4 podemos reduzir a nossa congruência em $22 \equiv 0$ mod4? Não, pois $22 \equiv 2$ mod4. Portanto, 1822 não foi ano bissexto.

b) O ano de 1900 foi bissexto?
Note que $1900 \equiv 300$ mod 400. Logo, a resposta é não.

Exemplo 4.5.2. *Na sequência da figura 4.2, as figuras são formadas por cubos colados uns aos outros. Se a superfície externa precisar ser pintada, observe que na etapa 1 com 1 cubo serão pintados 4 quadrados, na etapa 2 com 2 cubos, serão pintados 10 quadrados e na etapa 3 com 3 cubos, serão pintados 14 quadrados.*

Figura 4.2: Cubos

a) Quantos quadrados seriam pintados na décima etapa?
Observe que em cada fase o número de quadrados pintados é sempre um múltiplo da fase, somado a dois, ou seja na fase 10 o número será $10 \cdot 4 + 2 = 42$. Logo, o número de quadrados pintados será 42.

b) Há alguma fase em que 105 quadrados serão pintados?
Chamando o número de quadrados de x devemos ter $x \equiv 2 \mod 4$, mas $105 \equiv 1 \mod 4$. Portanto a resposta é não.

Exemplo 4.5.3. *Verifique se 7539 é múltiplo de 3.*

Pelo critério de divisibilidade por 3, poderíamos somar os algarísmos, porém pela congruência modular, podemos somar os restos de cada algarísmo na sua divisão por 3.

$$7 \equiv 1 \mod 3$$
$$5 \equiv 2 \mod 3$$
$$3 \equiv 0 \mod 3$$
$$9 \equiv 0 \mod 3$$

Podemos somar então, $1 + 2 + 0 + 0 = 3 \equiv 0 \mod 3$. Portanto 7539 é múltiplo de 3.

Observação: Um raciocínio análogo pode ser usado para os múltiplos de 9.

Exemplo 4.5.4. *Sabe-se que o maior número possível divisível por 11e menos que 300 é dado por* $300 - r$*, em que r representa o resto da divisão de 300 por 11. Assim, qual o maior número, menor que 300, que é divisível por 11?*

Para respondermos à pergunta basta estabelecermos a congruência, $300 \equiv 3 \mod 11$, sendo 3 o resto, temos que o maior número menor que 300 divisível por 11 é 300 - 3 = 297.

Exemplo 4.5.5. *Qual o menor número natural que se deve adicionar a 706 para se obter um número divisível por13?*

Estabelecendo a congruência, temos que: $706 \equiv 4 \mod 13$, logo devemos somar 9 ao resto, pois $4 + 9 = 13$ fazendo com que $706 + 9 = 715$ seja divisível por 13.

Como uma proposta de atividade lúdica a ser realizada no ensino fundamental e médio, afim de que os alunos se interessem ainda mais pelo tema da congruência modular, pode ser realizada uma competição de "tabuada modular". Como exemplo podemos mencionar a tabuada de 2 mod 6.

$$2 \cdot 1 = 2$$

$$2 \cdot 2 = 4$$

$$2 \cdot 3 = 0$$

$$2 \cdot 4 = 2$$

$$2 \cdot 5 = 4$$

$$2 \cdot 6 = 0$$

$$2 \cdot 7 = 2$$

$$2 \cdot 8 = 4$$

$$2 \cdot 9 = 0$$

$$2 \cdot 10 = 2$$

Além de analisar o padrão que ocorre nos resultados dos produtos, os alunos podem ampliar seus conceitos das operações percebendo que as propriedades matemáticas são aplicadas a outros ambientes que vão além dos tradicionais apresentados a eles até então, e que é justamente essa ampla capacidade de adaptações que fez da matemática a ferramente tão poderosa que temos, capaz de dar suporte ao avanço tecnológico sem igual alcançado no século 21.

