Universidade Federal
de São João del-Rei

Congruências e Aplicações em Polinômios

Leonardo Antônio Coelho

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação - Mestrado Profissional em Matemática em Rede Nacional, da Universidade Federal de São João Del-Rei, Campus Santo Antônio.

Orientador

Fábio Alexandre de Matos

São João Del-Rei
2019

AGRADECIMENTOS

Primeiramente, agradeço a Deus pela oportunidade de ter concluído esta etapa.

Aos meus pais, por terem me proporcionado condições para chegar até aqui, apesar de todas as dificuldades.

À minha esposa Sheila, por me apoiar, compreender e incentivar sempre.

À minha filha Alice, pela companhia sempre nos momentos de realização deste trabalho e pelo carinho.

Aos meus irmãos, pelo apoio durante todo este tempo.

Ao meu orientador professor Dr. Fábio Matos, pelo auxílio, disponibilidade e sugestões para lapidar a construção desta dissertação, sempre com muita paciência.

Aos professores que tive em minha longa trajetória de estudante, onde cada um deles contribuiu de alguma forma.

Aos professores Marcelo Veloso e Elias Vieira pela colaboração e disponibilidade.

Ao programa PROFMAT, por me permitir o crescimento intelectual e por proporcionar a diversos professores a evolução profissional.

Finalmente, agradeço a todos aqueles que contribuíram de alguma forma para a realização deste sonho. Deixo meu eterno agradecimento, pois sem vocês esta conquista teria sido muito mais difícil.

Dedico a apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação.

RESUMO

Este trabalho tem como objetivo utilizar congruência modular aplicada aos polinômios. Iremos utiliza-lá para a obtenção do resto da divisão entre dois polinômios e para o critério de irredutibilidade de Eisenstein. Será apresentada a congruência polinomial como uma base importante para o trabalho e o conceito de irredutibilidade polinomial. Apresentaremos as aplicações com a finalidade de estimular o uso pelos professores do ensino médio.

Palavras-chave: Polinômios, Congruência Polinomial, Critério de Irredutibilidade.

ABSTRACT

This work aims to use modular congruence for the polynomials. We will use the formula to get the rest of the separation between two principles and Eisenstein's irreducibility criterion. They will be a polynomial congruence as an important basis for the work and the concept of polynomial irreducibility. Applications for the purpose of stimulating use by high school teachers.

Key words: Polynomials, Polynomial Congruence, Irreducibility Criteria.

LISTA DE FIGURAS

SUMÁRIO

Capítulo 1

Introdução

Segundo [9], a congruência é o instrumento adequado quando se quer dar relevância ao resto da divisão euclidiana. Iremos utilizar exatamente essa ideia para obter o resto da divisão entre polinômios. As congruências foram introduzidas e estudadas por Gauss, no seu famoso "Disqusitiones Arithmeticae", publicado em 1801. As noções introduzidas por Gauss e suas notações foram rapidamente absorvidas e adotadas pelos matemáticos da época e são ainda até o momento presente. O estudo de congruências lineares pode vir a facilitar muito a vida de um estudante, diante do desafio de resolver questões envolvendo Teoria dos Números e principalmente os polinômios. Seguindo este raciocínio, apresentaremos ainda, uma importante aplicação de congruência para a verificação de irredutibilidade de um polinômio.

Tal assunto é de alta relevância e o nosso público alvo são os professores que lecionam no ensino médio e licenciandos em matemática. Na literatura o que encontramos à disposição são livros abordando o assunto de modo mais abrangente, saindo do foco de um aluno de ensino médio.

No capítulo 2, apresentamos os conceitos básicos envolvendo relações e operações binárias, priorizando as definições, propriedades e uma referência à estrutura de anel e de corpo. Em seguida, teremos a aritmética modular ou aritmética dos restos, que foi desenvolvida por Argand Gauss e é um excelente instrumento da teoria dos números, envolvendo o conceito de congruência e operador módulo no conjunto dos números inteiros. Finalizando o segundo capítulo, apresentamos o conceito de Anéis de Polinômios do mesmo modo como é estudado pelos alunos no ensino médio. Logo, temos a base para o entendimento das aplicações mostradas posteriormente e para o desenvolvimento dos capítulos subsequentes.

No capítulo 3, iremos abordar, em particular, a Congruência Polinomial módulo um número inteiro m e módulo um polinômio $d(x)$ não natural. Estes conceitos são fundamentais para o presente trabalho, pois se trata de uma aplicação de congruência à polinômios. Apresentamos o grau e as soluções de uma Congruência Polinomial módulo m assim como a possibilidade de haver o módulo composto.

O capítulo 4 traz o objeto de nosso estudo, isto é, a aplicação de congruências em polinômios para determinação do resto da divisão de um polinômio $p(x)$ por um polinômio $d(x)$. Podemos assim utilizar a Aritmética Modular de forma mais abrangente, tornando mais simples a obtenção de restos sem recorrer a dispositivos exaustivos e que demandam um tempo maior. Utilizamos, como exemplo, a resolução de questões de concursos de nível médio para acesso ao curso superior. Em seguida, abordaremos mais uma aplicação de congruência para verificar a irredutibilidade de um polinômio, em específico, o Critério de Irredutibilidade de Eisenstein, que possui como aplicação a congruência módulo p, onde p é número primo e utilizamos alguns exemplos para a aplicação do critério.

O capítulo 5 é destinado à implementação computacional da aplicação de congruência para obter o resto da divisão entre dois polinômios e do Critério de Irredutibilidade de Eisenstein. Procuramos uma forma mais interativa, objetiva e de fácil visualização do objeto de estudo.

Por fim, no último capítulo, chegamos à conclusão com as considerações finais, pensando que por meio deste trabalho, o professor de matemática do ensino básico possa ser motivado a inserir o ensino de congruências em seu planejamento, em particular no conteúdo de polinômios e mostrar as aplicações em sala de aula.

Capítulo 2

Conceitos Básicos

Neste capítulo, estudaremos duas estruturas fundamentais: anéis e corpos. Dentro desse contexto, abordaremos alguns resultados que são pré-requisitos necessários para o desenvolvimento dos demais capítulos.

2.1 Conjuntos, Relações e Operações Binárias

O estudo da teoria dos conjuntos foi iniciado por Georg Cantor (1845-1918), com uma série de artigos publicados a partir de 1874.

Por volta de 1870, quando estudava o problema de representação das funções reais, sua atenção se voltou para uma questão com a qual seu espírito tinha uma afinidade natural muito grande: a natureza do infinito. Esse foi o ponto de partida da criação da teoria dos conjuntos, que possui uma linguagem utilizada nas definições de vários elementos matemáticos.

2.1.1 Conjuntos

Entenderemos por conjunto uma coleção qualquer de objetos que chamaremos de elementos do conjunto. Por exemplo, o conjunto de alunos de uma sala de aula, o conjunto das vogais do alfabeto e o conjunto de atletas de um time de futebol. Em um conjunto é preciso ter uma regra clara que o define. Usaremos letras maiúsculas para simbolizar conjuntos e minúsculas para simbolizar elementos. Podemos descrever um conjunto por meio de palavras, regras, chaves e pelo diagrama de Venn.

Se x é um elemento do conjunto A, escrevemos $x \in A$ e leremos "x pertence a A". Caso contrário, escrevemos $x \notin A$ e leremos "x não pertence a A.

Podemos citar os exemplos de conjuntos numéricos clássicos, para os quais usaremos a seguinte nomenclatura: $\mathbb{N}$ (números naturais), $\mathbb{Z}$ (números inteiros), $\mathbb{Q}$ (números racionais), $\mathbb{R}$ (números reais) e $\mathbb{C}$ (números complexos).

Um conjunto sem elementos, é chamado de conjunto vazio e será denotado pelo símbolo $\varnothing$. Podemos citar como exemplo o conjunto $A = \{x \in \mathbb{R} \mid x^2 = -1\}$, ou seja, não há números reais que tornam a igualdade verdadeira, portanto o conjunto A não possui elementos, logo $A = \varnothing$.

Quando todo elemento de um conjunto A também é elemento de um conjunto B dizemos que A está contido em B ou A é subconjunto de B e denotamos por $A \subset B$. Consideraremos o conjunto vazio $\varnothing$ contido em qualquer conjunto. Assim, todo conjunto não vazio tem pelo menos dois subconjuntos, o conjunto vazio e ele mesmo.

Dois conjuntos A e B são iguais se possuem os mesmos elementos. Assim, temos claramente que $A = B$ se, e somente se, $A \subset B$ e $B \subset A$. Se o conjunto A não está contido no conjunto B, usaremos a notação $A \not\subset B$.

Em relação aos conjuntos numéricos temos: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

O conjunto dos elementos que pertencem simultaneamente a um conjunto A e a um conjunto B será denotado por

$$A \cap B = \{x : x \in A \text{ e } x \in B\} \textit{ e é chamado de interseção de } A \text{ e } B.$$

O conjunto dos elementos que pertencem a um conjunto A ou a um conjunto B será denotado por

$$A \cup B = \{x : x \in A \text{ ou } x \in B\} \textit{ e é chamado de união de } A \text{ e } B.$$

Claramente temos, quaisquer que sejam os conjuntos A e B, as seguintes propriedades:

$$A \cap \varnothing = \varnothing, \;\; A \cup \varnothing = A$$

$$(A \cap B) \subset A, \;\; A \subset (A \cup B).$$

Se $A \subset B$ também dizemos que B contém A e denotamos por $B \supset A$.

2.1.2 Produto cartesiano e Relação de Equivalência

Sejam A e B dois conjuntos não vazios. Definimos produto cartesiano dos conjuntos A e B como segue:

$$A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}$$

onde,

$$(a_1, b_1) = (a_2, b_2) \Leftrightarrow a_1 = a_2 \text{ e } b_1 = b_2.$$

Se $B = A$, denotamos por A^2 o produto $A \times A$.

Uma relação de equivalência em um conjunto A é um conjunto S de pares ordenados de elementos de A de modo que:

1. $(a, a) \in S$ para todo $a \in A$ (reflexividade).
2. $(a, b) \in S$ implica $(b, a) \in S$ (simetria).
3. $(a, b) \in S$, $(b, c) \in S$ implica $(a, c) \in S$ (transitividade).

O conjunto dos elementos $a \in A$, tais que $a\,S\,b$, para pelo menos um elemento $b \in B$, é chamado domínio da relação e é denotado por $D(S)$. E o conjunto dos elementos $b \in B$, tais que, para pelo menos um elemento $a \in A$, verifica-se $a\,S\,b$, é chamado de conjunto imagem da relação e é denotado por $Im(S)$.

Por exemplo, $S = \{(a, a) : a \in A\}$ define a relação de igualdade no conjunto A, que é evidentemente uma relação de equivalência em A.

Se $A = \mathbb{R}$ então a interpretação geométrica nos diz que o subconjunto S do plano $\mathbb{R}^2$ contém a reta $y = x$ e é simétrico em relação a essa mesma reta, diagonal dos 1º e 3º quadrantes do plano.

Por exemplo, se A é o conjunto de retas do plano, paralelismo define uma relação S entre pares de elementos do conjunto A.

Exemplo 2.1.1 *Em matemática, objetos diferentes em um contexto podem ser vistos como iguais em outro.*

Temos que $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, $i^5 = i$, $i^6 = -1$, $i^7 = -i$, $i^8 = 1$. *Temos que para efeito de achar potências da unidade imaginária i, os números são iguais se tiverem o mesmo resto na divisão por* 4, *ou seja, quando escrevemos aqui* $1 = 5$, *o número* 1 *não é igual ao número* 5 *como números inteiros, mas se olharmos como potência de i, possui a mesma imagem, portanto, segundo esse critério, podemos dizer que* 1 *é equivalente a* 5. *Assim, estamos dizendo que a potência i com expoente* 1 *é igual a potência i com expoente* 5. *Se existir uma função que relaciona o conjunto dos inteiros positivos com o conjunto dos números complexos, que leva um número inteiro positivo na potência i deste inteiro, alguns elementos possuem a mesma imagem, então para efeito de potência, os elementos são diferentes, mas como consequência são iguais.*

O que é necessário fazer para que estas distinções fiquem claras, é uma generalização apropriada da noção de igualdade, isto é, nós necessitamos de mecanismo formal para especificar quando duas quantidades são iguais ou não numa certa colocação. Tais mecanismos são as relações de equivalência.

Quando uma relação S em um conjunto A for de equivalência, vamos, em geral, usar a notação $\sim$ em vez de S.

Seja $\sim$ uma relação de equivalência em um conjunto A e seja $x \in A$, vamos definir agora o que chamamos por *classe de equivalência* $\overline{x}$ do elemento x em relação a $\sim$, a qual denotaremos por $\overline{x} = \{a \in A : a \sim x\}$.

Exemplo 2.1.2 *Seja* $A = \mathbb{Z} = \{\ldots, -k, \ldots, -1, 0, 1, \ldots, m, \ldots\}$ *e seja* n *um número inteiro arbitrariamente fixado.*

Vamos definir uma relação de equivalência em $\mathbb{Z}$ *do seguinte modo:* $x, x' \in \mathbb{Z}, x \sim x' \Leftrightarrow x - x'$ *é um múltiplo inteiro de* n.

Observe que $\sim$ *é uma relação de equivalência em* $\mathbb{Z} \times \mathbb{Z}$. *De fato:*

i) $\sim$ *é uma relação reflexiva, pois temos que* $x - x = 0 = n \cdot 0$ *para todo* $x \in \mathbb{Z}$, *logo* $x \sim x$.

ii) $\sim$ *é uma relação simétrica, pois temos que* $x - x' = n \cdot k_1$, *então* $x' - x = n \cdot (-k_1)$ *para todo* $x, x' \in \mathbb{Z}$, *logo* $x' \sim x$ *se, e somente se,* $x \sim x'$.

iii) $\sim$ *é uma relação transitiva, pois se* $x \sim x'$ *e* $x' \sim x''$, *então temos que* $x - x' = n \cdot k_1$ *e* $x' - x'' = n \cdot k_2$, *logo* $x - x' + (x' - x'') = n \cdot k_1 + n \cdot k_2$ *e portanto* $x' - x'' = n \cdot (k_1 + k_2)$ *ou seja,* $x' - x''$ *é múltiplo de* n, *logo* $x' \sim x''$.

Logo, $\sim$ *define uma relação de equivalência em* $\mathbb{Z}$. *Essa relação de equivalência recebe o nome de congruência módulo* n *e é geralmente indicada por* $\equiv (mod\, n)$.

Assim, $x, x' \in \mathbb{Z}$, $x \equiv x' (mod\, n)$ *se, e somente se,* $x - x'$ *é um múltiplo inteiro de* n. *Vamos agora calcular a classe* $\overline{x}$, *relativamente a* $\equiv (mod\, n)$. *Se* $x \in \mathbb{Z}$, $\overline{x} = \{a \in \mathbb{Z} : a \equiv x\, (mod\, n)\}$ *então* $a \in \overline{x}$ *se, e somente se,* $a - x = k \cdot n$, $k \in \mathbb{Z}$ *se, e somente se,* $a = x + k \cdot n$, $k \in \mathbb{Z}$. *Daí segue que:* $\overline{x} = \{x + kn : k \in \mathbb{Z}\}$.

Observe que se $n = 0$ *temos que* $\overline{x} = \{x\}$ *e que* $\equiv (mod\, 0)$ *nada mais é do que a relação de igualdade em* $\mathbb{Z}$, *e nesse caso existe um número infinito de classes* $\overline{x} = \{x\}$ *em* $\mathbb{Z}$. *Se* $n > 0$ *a relação* $\equiv (mod\, n)$ *nos fornece exatamente* n *classes distintas quais sejam* $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

Assim, por exemplo, $\equiv (mod\, 3)$ *nos fornece exatamente as classes* $\overline{0}, \overline{1}, \overline{2}$ *que são as classes dos números que deixam respectivamente restos* 0, 1 *e* 2 *na divisão por* 3.

Exemplo 2.1.3 *Seja o conjunto dos números inteiros em relação aos números que são congruentes módulo* 5 *nele definido. Determinamos as classes de equivalência em que todos os elementos possuem o mesmo resto. Classe dos elementos que deixam resto zero.*

$\overline{0} = \{x \in \mathbb{Z};\ x \equiv 0\, mod\, 5\} = \{0, \pm 5, \pm 10, \pm 15, \ldots\}$
$\overline{1} = \{x \in \mathbb{Z};\ x \equiv 1\, mod\, 5\} = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$
$\overline{2} = \{x \in \mathbb{Z};\ x \equiv 2\, mod\, 5\} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$
$\overline{3} = \{x \in \mathbb{Z};\ x \equiv 3\, mod\, 5\} = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$
$\overline{4} = \{x \in \mathbb{Z};\ x \equiv 4\, mod\, 5\} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$
$\overline{5} = \{x \in \mathbb{Z};\ x \equiv 5\, mod\, 5\} = \{0, \pm 5, \pm 10, \pm 15, \ldots\} = \overline{0}$

Podemos perceber que a classe $\overline{5}$ *é equivalente à classe* $\overline{0}$, *já que ambas possuem os mesmos elementos. Nota-se que as cinco classes descritas, descrevem todo o conjunto dos inteiros.*

Agora vamos definir a noção de conjunto quociente.

Seja $\sim$ uma relação de equivalência em um conjunto A, chamamos de conjunto quociente de A a relação de equivalência $\sim$ e denotamos por $A/_{\sim}$ ao conjunto de todas as classes de equivalência relativamente a relação $\sim$.

Assim,

$$A/_{\sim} = \{\overline{x} : x \in A\}.$$

Na relação $\equiv (mod\, n)$, $n > 0$ em $\mathbb{Z}$ temos $\mathbb{Z}_{/\equiv(mod\, n)} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ que também será representado por $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$.

Uma partição de um conjunto A é uma coleção de subconjuntos não vazios disjuntos de A cuja união é A. No exemplo 2.1.3, temos que uma partição do conjunto será $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$.

Em especial, os elementos do conjunto $\mathbb{Z}_m$ acima formam um sistema completo de restos módulo m, pois tomando quaisquer dois elementos distintos de $\mathbb{Z}_m$ como classe de equivalência, a interseção entre eles é o conjunto vazio e a união de todos eles formam o conjunto $\mathbb{Z}$. No caso em que os elementos forem iguais, a interseção é ele mesmo, ou seja, o próprio elemento.

Teorema 2.1.1 *As classes de equivalência de um conjunto A formam uma partição de A. Reciprocamente, para toda partição P de um conjunto A, existe uma relação de equivalência em A cujas classes de equivalência são os elementos de P.*

Demonstração. Seja $\equiv$ uma relação de equivalência em A. Para todo $a \in A$ temos $a \in \overline{a}$ pela propriedade reflexiva. Assim, $\overline{a} \neq \emptyset$ e a união de todas as classes de equivalência de A é A. Assumindo que $a \equiv b$, iremos supor que $c \in \overline{a}$, assim $a \equiv c$. Sabendo que $a \equiv b$ e que $\equiv$ é simétrica, então $b \equiv a$. Como $\equiv$ é transitiva, $b \equiv c$. Assim, $c \in \overline{b}$ e isso mostra que $\overline{a} \subset \overline{b}$. De forma análoga, para todo $b \in A$ temos $b \in \overline{b}$ pela propriedade reflexiva. Assim, $\overline{b} \neq \emptyset$ e a união de todas as classes de equivalência de A é A. Assumindo que $b \equiv a$, iremos supor que $c \in \overline{b}$, assim $b \equiv c$. Sabendo que $b \equiv a$ e que $\equiv$ é simétrica, então $a \equiv b$. Como $\equiv$ é transitiva, $a \equiv c$. Assim, $c \in \overline{a}$ e isso mostra que $\overline{b} \subset \overline{a}$. Logo $\overline{a} = \overline{b}$.

