UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

CLÓVIS JOÃO PISSARÉK

CONGRUÊNCIAS E POLINÔMIOS: UMA APLICAÇÃO

DISSERTAÇÃO

CURITIBA

2015

CLÓVIS JOÃO PISSARÉK

CONGRUÊNCIAS E POLINÔMIOS: UMA APLICAÇÃO

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do grau de “Mestre em Matemática”.

Orientador: Patrícia Massae Kitani, Dra.

CURITIBA

2015

Dados Internacionais de Catalogação na Publicação

P678c 2014 Pissarék, Clóvis João
Congruências e polinômios : uma aplicação / Clóvis João Pissarék.-- 2014.
60 f.: il.; 30 cm

Texto em português, com resumo em inglês.
Dissertação (Mestrado) - Universidade Tecnológica Federal do Paraná. Programa de Mestrado Profissional em Matemática em Rede Nacional, Curitiba, 2014.
Bibliografia: f. 60.

1. Congruências (Geometria). 2. Polinômios. 3. Anéis de polinômios. 4. Polinômios irredutíveis. 5. Matemática - Estudo e ensino. 6. Professores de matemática - Formação. 7. Matemática - Dissertações. I. Kitani, Patrícia Massae, orient. II .Universidade Tecnológica Federaldo Paraná - Programa de Mestrado Profissional em Matemática em Rede Nacional. III. Título.

CDD 22 -- 510

Biblioteca Central da UTFPR, Câmpus Curitiba

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
Câmpus Curitiba

Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Título da Dissertação No. 22

"Congruências e polinômios: uma aplicação"

por

Clóvis João Pissarék

Esta dissertação foi apresentada como requisito parcial à obtenção do grau de Mestre em Matemática, pelo Programa de Mestrado em Matemática em Rede Nacional - PROFMAT - da Universidade Tecnológica Federal do Paraná - UTFPR - Câmpus Curitiba, às 10h do dia 05 de dezembro de 2014. O trabalho foi aprovado pela Banca Examinadora, composta pelos doutores:

_____
Profa. Patrícia Massae Kitani, Dra.
(Presidente - UTFPR/Curitiba)

_____
Profa. Fernanda Diniz de Melo, Dra.
(UEM)

_____
Profa. Mari Sano, Dra.
(UTFPR/Curitiba)

Visto da coordenação:

_____
Prof. Ronie Peterson Dario, Dr.
(Coordenador do PROFMAT/UTFPR)

"A Folha de Aprovação assinada encontra-se na Coordenação do PROFMAT/UTFPR"

AGRADECIMENTOS

- À minha mãe Maria Rosi Leonardi por ser luz no meu caminho trilhado com tantas dificuldades para a obtenção do grau de mestre.
- À minha filha Jhuly da Silva Pissarék por ser elemento fundamental no propósito à atingir.
- Aos meus amigos de mestrado, em especial Éder Miotto por me ajudar com total dedicação e ajuda colossal.
- À CAPES pela recomendação do PROFMAT por meio do parecer do Conselho Técnico Científico da Educação Superior e pelo incentivo financeiro.
- À Sociedade Brasileira de Matemática que na busca da melhoria do ensino de Matemática na Educação Básica viabilizou a implementação do PROFMAT.
- À minha orientadora Patrícia Massae Kitani pelos benefícios trazidos e incorporados à minha vida através da execução deste trabalho.

RESUMO

PISSARÉK, Clóvis João. CONGRUÊNCIAS E POLINÔMIOS: UMA APLICAÇÃO. 60 f. Dissertação – Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Este trabalho tem como objetivo aprofundar o conhecimento dos professores do ensino médio e fundamental a respeito de congruência e polinômios. Apesar de congruência não ser abordado nas escolas, este assunto justifica alguns conceitos repassados aos alunos, como por exemplo a divisibilidade de um número por outro. A congruência ainda pode auxiliar na verificação de raízes de polinômios. Aqui, os polinômios são tratados como elementos de um anel, o anel dos polinômios, e vários resultados utilizados em sala de aula são justificados a partir da estrutura desse anel. Com esses dois conceitos, ainda é feito um breve estudo de congruência polinomial.