4.6 Congruência aplicada em polinômios

No anel dos polinômios podemos definir a mesma estrutura de divisão euclidiana existente no anel dos números inteiros, dessa forma podemos encontrar o resto da divisão de um polinômio por outro observando que dado um polinômio $p(x)$ com coeficientes inteiros, tem-se que: $p(x) = q(x) \cdot d(x) + r(x)$, onde $r(x)$ é o resto da divisão de $p(x)$ por $q(x)$. Uma vez que polinômios e números inteiros possuem propriedades aritméticas similares no que diz respeitos à fatoração única e à divisão com resto único. Podemos aplicar as propriedades de congruência dos inteiros nos polinômios como verificaremos a seguir.

Exemplo 4.6.1. *Calcule o resto da divisão de* $p(x) = x^2 + 5x + 6$ *por* $q(x) = x + 2$.

Por definição temos que:

$$x + 2 \equiv 0 \bmod(x + 2)$$

$$x \equiv -2 \bmod(x + 2), \text{ multiplicando por 5 ambos os membros}$$

$$5x \equiv -10 \bmod(x + 2) \text{ (a)}$$

$$x \equiv -2 \bmod(x + 2), \text{ elevando ao quadrado ambos os membros}$$

$$x^2 \equiv (-2)^2 \bmod(x + 2), \text{ temos}$$

$$x^2 \equiv 4 \bmod(x + 2) \text{ (b)}$$

podemos somar (a) e (b). Como o termo independente de $p(x)$ tem grau menor do que $q(x)$, podemos somá-lo livremente, pois o resto de sua divisão euclidiana por $x+2$ será ele próprio. Então temos,

$$x^2 + 5x + 6 \equiv 4 - 10 + 6 \bmod(x + 2)$$

obtemos então,

$$x^2 + 5x + 6 \equiv 0 \bmod(x + 2).$$

Portanto, o resto da divisão de $x^2 + 5x + 6$ por $x + 2$ é 0 (zero).

Exemplo 4.6.2. *(Colégio Naval - 2012). Seja* $P(x) = 2x^{2012} + 2012x + 2013$. *O resto* $r(x)$ *da divisão de* $p(x)$ *por* $d(x) = x^4 + 1$ *é tal que* $r(-1)$ *é:*

Sabemos que,

$$x^4 + 1 \equiv 0 \bmod(x^4 + 1),$$

então

$$x^4 \equiv -1 \bmod(x^4 + 1)$$

elevando ambos os membros a 503 temos,

$$(x^4)^{503} \equiv (-1)^{503} \bmod(x^4 + 1)$$

logo

$$x^{2012} \equiv -1 \text{ mod}(x^4 + 1)$$

multiplicando ambos os membros por 2 temos,

$$2x^{2012} \equiv -2 \text{ mod}(x^4 + 1)$$

como $2012x$ e 2013 tem grau menor do que $x^4 + 1$, podemos somá-los, então teremos

$$2x^{2012} + 2012x + 2013 \equiv 2012x + 2011 \text{ mod}(x^4 + 1)$$

o resto $r(x)$ é igual a $2012x + 2011$ e $r(-1) = 2012 \cdot (-1) + 2011 = -2012 + 2011 = -1$.

Exemplo 4.6.3. *(Colégio Naval - 2010). Sejam* $P(x) = 2x^{2010} - 5x^2 - 13x + 7$ *e* $q(x) = x^2 + x + 1$. *Tomando* $r(x)$ *como sendo o resto da divisão de* $p(x)$ *por* $q(x)$, *o valor de* $r(2)$ *será:*

Temos que

$$x^2 + x + 1 \equiv 0 \text{ mod}(x^2 + x + 1) \text{ então,}$$

$$x^2 \equiv -x - 1 \text{ mod}(x^2 + x + 1), \text{ (a)}$$

multiplicando por x ambos os membros teremos,

$$x^3 \equiv -x^2 - x \text{ mod}(x^2 + x + 1), \text{ mas por (a) temos que,}$$

$$x^3 \equiv -(-x - 1) - x \text{ mod}(x^2 + x + 1), \text{ o que equivale a,}$$

$$x^3 \equiv -1 \text{ mod}(x^2 + x + 1), \text{ elevando ambos os membros a 670, tem-se que,}$$

$$x^{2010} \equiv 1 \text{ mod}(x^2 + x + 1), \text{ multiplicando ambos os membros por 2,}$$