Vamos agora provar que duas classes de equivalência distintas são disjuntas. Com efeito, suponha que $\overline{a}$ e $\overline{b}$ possuem um elemento c em comum. Isso implica que $c \equiv a$ e $c \equiv b$. Pela propriedade transitiva $a \equiv b$ e, portanto, $\overline{a} = \overline{b}$. Se $A = A_1 \cup A_2 \cup \ldots \cup A_n$ e $A_i \cap A_j = \emptyset$, então $a \sim b$ para todo $a, b \in A_i$ e $i, j = 1, 2, \ldots, n$. □

Exemplo 2.1.4 *Pelo exemplo 2.1.3, temos que* $\mathbb{Z} = [0] \cup [1] \cup \ldots \cup [m-1]$.

2.1.3 Operação binária de um conjunto

Seja A um conjunto não vazio, uma operação binária interna em A, $*$, é uma função do produto cartesiano $A \times A$ em A.

Notação:

$$* : A \times A \longrightarrow A$$

$$(x, y) \longmapsto x * y$$

com $x \in A$, $y \in A$ e $(x * y) \in A$.

Exemplo 2.1.5 $(x, y) \longmapsto x - y$ *é uma operação interna em* $\mathbb{Z}$*, ou seja,* $* : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$
$(x, y) \longmapsto x - y$ *com* $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ *e* $(x - y) \in \mathbb{Z}$.

Exemplo 2.1.6 $(x, y) \longmapsto x - y$ *não é uma operação interna em* $\mathbb{N}$.
$(x, y) \longmapsto x - y$ *com* $x \in \mathbb{N}$, $y \in \mathbb{N}$ *e nem sempre* $(x - y) \in \mathbb{N}$, *pois se* $x - y < 0$ *temos que* $(x - y) \notin \mathbb{N}$

Uma operação binária $*$ é comutativa, associativa, distributiva em relação à soma, possui elemento neutro e possui elemento simetrizável. Se um conjunto não vazio possui duas operações binárias e satisfaz essas propriedades, é chamado de anel.

Usualmente, os símbolos (+) e (•) significam respectivamente operações de soma e multiplicação usuais em referência à adição e à multiplicação de números inteiros, que são as primeiras operações binárias conhecidas.

Com as operações usuais, o conjunto $\mathbb{Z}$ é um anel por satisfazer as duas operações binárias mencionadas acima. Iremos assumir como verdade as propriedades aritméticas sem as demonstrações.

Um anel é chamado de corpo se, e somente se, todo elemento não-nulo é invertível, ou seja $\forall x \in A, x \neq 0, \exists\, y \in A$, tal que $x \cdot y = y \cdot x = 1$.

Podemos considerar agora o conjunto S

$$S = \mathbb{Z} \times \mathbb{Z} \backslash \{0\} = \{(a, b);\ a,\ b \in \mathbb{Z} \text{ e } b \neq 0\}.$$

Para $(a, b), (c, d) \in S$, definimos

$$(a, b) \sim (c, d) \Longleftrightarrow a \cdot d = b \cdot c.$$

A relação binária acima é uma relação de equivalência em S.

Demonstração. De fato, para todo $(a, b) \in S$, temos $a \cdot b = b \cdot a$, logo $(a, b) \sim (a, b)$.

Suponhamos que $(a, b) \sim (c, d)$. Então, $a \cdot d = b \cdot c$ e $d \cdot a = a \cdot d = b \cdot c = c \cdot b$. Logo, $(c, d) \sim (a, b)$.

Suponhamos que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Então (I) $a \cdot d = b \cdot c$ e (II) $c \cdot f = d \cdot e$. Multiplicando a igualdade (I) por f e a igualdade (II) por b, obtemos $a \cdot d \cdot f = b \cdot c \cdot f = b \cdot d \cdot e$. Pelas propriedades da multiplicação em $\mathbb{Z}$, temos $d \cdot (a \cdot f) = d \cdot (b \cdot e)$. Como $d \neq 0$, pela lei do cancelamento em $\mathbb{Z}$, temos $a \cdot f = b \cdot e$. Portanto, $(a, b) \sim (e, f)$. □

Consideremos o conjunto quociente $\mathbb{Q} = S/\sim$. Então,

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}\backslash\{0\}/\sim = \{\overline{(a,b)};\ (a,b) \in \mathbb{Z} \times \mathbb{Z}\backslash\{0\}\}.$$

Denotamos por $\frac{a}{b}$ a classe de equivalência de (a,b), isto é, $\frac{a}{b} = \overline{(a,b)}$. Dessa maneira,

$$\frac{a}{b} = \overline{(a,b)} = \overline{(c,d)} = \frac{c}{d} \iff (a,b) \sim (c,d) \iff a \cdot d = b \cdot c$$

$$\mathbb{Q} = \left\{ \frac{a}{b};\ a,\ b \in \mathbb{Z} \text{ e } b \neq 0 \right\},\ \textit{onde}\ \ \frac{a}{b} = \frac{c}{d}\ \textit{se, e somente se,}\ a \cdot d = b \cdot c.$$

Chamamos o elemento $\frac{a}{b} \in \mathbb{Q}$ de fração e os elementos a e $b \neq 0$ em $\mathbb{Z}$, respectivamente, de numerador e denominador da fração. Podemos dar a $\mathbb{Q}$ uma estrutura de corpo.

2.2 Aritmética dos números inteiros

Segundo [7], no conjunto dos números naturais, a diferença entre a e b só está definida se $a \geqslant b$. Mas há questões envolvendo a ideia de subtração de números naturais em que o minuendo é menor que o subtraendo, por exemplo, gastar mais do que se tem. Para enfrentar essas questões, foi preciso ampliar o conjunto do números naturais, com a adjunção de novos números, os *números negativos*, introduzidos a princípio para possibilitar uma resposta a uma subtração qualquer de dois elementos de $\mathbb{N}$. Esse acontecimento gerou naturalmente a necessidade de estender as operações e relação de ordem de $\mathbb{N}$ ao novo conjunto, formado pelos números naturais e os números negativos.

A ideia intuitiva é que, por exemplo, todas as "diferenças" $0-1$, $1-2$, $2-3$, $3-4, \ldots$ de alguma maneira são "equivalentes"e representam o mesmo "número", um novo número que veio a ser indicado com o tempo por -1. De maneira análoga, introduzem-se os números -2, $-3, \ldots$. Obtidos esses novos números, é preciso ainda incorporá-los consistentemente ao conjunto dos números naturais.

i) Estender para o novo conjunto numérico, ou seja, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, +1, +2, +3, \ldots\}$, as operações de adição e multiplicação de números naturais. Isso significa, por exemplo, dar uma definição de adição no novo conjunto que, quando aplicada ao subconjunto dos números naturais (parte do novo conjunto), leve aos mesmos resultados que a adição de números naturais. Por exemplo, como $2 + 3 = (3-1) + (4-1) = (3+4) - (1+1) = 7 - 2 = 5$, é razoável esperar que $(-2) + (-3) = (1-3) + (1-4) = (1+1) - (3+4) = 2 - 7 = -5$ (notar que $2-7$ é uma das "diferenças"que definem -5).

ii) Estender para $\mathbb{Z}$ a ideia de "menor"e "maior"a partir das (e coerentemente com as) ideias correspondentes em $\mathbb{N}$. Feito isso, podemos, por fim, nos referir a $\mathbb{Z}$ como o

sistema (ou campo) dos números inteiros.

Obviamente, essas considerações visam apenas dar uma ideia despretensiosa da construção dos números inteiros. Esse desenvolvimento, que, quando feito com rigor e formalismo, é bastante trabalhoso e até tedioso.

2.2.1 Divisibilidade em $\mathbb{Z}$

Diz-se que o número inteiro a é divisor do número inteiro b, ou que o número b é divisível por a se é possível encontrar $c \in \mathbb{Z}$ tal que $b = ac$. Nesse caso, pode-se dizer também que b é múltiplo de a. Para indicar que a divide b, usaremos a notação $a \mid b$.

Por exemplo, -2 divide 6 porque $6 = (-2)(-3)$. Se $a \mid b$ e $a \neq 0$, o número inteiro c tal que $b = ac$ será indicado por b/a e chamado quociente de b por a.

A relação entre elementos de $\mathbb{Z}$, definida por $x \mid y$, possui as seguintes propriedades:

i) $a \mid a$ (reflexividade)

De fato, $a = a \cdot 1$.

ii) Se $a, b \geqslant 0$, $a \mid b$ e $b \mid a$, então $a = b$.

Por hipótese, $b = a \cdot c_1$ e $a = b \cdot c_2$. Se $a = 0 (b = 0)$, então $b = 0 (a = 0)$. Suponhamos, pois, $a, b > 0$. Como $a = ac_1c_2$, segue que $c_1c_2 = 1$. Mas c_1 e c_2 são inteiros e, portanto, essa igualdade só é possível para $c_1 = c_2 = 1$. De onde $a = b$.

iii) Se $a \mid b$ e $b \mid c$, então $a \mid c$. (transitividade)

iv) Se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$, quaisquer que sejam os inteiros x e y.

Por hipótese, $b = ad_1$ e $c = ad_2$. Daí, $bx = a(xd_1)$ e $cy = a(yd_2)$. Somando membro a membro essas igualdades, obtemos:

$$bx + cy = a(xd_1) + a(yd_2) = a(xd_1 + yd_2).$$

Então, devido à definição dada, $a \mid (bx + cy)$.

Dessa propriedade, segue em particular que:

- Se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$ e $a \mid (b - c)$.
- Se $a \mid b$, então $a \mid bx$, qualquer que seja o inteiro x.

v) Se $a \mid b$ e $c \mid d$, então $ac \mid bd$.

Por hipótese, $b = ar$ e $d = cs$ para convenientes inteiros r e s. Multiplicando-se membro a membro essas igualdades, obtém-se $bd = (ac)(rs)$.De onde $ac \mid bd$.

Uma propriedade característica dos números inteiros é a de ser vazio o conjunto $\{x \in \mathbb{Z};\ 0 < x < 1\}$. Isto implica que se $c \in \mathbb{Z}$ é tal que $c > 0$, então $c \geqslant 1$.

Da propriedade acima decorre a *Propriedade Arquimediana* de $\mathbb{Z}$, ou seja, se a, $b \in \mathbb{Z}$, com $b \neq 0$, então existe $n \in \mathbb{Z}$ tal que $nb > a$.

De fato, como $|b| > 0$, temos que $|b| \geqslant 1$, logo

$$(\,|a| + 1\,)|b| \geqslant |a| + 1 > |a| \geqslant a.$$

Na desigualdade acima tomamos $n = |a| + 1$, se $b > 0$ e $n = -(\,|a| + 1\,)$, se $b < 0$.

Mesmo quando um número inteiro a não divide o número inteiro b, Euclides, nos seus *Elementos*, utiliza, sem enunciar explicitamente, o fato de que é sempre possível efetuar a divisão de b por a, com resto. Este resultado, é um importante instrumento na obra de Euclides e apresentamos a demonstração abaixo.

Teorema 2.2.1 *Sejam a e b dois números inteiros com $a \neq 0$. Existem dois únicos números inteiros q e r tais que*

$$b = a \cdot q + r, \quad com \quad 0 \leqslant r < |a|.$$

Demonstração. Considere o conjunto

$$S = \{x = b - ay;\ y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Existência: Pela *Propriedade Arquimediana*, existe $n \in \mathbb{Z}$ tal que $n(-a) > -b$, logo $b - na > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo princípio da boa ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = b - aq$. Sabemos que $r \geqslant 0$. Vamos mostrar que $r < |a|$. Suponhamos por absurdo que $r \geqslant |a|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |a| + s$, logo $0 \leqslant s < r$. Mas isto contradiz o fato de r ser o menor elemento de S, pois $s = b - (q \pm 1)a \in S$, com $s < r$.

Unicidade: Suponha que $b = aq + r = aq' + r'$, onde $q,\ q',\ r,\ r' \in \mathbb{Z}$, $0 \leqslant r < |a|$ e $0 \leqslant r' < |a|$. Assim, temos que $-|a| < -r \leqslant r' - r < |a|$. Logo, $|r' - r| < |a|$.

Por outro lado, $a(q - q') = r' - r$, o que implica que

$$|a||q - q'| = |r' - r| < |a|,$$

o que só é possível se $q = q'$ e consequentemente, $r = r'$.

□

Nas condições do teorema acima, os números q e r são chamados, respectivamente, de quociente e de resto da divisão de b por a.

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

Exemplo 2.2.1 *O quociente e o resto da divisão de* 25 *por* 6 *são* $q = 4$ *e* $r = 1$. *O quociente e o resto da divisão de* -25 *por* 6 *são* $q = -5$ *e* $r = 5$.

Máximo divisor comum

Diremos que um número natural d é um máximo divisor comum (*mdc*) de dois números inteiros a e b, não simultaneamente nulos, se possuir as seguintes propriedades:

i) d é um divisor comum de a e de b, e

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

$$d = mdc(a, b) \Longrightarrow d \mid a \text{ e } d \mid b.$$

Lema 2.2.1 *Sejam* $a, b, n \in \mathbb{Z}$. *Se existe* $mdc(a, b - na)$, *então* $mdc(a, b)$ *existe e*

$$mdc(a, b) = mdc(a, b - na).$$

Demonstração. Seja $d = mdc(a, b - na)$. Como $d \mid a$ e $d \mid (b - na)$, segue que d divide $b = b - na + na$. Logo, d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b. Logo, c é um divisor comum de a e $b - na$ e, portanto, $c \mid d$. isso prova que $d = mdc(a, b)$. □

Algoritmo de Euclides

A seguir, apresentaremos a prova construtiva da existência do mdc da por Euclides (Os Elementos, Livro VII, Proposição 2). O método, chamado de *Algoritmo de Euclides*, é um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios. Dados $a, b \in \mathbb{N}$, podemos supor $a \leqslant b$. Se $a = 1$ ou $a = b$, ou ainda $a \mid b$, sabemos que $mdc(a, b) = a$. Suponhamos, então, que $1 < a < b$ e que $a \nmid b$. Logo, pela divisão euclidiana, podemos escrever

$$b = aq_1 + r_1, \quad \text{com } 0 < r_1 < a.$$

Temos duas possibilidades:

a) $r_1 \mid a$, e, em tal caso, pelo Lema 2.2.1,

$$r_1 = mdc(a, r_1) = mdc(a, b - q_1 a) = mdc(a, b),$$

e termina o algoritmo, ou

b) $r_1 \nmid a$, e, em tal caso, podemos efetuar a divisão de a por r_1, obtendo

$$a = r_1 q_2 + r_2, \quad \text{com } 0 < r_2 < r_1.$$

Novamente, temos duas possibilidades:

a') $r_2 \mid r_1$, e, em tal caso, novamente pelo Lema 2.2.1,

$$r_2 = mdc(r_1, r_2) = mdc(r_1, a - q_2 r_1) = mdc(r_1, a) = mdc(b - q_1 a, a) = mdc(b, a) = mdc(a, b),$$

e paramos, pois termina o algoritmo, ou

b') $r_2 \nmid r_1$, e, em tal caso, podemos efetuar a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 q_3 + r_3 \quad \text{com } 0 < r_3 < r_2.$$

Este procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais $a > r_1 > r_2 > \cdots$ que não possui menor elemento, o que não é possível pela Propriedade da Boa Ordenação. Logo, para algum n, temos que $r_n \mid r_{n-1}$, o que implica que $mdc(a, b) = r_n$.

O algoritmo acima pode ser sintetizado e realizado na prática, como mostramos a seguir. Inicialmente, efetuamos a divisão $b = aq_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

	q_1	
b	a	
r_1		

A seguir, continuamos efetuando a divisão $a = r_1 q_2 + r_2$ e colocamos os números envolvidos no diagrama

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Prosseguindo, enquanto for possível, teremos

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
b	a	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = mdc(a, b)$
r_1	r_2	r_3	r_4	$\cdots$	r_n		

Exemplo 2.2.2 *Calcule o mdc de* 23732 *e* 180.

	131	1	5	2	3	
23732	180	152	28	12	4	
152	28	12	4	0		

Observe que, no exemplo acima, o Algoritmo de Euclides nos fornece

$4 = 28 - 2 \cdot 12$

$12 = 152 - 5 \cdot 28$

$28 = 180 - 1 \cdot 152$

$152 = 23732 - 131 \cdot 180.$

Donde se segue que

$4 = 28 - 2 \cdot 12 = 28 - 2 \cdot (152 - 5 \cdot 28) = 11 \cdot 28 - 2 \cdot 152 = 11 \cdot (180 - 1 \cdot 152) - 2 \cdot 152 = 11 \cdot 180 - 13 \cdot 152 = 11 \cdot 180 - 13 \cdot (23732 - 131 \cdot 180) = 1714 \cdot 180 - 13 \cdot 23732.$

Temos, então, que

$$mdc(23732, 180) = 4 = 1714 \cdot 180 + (-13) \cdot 23732.$$

Conseguimos então, através do uso do Algoritmo de Euclides de trás para frente, escrever $4 = mdc(23732, 180)$ como múltiplo de 180 mais um múltiplo de 23732.

O Algoritmo de Euclides nos fornece, portanto, um meio prático de escrever o *mdc* de dois números como soma de dois múltiplos dos números em questão.

Na divisão de um inteiro n por 2 há duas possibilidades: o resto ser 0 ou 1. No primeiro caso, o número é divisível por 2 e é chamado número par. Consequentemente, os números pares apresentam-se sob a forma $2t$, em que t é um inteiro. Se o resto for 1, o número pode ser expresso por $n = 2t + 1$, para algum inteiro t, e é chamado número ímpar. No caso da divisão de um inteiro n por 3, os restos possíveis são 0, 1, ou 2 e, portanto, $n = 3t$, $n = 3t + 1$ ou $n = 3t + 2$, exclusivamente. E assim por diante [7].

2.2.2 Equações Diofantinas

Segundo [7], Diofanto de Alexandria viveu, provavelmente, no século III d.C. De sua produção matemática conhecem-se apenas os fragmentos de uma obra que trata de números poligonais e a extremamente original e criativa *Arithmetica*, graças à qual ele é às vezes considerado o pai da algébra.

Devido à *Arithmetica*, hoje são chamadas *equações diofantinas* todas as equações polinomiais (não importa o número de incógnitas) com coeficientes inteiros, sempre que seu estudo seja feito tomando como universo das variáveis o conjunto dos números inteiros.

As equações Diofantinas, de forma geral, podem ser escritas como

$$\sum_{i=1}^{n} a_i x_i^{n_i} = c.$$

Temos em especial as equações diofantinas lineares em duas incógnitas do tipo:

$$ax + by = c$$

em que a e b são inteiros não nulos. Uma solução da equação acima é o par (x_0, y_0) de inteiros tais que a sentença

$$ax_0 + by_0 = c$$

é verdadeira.

Proposição 2.2.1 *Uma equação diofantina linear $ax + by = c$ tem solução se, e somente se, $d = mdc(a, b)$ é um divisor de c.*

Demonstração. ($\Rightarrow$) Se (x_0, y_0) é uma solução, vale a igualdade

$$ax_0 + by_0 = c.$$

Como $d \mid a$ e $d \mid b$, então $d \mid c$, devido à propriedade da divisibilidade.