Palavras-chave: Congruência, Função Polinomial, Congruência Polinomial.

ABSTRACT

PISSARÉK, Clóvis João. CONGRUENCES AND POLYNOMIALS: AN APPLICATION. 60 f. Dissertação – Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

The aim of this work is to deepen the knowledge of elementary and high school teachers about congruence and polynomials. Although congruence is not studied in schools, this subject justifies some concepts passed to the students, such as the divisibility of one number by another. The congruence can also help to verify roots of polynomials. Here, polynomials are treated as elements of a ring, the ring of polynomials, and several results used in the classroom are justified from the structure of this ring. These concepts are used for a brief study of polynomial congruence.

Keywords: Congruency, polynomial function, polynomial congruence.

SUMÁRIO

1 INTRODUÇÃO

Este trabalho teve início quando surgiu uma dúvida em resolver o seguinte problema de congruência polinomial, do segundo exame de qualificação de 2013 do PROFMAT:

" *Determinar todos os inteiros X que são soluções da congruência*

$$X^{49} + X^{14} + X^{12} - 2X \equiv 0 \ (mod\ 7)"$$

Como congruência polinomial não é um assunto visto em turmas do ensino fundamental e médio, então resolvemos estudar os conceitos de congruência e polinômios de modo mais aprofundado e, por fim, unir esses dois assuntos num estudo um pouco mais avançado para a resolução de problemas de congruência polinomial.

O assunto congruência também não é estudado nas escolas, mas vários trabalhos envolvendo esse assunto e a possibilidade de abordagem em sala de aula foram discutidas em alguns trabalhos do próprio PROFMAT. Carl Friedrich Gauss foi o pai da congruência, apresentando a congruência a partir de um trabalho realizado em 1801, Disquisitiones Arithmeticae, quando tinha exatos 24 anos de idade. Várias ideias usadas na teoria dos números foram colocadas nesse trabalho, até mesmo a simbologia usada na congruência atual foi a mesma que Gauss usou no princípio. Dentre as vastas aplicações de congruência, podemos citar seu uso no sistema de código de barra, no dígito verificador do Cadastro de Pessoas Físicas na Receita Federal (CPF), saber qual dia da semana será daqui a n dias, critérios de divisibilidade de um número por outro, etc. Em provas da OBMEP também surgem com certa frequência problemas que podem ser resolvidas utilizando congruências.

O outro assunto estudado neste trabalho é polinômio. Polinômios aparecem em várias áreas da matemática e outras ciências. Por exemplo, eles são utilizados para formar equações polinomiais, que codificam grande variedade de problemas, desde problemas de palavras elementares a problemas complicados nas ciências, eles são usados para definir as funções polinomiais, que aparecem nas definições que variam de química básica e física, para a economia e ciências sociais, são utilizados no cálculo e análise numérica para aproximar outras funções, en-

tre outras. Nas escolas, polinômio é um tópico enfrentado com certa resistência entre os alunos. Para que isto não ocorra, é necessário um bom preparo dos professores. Neste sentido, fizemos um aprofundamento teórico do assunto. Aqui, polinômio foi trabalhado como elemento de um anel, o anel dos polinômios. A estrutura desse anel justifica vários resultados utilizados em sala de aula, como o algoritmo da divisão euclidiana, a fatoração (redutibilidade / irredutibilidade), número de raízes num polinômios, etc.

Este trabalho foi dividido em 3 capítulos. O primeiro capítulo trata de conceitos básicos de congruências e resultados clássicos como o Teorema de Euler e o Pequeno Teorema de Fermat. No segundo capítulo, tratamos de polinômios como elementos do anel de polinômios. É feito um estudo dos principais resultados sobre esse anel, dando uma especial atenção aos critérios de irredutibilidade. Encontrar raízes de polinômios é um problema antigo, mas não existem métodos gerais para encontrá-los. Para polinômios de grau menor ou igual a 4 são conhecidos os métodos para encontrar as raízes. Por volta de 1824, Niels Henrik Abel demostrou que não há uma fórmula geral por radicais para resolver equações de grau no mínimo 5. Entretanto, sabia-se que alguns casos particulares dessas equações podiam ser resolvidas por radicais. Para polinômios de grau maior ou igual a 5, Evariste Galois delineou pela primeira vez o conceito de grupo, associando a cada equação um grupo de permutações e mostrando que a resolução através de radicais dependia de uma propriedade que esses grupos poderiam ou não dispor. Não fizemos este estudo, mas focamos uma parte deste capítulo visando a redutibilidade de um polinômio, pois uma vez que o polinômio está fatorado, reduzimos a busca das raízes sobre os polinômios de grau menor, dos que compõem a fatoração. Para finalizar, no último capítulo é feito um estudo visando a resolução de congruência polinomial, onde os principais teoremas que auxiliam no nosso estudo são o Teorema Chinês dos Restos e o Lema de Hensel.