$$2x^{2010} \equiv 2 \text{ mod}(x^2 + x + 1),$$

por (a) temos que $-5x^2 = -5 \cdot (-x - 1) = 5x + 5$ somando aos termos de menor grau, tem-se

$$2x^{2010} - 5x^2 - 13x + 7 \equiv 5x + 5 - 13x + 7 + 2 \text{ mod}(x^2 + x + 1), \text{ resultando em}$$

$$2x^{2010} - 5x^2 - 13x + 7 \equiv -8x + 14 \text{ mod}(x^2 + x + 1),$$

Portanto, $r(x) = -8x + 14$ e $r(2) = -8 \cdot 2 + 14 = -2$.

Exemplo 4.6.4. *(Unicamp). Determine o resto da divisão de* $x^{100} + x + 1$ *por* $x^2 - 1$

Como

$$x^2 - 1 \equiv 0 \bmod(x^2 - 1)$$

então,

$$x^2 \equiv 1 \bmod(x^2 - 1)$$

logo,

$$x^{100} + x + 1 = (x^2)^{50} + x + 1 \equiv 1^{50} + x + 1 = x + 2 \bmod (x^2 - 1).$$

o resto da divisão é $x + 2$.

Exemplo 4.6.5. *(UEL). Na divisão de* $x^5 + 2x^4 - 3x^3 + x^2 - 3x + 2$ *por* $x^2 + x + 1$*, determine o resto.*

$$x^2 + x + 1 \equiv 0 \bmod(x^2 + x + 1)$$

$$x^2 \equiv -x - 1 \bmod(x^2 + x + 1)$$

$$x^2 \equiv -(x + 1) \bmod(x^2 + x + 1)$$

$$x^3 \equiv 1 \bmod(x^2 + x + 1)$$

$$x^4 \equiv x \bmod(x^2 + x + 1)$$

$$x^5 \equiv -x - 1 \bmod(x^2 + x + 1)$$

logo,

$$x^5+2x^4-3x^3+x^2-3x+2 \equiv -x-1+2x-3-x-1-3x+2 = -3x-3 \bmod(x^2+x+1)$$

Portanto, o resto da divisão é $-3x - 3$.

Exemplo 4.6.6. *(UFPI). Se o polinômio* $x^5 - 2x^4 + ax^3 + bx^2 - 2x + 1$ *for divisível pelo polinômio* $x^2 - 2x + 1$*, então determine o valor de* $a + b$*.*

temos que,

$$x^2 - 2x + 1 \equiv 0 \bmod(x^2 - 2x + 1)$$

$$x^2 \equiv 2x - 1 \bmod(x^2 - 2x + 1)$$

$$x^3 \equiv 3x - 2 \bmod(x^2 - 2x + 1)$$

$$x^4 \equiv 4x - 3 \bmod(x^2 - 2x + 1)$$

$$x^5 \equiv 5x - 4 \bmod(x^2 - 2x + 1)$$

$x^5 - 2x^4 + ax^3 + bx^2 - 2x + 1 \equiv 5x - 4 - 2(4x - 3) + a(3x - 2) + b(2x - 1) - 2x + 1 = 5x - 4 - 8x + 6 + 3ax - 2a + 2bx - b - 2x + 1 \equiv (3a + 2b - 5)x + (-2a - b + 3) \bmod(x^2 - 2x + 1)$ portanto o resto é $(3a + 2b - 5)x + (-2a - b + 3)$. Como o polinômio é divisível por $(x^2 - 2x + 1)$, devemos ter $(3a + 2b - 5)x + (-2a - b + 3) = 0x + 0$.

$$\begin{cases} 3a + 2b - 5 = 0 \\ -2a - b + 3 = 0 \end{cases}$$

resolvendo o sistema temos que $a = 1$ e $b = 1$. Logo, $a + b = 2$.

Exemplo 4.6.7. *(UNITAU). Encontre o valor de b para o qual o polinômio* $p(x) = 15x^{16} + bx^{15} + 1$ *seja divisível por* $x - 1$.