($\Leftarrow$) Como $d = mdc(a, b)$, então, podem-se determinar $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = d$. Mas, por hipótese, $d \mid c$ e, portanto, $c = dq$ para algum inteiro q. De onde,

$$c = dq = (ax_0 + by_0)q = a(x_0q) + b(y_0q).$$

o que mostra que o par (x_0q, y_0q) é solução da equação considerada.

□

É importante observar que, se (x_0, y_0) é uma solução de $ax + by = c$, com $a, b > 0$, então $(-x_0, y_0)$, $(x_0, -y_0)$, e $(-x_0, -y_0)$ são soluções respectivamente de $(-a)x+by = c$, $ax+(-b)y = c$ e $(-a)x + (-b)y = c$.

Exemplo 2.2.3 *Encontrar uma solução da equação diofantina* $26x+31y = 2$. *Como* $mdc(26, 31) = 1$, *então a equação tem solução. Usaremos o método das divisões sucessivas para exprimir o máximo divisor comum de* 26 *e* 31 *por meio de uma identidade de Bezout:*

$$31 = 26 \cdot 1 + 5$$

$$26 = 5 \cdot 5 + 1$$

$$5 = 1 \cdot 5.$$

Assim:

$$1 = 26 - 5 \cdot 5 = 26 - (31 - 26 \cdot 1) \cdot 5 = 26 \cdot 6 + 31 \cdot (-5).$$

Então, $(x_0, y_0) = (6, -5)$ *e, portanto, o par* $(2 \cdot 6, 2 \cdot (-5)) = (12, -10)$ *é uma solução da equação dada. Consequentemente* $(-12, -10)$, $(12, 10)$ *e* $(-12, 10)$ *são soluções, respectivamente, de* $(-26)x + 31y = 2$, $26x - 31y = 2$ *e* $(-26)x + (-31)y = 2$.

Proposição 2.2.2 *Se a equação diofantina* $ax + by = c$ *tem uma solução* (x_0, y_0)*, então tem infinitas soluções e o conjunto destas é*

$$S = \{(x_0 + (b/d)t, y_0 - (a/d)t) \mid t \in \mathbb{Z}\}$$

em que $d = mdc(a, b)$.

Demonstração. Mostremos primeiro que todo par $(x_0 + (b/d)t, y_0 - (a/d)t)$ é solução da equação considerada. De fato,

$$a(x_0 + (b/d)t) + b(y_0 - (a/d)t) = ax_0 + by_0 + [(ab - ba)/d]t = ax_0 + by_0 = c$$

pois (x_0, y_0) é solução, por hipótese.
De outra parte, seja (x', y') uma solução genérica da equação. Então:

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

daí:

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

Mas, como d é divisor de a e de b, então $a = dr$ e $b = ds$, para convenientes inteiros r e s, primos entre si. Logo,

$$dr(x' - x_0) = ds(y_0 - y')$$

e, portanto:

$$r(x' - x_0) = s(y_0 - y').$$

Essa igualdade mostra que r divide $s(y_0 - y')$. Mas, como r e s são primos entre si, então r divide $y_0 - y'$. Logo:

$$y_0 - y' = rt$$

para algum $t \in \mathbb{Z}$. Considerando-se que $r = a/d$, então

$$y' = y_0 - (a/d)t$$

observando-se agora que, em consequência,

$$r(x' - x_0) = s(y_0 - y') = srt$$

obtém-se:

$$x' = x_0 + (b/d)t.$$

□

É interessante e talvez surpreendente observar que o fato de uma equação diofantina $ax + by = c$ ter infinitas soluções (quando tem uma) significa, geometricamente, que a reta de equação $ax + by = c$ possui uma infinidade de pontos de coordenadas inteiras do plano cartesiano.

Exemplo 2.2.4 *Determinar todas as soluções da equação diofantina* $43x + 5y = 250$.
Como $mdc(43, 5) = 1$, *que obviamente divide* 250, *a equação tem soluções. É importante lembrar que, se* (x_0, y_0) *é solução de* $43x + 5y = 1$, *então* $(250x_0, 250y_0)$ *é solução da equação dada. Por divisões sucessivas, podemos achar uma solução da equação* $43x + 5y = 1$. *Assim*

$$43 = 5 \cdot 8 + 3$$

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1.$$

segue que
$1 = 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) \cdot 1 = 3 \cdot 2 + 5 \cdot (-1) = (43 - 5 \cdot 8) \cdot 2 + 5 \cdot (-1) = 43 \cdot 2 + 5 \cdot (-17)$
e, portanto, uma solução de $43x + 5y = 1$ *é* $(2, -17)$. *Logo, uma solução de* $43x + 5y = 250$ *é* $(500, -4250)$. *De onde a solução geral da equação pode ser expressa por*

$$(500 + 5t, -4250 - 43t).$$

Exemplo 2.2.5 *A equação* $9x + 12y = 1$ *não admite solução, pois* $(9, 12) = 3$ *e* $3 \nmid 1$.

Exemplo 2.2.6 *Resolva a equação* $28x + 90y = 22$. *Inicialmente, temos que calcular o* $mdc(28, 90)$.

	3	4	1	2
90	28	6	4	2
6	4	2	0	

Visto que $mdc(28, 90) = 2$ *e* $2 \mid 22$ *a equação admite soluções. Usando o algoritmo de trás para frente, temos.*

$$90 = 3 \cdot 28 + 6 \longrightarrow 6 = 90 - 3 \cdot 28$$
$$28 = 4 \cdot 6 + 4 \longrightarrow 4 = 28 - 4 \cdot 6$$
$$6 = 1 \cdot 4 + 2 \longrightarrow 2 = 6 - 1 \cdot 4.$$

Segue que

$$\begin{aligned} 2 = 6 - 1 \cdot (28 - 4 \cdot 6) &= (-1) \cdot 28 + 5 \cdot 6 \\ &= (-1) \cdot 28 + 5 \cdot (90 - 3 \cdot 28) \\ &= (-16) \cdot 28 + 5 \cdot 90. \end{aligned}$$

Logo, $2 = (-16) \cdot 28 + 5 \cdot 90$*. Multiplicando ambos os membros desta igualdade por* 11*, temos*

$$22 = (-176) \cdot 28 + 55 \cdot 99.$$

Portanto, uma solução particular da equação é dada por $(x_0, y_0) = (-176, 55)$*. Logo, a solução geral é*

$$x = -176 + t \cdot 45 \quad e \quad y = 55 - t \cdot 14, \quad t \in \mathbb{Z}.$$

A equação $ax + by = n$ foi resolvida pelo matemático hindu do século VII, Brahmagupta. Muitas outras equações Diofantinas foram estudadas. Algumas, por exemplo, as que consideramos aqui neste estudo, resolvem-se utilizando métodos elementares, outras requerem métodos mais sofisticados. Uma equação estudada desde a antiguidade é a equação pitagórica:

$$x^2 + y^2 = z^2.$$

Esta equação possui infinitas soluções e existem fórmulas que permitem gerar todas elas. Pierre de Fermat afirmou, sem dar uma demonstração, que a equação

$$x^n + y^n = z^n.$$

para $n > 2$ não admitia soluções em inteiros positivos. A esta afirmação chama-se de o Último Teorema de Fermat.

Exemplo 2.2.7 *Equação Diofantina* $x^3 - 117y^3 = 5$

Vamos mostrar que esta equação não possui soluções inteiras. De fato, suponhamos, por absurdo, que x_0*,* y_0 *seja uma solução inteira da equação. Então*

$$x_0^3 \equiv 5 \, mod \, 9$$

já que $117 \equiv 0 \, mod \, 9$*.*

Mas, sendo x_0 *congruente a* 0, 1, 2, 3, 4, 5, 6, 7 *ou* 8 *módulo* 9*, segue por contas elementares*

que x_0^3 *é congruente a* 0, 1 *ou* 8, *módulo* 9. *Logo, a congruência* $x_0^3 \equiv 5 \, mod \, 9$ *não possui solução, o que fornece uma contradição.*

Teorema 2.2.2 (Teorema de Fermat) *Sejam a um número natural e p um número primo tal que* $mdc(a, p) = 1$. *Com essas condições, pode-se afirmar que* $a^{p-1} \equiv 1 \, mod \, p$.

Considere o conjunto $A = a, 2a, 3a, 4a, \ldots, (p-1)a$.

Lema 2.2.2 *Todos os elementos de A são incongruentes entre si (módulo p), dois a dois.*

Demonstração. Suponha que existam dois elementos distintos de A tais que sejam congruentes entre si na divisão por p. Logo, $k.a - t.a \equiv 0 \, mod \, p \Rightarrow k - t \equiv 0 \, mod \, p$, pois se tem que o $mdc(a, p) = 1$. Assim, $k \equiv t \, mod \, p$, mas como são menores que p, temos que $k = t$, mas isso é absurdo, pois por hipótese $k \neq t$.

Logo, se A tem $(p-1)$ elementos e todos são incongruentes entre si na divisão por p, temos que em A existem todos os possível restos (diferentes de zero) na divisão por p. A multiplicação de todos os elementos de A é congruente à multiplicação de todos os restos respectivos na congruência módulo p.

$$a \cdot (2a) \cdot (3a).(4a) \cdots (p-1) \cdot a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv mod \, p.$$

$a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdots (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv mod \, p$ como $1 \cdot 2 \cdot 3 \cdots (p-1)$ é primo com p, podemos simplificar os termos comuns de ambos os lados da congruência e, assim

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

□

Colorário 2.2.1 *Sejam a um número natural e p um número primo, temos que:*

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

que é o resultado direto do Teorema de Fermat.

2.2.3 Congruências Lineares (Congruência módulo m)

A congruência módulo m é uma congruência no anel dos inteiros. Apresentaremos agora, as definições e demonstrações de propriedades sobre a congruência módulo m, assim como algumas aplicações.

Exemplo 2.2.8 *Observe que*

a) $12 \equiv r \, mod \, 5$, *logo* $r = 2$, *pois é resto da divisão de 12 por 5. Logo* $12 \equiv 2 \, mod \, 5$.

b) $17 \equiv 11 \, mod \, 6$, *pois os restos das divisões de 17 por 6 e de 11 por 6 são os mesmos e iguais a 5.*

c) $13 \not\equiv 7 \, mod \, 5$, *pois os restos das divisões de 13 por 5 e de 7 por 5 são 3 e 2 respectivamente.*

Proposição 2.2.3 *Sejam $a, b, c \in \mathbb{Z}$ com $m > 0$. Então, $a \equiv b \, mod \, m$ se, e somente se, m divide $b - a$.*

Demonstração. Pelo algoritmo de divisão, podemos escrever

$$a = mq_1 + r_1 \text{ e } b = mq_2 + r_2$$

onde $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Sem perda de generalidade, podemos supor que $r_1 \leq r_2$. Podemos escrever então

$$b - a = m.(q_2 - q_1) + r_2 - r_1.$$

Logo, m divide $b - a$ se, e somente se, m divide $r_2 - r_1$. Por ser $0 \leq r_2 - r_1 < m$, segue que m divide $b - a$ se, e somente se $r_2 - r_1 = 0$, ou seja, se, e somente se $r_2 = r_1$.

□

Proposição 2.2.4 *Sejam a, b, c, d inteiros quaisquer e seja m um número inteiro maior do que 1. Se $a \equiv b \, mod \, m$ e $c \equiv d \, mod \, m$, então $a \pm c \equiv b \pm d \, mod \, m$.*

Demonstração. Se $a \equiv b \, mod \, m$ e $c \equiv d \, mod \, m$, então m divide $b - a$ e m divide $d - c$. Logo, m divide

$$(b - a) \pm (d - c) = (b \pm d) - (a \pm c)$$

mostrando que $(b \pm d) \equiv (a \pm c) \, mod \, m$.

Concluímos, então, que as congruências de mesmo módulo somam-se e se subtraem membro a membro tal qual as igualdades.

□

Colorário 2.2.2 *Sejam dois números inteiros tais que $a \equiv b \, mod \, m$. Logo, sendo c outro número inteiro, tem-se que $(a \pm c) \equiv (b \pm c) \, mod \, m$,*

Demonstração. Como $c \equiv c \, mod \, m$, pela Proposição 2.2.4, temos que $(a \pm c) \equiv (b \pm c) \, mod \, m$.
□

Proposição 2.2.5 *Sejam a, b, c, d inteiros quaisquer e seja m um número inteiro maior do que 1. Se $a \equiv b \, mod \, m$ e $c \equiv d \, mod \, m$, então $a \cdot c \equiv b \cdot d \, mod \, m$.*

Demonstração.

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

Como $a \cdot c - b \cdot d = a \cdot (c - d) + d \cdot (a - b)$,

segue que m divide $a \cdot c - b \cdot d$, então $a \cdot c \equiv b \cdot d \, mod \, m$.

□

Colorário 2.2.3 *Sejam dois números inteiros tais que $a \equiv b \, mod \, m$. Logo, sendo c outro número inteiro, tem-se que $(a \cdot c) \equiv (b \cdot c) \, mod \, m$,*

Demonstração. Como $c \equiv c \, mod \, m$, pela Proposição 2..2.5, temos que $(a \cdot c) \equiv (b \cdot c) \, mod \, m$.
□

Exemplo 2.2.9 *Calcular o resto da divisão de $5^{131} + 7^{131} + 11^{131} + 13^{131}$ por 9.*

Solução:

$5^{131} + 7^{131} + 11^{131} + 13^{131} \equiv (-4)^{131} + (-2)^{131} + (2)^{131} + (4)^{131} \equiv 0 \, mod \, 9$,

logo o resto da divisão da expressão numérica por 9 será 0.

Exemplo 2.2.10 *Determinar qual é o algarismo das unidades na representação decimal do número $N = (22222^{55555} + 55555^{22222})^{33333} + (33333^{77777} + 77777^{33333})^{44444}$.*

Solução:

$$N = ((22222^4)^{13888} \cdot 22222^3 + 55555^{22222})^{33333} + ((33333^2)^{38888} \cdot 33333 + (77777^2)^{16666} \cdot 77777))^{44444}$$

Basta fazer a congruência módulo 10 e teremos:

$22222 \equiv 2 \, mod \, 10, \; 55555 \equiv 5 \, mod \, 10, \; 33333 \equiv 3 \, mod \, 10, \; e \; 77777 \equiv 7 \, mod \, 10.$

Logo,

$N \equiv ((2^4)^{13888} \cdot 2^3 + 5^{22222})^{33333} + ((3^2)^{38888} \cdot 3 + (7^2)^{16666} \cdot 7))^{44444}$

Temos que

$$2^4 \equiv 6 \, mod \, 10$$

$$5^{22222} \equiv 5 \, mod \, 10$$

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

$$7^2 \equiv -1 \, mod \, 10$$

$N \equiv ((6)^{13888} \cdot 8 + 5)^{33333} + ((-1)^{38888} \cdot 3 + (-1)^{16666} \cdot 7))^{44444}$

$$6^{13888} \equiv 6 \, mod \, 10$$

$N \equiv (6 \cdot 8 + 5)^{33333} + (1 \cdot 3 + 1 \cdot 7))^{44444}$

$$6 \cdot 8 \equiv 8 \, mod \, 10$$

$N \equiv (8+5)^{33333} + (3+7)^{44444} = (13)^{33333} + (10)^{44444}$

$$13 \equiv 3 \, mod \, 10$$

$$10 \equiv 0 \, mod \, 10$$

$N \equiv (3)^{33333} + (0)^{44444}$
$N \equiv 3^{33333} = (3^2)^{16666} \cdot 3 \equiv (-1)^{16666} \cdot 3 = 1 \cdot 3 = 3.$
Logo, o algarismo das unidades de N é igual a 3.

Exemplo 2.2.11 *Qual o resto da divisão de* 1389^{8756} *por* 17 *?*

$$1389 \equiv 12 \, mod \, 17$$

$$12^{16} \equiv 1 \, mod \, 17$$

$$(12^{16})^{547} \equiv 1^{547} \, mod \, 17$$

$$12^{8752} \equiv 1 \, mod \, 17$$

$$12^2 = 144 \equiv 8 \, mod \, 17$$

$$(12^2)^2 \equiv 8^2 \equiv 13 \, mod \, 17$$

$$12^4 \equiv 13 \, mod \, 17$$

$$1389^{8756} \equiv 12^{8756} = 12^{8752} \cdot 12^4 \equiv 1 \cdot 13 = 13 \, mod \, 17.$$

Logo, o resto da divisão de 1389^{8756} *por* 17 *será igual a* 13*.*

2.3 Polinômios

Seja F um corpo, um polinômio na variável x sobre F é uma expressão da forma:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

onde $a_i \in F$ para qualquer i e $n \in \mathbb{N}$.

O conjunto de todos os polinômios na variável x com coeficientes em um corpo F é denotado por $F[x]$, isto é, quando escrevemos $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ e dizemos que $p(x) \in F[x]$, temos que os elementos $a_i \in F$ são chamados de coeficientes do polinômio.

Sabemos que uma função $p : \mathbb{R} \longmapsto \mathbb{R}$ é chamada de função polinomial se existirem $a_0, a_1, \ldots, a_n \in \mathbb{R}$ tais que $p(x) = a_0 + a_1 x + \cdots + a_n x^n, \forall\, x \in \mathbb{R}$.

A correspondência que associa a cada polinômio $P(X)$ à função polinomial $p(x)$, ou seja, $P(X) = a_0 + a_1 X + \cdots + a_n X^n \longmapsto p(x) = a_0 + a_1 x + \cdots + a_n x^n$ é uma função sobrejetiva por definição e injetiva porque funções polinomiais são iguais se, e somente se possuem os mesmos coeficientes, portanto os polinômios no domínio serão iguais. Dessa forma, esta correspondência de que cada polinômio associa à função polinomial é uma bijeção. Por este motivo, não faremos distinção entre o polinômio $P(X)$ e a função polinomial $p(x)$.

Ao utilizar a notação $p(x)$ para polinômio, queremos dizer que $p(x)$ indica que p é um elemento do anel, mas por abuso de notação também irá representar a função polinomial, ou seja, a imagem da função polinomial que leva o elemento no corpo através do polinômio.

Observações 2.3.1

1. *Dizemos que dois polinômios* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *e* $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ *sobre* F *são iguais se, e somente se,* $a_i = b_i$ *em* $F, \forall\, i \in \mathbb{N}$.

2. *Se* $p(x) = 0x^n + 0x^{n-1} + \cdots + 0x + 0$, *indicaremos* $p(x)$ *por* 0 *e o chamamos de o polinômio identicamente nulo sobre* F. *Assim, um polinômio* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *sobre* F *é identicamente nulo se, e somente se,* $a_i = 0 \in F, \forall\, i \in \mathbb{N}$.

3. *Se* $a \in F$, *indicaremos por* a *ao polinômio* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *onde* $a_0 = a$, *e* $a_i = 0\ \forall\, i \geq 1$. *Chamamos ao polinômio* $p(x) = a, a \in F$ *de um polinômio constante* a.

4. *Se* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *é tal que* $a_n \neq 0$ *e* $a_j = 0\ \forall\, j > n$ *dizemos que* n *é o grau do polinômio* $p(x)$, *e nesse caso indicamos por* $\partial p(x) = n$.

5. *O grau do polinômio* 0 *não está definido e* ∂ *pode ser interpretada como uma função do conjunto de todos os polinômios diferentes de zero no conjunto* $\mathbb{N}$.

   Assim,

$$\partial : F[x] - 0 \longrightarrow \mathbb{N}$$

$$p(x) \longrightarrow \partial p(x) = \textit{grau de } p(x).$$

Podemos definir as operações de soma e produto no conjunto $F(x)$. Sejam dois elementos do conjunto $F(x)$,

$$p(x) = a_n x^n + \cdots + a_1 x + a_0 \quad \text{e} \quad g(x) = b_r x^r + \cdots + b_1 x + b_0.$$

definimos
$p(x) + g(x) = c_k x^k + \cdots + c_0$ onde $c_i = (a_i + b_i) \in F$, e
$p(x) \cdot g(x) = c_k x^k + \cdots + c_0$ onde
$c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \ldots,$
$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0, k \in \mathbb{N}$.