Vamos enunciar os principais resultados e exemplificá-los. Esses assuntos não são vistos diretamente no ensino fundamental e médio mas aparece implicitamente em Olimpíadas de Matemática. O aluno não irá desenvolver na forma como iremos abordar, mas como este material visa apoiar professores, resolveremos alguns problemas de modo mais formal, com o símbolo $\equiv$ de congruência e suas propriedades.

2 CONGRUÊNCIAS

Neste capítulo inicial iremos trabalhar com o conceito de congruência. Carl Friedrich Gauss foi o grande introdutor da congruência, mostrando ao mundo a congruência a partir de um trabalho realizado em 1801, Disquisitiones Arithmeticae, quando tinha apenas 24 anos de idade. Várias ideias usadas na teoria dos números foram colocadas nesse trabalho, até mesmo o símbolo usado na congruência atual foi o que Gauss usou naquela época.

Definição 2.1. [Congruências] Seja m um número natural diferente de zero. Diremos que dois números naturais a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se $a \equiv b \ mod \ m$.

Exemplo 2.2. Aritmética dos Restos

1) $15 \equiv 8$ *mod* 7 pois o resto das divisões de 15 e de 8 por 7 são os mesmos.

2) $16 \equiv 31$ *mod* 5, pois o resto das divisões de 16 e de 31 por 5 são os mesmos.

3) $14 \not\equiv 7$ *mod* 4, pois o resto da divisão de 14 por 4 é 2, enquanto o resto da divisão de 7 por 4 é 3.

Os seguintes resultados seguem direto do algoritmo da divisão.

Proposição 2.3. *Todo número inteiro a é congruente módulo m a um e somente um dos números* $0, 1, 2, 3, \ldots, m-1$.

Proposição 2.4. *Sejam a um número inteiro qualquer e m um inteiro maior do que 1. Suponha que r seja um número inteiro tal que* $0 \leq r < m$ *e* $a \equiv r \ mod \ m$. *Então o resto da divisão de a por m é r.*

Teorema 2.5. *Seja $m \in \mathbb{N}$, com $m > 1$. Para todos $a, b, c \in \mathbb{N}$, tem-se que*

(i) $a \equiv a \ mod \ m$,

(ii) se $a \equiv b \ mod \ m$, então $b \equiv a \ mod \ m$,

(iii) se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, então $a \equiv c \ mod \ m$.

Teorema 2.6. *Suponha que $a, b \in \mathbb{N}$ são tais que $b \geq a$. Tem-se que $a \equiv b \ mod \ m$ se, e somente se, $m \mid b - a$.*

Demonstração:

Sejam $a = mq + r$, com $r < m$ e $b = mq' + r'$, com $r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = m(q' - q) + (r' - r), \text{ se } r' \geqslant r$$

$$b - a = m(q' - q) - (r - r'), \text{ se } r \geqslant r'$$

onde $r' - r < m$, ou $r - r' < m$. Portanto, $a \equiv b \ mod \ m$ se, e somente se, $r = r'$, o que é equivalente a dizer que $m \mid b - a$.

■

Teorema 2.7. *Sejam $a, b, c, d, m \in \mathbb{N}$, com $m > 1$.*

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

ii) Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $ac \equiv bd \ mod \ m$.

Demonstração:

Suponhamos que $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$. Podemos, sem perda de generalidade, supor que $b \geqslant a$ e $d \geqslant c$. Logo, temos que $m \mid b - a$ e $m \mid d - c$.