Sabemos que,

$$x - 1 \equiv 0 \bmod(x - 1),$$

$$x \equiv 1 \bmod(x - 1),$$

Logo,

$$x^{16} \equiv 1^{16} \bmod(x - 1) \text{ e },x^{15} \equiv 1^{15} \bmod(x - 1)$$

então,

$$15x^{16} + bx^{15} + 1 \equiv 15 \cdot 1 + b \cdot 1 + 1 = 16 + b \bmod(x - 1).$$

Como $p(x)$ é divisível por $x - 1$, temos que o resto é igual a zero, ou seja, $16 + b = 0$ e $b = -16$.

Exemplo 4.6.8. *(Colégio Naval). Determine o resto da divisão de* $p(x) = x^{127} + x^{10} + 1$ *por* $d(x) = x^3 + 1$

Sabendo que,

$$x^3 + 1 \equiv 0 \bmod(x^3 + 1)$$

segue que,

$$x^3 \equiv -1 \bmod(x^3 + 1)$$

logo,

$$x^{127}+x^{10}+1 = x^{126}x+x^9x+1 = (x^3)^{42}+(x^3)^3x+1 \equiv (-1)^{42}x+(-1)^3x+1 = x-x+1 = 1 \bmod(x^3 + 1).$$

Portanto, o resto da divisão de $p(x)$ por $d(x)$ é igual a 1.

Exemplo 4.6.9. *(IME). Prove que:* $p(x) = x^{999}+x^{888}+x^{777}+\cdots+x^{111}+1$ *é divisível por;* $d(x) = x^9 + x^8 + x^7 + \cdots + x + 1$

Observe inicialmente que, para um polinômio $(x^n - 1)$ vale a seguinte igualdade: $(x^n-1) = (x-1)\cdot(x^{n-1}+x^{n-2}+\cdots+x+1)$. De fato, pois se aplicarmos a propriedade distributiva ao segundo membro da igualdade teremos, $(x-1)\cdot(x^{n-1}+x^{n-2}+\cdots+x+1) = x^n + x^{n-1} + x^{n-2} + \cdots + x^2 + x - x^{n-1} - x^{n-2} - \cdots - x - 1 = x^n - 1$

Pela igualdade acima, temos que:

$$(x^{10} - 1) = (x - 1)(x^9 + x^8 + x^7 + \cdots + x + 1)$$

segue então que,

$$x^{10} - 1 \equiv 0 \bmod(x^9 + x^8 + x^7 + \cdots + x + 1)$$

e,

$$x^{10} \equiv 1 \bmod(x^9 + x^8 + x^7 + \cdots + x + 1)$$

logo,

$x^{999}+x^{888}+x^{777}+\cdots+x^{111}+1 = (x^{10})^{99}x^9+(x^{10})^{88}x^8+(x^{10})^{77}x^7+\cdots+(x^{10})^{11}x+1 \equiv x^9 + x^8 + x^7 + \cdots + x + 1 \bmod(x^9 + x^8 + x^7 + \cdots + x + 1)$

Portanto,

$$x^{999} + x^{888} + x^{777} + \cdots + x^{111} + 1 \equiv 0 \bmod(x^9 + x^8 + x^7 + \cdots + x + 1)$$

provando que $p(x)$ é divisível por $d(x)$.

Exemplo 4.6.10. *(CHINA). Se* $p(x) = x^{99} + x^{98} + \cdots + x + 1$*, qual é o resto quando* $p(x^{100})$ *é dividido por* $p(x)$*?*

Sabendo que,

$$x^{100} - 1 = (x - 1)(x^{99} + x^{98} + \cdots + x + 1)$$

tem-se que,

$$x^{100} - 1 \equiv 0 \bmod x^{98} + \cdots + x + 1)$$

logo,

$$x^{100} \equiv 1 \bmod x^{98} + \cdots + x + 1)$$

Observando que,

$p(x^{100}) = (x^{100})^{99} + (x^{100})^{98} + \cdots + (x^{100}) + 1 = 1^{99} + 1^{98} + \cdots + 1^1 + 1 = 1 + 1 + 1 + \cdots + 1 + 1 = 100 \bmod (x^{98} + \cdots + x + 1)$ concluímos que o resto da divisão de $p(x^{100})$ por $p(x)$ é igual a 100.