A arimética de $F[x]$ é semelhante à de $\mathbb{Z}$, pois os conjuntos são fechados em relação às operações de soma e de multiplicação. Além disso, ambos não possuem inverso multiplicativo.

A aritmética de $F[x]$ é semelhante à de $\mathbb{Z}$, não apenas pelas propriedades e por possuírem conjuntos fechados em relação às operações de soma e de multiplicação, mas são semelhantes na estrutura, ou seja, os dois possuem estrutura euclidiana parecida.

Podemos observar que a definição acima de produto provém da regra $x^n.x^r = x^{n+r}$ e da propriedade distributiva. Convencionam-se também as regras $x^0 = 1$ e $x^1 = x$.

Verificamos, facilmente, que $F[x], +, \cdot$ é um domínio de Integridade em que o polinômio 0 é o elemento neutro de $F[x]$ e o polinômio constante 1 é a unidade de $F[x]$.

Se identificarmos os elementos $a \in F$ com os polinômios constantes $p(x) = a$, podemos pensar em $F[x]$ contendo o corpo F.

Segue imediatamente das definições que a função grau ∂ possui as seguintes propriedades:

(i) $\partial(p(x)+g(x)) \leq max\{\partial p(x), \partial g(x)\}$, quaisquer que sejam os polinômios não nulos $p(x), g(x) \in F[x]$ tais que $p(x) + g(x) \neq 0$.

(ii) $\partial(p(x) \cdot g(x)) = \partial p(x) + \partial g(x)$, quaisquer que sejam os polinômios não nulos $p(x), g(x) \in F[x]$.

Se um polinômio $p(x) \neq 0$ possui um inverso multiplicativo em $F[x]$, então existe $q(x) \neq 0$ em $F[x]$ tal que $p(x) \cdot q(x) = 1$. Pela propriedade (ii) acima, segue que $p(x) = a \neq 0$ é um polinômio constante. Portanto, os únicos polinômios invertíveis em $F[x]$ são os polinômios constantes não nulos.

Exemplo 2.3.1 a) *O polinômio* $p(x) = 2x^3 - 7x + 11$ *tem coeficientes racionais com* $a_3 = 2, a_2 = 0, a_1 = -7$ *e* $a_0 = 11$, *ou seja,* $p(x) \in \mathbb{Q}[x]$. *Podemos dizer que* $p(x) \in R[x]$ *ou* $p(x) \in \mathbb{C}[x]$, *pois* $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

b) *O polinômio* $q(x) = (1 + i)x^4 - 5x^2 - 3ix + 7$ *tem coeficientes complexos com* $a_4 = 1 = i, a_3 = 0, a_2 = -5, a_1 = -3i$ *e* $a_0 = 7$, *ou seja,* $q(x) \in \mathbb{C}[x]$.

Podemos dizer que $q(x) \notin \mathbb{R}[x]$.

2.3.1 Divisão de Polinômios

A Divisão de polinômios é uma das mais importantes ferramentas de cálculo já desenvolvidas. Para efetuarmos a divisão, utilizaremos o algoritmo da divisão de Euclides. Podemos citar que no conjunto dos números inteiros, finalizamos a divisão, quando o resto vier a ser menor do que o divisor. O que difere na divisão de polinômios, é que a finalização acontece, quando o grau do resto for menor do que o grau do divisor.

Teorema 2.3.1 *Algoritmo da Divisão*

Sejam $p(x), g(x) \in F[x]$ e $g(x) \neq 0$, então existem únicos $q(x), r(x) \in F[x]$ tais que

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

onde ou $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

Demonstração. Sejam $p(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$, $(\partial g(x) = m)$

Primeiro vamos verificar a existência:

Se $p(x) = 0$, basta tomar $q(x) = r(x) = 0$. Suponhamos $p(x) \neq 0$. Assim, grau $p = n$. Se $n < m$, basta tomar $q(x) = 0$ e $r(x) = p(x)$. Assim, podemos assumir $n \geqslant m$.

Agora, seja $p_1(x)$ o polinômio definido por

$$p(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + p_1(x).$$

É fácil observarmos que $\partial p_1 < \partial p$: Vamos demonstrar o teorema por indução sobre $\partial p = n$.

Se $n = 0, n \geqslant m \Rightarrow m = 0$ e, portanto, $p(x) = a_0 \neq 0, g(x) = b_0 \neq 0$, temos $p(x) = a_0 b_0^{-1} g(x)$ e basta tomar $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$.

Pela igualdade $p_1(x) = p(x) - a_n b_m^{-1} x^{n-m} g(x)$ e $\partial p_1 x < \partial p(x) = n$ temos pela hipótese de indução que: $\exists\, q_1(x), r_1(x)$ tais que:

$$p_1(x) = q_1(x) \cdot g(x) + r_1(x)$$

onde $r_1(x) = 0$ ou $\partial r_1(x) < \partial g(x)$. Daí segue imediatamente que: $p(x) = (q_1(x) + a_n b_m^{-1} x^{n-m}) g(x) + r_1(x)$ e, portanto, tomando $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r_1(x) = r(x)$ provamos a existência dos polinômios $q(x)$ e $r(x)$ tais que $p(x) = q(x) \cdot g(x) + r(x)$, e $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

Agora vamos provar a unicidade. Sejam $q_1(x), q_2(x), r_1(x)$ e $r_2(x)$ tais que:

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

onde $r_i(x) = 0$ ou $\partial r_i(x) < \partial g(x), i = 1, 2$. Daí segue: $(q_1(x) - q_2(x)) \cdot g(x) = r_2(x) - r_1(x)$.

Mas se $q_1(x) \neq q_2(x)$ o grau do polinômio do lado esquerdo da igualdade acima é maior ou igual a $\partial g(x)$, enquanto que o grau $\partial(r_2(x) - r_1(x)) < \partial g(x)$, o que é uma contradição. Logo, $q_1(x) = q_2(x)$ e daí segue $r_1(x) = p(x) - q_1(x)g(x) = p(x) - q_2(x)g(x) = r_2(x)$,verificando o resultado.

□

A demonstração acima é válida somente para corpo, justamente pelo fato de precisarmos dos inversos para os cálculos no algoritmo da divisão de polinômios. Esta divisão pode ocorrer em outros conjuntos desde que seja possível encontrar os inversos dos termos de maior grau, temos uma divisão única. Não conseguimos, por exemplo, dividir dois polinômios com coeficientes inteiros, no sentido da divisão euclidiana, porque podemos não ter os coeficientes, pois os inversos podem não ser números inteiros, mas se todos possuírem inversos, então a divisão é possível.

Observação 2.3.1 *Se todos os polinômios tiverem como coeficientes* 1 *e* -1*, conseguimos efetuar a divisão devido a existência dos inversos, como, por exemplo, o polinômio* $x^3 + x + 1$ *dividido por* $x + 1$*.*

A necessidade de que a estrutura algébrica seja um corpo para se ter o algoritmo da divisão se dá pela existência dos inversos dos coeficientes. Para "abaixar"o grau do polinômio, é preciso do inverso do termo de maior grau do divisor b_{n-1}*. Se o termo de maior grau for 1, apenas dividimos e não precisaríamos do inverso.*

Caso não seja corpo, a divisão pode existir para alguns casos, desde que seja possível encaixar nas hipóteses da demonstração, logo será possível a realização da divisão.

Se o polinômio for mônico, conseguimos dividir por qualquer polinômio mônico e não precisaremos supor que é corpo.

2.3.2 Raízes de funções polinomiais

As raízes polinomiais possuem grande importância para a decomposição de um polinômio e para a construção de gráficos de funções polinomiais, afinal, com essas raízes podemos encontrar os pontos onde a função intersecta o eixo das abscissas.

Se $p(x) = a_0 + a_1x + \cdots + a_nx^n$ é um polinômio não nulo em $F(x)$ e $\alpha \in F$ é tal que $p(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0 \in F$, dizemos que α é uma raiz de $p(x)$ em F.

Se $\partial q = 1$, então $\partial r < 1$, ou seja, $\partial r = 0$, logo o resto r é uma constante ou $r \equiv 0 \, mod \, q(x)$.

Teorema 2.3.2 *[Teorema do resto]. Se* F *é um corpo,* $a \in F$ *e* $p(x) \in F[x]$*, então* $p(a)$ *é o resto da divisão de* p *por* $x - a$*.*

Demonstração. Se o quociente e o resto da divisão de p por $x - a$ em $F[x]$ são, respectivamente, q e r, então:

$$p(x) = (x - a) \cdot q(x) + r(x).$$

em que $\partial(r) < \partial(x-a) = 1$ ou $r = 0$, pelo teorema 2.3.1. Substituindo-se a variável por a na equação acima, temos

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

e, como r é um polinômio constante, então $r(a) = r$. De onde, $r = p(a)$. □

Convém observar que o quociente q pode ser um elemento de $F[x]$ em que seu grau é uma unidade a menos que o do divisor de p. De fato, como $r = 0$ ou $\partial(r) = 0$, então $\partial(p) = \partial((x-a)\cdot q) = \partial(x-a) + \partial(q) = 1 + \partial(q)$ e, portanto $\partial(q) = \partial(p) - 1$. Ademais, p e q têm o mesmo coeficiente dominante. Pelo princípio de identidade de polinômios, observa-se que, o coeficiente dominante de p é igual ao produto do coeficiente dominante de $(x-a)$, que é igual a 1, pelo coeficiente dominante de q, uma vez que r é uma constante.

Um polinômio pode ter coeficientes em um corpo F e não possuir raízes neste corpo. Podemos provar uma proposição que limita o números dessas raízes em um corpo.

Seja F um corpo. Se $L \supset F$ é um corpo, dizemos que L é uma extensão de F. Observe que o polinômio $x^2 + 1$ não possui raízes em $\mathbb{R}$, mas possui duas raízes em $\mathbb{C} \supset \mathbb{R}$

Proposição 2.3.1 *Seja F um corpo e seja $p(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio não nulo em $F(x)$ de grau n, então o número de raízes de $p(x)$ em F é no máximo igual a $\partial p(x) = n$.*

Demonstração. Se $p(x)$ não possui raízes em F a proposição está provada.

Suponhamos que $\alpha \in F$ seja uma raiz de $p(x)$.

Como $g(x) = x - \alpha \in F[x]$, podemos usar o algoritmo da divisão.

Assim, $\exists\, q(x), r(x) \in F[x]$ tais que: $p(x) = q(x)\cdot(x-\alpha) + r(x)$ onde $r(x) = 0$ ou $\partial r(x) < \partial g(x) = 1$. Assim, $r(x) = b_0$ é um polinômio constante e temos $p(x) = q(x)(x-\alpha) + b_0$. Como $p(\alpha) = 0$ segue que $0 = 0 + b_0$, ou seja, $r(x) = b_0 = 0$ e $p(x) = q(x)\cdot(x-\alpha)$ onde $\partial q(x) = n - 1$.

Agora, como não existem divisores de zero em um corpo, segue que se $\beta \in F$ é uma raiz qualquer de f, então $f(\beta) = (\beta - \alpha)\cdot q(\beta) = 0$ implica $\beta = \alpha$ ou β é também uma raiz de $q(x) \in F[x]$. Assim, as raízes de f são α e as raízes de $q(x)$ são β.

Vamos usar indução sobre $\partial p = n$.

Ora se $n = 0$, p não possui raízes em F e, nesse caso, já vimos que nada há a demonstrar.

Agora, por indução $\partial q(x) < \partial p(x) = n$, $q(x)$ possui no máximo $\partial q(x) = n - 1$ raízes em F e, portanto, $p(x)$ possui no máximo n raízes em F.

□

Observação 2.3.2 *Seja p um polinômio de grau n, ou seja, $\partial p = n$ com $n+1$ raízes. Temos, então, que p pode ser escrito como $n+1$ polinômios de grau 1, mas o grau do polinômio produto é a soma dos graus dos fatores, então p possui grau $n+1$, o que é um absurdo, logo o polinômio p não pode ter mais que n raízes.*

Observe que o polinômio $x^3 - 2$ não possui raízes em $\mathbb{Q}$, possui apenas uma raiz em $\mathbb{R}$ e possui 3 raízes em $\mathbb{C}$, ou seja, o polinômio $x^3 - 2$ se fatora em $\mathbb{C}[x]$.

2.3.3 Multiplicidade de uma raiz

As raízes de um polinômio podem ser todas distintas ou não. O número de vezes que uma mesma raiz aparece, indica a sua multiplicidade.

Seja um polinômio $p(x) \in F[x]$, $\alpha \in F$, e um inteiro $s \geq 1$. Dizemos que α é uma raiz de $p(x)$ de multiplicidade s se $(x-\alpha)^s$ divide $p(x)$, mas $(x-\alpha)^{s+1}$ não divide $p(x)$.

As raízes de multiplicidade 1 são ditas raízes simples e as de multiplicidade ≥ 2 são ditas raízes múltiplas.

Teorema 2.3.3 *Seja F um corpo, $p(x) \in F[x]$, $\alpha \in F$, e seja $s \geq 1$ um inteiro. Então as afirmações seguintes são equivalentes:*

(i) *α é uma raiz de $p(x)$ de multiplicidade s.*

(ii) *Existe um polinômio $q(x) \in F[x]$ tal que $p(x) = (x-\alpha)^s q(x)$ com $q(\alpha) \neq 0$.*

Demonstração. $(i) \Longrightarrow (ii)$. Temos que $p(x) \in F[x]$, e $\alpha \in F$. Então $p(\alpha) = 0$ se, e somente se existe um polinômio $q(x) \in F[x]$ tal que $p(x) = (x-\alpha) \cdot q(x)$.

$(ii) \Longrightarrow (i)$. Devemos mostrar que $(x-\alpha)^{s+1}$ não divide $p(x)$. Suponha que $(x-\alpha)^{s+1}$ divida $p(x)$. Temos então $(x-\alpha)^s q(x) = p(x) = (x-\alpha)^{s+1} h(x)$ para algum $h(x) \in F[x]$, logo $(x-\alpha)^s[q(x) - (x-\alpha)h(x)] = 0$. Como $(x-\alpha)^s$ é um polinômio mônico, obtemos $q(x) = (x-\alpha)h(x)$ e, portanto, $q(\alpha) = 0$, o que contradiz nossa hipótese.

□

Se α_1 é uma raiz de $p(x)$ de multiplicidade s_1 e se α_2 é um raiz de $p(x)$ de multiplicidade s_2, então a soma das multiplicidades das raízes é igual ao grau do polinômio $p(x)$, ou seja, $\partial p(x) = s_1 + s_2$.

Exemplo 2.3.2 *Vamos determinar as raízes do polinômio $p(x) = x^3 + x^2 - 5x + 3 \in \mathbb{Q}[x]$.*

Podemos verificar que 1 é uma raiz de $p(x)$:

$$p(1) = 1 + 1 - 5 + 3 = 0.$$

Assim, $x - 1$ divide $p(x)$ e temos $p(x) = (x-1).q(x)$, onde $q(x) = x^2 + 2x - 3 \in \mathbb{Q}[x]$.

Podemos notar que 1 também é raiz de $q(x)$:

$$q(1) = 1 + 2 - 3 = 0.$$

De fato, $q(x) = (x-1).(x+3)$ e, portanto,

$p(x) = (x-1)^2(x+3)$

Logo -3 também é raiz de $p(x)$. Neste caso, $p(x)$ tem 3 raízes em $\mathbb{Q}$, onde 1 é uma raiz múltipla.

Temos que $(x-1)^2$ divide $p(x) = x^3 + x^2 - 5x + 3$ em $\mathbb{Q}[x]$, mas $(x-1)^3$ não divide $p(x)$. Portanto, 1 é raiz de multiplicidade 2, enquanto -3 é raiz simples de $p(x)$.

Teorema 2.3.4 *[Teorema Fundamental da Álgebra]*
Todo polinômio $p(x) \in C[x]$ de grau $n \geqslant 1$ possui pelo menos uma raiz complexa distinta.

Segundo [3], o Teorema Fundamental da Álgebra, provado por Gauss em sua tese de doutorado em 1798, garante que não ocorre com polinômios com coeficientes complexos o fato de polinômios com coeficientes em um corpo F não possuir raízes neste corpo F.

O famoso Teorema Fundamental da Álgebra garante que $\mathbb{C}$ é algebricamente fechado. Este Teorema possui uma longa história de muitas demonstrações, nenhuma delas porém se faz com métodos puramente algébricos, devendo-se sempre usar métodos da análise. Vamos ao longo do texto admitir este resultado cuja demonstração encontra-se nas seguintes referências: W. K. Clifford, Mathematical Papers 1968 ou L. H. Jacy Monteiro, Elementos de Álgebras - IMPA 1969.

Exemplo 2.3.3 **a)** *O polinômio $p(x) = x^2 - 5$ em $\mathbb{Q}[x]$ não tem raízes em $\mathbb{Q}$, mas possui raízes $\sqrt{5}$ e $-\sqrt{5}$ em $\mathbb{R}[x]$.*

$p(x) = x^2 - 5 \in F[x]$, *com* $F = \mathbb{Q}$ *e raízes de* $p(x)$ *em* $K = \mathbb{R}$

b) *O polinômio $p(x) = x^2 + 1$ em $\mathbb{R}[x]$ não possui raízes em $\mathbb{R}$, mas possui raízes em $\mathbb{C}$ que são os complexos i e $-i$.*

$p(x) = x^2 + 1 \in F[x]$, *com* $F = \mathbb{R}$ *e raízes de* $p(x)$ *em* $K = \mathbb{C}$.

O Teorema Fundamental da Álgebra diz que, ao considerarmos um polinômio em $F[x]$ com $F \subset \mathbb{C}$, este polinômio tem raízes em $\mathbb{C}$. Mas é claro que este polinômio pode ter raízes em um corpo contido em $\mathbb{C}$, como, por exemplo:

$$p(x) = (x^2 + 1)(x^2 - 2) \in \mathbb{Q}[x] \text{ possui raízes } \pm \sqrt{2} \in \mathbb{R} \subset \mathbb{C} \text{ e } \pm i \in \mathbb{C}.$$

Com o Teorema Fundamental da Álgebra, podemos afirmar que um polinômio $p(x) \in \mathbb{C}[x]$ de grau $n \geq 1$ contém todas as suas raízes em $\mathbb{C}$.

De fato, tomando uma raiz $z \in \mathbb{C}$ de $p(x)$ temos $p(x) = (x - z)q(x)$, com $q(x) \in \mathbb{C}$. Se $\partial q(x) \geq 1$, então $q(x)$ possui raiz em $\mathbb{C}$ e repetimos o processo.

Teorema 2.3.5 *Seja $p(x) = a_n x^n + \cdots + a_1 x + a_0$ um polinômio em $\mathbb{R}[x]$ (coeficientes reais). Se o número complexo $z = \alpha + \beta i \in \mathbb{C}$ é uma raiz de $p(x)$, então seu conjugado $\overline{z} = \alpha - \beta i$ também é raiz de $p(x)$.*

Demonstração. Consideremos $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$ e suponhamos que $z = \alpha + \beta i \in \mathbb{C}$ seja uma raiz de $p(x)$. Desse modo,

$$p(z) = a_n z^n + \cdots + a_1 z + a_0 = 0.$$

Podemos observar, inicialmente, que como $a_i \in \mathbb{R}$ temos $\overline{a_i} = a_i\,, \forall i = 1, \ldots, n$. Vamos calcular $p(\overline{z})$

$$p(\overline{z}) = a_n\overline{z}^n + \cdots + a_1\overline{z} + a_0$$

$$p(\overline{z}) = \overline{a_n}\,\overline{z}^n + \cdots + \overline{a_1}\,\overline{z} + \overline{a_0}$$

$$p(\overline{z}) = \overline{a_n z^n + \cdots + a_1 z + a_0} = 0$$

Portanto, $\overline{z} = \alpha - \beta i$ também é raiz de $p(x)$.