(i) Basta observar que $m \mid (b - a) + (d - c)$ e, portanto, $m \mid (b + d) - (a + c)$, o que prova essa parte do resultado.

(ii) Basta notar que $bd - ac = d(b - a) + a(d - c)$ e concluir que $m \mid bd - ac$

■

O exemplo a seguir é uma aplicação do Teorema anterior

Exemplo 2.8. Questão sobre congruências

(Olimpíadas de matemática - Obmep - 1ª fase 2011 - Nível 2 questão 2)

Qual é o resto da divisão de $1 \times 2 \times 3 \times 4 \times \cdots \times 2011 + 21$ por 8?

Como $1 \times 2 \times 3 \times 4 \times \cdots \times 2011$ é múltiplo de 8 então:

$1 \times 2 \times 3 \times 4 \times \cdots \times 2011 \equiv 0 \; mod \; 8$ temos

$21 \equiv 5 \; mod \; 8$ logo o resto da divisão de

$1 \times 2 \times 3 \times 4 \times \cdots \times 2011 + 21$ por 8 é 5.

Exemplo 2.9. Questão sobre congruências

(Olimpíadas de matemática - Obmep - 1ª fase 2013 - Nível 3 questão 2)

Quantos sinais de adição foram utilizados na expressão

$2+0+1+3+2+0+3+1+\cdots+2+0+1 = 2013$?

Pegue os blocos que estão se repetindo $\Rightarrow 2+0+1+3 = 6$ e tem quatro sinais

(tem o + antes do 2)

Agora, como o resultado é 2013, divide por um bloco para saber quantos blocos são:

$2013 \div 6 = 335,5$, ou seja, $2013 \equiv 3 \; mod \; 6$

Como cada bloco tem quatro sinais, multiplica-se 335,5 por 4 $\Rightarrow$ 335,5 $\times$ 4 = 1342

Assim temos 335 blocos com 4 sinais e como o primeiro bloco tem 3 sinais consideramos um sinal a mais, compensaremos tirando um sinal do bloco final +2+0+1, assim fica bem explicado o porquê de multiplicar 335,5 blocos por 4 tendo o resultado do número de sinais da expressão ficado num total de 1342 blocos.

Corolário 2.10. *Para todos $n \in \mathbb{N}^*$, $a, b \in \mathbb{N}$, com $m > 1$, se $a \equiv b \; mod \; m$, então, $a^n \equiv b^n \; mod \; m$.*

Corolário 2.11. *Sejam $a, b, m \in \mathbb{N}^*$, com $m > 1$. Se $a + b \equiv 0 \; mod \; m$, então, para todo $n \in \mathbb{N}$, tem-se que*

$$a^{2n} \equiv b^{2n} \; mod \; m \; e \; a^{2n+1} + b^{2n+1} \equiv 0 \; mod \; m.$$

Demonstração:

O resultado é claramente válido para $n = 0$. Podemos ainda supor, sem perda de generalidade, que $a \geqslant b$. Como $a+b \equiv 0 \; mod \; m$, segue-se que $m \mid a+b$ e, portanto, $m \mid (a+b)(a-b)$.

Como $(a+b)(a-b) = a^2 - b^2$, segue-se que $a^2 \equiv b^2 \; mod \; m$. Aplicando o corolário 2.10, temos que $a^{2n} \equiv b^{2n} \; mod \; m$ para todo $n \in \mathbb{N}^*$. Por outro lado, como

$$a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - ba^{2n-1} + \cdots - b^{2n-1}a + b^{2n}),$$

e $m \mid a+b$, segue-se que $m \mid a^{2n+1} + b^{2n+1}$ e, portanto, $a^{2n+1} + b^{2n+1} \equiv 0 \; mod \; m$.

■

Observação: o corolário acima será de grande utilidade no que se segue e substitui as seguintes relações:

$$a \equiv -b \; mod \; m \Longrightarrow a^{2n} \equiv b^{2n} \; mod \; m \quad e \quad a^{2n+1} \equiv -b^{2n+1} \; mod \; m,$$

já que não trabalhamos com números negativos.

Com os resultados anteriores podemos explicar alguns critérios de divisibilidade.