Considerações finais

Considerando a realidade escolar, a proposta do trabalho é de expandir os conceitos de congruência na educação básica, especificamente ao aluno da segunda fase do ensino fundamental e do ensino médio visto que o tema das congruências é abordado somente no ensino superior e em turmas preparatórias para olimpíadas de matemática. Porém seus princípios básicos são passíveis de restrições e adaptações de forma que o estudante destes níveis possa compreender e aplicar em diversas situações do seu nível de aprendizado.

Apesar de a congruência modular não fazer parte do currículo da educação básica, seus princípios estão presentes no cotidiano dos jovens adolescentes, através dos códigos de barras, CPF's, da divisão das horas nos relógios analógicos, etc. Quando consideramos o vível de abstração da matemática, a proposta de intervenção pedagógica deste trabalho a trará para a realidade do aluno, tornando assim mais concretos os seus princípios, e em consequência despertando o seu interesse e prazer pelo estudo desta disciplina.

Pretende-se com a proposta fornecer ao professor uma ferramenta que lhe possibilite a realização de abordagens interessantes do ponto de vista do aluno para o estudo da divisibilidade, e suas aplicações, a fim de que seja um elemento a mais para que se reverta o quadro atual de baixo nível de compreensão dos conceitos matemáticos revelado na última avaliação do PISA em 2018, e especialmente que seja mudada a situação da educação matemática brasileira para que o aluno possa se qualificar tanto para a vida profissional, quanto para o exercício da cidadania, qualificação esta que até o momento dos últimos testes aplicados foi revelada insuficiente.

Foi sugerida aqui uma sugestão de ensino diferenciado para a melhora do nível de conhecimento dos alunos da educação básica, deixamos como uma motivação para os professores comprometidos com a educação dos jovens estudantes para que pesquisem

e utilizem outros temas da matemática (pois são inúmeros) que estão presentes na vida moderna, com seus avanços tecnológicos, tendo em vista que os jovens estão imersos no mundo das tecnologias, aplicativos de celular, internet, jogos virtuais, etc. Há uma grande quantidade de temas interessantes relacionados diretamente com a matemática, como criptografia, linguagens de programação, robótica, que serão grandes instrumentos para despertar ainda mais no aluno o interesse e a paixão pelo estudo desta disciplina que foi considerada por Carl Friedrich Gauss como a rainha das ciências.

Referências Bibliográficas

BOYER, C. B. **História da matemática**. São Paulo: Editora da universidade de São Paulo, 1974.

CARVALHO, A. L. T.; REIS, L. F. **Matemática**. Tatuí: Casa Publicadora Brasileira, 2017.

DANTE, L. R. **Matemática conceitos e aplicações**. 1. ed. São Paulo: Ática, 2011.

DOMINGUES, H. H.; IEZZI, G. **Álgebra moderna**. 4. ed. São Paulo: Atual, 2003.

EDUCAÇÃO, M. d. Lei de diretrizes e bases da educação brasileira. Brasília, 1996.

_____. Base nacional comum curricular. Brasília, 2017.

FIORENTINI, D. **Alguns Modos de Ver e Conceder o Ensino de Matemática no Brasil**. Campinas: Editora da Unicamp, 1995.

GARCIA, A.; LEQUAIN, Y. **Elementos de álgebra**. Rio de Janeiro: Projeto Euclides, 2001.

GASPARIN, J. L. **Motivar Para a Aprendizagem Significativa**. Porto Alegre: Jornal Mundo Jovem, 2001.

HERNSTEIN, N. **Tópicos de álgebra**. São Paulo: Polígonos, 1970.

JANESCH, O. R.; TANEJA, I. J. **Álgebra 1**. 2. ed. Florianópolis: UFSC. Licenciatura em Matemática na Modalidade a Distância, 2011.

PISA, I. revela baixo desempenho escolar em leitura, matemática e ciências no brasil. **Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira**, 2018.

RUY, J. G. J.; CASTRUCCI, B. **A Conquista da Matemática**. São Paulo: FTD, 2015.