□

Para não cometer erros, devemos atentar para o fato dos coeficientes dos polinômios serem reais. Por exemplo, o polinômio.

Exemplo 2.3.4 *O polinômio $p(x) = x^2 + 2ix + 3$ possui o número complexo $z = i$ como raiz, pois:*

$$p(i) = i^2 + 2i \cdot i + 3 = -1 - 2 + 3 = 0$$

mas o conjugado $\overline{z} = -i$ não é raiz de $p(x)$, já que:

$$p(-i) = (-i)^2 + 2i(-i) + 3 = -1 + 2 + 3 = 4 \neq 0.$$

Isto aconteceu devido ao polinômio $p(x)$ não ter coeficientes reais.

Colorário 2.3.1 *Todo polinômio $p(x) \in \mathbb{R}[x]$ de grau ímpar possui pelo menos uma raiz real.*

Demonstração. Pelo Teorema Fundamental da Álgebra, $p(x)$ tem uma raiz em $\mathbb{C}$. Como as raízes complexas aparecem em pares (raiz z e raiz conjugada $\overline{z}$) e como $p(x)$ tem grau ímpar, não é possível que todas as raízes de $p(x)$ sejam complexas da forma $\alpha + \beta i \in \mathbb{C}$, com $\beta \neq 0$. Portanto, pelo menos uma das raízes deve ser real.

□

2.3.4 Fatoração Única

A fatoração é uma ferramenta essencial para muitas aplicações. No conjunto inteiros, temos diversos problemas envolvendo números primos e criptografia. A fatoração polinomial é de extrema importância na resolução de equações de grau maior que um. Basicamente, o objetivo consiste em transformar um polinômio em multiplicação de polinômios de grau menor.

Se $u \in F - \{0\}$ e se $p_1(x), \ldots, p_m(x)$ são polinômios irredutíveis sobre F vamos usar a expressão $p(x) = u \cdot p_1(x) \ldots p_m(x)$ de tal modo que incluiremos na mesma possibilidade $p(x) = u$ no caso de $m = 0$.

Teorema 2.3.6 *Seja F um corpo, então todo polinômio $p(x) \in F[x] - \{0\}$ pode ser escrito na forma,*

$$p(x) = u \cdot p_1(x) \dots p_m(x)$$

onde $u \in F - \{0\}$ e $p_1(x), p_2(x), \dots, p_m(x)$ são polinômios irredutíveis sobre F.(não necessariamente distintos). Destaca-se, ainda, que essa expressão é única a menos da constante u e da ordem dos polinômios $p_1(x), \dots, p_m(x)$.

Demonstração. Seja $p(x) \in F(x) - \{0\}$. Vamos provar por indução sobre $\partial p(x) = n$. Se $n = 0, p(x) = u$ é uma constante não nula. Assim, podemos assumir $\partial p(x) = n \geqslant 1$.

Vamos supor pela hipótese de indução que todo polinômio não nulo de grau menor que n pode ser escrito na expressão desejada, e vamos demonstrar que $p(x)$ também pode ser escrito naquela expressão.

Suponhamos, por absurdo, que $p(x)$ não possa ser escrito como produto de polinômios irredutíveis. Então, $p(x)$ é um polinômio redutível sobre F.

Assim,

$$\text{existe } g(x), h(x) \in F[x],\ 1 \leqslant \partial g(x) < n,\ 1 \leqslant \partial h(x) < n$$

tais que $p(x) = g(x) \cdot h(x)$.

Agora, por indução, temos

$$g(x) = a \cdot p_1(x) \dots p_r(x),\ a \in F - \{0\} \quad \text{e} \quad p_1(x), \dots, p_r(x)$$

polinômios irredutíveis sobre F. Analogamente,

$$h(x) = b \cdot p_{r+1}(x) \dots p_m(x),\ b \in F - \{0\} \quad \text{e} \quad p_{r+1}(x), \dots, p_m(x)$$

polinômios irredutíveis sobre F.

Assim, $p(x) = u \cdot p_1(x) \dots p_m(x)$, onde $u = ab \in F - \{0\}$ e $p_1(x), \dots, p_m(x)$ polinômios irredutíveis sobre F.

Vamos agora demonstrar a unicidade da expressão.

Suponhamos

$$p(x) = u \cdot p_1(x) \dots p_m(x) = u' \cdot p'_1(x) \dots p'_s(x)$$

onde $u, u' \in F - \{0\}$ e $p_1(x), \dots p_m(x)$, $p'_1(x), \dots p'_s(x)$ são polinômios irredutíveis sobre F.

Assim, temos,

$$p_1(x) \mid p'_1(x) \dots p'_s(x)$$

e daí segue que $\exists\, u'_i \in F - \{0\}$ tal que $p'_i(x) = u'_i \cdot p_1(x)$ (nesse caso dizemos que $p'_i(x)$ e $p_1(x)$ são associados em $F[x]$).

Abaixo, o teorema segue por indução sobre m.

Se $m = 1$ e $p_1(x)$ irredutível, temos que necessariamente $s = 1$ e $p_1(x)$ e $p_i'(x)$ são associados em $F[x]$.

Suponhamos $m > 1$. De $p_i'(x) = u_i' \cdot p_1(x)$ e sendo $F[x]$ um domínio temos que:

$$u \cdot p_2(x) \dots p_m(x) = u' \cdot u_i \cdot p_1'(x) \dots p_{i-1}(x) \cdot p_{i+1}(x) \dots p_s(x)$$

e daí segue pela hipótese de indução que $m - 1 = s - 1$ (isto é, $m = s$) e mais cada $p_j'(x)$ está associado com algum $p_i(x)$ através de uma constante. A partir dessas conclusões, termina-se a demonstração do teorema.

□

2.3.5 Irredutibilidade de polinômios em um corpo F

Podemos fazer um paralelo e dizer que os polinômios irredutíveis correspondem aos inteiros primos. No decorrer do texto, perceberemos que a irredutibilidade de um polinômio, depende do ambiente onde ele é considerado.

Um polinômio não-nulo $p(x)$ é dito irredutível em $F[x]$ se:

i) $\partial(p(x)) > 0$

ii) Quando escrevemos $p(x)$ como produto $p(x) = d(x)h(x)$, onde $d(x), h(x) \in F[x]$, então, necessariamente, temos $\partial(d(x)) = 0$ ou $\partial(h(x)) = 0$.

Um polinômio não constante que não é irredutível será chamado de redutível. Logo, se um polinômio $p(x)$ de grau maior ou igual a 1 é redutível sobre F, então ele pode ser escrito como um produto

$p(x) = d(x)h(x)$, com $d(x), h(x) \in F[x]$ e $\partial(d(x)) > 0$ e $\partial(h(x)) > 0$.

Podemos perceber que, independente do corpo F, qualquer polinômio $p(x)$ de grau 1 em $F[x]$ é irredutível sobre F.

Assim, escrevemos:

$p(x) = d(x).h(x)$, com $d(x), h(x) \in F[x]$.

Logo

$\partial(p(x)) = \partial(d(x)h(x)) = \partial(d(x)) + \partial(h(x))$

Como $\partial(p(x)) = 1$, temos

$\partial(d(x)) = 0$ e $\partial(h(x)) = 1$ ou $\partial(d(x)) = 1$ e $\partial(h(x)) = 0$.

Dado um polinômio $p(x) = x^4 - 5x^2 + 1$ pertencente a $\mathbb{Q}[x]$, queremos testar a redutibilidade de $p(x)$ em $\mathbb{Q}[x]$, então basta testarmos a redutibilidade de $p(x)$ em $Z[x]$, conforme o Lema de Gauss. Como $p(x)$ é um polinômio do quarto grau, as fatorações possíveis

pelo grau seriam quatro fatores do primeiro grau, ou dois fatores do primeiro grau e um fator do segundo grau, ou um fator do primeiro grau e um fator do terceiro grau ou, ainda, dois fatores de segundo grau. Temos que as três primeiras possibilidades dizem respeito a existência de pelo menos uma raiz racional (teorema do fator). Através do teste da raiz racional, os possíveis candidatos as raízes de $p(x)$ em $\mathbb{Q}[x]$ seriam 1 e -1. Como $p(1) = -3 \neq 0$ e $p(-1) = -3 \neq 0$, então $p(x)$ não possui raízes racionais, logo a conclusão é que não irá possuir fatores de primeiro grau. A única possibilidade de fatoração para $p(x)$ seria, então, na forma de dois fatores do segundo grau.

$$p(x) = (a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0), com\, a_0, a_1, b_0, b_1 \in \mathbb{Z}.$$

Como $p(x)$ é um polinômio mônico, ou seja, o coeficiente do termo de maior grau é unitário, temos então que $a_2 = b_2 = 1$.

Assim, temos:

$$\begin{aligned} p(x) &= (a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0). \\ &= x^4 + b_1x^3 + b_0x^2 + a_1x^3 + a_1b_1x^2 + a_1b_0x + a_0x^2 + a_0b_1x + a_0b_0. \\ &= x^4 + (a_1 + b_1)x^3 + (a_0 + a_1b_1 + b_0)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0 = x^4 - 5x^2 + 1. \end{aligned}$$

Pela igualdade de polinômios, obtemos:

$$a_1 + b_1 = 0$$

$$a_0 + a_1b_1 + b_0 = -5$$

$$a_1b_0 + a_0b_1 = 0$$

$$a_0b_0 = 1.$$

Como $a_0b_0 = 1$ em $\mathbb{Z}$, temos então que $a_0 = b_0 = 1$ ou $a_0 = b_0 = -1$, e como $a_1 + b_1 = 0$, temos que $b_1 = -a_1$.

Substituindo na equação $a_0 + a_1b_1 + b_0 = -5$, concluímos que

$$1 + a_1(-a_1) + 1 = -5$$

$$-(a_1)^2 + 1 + 1 = -5$$

$$(a_1)^2 - 1 - 1 = 5$$

$$(a_1)^2 - 2 = 5$$

$$(a_1)^2 = 7$$

ou

$$-1 + a_1(-a_1) - 1 = -5$$

$$-(a_1)^2 - 1 - 1 = -5$$

$$(a_1)^2 + 1 + 1 = 5$$

$$(a_1)^2 + 2 = 5$$

$$(a_1)^2 = 3.$$

Como não existem inteiros cujos quadrados são 7 ou 3, ficamos impossibilitados de fatorar $p(x)$ em $\mathbb{Z}[x]$.

Como o polinômio $p(x)$ é irredutível em $\mathbb{Z}[x]$, logo também será em $\mathbb{Q}[x]$. (Lema de Gauss que será enunciado e demonstrado no capítulo 4 - Proposição 4.2.1).

No estudo dos números inteiros $\mathbb{Z}$, alguns números naturais maiores que um não podem ser escritos como produto de dois naturais, simultaneamente maiores que um, e estes eram denominados de números primos. No conjunto de $F[x]$, temos polinômios que correspondem aos números primos em $\mathbb{Z}$, ou seja, polinômios não-nulos de grau maior que zero e que não podem ser escritos como produto de dois polinômios de graus maiores que zero em $F[x]$.

Exemplo 2.3.5 *O polinômio $x^2 + 1$ é irredutível em $\mathbb{R}[x]$, mas é redutível em $\mathbb{C}[x]$.*

Temos que $x^2 + 1 = (x - i) \cdot (x + i)$, $(x - i) \in \mathbb{C}[x]$ e $(x + i) \in \mathbb{C}[x]$.

Proposição 2.3.2 *Se $p(x) \in F[x]$ é polinômio de grau $n \geqslant 2$ e possui pelo menos uma raiz em F, então $p(x)$ é redutível em $F[x]$.*

Demonstração. Se $a \in F$ é raiz de $p(x)$, então temos que $x - a$ divide $p(x)$, ou seja, podemos escrever

$p(x) = (x - a)d(x)$, onde $d(x) \in F[x]$.

$p(x)$ tem grau n

$(x - a)$ tem grau 1

$d(x)$ tem grau $n - 1$

Como $n \geqslant 2$, então $n - 1 \geqslant 1$ e, assim, vamos ter $p(x)$ redutível em $F[x]$.

□

Teorema 2.3.7 *Se $p \in F[x] - \{0\}$, $\partial p \leq 3$, então p é redutível em $F[x]$ se, e somente se, p possui raízes em F.*

Demonstração. Se $\partial p = 1$, então p possui uma raiz.

Se $\partial p = 2$, então temos duas raízes reais ou duas raízes complexas ($a + bi$ e $a - bi$).

Se $\partial = 3$, então p pode ser escrito como produto de um polinômio de grau 2 por um polinômio de grau 1. Logo, em todos os casos temos raízes.

□

Teorema 2.3.8 *Um polinômio $p(x)$ em $\mathbb{C}[x]$ é irredutível sobre $\mathbb{C}$ se, e somente se, $p(x)$ tem grau 1.*

Demonstração. Claro que se $\partial p(x) = 1$, temos $p(x)$ irredutível sobre $\mathbb{C}$. Reciprocamente, se $p(x)$ é irredutível sobre $\mathbb{C}$ e de grau n, então n não pode ser > 1, pois se for, será um produto com mais de um fator e, assim, será redutível sobre $\mathbb{C}$. Esta contradição garante $n = 1$.

□

Exemplo 2.3.6 *Dividir o polinômio $p(x) = 2x^4 + 3x^2 + x - 4$ por $d(x) = x^3 - 2x^2 + x - 1$ em $R[x]$. Podemos notar que*

$$n = \partial(p(x)) = 4$$

$$m = \partial(d(x)) = 3$$

$$a_n = 2$$

$$b_m = 1.$$

Logo,

$$\frac{a_n}{b_m} x^{n-m} = 2x$$

assim,

$$\frac{a_n}{b_m} x^{n-m} d(x) = 2x^4 - 4x^3 + 2x^2 - 2x$$

e, portanto,

$$h(x) = p(x) - \frac{a_n}{b_m} x^{n-m} d(x) = 4x^3 + x^2 + 3x - 4$$

e continuando o processo das divisões sucessivas, até que tenhamos o grau de $h(x)$ menor que o grau de $d(x)$, temos $q(x) = 2x + 4$ e $r(x) = 9x^2 - x$.

Capítulo 3

Congruência Polinomial

Segundo [2], sobre o anel de polinômios, podemos definir a mesma estrutura modular utilizando a divisão euclidiana, porque a partir dela temos os restos e as classes de equivalência. Utilizando-se da mesma ideia, iremos encontrar os restos da divisão de polinômios, assim como utilizamos para encontrar o resto da divisão de 3^{223} por 7. A ideia é transportar os exemplos de divisibilidade envolvendo potência utilizando congruência para congruência de polinômios, pois os polinômios possuem estrutura aritmética parecida com a dos número inteiros, como a divisão euclidiana, a fatoração única e a divisão com resto único. Logo, podemos trazer para a mesma ideia de congruência, utilizando a congruência de polinômios em vez de congruência de inteiros, mas utilizando a mesma definição.

3.1 Congruência Polinomial módulo m. [2]

Chama-se congruência polinomial com uma incógnita toda congruência da forma geral:

$$p(x) \equiv 0 \, mod \, m. \tag{3.1}$$

onde $p(x)$ é um polinômio de grau $n \geqslant 1$ com coeficientes inteiros:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

e m é um inteiro positivo, módulo da congruência (3.1)

Para $n = 1$, temos a congruência linear com uma incógnita:

$$p(x) = a_1 x + a_0 \equiv 0 \, mod \, m.$$

A congruência linear acima é equivalente a uma Equação Diofantina Linear em duas

variáveis, ou seja,

$$a_1x + a_0 \equiv 0 \, mod \, m \Longrightarrow a_1x \equiv -a_0 \, mod \, m \Longrightarrow a_1X - mY = -a_0 \Longrightarrow mY - a_1X = a_0.$$

Se o grau de $p(x)$ é maior do que 1, então a congruência

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \equiv 0 \, mod \, m$$

equivale à Equação Diofantina não linear $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + mY = a_0$.

3.1.1 Grau de uma congruência polinomial

A congruência polinomial (3.1) diz-se de grau $\partial p(x)$ se, e somente se $a_{\partial p}$ é coeficiente de maior potência de x que é incongruente a 0 módulo m:

$$a_{\partial p} \not\equiv 0 \, mod \, m.$$

Se o grau $\partial p < n$, com n sendo o grau de $p(x)$, isto significa que

$$a_{\partial p+1} \equiv a_{\partial p+2} \equiv \ldots \equiv a_n \equiv 0 \, mod \, m.$$

Em particular, se $a_n \not\equiv 0 \, mod \, m$, então a congruência polinomial (3.1) é de grau n. No caso em que todos os coeficientes do polinômio $p(x)$ são congruentes a 0 módulo m, então diz-se que o grau de congruência polinomial (3.1) é indefinido. Logo, o grau da congruência polinomial (3.1) depende do seu módulo m e nem sempre coincide com o grau do polinômio $p(x)$, que é sempre n, qualquer que seja o módulo m.

Exemplo 3.1.1 *Dado o polinômio* $p(x) = 30x^4 - 60x^3 + 12x^2 - 6x + 3$

Iremos verificar o coeficiente de maior potência de x que é incongruente a 0 *módulo m. Esta potência define o grau da congruência polinomial.*

A congruência polinomial

$p(x) \equiv 0 \, mod \, 12$ *é de grau* 4, *pois* $30 \not\equiv 0 \, mod \, 12$ *e como 30 é o coeficiente do monômio que possui expoente* 4, *a congruência possui grau igual a* 4.

$p(x) \equiv 0 \, mod \, 7$ *é de grau* 4, *pois* $30 \not\equiv 0 \, mod \, 7$ *e como 30 é o coeficiente do monômio que possui expoente* 4, *a congruência possui grau igual a* 4.

$p(x) \equiv 0 \, mod \, 5$ *é de grau* 2, *pois* $30 \equiv 0 \, mod \, 5$, $60 \equiv 0 \, mod \, 5$, $12 \not\equiv 0 \, mod \, 5$ *e como 12 é o coeficiente do monômio que possui expoente* 2, *a congruência possui grau igual a* 2.

$p(x) \equiv 0 \, mod \, 6$ *é de grau* 0, *pois* $30 \equiv 0 \, mod \, 6$, $60 \equiv 0 \, mod \, 6$, $12 \equiv 0 \, mod \, 6$, $6 \equiv 0 \, mod \, 6$ *e* $3 \not\equiv 0 \, mod \, 6$ *e como 3 é o coeficiente do monômio que possui expoente* 0, *ou seja, é o termo*

independente, então a congruência possui grau igual a 0.