DIVISIBILIDADE por 3.

Escrevamos um número a na sua representação decimal: $a = a_r \cdots a_1 a_0$.

Restos da divisão por 3: Como $10^n \equiv 1 \; mod \; 3$, temos que

$a = a_r \cdot 10^r + \cdots + a_1 \cdot 10 + a_0 \cdot 1 \equiv a_r + \cdots + a_1 + a_0 \; mod \; 3$,

Logo o resto da divisão de a por 3 é igual ao resto da divisão de

$b = a_r + \cdots + a_1 + a_0$ por 3.

DIVISIBILIDADE por 9.

Escrevamos um número a na sua representação decimal: $a = a_r \cdots a_1 a_0$.

Restos da divisão por 9: Como $10^n \equiv 1 \; mod \; 9$, temos que

$a = a_r \cdot 10^r + \cdots + a_1 \cdot 10 + a_0 \cdot 1 \equiv a_r + \cdots + a_1 + a_0 \; mod \; 9$,

Logo o resto da divisão de a por 9 é igual ao resto da divisão de

$b = a_r + \cdots + a_1 + a_0$ por 9.

DIVISIBILIDADE por 11.

Escrevamos um número a na sua representação decimal: $a = a_r \cdots a_1 a_0$.

Restos da divisão por 11: Como $10^n \equiv 1 \; mod \; 11$ se n é par e

$10^n \equiv 10 \, mod \, 11$ se n é ímpar temos que

$a \equiv a_0 + 10a_1 + a_2 + 10a_3 + \cdots \, mod \, 11$, logo o resto da divisão

de a por 11 é igual ao resto da divisão de $b = a_0 + 10a_1 + a_2 + 10a_3 + \cdots$, por 11,

ao qual podemos aplicar novamente a regra acima etc.

Teorema 2.12. *Sejam $a, b, c, m \in \mathbb{N}$, com $m > 1$. Tem-se que*

$$a + c \equiv b + c \, mod \, m \quad \Longleftrightarrow \quad a \equiv b \, mod \, m.$$

Demonstração:

Se $a \equiv b \, mod \, m$, segue-se imediatamente do Teorema 2.7 que $a + c \equiv b + c \, mod \, m$, pois $c \equiv c \, mod \, m$. Reciprocamente, suponhamos que $a + c \equiv b + c \, mod \, m$. Sem perda de generalidade, podemos supor $b + c \geqslant a + c$. Logo, $m \mid b + c - (a + c)$, o que implica que $m \mid b - a$ e, consequentemente, $a \equiv b \, mod \, m$.

■

O Teorema a seguir mostra que o cancelamento no caso do produto não é válido em geral.

Exemplo 2.13. *Seja a congruência* $14 \equiv 6 \, mod \, 8$. *Vamos mostrar que não é válida a lei do cancelamento no caso do produto.*

Como $14 \equiv 6 \ mod \ 8$ e $7 \cdot 2 \equiv 3 \cdot 2 \ mod \ 8$ são a mesma congruência, se cancelarmos o termo 2 que é o termo semelhante da segunda congruência teremos: $7 \equiv 3 \, mod \, 8$. O que é um absurdo.

Logo, a lei do cancelamento para o produto não é válida em geral.

Teorema 2.14. *Sejam $a, b, c, m \in \mathbb{N}$, com $c \neq 0$ e $m > 1$. Temos que*

$$ac \equiv bc \, mod \, m \Longleftrightarrow a \equiv b \, mod \, \frac{m}{mdc(c,m)}.$$

Demonstração:

Podemos supor, sem perda de generalidade, que $bc \geqslant ac$. Como $\frac{m}{mdc(c,m)}$ e $\frac{c}{mdc(c,m)}$ são coprimos, temos que

$$ac \equiv bc \ mod \ m \iff m \mid (b-a)c \iff \frac{m}{mdc(c,m)} \mid (b-a)\frac{c}{mdc(c,m)}$$

$$\iff \frac{m}{mdc(c,m)} \mid b-a \iff a \equiv b \ mod \ \frac{m}{mdc(c,m)}.$$

■

Corolário 2.15. *Sejam $a,b,c,m \in \mathbb{N}$, com $m > 1$ e $mdc(c,m) = 1$. Temos que*

$$ac \equiv bc \ mod \ m \iff a \equiv b \ mod \ m.$$

Lema 2.16 (Euclides)**.** *Sejam $a,b,n \in \mathbb{N}$ com $a < na < b$. Então $mdc(a,b) = mdc(a,b-na)$.*

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 $d = mdc(a,b)$.