$p(x) \equiv 0 \, mod \, 3$ *é indefinido, pois* $30 \equiv 0 \, mod \, 3$, $60 \equiv 0 \, mod \, 3$, $12 \equiv 0 \, mod \, 3$, $6 \equiv 0 \, mod \, 3$ *e* $3 \not\equiv 0 \, mod \, 3$ *e como não temos coeficientes dos monômios incongruentes a zero módulo* 3*, então o grau é indefinido.*

3.1.2 Soluções de uma congruência polinomial

Todo inteiro a tal que $p(a) \equiv 0 \, mod \, m$ diz-se uma solução da congruência polinomial (3.1). Se a é uma solução da congruência polinomial (3.1), então $p(a) \equiv 0 \, mod \, m$ e se $a \equiv b \, mod \, m$, então $p(b) \equiv 0 \, mod \, m$, logo b também é uma solução da congruência polinomial (3.1). Assim, por transitividade, temos que $p(a) \equiv p(b) \, mod \, m$.

$$p(a) \equiv 0 \, mod \, m \text{ e } p(b) \equiv 0 \, mod \, m$$

implica $p(a) \equiv p(b) \, mod \, m$.

Por convenção geral, sempre que se fala de soluções distintas de congruência polinomial (3.1), deve-se entender que se trata de soluções incongruentes módulo m. Sejam a uma solução qualquer da congruência polinomial (3.1) e $S = r_1, r_2, \ldots, r_m$ um sistema completo de restos módulo m, então o inteiro a é congruente módulo m a um único elemento de r_i do conjunto S: $a \equiv r_i \, mod \, m$, o que implica:

$$p(r_i) \equiv p(a) \equiv 0 \, mod \, m$$

isto é, r_i é solução da congruência polinomial (3.1). Portanto, as soluções desta congruência são os elementos r_i do conjunto S tais que $p(r_i) \equiv 0 \, mod \, m$. Em particular, como o conjunto $S_0 = 0, 1, 2, \ldots, m-1$ é um sistema completo de restos módulo m, segue-se que todas as soluções da congruência polinomial (3.1) são elementos deste conjunto S_0 e, por conseguinte, esta congruência pode ter, quando muito, m soluções.

Consideremos, por exemplo, a congruência polinomial:

$$p(x) = x^5 + x + 1 \equiv 0 \, mod \, 7.$$

O conjunto $S_0 = 0, 1, 2, 3, 4, 5, 6$ é um sistema completo de restos módulo 7, já que m varia de 0 a $m - 1$.

$$p(0) = 0^5 + 0 + 1 = 1 \not\equiv 0 \, mod \, 7$$

$$p(1) = 1^5 + 1 + 1 = 3 \not\equiv 0 \, mod \, 7$$

$$p(2) = 2^5 + 2 + 1 = 35 \equiv 0 \, mod \, 7$$

$$p(3) = 3^5 + 3 + 1 = 247 \not\equiv 0 \, mod \, 7$$

$$p(4) = 4^5 + 4 + 1 = 1029 \equiv 0 \, mod \, 7$$

$$p(5) = 5^5 + 5 + 1 = 3131 \not\equiv 0 \, mod \, 7$$

$$p(6) = 6^5 + 6 + 1 = 7783 \not\equiv 0 \, mod \, 7.$$

Como 2 e 4 são os únicos valores do conjunto S_0 tais que

$$p(2) \equiv 0 \, mod \, 7$$

$$p(4) \equiv 0 \, mod \, 7$$

segue-se que a congruência polinomial considerada apresenta apenas duas soluções:

$$x \equiv 2 \, mod \, 7 \text{ e } x \equiv 4 \, mod \, 7.$$

Logo, as duas soluções da congruência polinomial são elementos r_i do conjunto S_0 tais que $p(r_i) \equiv 0 \, mod \, m$.

É fácil perceber que as soluções da congruência polinomial $p(x)$ módulo m são valores de $x \equiv a \, mod \, m$ tais que $p(a)$ sejam múltiplos de m.

3.1.3 Congruências polinomiais com módulo composto

Para resolver a congruência polinomial, utilizaremos, de forma geral, o Teorema Chinês do Resto para encontrar as soluções. Teremos, assim, uma das aplicações de congruência modular com módulo composto nos polinômios.

Teorema 3.1.1 *Seja m um inteiro positivo tal que $m = m_1 m_2 \cdots m_k$, onde $m_1, m_2, \ldots, m_k$ são inteiros positivos primos entre si dois a dois. Então, o inteiro a é uma solução da congruência polinomial:*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \, mod \, m \tag{3.2}$$

se, e somente se a é uma solução do seguinte sistema de k congruências polinomiais:

$$\begin{aligned} p(x) &\equiv 0 \, mod \, m_1 \\ p(x) &\equiv 0 \, mod \, m_2 \\ &\vdots \\ p(x) &\equiv 0 \, mod \, m_k \end{aligned} \tag{4}$$

Demonstração. $\Longrightarrow$ Suponhamos que o inteiro a é uma solução da congruência polinomial (4). Então:

$$p(a) \equiv 0 \, mod \, m \text{ e } m \mid p(a).$$

E como $m_i \mid m$, para $i = 1, 2, \ldots, k$, segue-se que

$$m_i \mid p(a) \text{ e } p(a) \equiv 0 \, mod \, m_i \, , \; i = 1, 2, \ldots, k$$

isto é, o inteiro a é uma solução do sistema (3.1). $\Longleftarrow$ Reciprocamente, suponhamos que o inteiro a é uma solução do sistema (3.1). Então:

$$p(a) \equiv 0 \, mod \, m_i \, , \; i = 1, 2, \ldots, k$$

isto é, $p(a)$ é uma solução do sistema:

$$x \equiv 0 \, mod \, m_1$$

$$x \equiv 0 \, mod \, m_2$$

$$\vdots$$

$$x \equiv 0 \, mod \, m_k.$$

Logo, pelo "Teorema Chinês do resto":

$$p(a) \equiv 0 \, mod \, (m_1 m_2 \ldots m_k)$$

isto é, o inteiro a é uma solução da congruência polinomial (3.2).

□

Consoante a este teorema, a resolução da congruência polinomial (3) no caso em que o módulo m admite a fatoração canônica é:

$$m = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$

reduz-se à resolução de congruências polinomiais da forma:

$$p(x) \equiv 0 \, mod \, p^a$$

isto é, congruências polinomiais cujo módulo é uma potência de um número primo.

Exemplo 3.1.2 *Como exemplo, podemos resolver a congruência polinomial:*

$$p(x) = x^3 + 19x^2 - x + 23 \equiv 0 \, mod \, 42.$$

Resolução: Por ser $42 = 2 \cdot 3 \cdot 7$*, temos as três congruências polinomiais:*

$$p(x) \equiv 0 \, mod \, 2$$

$$p(x) \equiv 0 \, mod \, 3$$

$$p(x) \equiv 0 \, mod \, 7$$

cujas soluções respectivas são:

$x \equiv 1 \, mod \, 2, \; pois \; p(1) = (1)^3 + 19 \cdot (1)^2 - (1) + 23 = 42 \equiv 0 \, mod \, 2$
$x \equiv -1 \, mod \, 3, \; pois \; p(-1) = (-1)^3 + 19 \cdot (-1)^2 - (-1) + 23 = 42 \equiv 0 \, mod \, 3$
$x \equiv 1 \, mod \, 3, \; pois \; p(1) = (1)^3 + 19 \cdot (1)^2 - (1) + 23 = 42 \equiv 0 \, mod \, 3$
$x \equiv -1 \, mod \, 7, \; pois \; p(-1) = (-1)^3 + 19 \cdot (-1)^2 - (-1) + 23 = 42 \equiv 0 \, mod \, 7$
$x \equiv 1 \, mod \, 7, \; pois \; p(1) = (1)^3 + 19 \cdot (1)^2 - (1) + 23 = 42 \equiv 0 \, mod \, 7$
$x \equiv 2 \, mod \, 7, \; pois \; p(2) = (2)^3 + 19 \cdot (2)^2 - (2) + 23 = 105 \equiv 0 \, mod \, 7.$

Logo, a congruência polinomial dada tem 6 ***soluções incongruentes*** *módulo* 42 *dadas pelos 6 sistemas de congruências lineares:*

$$\begin{cases} x \equiv a \, mod \, 2 \\ x \equiv b \, mod \, 3 \\ x \equiv c \, mod \, 7 \end{cases}$$

onde $a \in \{1\}$, $b \in \{-1, 1\}$, $c \in \{-1, 1, 2\}$.
Utilizando o "Teorema Chinês do resto", obtemos:

$$21x_1 \equiv 1 \, mod \, 2, \; logo, \; x_1 = 1$$
$$14x_2 \equiv 1 \, mod \, 3, \; logo, \; x_2 = -1$$
$$6x_3 \equiv 1 \, mod \, 7, \; logo, \; x_3 = -1.$$

$$x \equiv 21 \cdot x_1 \cdot a - 14 \cdot x_2 \cdot b - 6 \cdot x_3 \cdot c \; mod \, (2 \cdot 3 \cdot 7)$$

$$x \equiv 21 \cdot (1) \cdot a + 14 \cdot (-1) \cdot b + 6 \cdot (-1) \cdot c \; mod \, (2 \cdot 3 \cdot 7)$$

$$x \equiv 21 \cdot a - 14 \cdot b - 6 \cdot c \; mod \, (2 \cdot 3 \cdot 7)$$

$$x \equiv 21a - 14b - 6c \, mod \, 42.$$

Com uma possibilidade para a, duas possibilidades para b e três possibilidades para c.
Portanto, as $1 \cdot 2 \cdot 3 = 6$ *soluções da congruências polinomial* $p(x)$ *são:*

$x \equiv 21 \cdot (1) - 14 \cdot (-1) - 6 \cdot (-1) = 21 + 14 + 6 = 41 \, mod \, 42$
$x \equiv 21 \cdot (1) - 14 \cdot (-1) - 6 \cdot (1) = 21 + 14 - 6 = 29 \, mod \, 42$
$x \equiv 21 \cdot (1) - 14 \cdot (-1) - 6 \cdot (2) = 21 + 14 - 12 = 23 \, mod \, 42$
$x \equiv 21 \cdot (1) - 14 \cdot (1) - 6 \cdot (-1) = 21 - 14 + 6 = 13 \, mod \, 42$
$x \equiv 21 \cdot (1) - 14 \cdot (1) - 6 \cdot (1) = 21 - 14 - 6 = 1 \, mod \, 42$
$x \equiv 21 \cdot (1) - 14 \cdot (1) - 6 \cdot (2) = 21 - 14 - 12 = -5 \, mod \, 42.$

3.2 Congruência Polinomial módulo d(x)

A associação da divisão euclidiana à notação em módulo é bastante útil com os números inteiros e aplicável também para os polinômios, simplificando bastante a resolução dos problemas.

A grande vantagem da aplicação da congruência é substituir as potências grandes de x por outros termos que são exatamente o resto da divisão dessa potência pelo módulo em questão.

Sejam os polinômios:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

$$d(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

$$q(x) = q_\alpha x^\alpha + q_{\alpha-1} x^{\alpha-1} + \cdots + q_1 x + q_0$$

com $m \leqslant n$ e $\alpha = n - m$.

Como $\partial r(x) < \partial d(x)$ e $0 \leqslant \alpha \leqslant n$, então $0 \leqslant \partial r(x) \leqslant n - 1$

Pelo algoritmo da divisão de polinômios, temos:

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

Como $d(x) \mid (p(x) - r(x))$, então $p(x) \equiv r(x) \, mod \, d(x)$.

Logo $p(x) - r(x) \equiv 0 \, mod \, d(x)$.

Mas $p(x) - r(x) = d(x) \cdot q(x)$, assim $d(x) \cdot q(x) \equiv 0 \, mod \, d(x)$, ou seja,

$d(x) \equiv 0 \, mod \, d(x)$ ou $q(x) \equiv 0 \, mod \, d(x)$.

Como $d(x) \nmid q(x)$, então $q(x) \not\equiv 0 \, mod \, d(x)$, logo concluímos que

$d(x) \equiv 0 \, mod \, d(x)$.

As congruências $p(x) \equiv r(x) \, mod \, d(x)$ e $d(x) \equiv 0 \, mod \, d(x)$ serão aplicadas para determinação do resto da divisão de dois polinômios.

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv r(x) \, mod \, d(x)$$

$$b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \equiv 0 \, mod \, d(x).$$

Capítulo 4

Aplicações de Congruências em polinômios

Podemos propor uma oficina de resolução de problemas com a finalidade de trabalhar as aplicações de congruências para a determinação do resto da divisão de polinômios e para verificação da irredutibilidade de um polinômio. Assim, iremos utilizar os exemplos a seguir, mostrando, primeiramente, como é resolvido pelo método tradicional e, posteriormente, com o uso da congruência.

4.1 Determinação do resto da divisão de polinômios

Exemplo 4.1.1 *Determine o resto da divisão do polinômio* $p(x) = x^8 - 3x^7 + x^6 - 10x^5 + 5x^4 - 2x^3 + x^2 - 3x + 4$ *pelo polinômio* $d(x) = x^2 - 1$.

a) *Primeiro Método de Resolução: Divisão de Euclides.*

Realizando a divisão pelo método da chave, obtemos:

$$
\begin{array}{rl|l}
x^8-3x^7+x^6-10x^5+5x^4-2x^3+x^2-3x+4 & & x^2-1 \\
\underline{-x^8\qquad +x^6} & & x^6-3x^5+2x^4-13x^3+7x^2-15x+8 \\
-3x^7+2x^6-10x^5 & & \\
\underline{+3x^7\qquad -3x^5} & & \\
+2x^6-13x^5+5x^4 & & \\
\underline{-2x^6\qquad +2x^4} & & \\
-13x^5+7x^4-2x^3 & & \\
\underline{+13x^5\qquad -13x^3} & & \\
+7x^4-15x^3+x^2 & & \\
\underline{-7x^4\qquad +7x^2} & & \\
-15x^3+8x^2-3x & & \\
\underline{+15x^3\qquad -15x} & & \\
+8x^2-18x+4 & & \\
\underline{-8x^2\qquad +8} & & \\
-18x+12 & &
\end{array}
$$

Obtendo os elementos do quociente, temos

$x^8 \cdot \frac{1}{x^2} = x^6$, $\quad -3x^7 \cdot \frac{1}{x^2} = -3x^5$, $\quad 2x^6 \cdot \frac{1}{x^2} = 2x^4$, $\quad -13x^5 \cdot \frac{1}{x^2} = -13x^3$, $\quad 7x^4 \cdot \frac{1}{x^2} = 7x^2$,

$-15^3 \cdot \frac{1}{x^2} = -15x$, $\quad 8x^2 \cdot \frac{1}{x^2} = 8.$

resto $r(x) = -18x + 12$ *e o quociente* $x^6 - 3x^5 + 2x^4 - 13x^3 + 7x^2 - 15x + 8.$

Logo,

$p(x) = (x^2 - 1)(x^6 - 3x^5 + 2x^4 - 13x^3 + 7x^2 - 15x + 8) + (-18x + 12).$

b) *Segundo Método de Resolução: Fatoração do divisor e escrevendo o resto na forma* $(ax + b)$.

Utilizando a fatoração, temos que $d(x) = x^2 - 1 = (x - 1)(x + 1)$.

Assim,

dividimos o polinômio $p(x)$ *por* $x - 1$ *e o resto será* $p(1) = -6$ *pelo teorema do resto.*

Dividimos o polinômio $p(x)$ *por* $x + 1$ *e o resto será* $p(-1) = 30$ *pelo teorema do resto.*

Logo, o resto do polinômio $p(x)$ *por* $(x - 1).(x + 1)$ *será da forma* $r(x) = ax + b$, *ou seja, um polinômio de primeiro grau.*

Como $(x - 1).(x + 1) = x^2 - 1$, *então pela divisão euclidiana, temos:*

$p(x) = (x^2 - 1).q(x) + r(x)$, *ou seja,* $p(x) = (x^2 - 1).q(x) + (ax + b)$.

Então,

$p(1) = (1^2 - 1).q(1) + a.(1) + b = -6,$

logo, $a + b = -6$.

$p(-1) = ((-1)^2 - 1).q(-1) + a.(-1) + b = 30$,

logo, $-a + b = 30$.

Resolvendo o sistema acima, temos $a = -18$ *e* $b = 12$.

Assim, o resto é $r(x) = -18x + 12$.

Não conseguimos aplicar este método, por exemplo, para um divisor igual a $x^2 + 1$, *pois é impossível fatorar como produto de termos do primeiro grau, ou seja, é irredutível sobre os inteiros.*

Conforme o item 3.2, *utilizaremos a congruência módulo* $d(x)$ *para a resolução do método a seguir.*

c) *Terceiro Método de Resolução: Aplicação da congruência polinomial.*

Como $x^2 - 1 \equiv 0 \, mod \, (x^2 - 1)$, *onde* $(x^2 - 1) \notin \mathbb{N}$

então $x^2 \equiv 1 \, mod \, (x^2 - 1)$.

Logo

$$
\begin{aligned}
& x^8 - 3x^7 + x^6 - 10x^5 + 5x^4 - 2x^3 + x^2 - 3x + 4 \\
&= (x^2)^4 - 3(x^2)^3x + (x^2)^3 - 10(x^2)^2x + 5(x^2)^2 - 2(x^2)x + x^2 - 3x + 4 \\
&\equiv (1)^4 - 3(1)^3x + (1)^3 - 10(1)^2x + 5(1)^2 - 2(1)x + 1 - 3x + 4 \\
&= 1 - 3x + 1 - 10x + 5 - 2x + 1 - 3x + 4 \\
&= -18x + 12 \, mod \, (x^2 - 1).
\end{aligned}
$$

Assim, o resto da divisão de $p(x)$ *por* $d(x)$ *é igual a* $r(x) = -18x + 12$.

Exemplo 4.1.2 *(UNICAMP): Determine o resto da divisão de* $x^{100} + x + 1$ *por* $x^2 - 1$.
Como $x^2 - 1 \equiv 0 \, mod \, (x^2 - 1)$
então $x^2 \equiv 1 \, mod \, (x^2 - 1)$.
Logo $x^{100} + x + 1 = (x^2)^{50} + x + 1 \equiv 1^{50} + x + 1 = x + 2 \, mod \, (x^2 - 1)$.
O resto da divisão é igual a $x + 2$.

Exemplo 4.1.3 *(UNIUBE): Encontre o resto* $r(x)$ *da divisão de* $p(x) = x^{2001}$ *por* $q(x) = x^2 - 1$.
Temos que $x^{2001} \equiv r \, mod \, (x^2 - 1)$.
Como $x^2 \equiv 1 \, mod \, (x^2 - 1)$.
Logo $x^{2001} = (x^2)^{1000}x \equiv 1^{1000}x = x \, mod \, (x^2 - 1)$.
O resto da divisão de $p(x)$ *por* $q(x)$ *é igual a* x.

Exemplo 4.1.4 *(UEL): Na divisão de* $x^5 + 2x^4 - 3x^3 + x^2 - 3x + 2$ *por* $x^2 + x + 1$, *determine o resto.*
$x^2 + x + 1 \equiv 0 \, mod \, (x^2 + x + 1)$.
$x^2 + x \equiv -1 \, mod \, (x^2 + x + 1)$.
$x^2 \equiv -x - 1 \, mod \, (x^2 + x + 1)$.

$x^2 \equiv -(x+1)\ mod\ (x^2+x+1)$.
$x^3 \equiv 1\ mod\ (x^2+x+1)$.
$x^4 \equiv x\ mod\ (x^2+x+1)$.
$x^5 \equiv -x-1\ mod\ (x^2+x+1)$.
Logo
$x^5+2x^4-3x^3+x^2-3x+2 \equiv -x-1+2x-3.1-x-1-3x+2 = -3x-3\ mod\ (x^2+x+1)$.
O resto da divisão é igual a $-3x-3$.