■

Observação: Com a mesma técnica usada na prova do Lema de Euclides, poder-se-ia provar que, para todos $a,b,n \in \mathbb{N}$, com $na > b$, tem-se $mdc(a,b) = mdc(a,na+b)$.

Exemplo 2.17. Determinar os valores de a e n para os quais $a+1$ divide $a^{2n+1}-1$.

Note que

$mdc(a+1,a^{2n+1}-1) = mdc(a+1,a(a^{2n}-1)+a-1) = mdc(a+1,a-1)$.

Portanto, $a+1 \mid a^{2n+1}-1$, para algum $n \in \mathbb{N}$, se e somente se,

$a+1 = mdc(a+1,a^{2n+1}-1) = mdc(a+1,a-1)$, o que ocorre se, e somente se, $a = 1$.

Teorema 2.18. *Sejam $a,b \in \mathbb{N}, m,n,m_1,\ldots,m_r \in \mathbb{N} \setminus \{0,1\}$. Temos que*

i) se $a \equiv b \ mod \ m$ e $n \mid m$, então $a \equiv b \ mod \ n$;

ii) $a \equiv b \ mod \ m_i, i = 1,\ldots,r \iff a \equiv b \ mod \ [m_1,\ldots,m_r]$, onde $[m_1,\ldots,m_r]$ denota o mínimo múltiplo comum de $m_1,m_2,\ldots,m_r$

iii) se $a \equiv b \ mod \ m$, então $mdc(a,m) = mdc(b,m)$.

Demonstração:

Suponhamos, sem perda de generalidade, que $b \geqslant a$.

(i) Se $a \equiv b \; mod \; m$, então $m \mid \; b-a$. Como $n \mid m$, segue-se que $n \mid b-a$. Logo,

$a \equiv b \; mod \; n$.

(ii) Se $a \equiv b \; mod \; m_i, i = 1, \ldots, r$, então $m_i \mid b-a$, para todo i. Sendo $b-a$ um múltiplo de cada m_i, segue-se que $[m_1, \ldots, m_r] \mid b-a$, o que prova que $a \equiv b \; mod [m_1, \ldots, m_r]$. A recíproca decorre do ítem (i).

(iii) Se $a \equiv b \; mod \; m$, então $m \mid b-a$ e, portanto, $b = a+tm$ com $t \in \mathbb{N}$. Logo, pelo Lema de Euclides, temos que

$$mdc(a,m) = mdc(a+tm,m) = mdc(b,m).$$

■

Definição 2.19. [Função ϕ de Euler] Para cada inteiro $n \geq 1$, indicaremos por $\phi(n)$ o número de inteiros positivos, menores ou iguais a n, que são relativamente primos com n. A função assim definida chama-se função $\phi \; de \; Euler$.

Por exemplo, se $n = 4$, os inteiros positivos menores ou iguais a 4, relativamente primos com 4, são 1 e 3, assim $\phi(4) = 2$. Analogamente, temos $\phi(5) = 4$, $\phi(6) = 2$ e, se p é primo, $\phi(p) = p-1$.

Vamos finalizar o capítulo com dois Teoremas Clássicos envolvendo congruência

Teorema 2.20 (Euler)**.** *Sejam* $n, a \in \mathbb{N}$ *com* $n > 1$ *e* $mdc(a,n) = 1$. *Então,*

$$a^{\varphi(n)} \equiv 1 \; mod \; n.$$

Demonstração:

Dado n, vamos considerar o conjunto de números compreendidos entre 1 e $(n-1)$ que são relativamente primos com n, que denotaremos

$A = \{x_1, x_2, \ldots, x_t\}$, isto é, cada x_i é tal que $1 \leq x_i \leq n-1$ e $mdc(x_i, n) = 1$.