Exemplo 4.1.5 *(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
$x^2-2x+1 \equiv 0\ mod\ (x^2-2x+1)$.
$x^2 \equiv 2x-1\ mod\ (x^2-2x+1)$.
$x^3 \equiv 3x-2\ mod\ (x^2-2x+1)$.
$x^4 \equiv 4x-3\ mod\ (x^2-2x+1)$.
$x^5 \equiv 5x-4\ mod\ (x^2-2x+1)$.
$x^5-2x^4+ax^3+bx^2-2x+1 \equiv 5x-4-2(4x-3)+a(3x-2)+b(2x-1)-2x+1$
$= 5x-4-8x+6+3ax-2a+2bx-b-2x+1 = (3a+2b-5)x+(-2a-b+3)$
Como o resto é igual a $(3a+2b-5)x+(-2a-b+3)$ *e como o polinômio é divisível por* x^2-2x+1, *então* $(3a+2b-5)x+(-2a-b+3) = 0x+0$.

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

Resolvendo o sistema temos $a=1$ *e* $b=1$.
Logo o valor da soma $a+b$ *é igual a* 2.

Exemplo 4.1.6 *Determine o resto de* $p(x)=x^5+x+1$ *por* $g(x)=x^3-1$.
$x^3-1 \equiv 0\ mod\ (x^3-1)$.
$x^3 \equiv 1\ mod\ (x^3-1)$.
Logo $x^5+x+1 = x^2x^3+x+1 \equiv x^2.1+x+1 = x^2+x+1\ mod\ (x^3-1)$.
O resto da divisão de $p(x)$ *por* $g(x)$ *é igual a* x^2+x+1.

Exemplo 4.1.7 *(UNITAU) Encontre o valor de b para o qual o polinômio*
$p(x)=15x^{16}+bx^{15}+1$ *seja divisível por* $x-1$.
$x-1 \equiv 0\ mod\ (x-1)$,
$x \equiv 1\ mod\ (x-1)$.
Logo $x^{16} \equiv 1^{16}\ mod\ (x-1)$ *e* $x^{15} \equiv 1^{15}\ mod\ (x-1)$, *então*
$15x^{16}+bx^{15}+1 \equiv 15.1+b.1+1 = 16+b\ mod\ (x-1)$.
Como $p(x)$ *é divisível por* $x-1$, *então temos que o resto é igual a zero, logo* $16+b=0$, $b=-16$.

Exemplo 4.1.8 *(Colégio Naval) Determine o resto da divisão de* $p(x) = x^{127} + x^{10} + 1$ *por* $d(x) = x^3 + 1$.

$x^3 + 1 \equiv 0 \, mod \, (x^3 + 1)$.

$x^3 \equiv -1 \, mod \, (x^3 + 1)$.

Logo $x^{127} + x^{10} + 1 = x^{126}x + x^9x + 1 = (x^3)^{42}x + (x^3)^3x + 1$.

$(x^3)^{42}x + (x^3)^3x + 1 \equiv (-1)^{42}x + (-1)^3x + 1 = x - x + 1 = 1 \, mod \, (x^3 + 1)$.

O resto da divisão de $p(x)$ *por* $d(x)$ *será igual a* 1.

Atividades propostas:

Espera-se que os alunos resolvam os exercícios seguintes utilizando a congruência polinomial.

Exercício 4.1.1 *(IME/2015): Encontre o resto da divisão do polinômio* $p(x) = x^{26} - x^{25} - 6x^{24} + 5x^4 - 16x^3 + 3x^2$ *por* $d(x) = x^3 - 3x^2 - x + 3$.

Exercício 4.1.2 *(ITA/2016): Determine o resto da divisão de* $(1 + x + x^2)^{40}$ *por* $(1 + x)^3$.

Exercício 4.1.3 *(IME): Provar que* $p(x) = x^{999} + x^{888} + x^{777} + \cdots + x^{111} + 1$ *é divisível pelo polinômio* $d(x) = x^9 + x^8 + x^7 + \cdots + x^1 + 1$.

4.2 Critério de Irredutibilidade de Eisenstein

Podemos constatar no capítulo anterior, que a irredutibilidade, utilizando a definição, é muito trabalhosa e dispendiosa em relação ao tempo (como apresentado na introdução de irredutibilidade). Segundo [5], para discutir, por exemplo, a irredutibilidade de um polinômio do décimo quinto grau, teriam várias combinações possíveis em relação ao grau, para a fatoração do polinômio.

Os critérios de irredutibilidade são eficientes e precisos a fim de simplificar nossa tarefa e assim chegar, de forma ágil, ao objetivo. Não podemos aplicar o critério de Eisenstein a todos os polinômios que são irredutíveis sobre os números racionais, mas é possível a verificação da irredutibilidade em casos importantes, com pouco esforço. O Critério de Eisenstein é aplicado diretamente ou através de uma transformação do polinômio original.

Proposição 4.2.1 *(Lema de Gauss)*

Se $p(x) \in \mathbb{Z}[x]$ *é um polinômio irredutível sobre* $\mathbb{Z}[x]$, *então* $p(x)$ *também é irredutível sobre* $\mathbb{Q}[x]$.

Demonstração. *Um polinômio* $f(x) \in \mathbb{Z}[x]$ *é primitivo se o MDC de seus coeficientes é igual a* 1. *O produto de dois polinômios primitivos* $f(x)$ *e* $g(x) \in \mathbb{Z}[x]$ *também é primitivo:*

Supondo que tal produto não seja primitivo, então existe um número primo p que divide todos os coeficientes de $f(x).g(x)$, *portanto este produto será nulo em* $\mathbb{Z}_{\mathbb{P}}[x]$, *logo um dos polinômios deverá*

ser nulo em $\mathbb{Z}_{\mathbb{P}}[x]$. Se $f(x)$ é nulo, então todos os seus coeficientes serão divisíveis por p, dessa forma, teríamos um absurdo; $g(x)$ também não pode ser nulo. Assim, um produto de polinômios primitivos deve ser primitivo.

Supondo que $p(x)$ possa ser fatorado sobre $\mathbb{Q}[x]$, onde $p(x) = q(x).h(x)$, sendo m_1 o MMC dos denominadores dos coeficientes em $q(x)$, temos $m_1.q(x)$ primitivo.

Sendo m_2 o MMC dos denominadores dos coeficientes em $h(x)$, temos $m_2.h(x)$ primitivo.

Então:

$$m_1 m_2 p(x) = m_1 q(x) m_2 h(x).$$

O lado direito será primitivo o que implica que o lado esquerdo também será primitivo. Isso só será possível se m_1 e m_2 são ± 1 o que faz com que a fatoração inicial já fosse em $\mathbb{Z}[x]$.

□

Teorema 4.2.1 (Critério de Irredutibilidade de Eisenstein)
Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0 \in \mathbb{Z}[x]$ um polinômio de grau $n \geq 1$. Suponha que exista um número primo p tal que:

i) $a_n \not\equiv 0 \, mod \, p$.

ii) $a_i \equiv 0 \, mod \, p$ *para* $0 \leq i \leq n-1$.

iii) $a_0 \not\equiv 0 \, mod \, p^2$.

Então $f(x)$ é irredutível em $\mathbb{Z}[x]$.

Demonstração. Suponha, por absurdo, que f não seja irredutível e que $f = g.h \, ; g, h \in \mathbb{Z}[x]$

Escrevendo os polinômios g e h na forma estendida

$g(x) = b_r x^r + b_{r-1}x^{r-1} + \cdots + b_1 x^1 + b_0 \in \mathbb{Z}[x]$, $r \geq 1$

$h(x) = c_s x^s + c_{s-1}x^{s-1} + \cdots + c_1 x^1 + c_0 \in \mathbb{Z}[x]$, $s \geq 1$, $b_r, c_s \neq 0$ e $r, s < n$.

De (*iii*), temos que b_0 e c_0 não podem ser ambos divisíveis por p. Supomos, sem perda de generalidade, que p divide apenas c_0, tome:

$m = MIN\{k \mid k \in \{0, 1, 2, \ldots, s\}\}$ tal que $c_k \not\equiv 0 \, mod \, p$, logo $m \geq 1$, pois $c_0 \equiv 0 \, mod \, p$. Note que $n > s \geq m$.

Também, pode-se verificar que $a_m = b_0 c_m + b c_{m-1} + \cdots + b_{m-i} c_i$ para algum i entre 0 e m. Como b_0 e c_m não são divisíveis por p, então $c_{m-1}, \ldots, c_i$ são divisíveis por p. Temos que $a_m \equiv b_0 \, mod \, p$ e $a_m \not\equiv \, mod \, p$, segue de (i) e de (ii) que $m = n$, o que implica que $s = n*$, absurdo.

□

Segue da definição de congruência que $a \equiv b \, mod \, p$, ou seja, $p \mid (b - a)$, então outra maneira de enunciar o Critério de Eisenstein seria:

Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0 \in \mathbb{Z}[x]$ um polinômio de grau $n \geq 1$. Suponha que exista um número primo p tal que:

i) $p \nmid a_n$.

ii) $p \mid a_i \, \forall \, i \in \{0, 1, \ldots, n-1\}$.

iii) $p^2 \nmid a_0$.

Então $f(x)$ é irredutível em $\mathbb{Z}[x]$.

Exemplo 4.2.1 *Mostre que* $p(x) = x^4 - 2x^2 + 8x + 2 \in \mathbb{Z}[x]$ *é irredutível em* $\mathbb{Q}[x]$. *Completando o polinômio,* $p(x)$ *fica* $1x^4 + 0x^3 - 2x^2 + 8x + 2$.

Seja $p = 2$, *então temos que:*

$$
\begin{gathered}
1 \not\equiv 0 \, mod \, 2, \, ou \, seja, \, 2 \nmid 1 \\
0 \equiv 0 \, mod \, 2, \, ou \, seja, \, 2 \mid 0 \\
-2 \equiv 0 \, mod \, 2, \, ou \, seja, \, 2 \mid -2 \\
8 \equiv 0 \, mod \, 2, \, ou \, seja, \, 2 \mid 8 \\
2 \equiv 0 \, mod \, 2, \, ou \, seja, \, 2 \mid 2 \\
2 \not\equiv 0 \, mod \, 2^2, \, ou \, seja, \, 2^2 \nmid 2.
\end{gathered}
$$

Logo, $p(x)$ *é irredutível em* $\mathbb{Z}[x]$. *(Teorema* 4.2.1*)*
Se $p(x) \in \mathbb{Z}[x]$ *é irredutível sobre* $\mathbb{Z}[x]$, *então* $p(x)$ *é irredutível sobre* $\mathbb{Q}[x]$. *(Gauss)*

Exemplo 4.2.2 *Prove que* $p(x) = x^3 + 2x + 10$ *é irredutível em* $\mathbb{Q}[x]$.
Completando o polinômio, $p(x)$ *fica* $x^3 + 0x^2 + 2x + 10$.
Tomando $p = 2$ *primo, temos que:*

$$
\begin{gathered}
1 \not\equiv 0 \, mod \, 2, \, ou \, seja, \, 2 \nmid 1 \\
0 \equiv 0 \, mod \, 2, \, ou \, seja, \, 2 \mid 0 \\
2 \equiv 0 \, mod \, 2, \, ou \, seja, \, 2 \mid 2 \\
10 \equiv 0 \, mod \, 2, \, ou \, seja, \, 2 \mid 10 \\
10 \not\equiv 0 \, mod \, 2^2, \, ou \, seja, \, 2^2 \nmid 10.
\end{gathered}
$$

Assim, pelo critério de Eisenstein, $p(x)$ *é irredutível sobre os racionais.*

Exemplo 4.2.3 *Demonstre que a raiz quadrada de todo número primo é irracional.*

Seja p *um número primo qualquer e considere o polinômio* $p(x) = x^2 - p$. *Agora observe que* p *não é divisor de* $a_2 = 1$, *mas sim de* $a_1 = 0$ *e de* $a_0 = -p$, *além disso,* p^2 *não divide* $a_0 = -p$. *O critério de Eisenstein nos assegura que o polinômio* $p(x)$ *é irredutível em* $\mathbb{Q}[x]$. *Isto implica que* $p(x)$ *não tem raízes racionais, portanto* $\sqrt{p}$ *é irracional.*

Observe que $x^2 - p = (x + \sqrt{p})(x - \sqrt{p})$.

Exemplo 4.2.4 *Aplicação após translação $p(x+a)$.*

Quando o critério de Eisenstein não se aplica para nenhum número primo, então há a possibilidade de aplicá-lo para algum número primo após a substituição de x por $x+a$ no polinômio $p(x)$, onde a é um número inteiro.Se o polinômio obtido $p(x+a)$ for irredutível, então concluímos que o polinômio original $p(x)$ também será irredutível.

Considere, por exemplo, um polinômio $p(x) = x^2+x+2$, em que o coeficiente de x não é divisível por nenhum primo, portando o critério de Eisenstein não se aplica. Substituindo x por $x+3$, obtemos o polinômio $x^2+7x+14$, que satisfaz o critério de Eisenstein para o número primo $p=7$. Como esta substituição é um automorfismo do anel $\mathbb{Q}[x]$, o fato de se obter um polinômio irredutível implica que o polinômio original é irredutível.

Podemos dizer também que o polinômio $p(x)$ é mônico de grau 2, logo só poderia ser redutível se tivesse uma raiz inteira, o que na verdade não possui, no entanto, o uso da substituição para a aplicação do critério de Eisenstein é uma maneira de estender a sua utilidade.

Exemplo 4.2.5 *Aplicação invertendo a ordem dos coeficientes de $p(x)$*

Outra possibilidade para transformar um polinômio de modo a satisfazer o critério, que pode ser combinada com a aplicação de um deslocamento, é inverter a ordem de seus coeficientes, contanto que o seu termo constante seja diferente de zero (afinal, se não fosse o polinômio já seria divisível por x). Isto pode ser feito porque esses polinômios são redutíveis em $\mathbb{R}[x]$ se , e somente se, eles são redutíveis em $R[x,x^{-1}]$ (para qualquer domínio de integridade $\mathbb{R}$), e neste anel a substituição de x por x^{-1} inverte a ordem dos coeficientes (de forma simétrica em relação ao coeficiente constante, mas uma subsequente mudança no expoente corresponde à multiplicação por uma unidade). Como um exemplo, $2x^5-4x^2-3$ satisfaz o critério para $p=2$, depois de inverter os seus coeficientes e (sendo primitivo) é , portanto, irredutível em $\mathbb{Z}[x]$.

Exemplo 4.2.6 *Aplicação nos polinômios ciclotômicos*

Podemos usar o critério de Eisenstein também para verificar a irredutibilidade de polinômios ciclotômicos para números primos p. Um polinômio ciclotômico é obtido dividindo o polinômio x^p-1 pelo fator $x-1$, correspondente à sua raiz igual a 1 (mas se $p>2$, a unidade é sua única raiz racional).

$$\frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\cdots+x+1.$$

Como os coeficientes são iguais a 1, não podemos aplicar o critério de Eisenstein diretamente, mas fazendo a substituição de x por $x+1$, o critério será aplicado para o número primo p.

$$\frac{(x+1)^p-1}{x} = x^{p-1}+\binom{p}{p-1}x^{p-2}+\cdots+\binom{p}{2}x+\binom{p}{1}.$$

Assim, os coeficientes não-líderes são divisíveis por p, utilizando da propriedade dos coeficientes binomiais, e o coeficiente constante sendo igual a p, não sendo, portanto, divisível por p^2. Podemos também utilizar da identidade $(a+b)^p = a^p+b^p$ (baseada nas mesmas propriedades dos coeficientes

binomiais, dando origem ao endomorfismo de Frobenius), para calcular a redução módulo p do quociente de polinômios.

$$\frac{(x+1)^p - 1}{x} = \frac{x^p + 1^p - 1}{x} = \frac{x^p}{x} = x^{p-1} \, (mod\, p).$$

Desta forma, os coeficientes não-líderes do quociente são todos divisíveis por p, restando a verificação do termo constante igual a p do quociente, fazendo a substituição de x por 1 *(em vez de* $x + 1$*) na forma expandida* $x^{p-1} + \cdots + x + 1$.

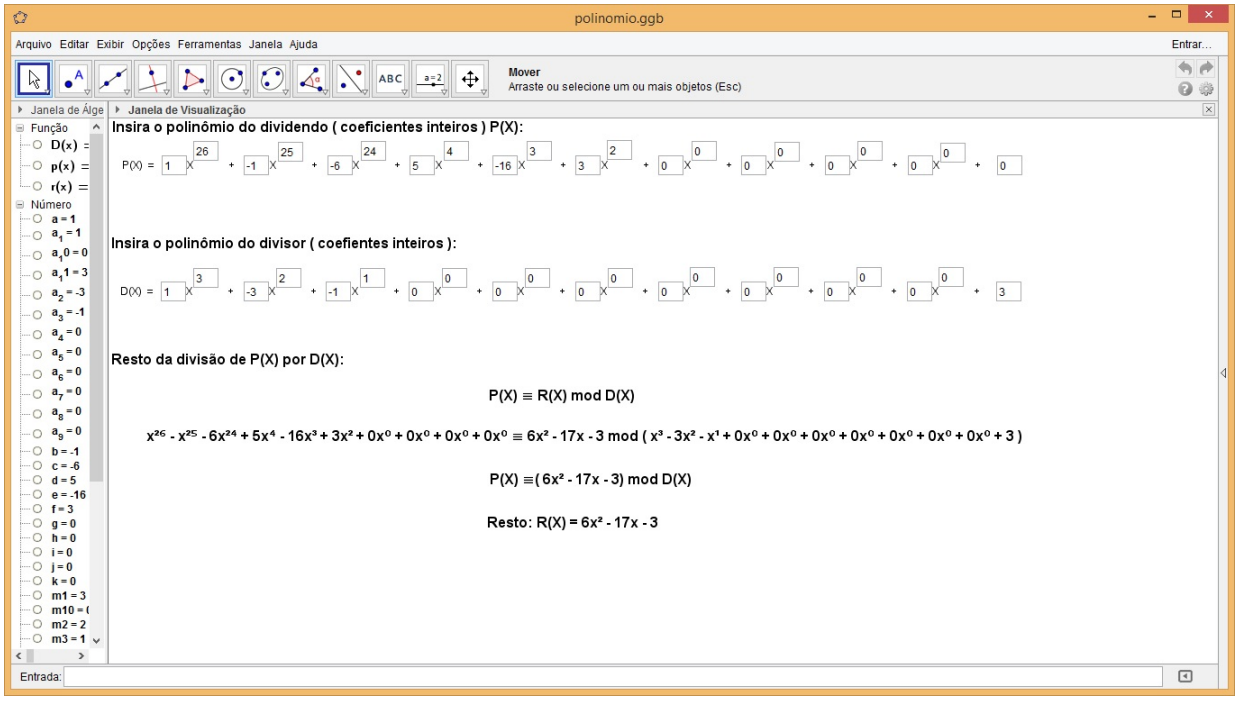
Capítulo 5

Implementação Computacional

A seguir, utilizaremos o GeoGebra como uma interface para a interação entre o usuário e o tema Congruência Polinomial proposto neste trabalho. O GeoGebra é um software gratuito de matemática dinâmica desenvolvido para o ensino e aprendizagem nos vários níveis de ensino, que aborda Geometria, Álgebra e Cálculo. A principal função da implementação é retornar o resto $R(X)$ da divisão entre dois polinômios quaisquer $P(X)$ e $D(X)$, tal que $P(X) \equiv R(X) \, mod \, D(X)$.

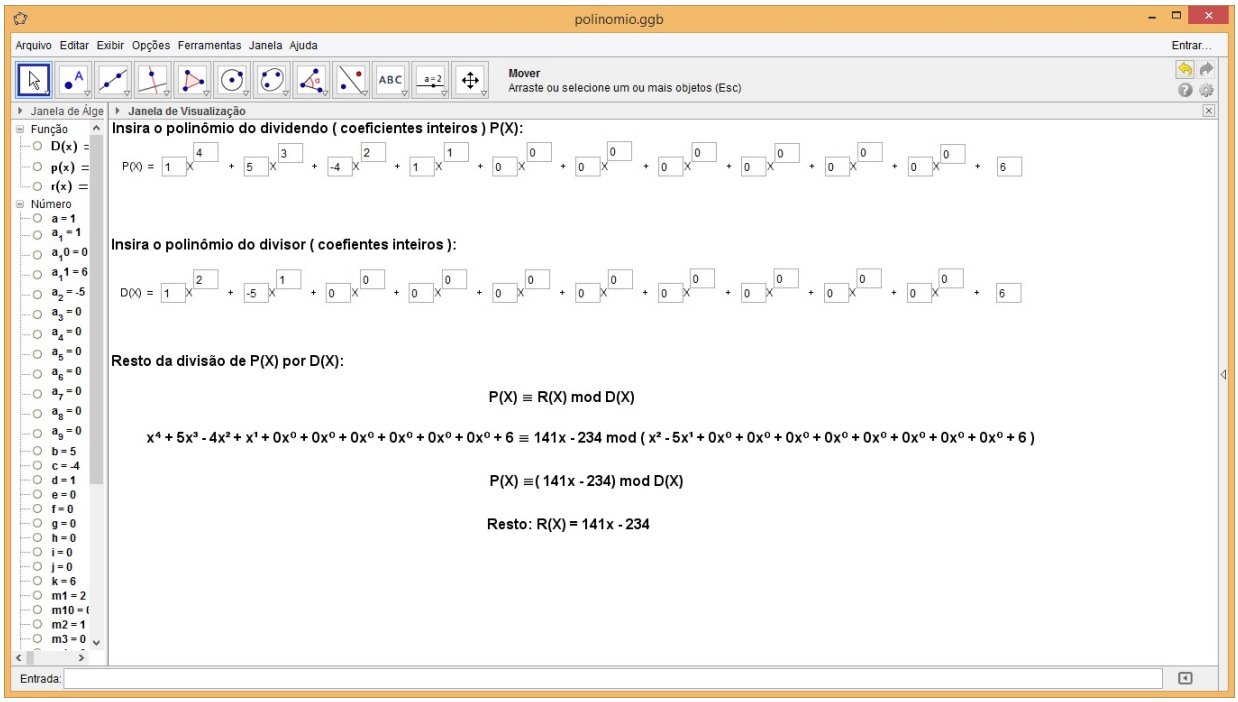
Devemos, primeiramente, inserir os valores dos coeficientes e das potências de x do dividendo $P(X)$ (limitado a 11 coeficientes). Em seguida, inserimos os valores dos coeficientes e das potências de x do divisor $D(X)$ (limitado a 11 coeficientes). Nesse momento, é importante lembrar que os coeficientes dos dois polinômios devem ser inteiros e $\partial D(X) < \partial P(X)$. Após a inserção, teremos a visualização do resto $R(X)$ da divisão entre os dois polinômios, obtendo assim uma interatividade entre o aluno e o conteúdo proposto através do programa.

Figura 5.1: Congruência Polinomial ($\partial P(X) = 26$ e $\partial D(X) = 3$)



Geogebra - Leonardo (2019)

Figura 5.2: Congruência Polinomial ($\partial P(X) = 4$ e $\partial D(X) = 2$)



Geogebra - Leonardo (2019)

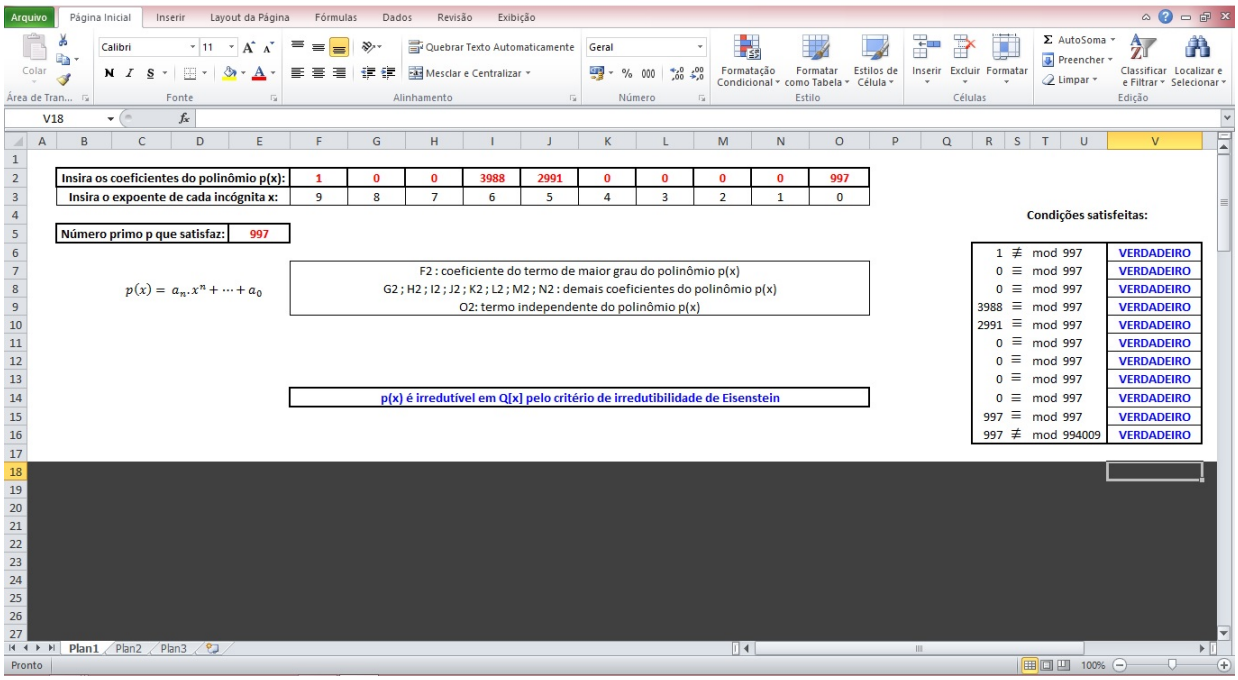
A seguir, utilizaremos uma planilha eletrônica também como uma interface para a interação entre o usuário e o tema Critério de Irredutibilidade de Eisenstein proposto neste trabalho. A planilha utilizada pode ser o software Microsoft Office Excel ou o

BrOffice Calc, que é um sofwtare livre. A principal função da implementação é verificar se um polinômio é irredutível pelo Critério de Irredutibilidade de Eisentein. Primeiramente, na planilha 1, inserimos na primeira linha da tabela, os coeficientes do polinômio $p(x)$ em cada célula, com limitação de 10 coeficientes e, na planilha 2, teremos o polinômio completo sendo apresentado. Em seguida, na segunda linha da tabela, inserimos cada potência de x dos respectivos coeficientes do polinômio $p(x)$. Desse modo, ocorre a busca pelo número primo p que satisfaz todas as condições do Critério de Eisenstein e, caso ele exista, será apresentado no campo "Número primo p que satisfaz". Caso não exista, será apresentado o número zero e a frase "Não existe número primo que satisfaz os critérios de irredutiblidade de Eisenstein".

Na tabela a direita, temos a verificação de todas as condições necessárias para satisfazer o Critério de Eisentein com o número primo p encontrado.

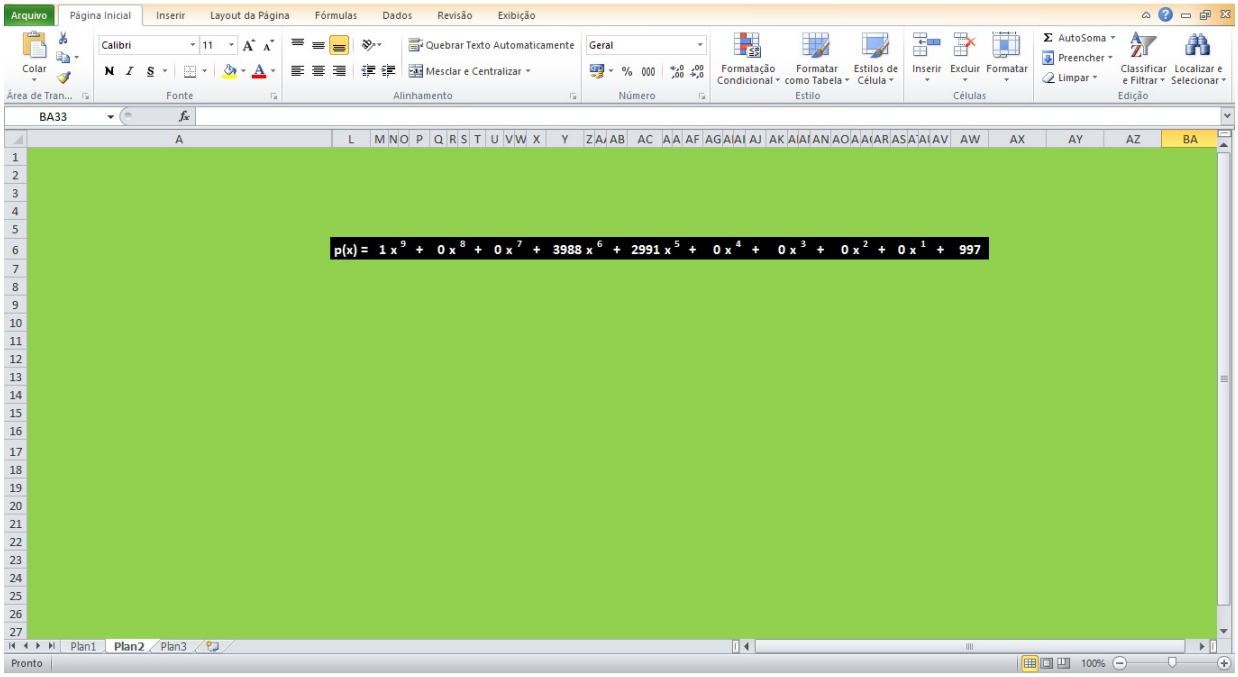
Finalmente, será apresentado como resultado a frase "$p(x)$ é irredutível em $\mathbb{Q}[x]$ pelo critério de irredutibilidade de Eisenstein", caso seja encontrado o número primo p que satisfaça todas as condições ou o resultado será a frase "Inconclusivo", caso não seja encontrado o número primo p que obedeça as condições. Importante ainda ressaltar que a implementação funciona para buscar números primos existentes no intervalo até 1000.

Figura 5.3: Critério de Irredutibilidade de Eisenstein (condições satisfeitas)



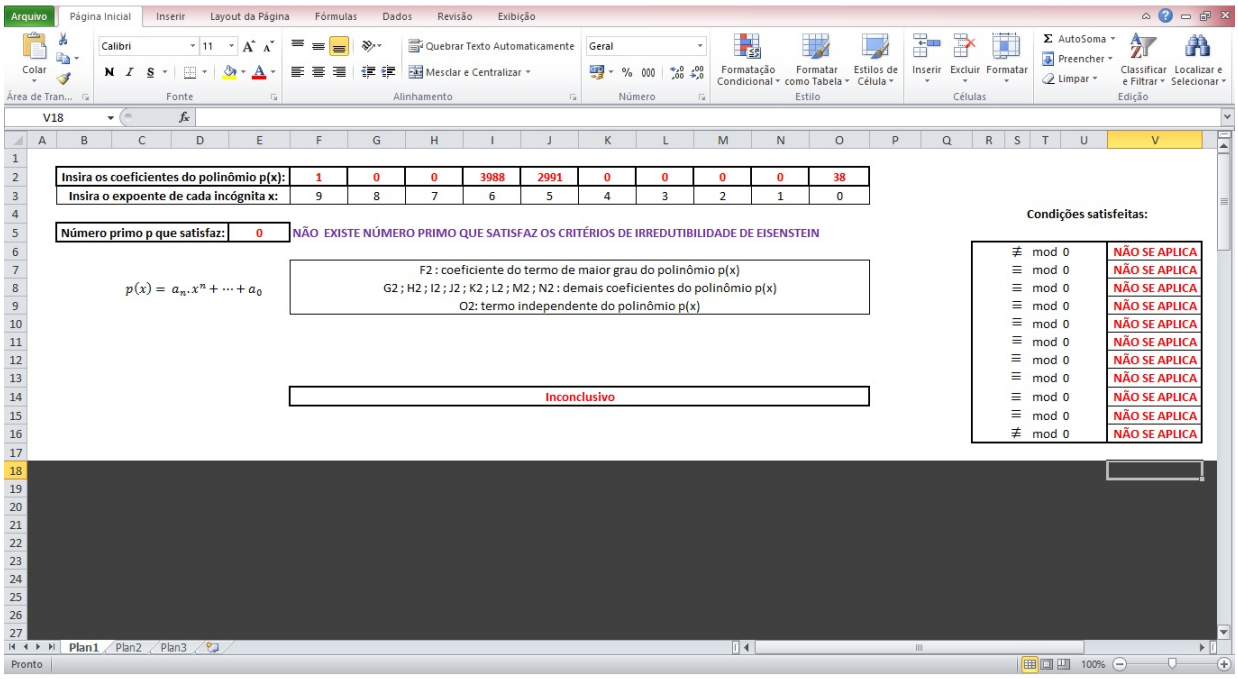
Planilha Eletrônica - Leonardo (2019)

Figura 5.4: Polinômio ($\partial p(x) = 9$)



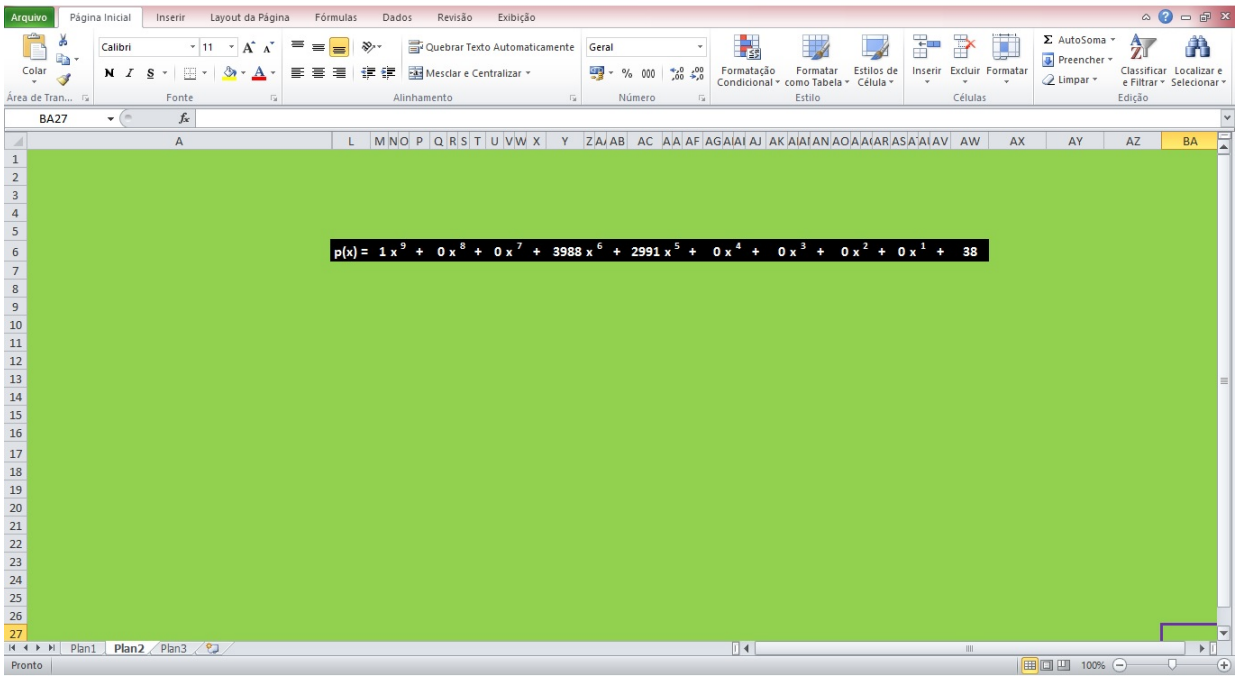
Planilha Eletrônica - Leonardo (2019)

Figura 5.5: Critério de Irredutibilidade de Eisenstein (condições não satisfeitas)



Planilha Eletrônica - Leonardo (2019)

Figura 5.6: Polinômio ($\partial p(x) = 9$)



Planilha Eletrônica - Leonardo (2019)

Capítulo 6

Considerações Finais

No contexto escolar, a proposta didática é da expansão do estudo de congruências na educação básica, em específico nas séries finais do ensino médio, já que o assunto é visto apenas em cursos de nível superior e na preparação para as olimpíadas de matemática.

A proposta é de utilização da congruência como mecanismo que facilita a resolução de problemas relacionados aos polinômios, ou seja, congruência módulo $d(x)$, onde $d(x)$ é um polinômio na variável x. Por observação, é fácil verificar que há diversos trabalhos sobre aplicações de congruências, citando por exemplo: Critérios de divisibilidade, Código de barras, Sistemas de identificação (cpf, cartão de crédito), Criptografia, Calendário e Equações Diofantinas. Todas estas citações são referentes a utilização da congruência módulo m, onde m é um número natural diferente de zero. O intuito é mostrar a abrangência da congruência nesta parte da álgebra que é vista pelos alunos como um conteúdo bastante abstrato, sendo interessante uma abordagem nos livros didáticos para ser ensinado nas séries finais. Importante ressaltar que o aluno perceba a relação existente entre os conteúdos matemáticos estudados e não como temas isolados sem comunicação.

A demonstração das aplicações da matemática é fundamental para motivar nos alunos a habilidade de interpretação, de investigação e de capacidade crítica valorizando a disciplina como um todo. Fica a sugestão para todos os professores do ensino médio, a criação de oficinas e minicursos com a finalidade de estabelecer metodologias para o estudo de congruências aplicado à álgebra.

Bibliografia

[1] Gonçalves A., *Polinômios em uma variável*. Introdução à Àlgebra - Projeto Euclides, Vol. 1, pp. 63–82, 1979.

[2] Alencar Filho, E., *Teorema de Fermat*. Teoria das Congruências, Vol. 1, pp. 62–71, 1986.

[3] Vieira, A.C., *Corpos*. Fundamentos de Álgebra II, Vol. 1, pp. 12–80, 2011.

[4] Moreira, F.R.S., *Artigo*. Congruências Lineares, pp. 01–08, 2006.

[5] Araujo, K.V., *Critérios de irredutibilidade*. Estruturas Algébricas II, Vol. 1, pp. 71–78, 2009.

[6] Garcia, A. e Lequain, Y., *Polinômios*. Elementos de Álgebra - Projeto Euclides, Vol. 1, pp. 71–84, 2001.

[7] Domingues, H.H. e Iezzi, G., *Introdução à aritmética dos números inteiros*. Álgebra Moderna, Vol. 1 , 4ª ed. , pp. 49–53, 2003.

[8] Hefez, A., *A Aritmética dos restos*. Iniciação à Aritmética - Programa de Iniciação Científica obmep, Vol. 1, pp. 81–96, 2009.

[9] Hefez, A., *Equações Diofantinas*. Curso de Álgebra, Vol. 1, 3ª ed. , pp. 101–105, 2002.

[10] Hefez, A., *Polinômios*. Curso de Álgebra, Vol. 2, 1ª ed. , pp. 15–32, 2002.

[11] Marques, C.M., *Anéis*. Introdução à Teoria de Anéis, pp. 10–16, 1999.