Agora, dado outro número a tal que $mdc(a,n) = 1$, consideramos o conjunto de números $B = \{x_1 a, \; x_2 a, \ldots, \; x_t a\}$.

Como $x_i a$ é relativamente primo com n, o resto da divisão de $x_i a$ por n deve ser um dos elementos de A.

Ainda, como $x_i a \equiv x_j \ (mod\ n)$ para algum j e como $mdc(a,n) = 1$ então:

$x_i a \equiv x_j \ (mod\ n)$ p/ um único j pois se $x_i a \equiv x_j \ (mod\ n)$ e $x_i a \equiv x_k \ (mod\ n)$ então:

$x_j \equiv x_k \ (mod\ n)$, logo $j = k$ não pode pois $1 \leq x_i \leq n-1$, ou seja, temos que cada um dos elementos de B são congruentes a algum elemento de A.

Temos então que:

$x_1 a \equiv (x_i)_1 \ (mod\ n)$

$x_2 a \equiv (x_i)_2 \ (mod\ n)$

.....

$x_t a \equiv (x_i)_t \ (mod\ n)$,

em que os elementos $(x_i)_1, (x_i)_2, \ldots, (x_i)_t$ são os de A em outra ordem.

Multiplicando essas congruências, temos

$x_1 x_2 \ldots x_t \cdot a^t \equiv x_1 x_2 \ldots x_t \ (mod\ n)$.

Como cada $x_i, 1 \leq i \leq t$, é relativamente primo com n, temos que $mdc(x_1 x_2 \ldots x_t, n) = 1$ e podemos cancelar para obter $a^t \equiv 1 \ (mod\ n)$.

Notemos, finalmente, que o conjunto $A = \{x_1, x_2, \ldots, x_t\}$ das considerações anteriores está formado precisamente pelos inteiros positivos, menores ou iguais a n, relativamente primos com n; logo $t = \phi(n)$.

Desta forma completamos a demonstração do Teorema de Euler.

■

Corolário 2.21 (Pequeno Teorema de Fermat)**.** *Sejam $a, p \in \mathbb{N}$, onde p é um número primo e $mdc(a,p) = 1$. Tem-se que*

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

Demonstração: Basta notar que, sendo p primo, $\varphi(p) = p - 1$.

■

3 POLINÔMIOS

Em matemática, a teoria de anéis é o estudo de estruturas algébricas com duas operações binárias, adição $(+)$ e multiplicação $(\cdot)$, e que possuem propriedades similares às dos inteiros.

A teoria moderna dos anéis teve origem no século XIX, em duas fontes distintas: em Richard Dedekind(1831-1916), que introduziu em 1871 a noção de ideal, no seu trabalho de generalizar o Teorema Fundamental da Aritmética (da factorização única em primos) a contextos mais abstractos, e no trabalho de David Hilbert (1862-1945). O termo anel (Zahlring) foi criado por Hilbert no artigo Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker Vereiningung, Vol. 4, 1897. Edmund Lasker (1868-1941) e F. S. Macaulay (1862-1927) tiveram participação no desenvolvimento da teoria de anéis de polinômios.

A matemática que mais contribuiu para o avanço do ponto de vista abstrato na teoria dos anéis foi Emmy Noether (1882-1935). É costume indicar o seu artigo "Ideal theory in rings" de 1921 como origem da teoria abstrata dos anéis. O seu tratamento axiomático, muito elegante, constituiu uma novidade ao tempo.

Em teoria dos anéis, um ideal é um subconjunto especial de um anel. O conceito generaliza de uma maneira apropriada algumas propriedades de grande importância para os números inteiros como os "números pares"e os números "múltiplos de 3".

Por exemplo, em anéis estuda-se ideais primos ao invés de números primos, define-se ideais coprimos como generalizações dos números coprimos e pode-se provar o teorema chinês dos restos para ideais. Podemos ainda fazer analogias com o algoritmo da divisão e fatoração em primos dos números inteiros com a dos polinômios.

Definição 3.1. [Anel] Um anel comutativo com unidade $(A,+,\cdot)$ é um conjunto A com pelo menos dois elementos, munido de uma operação denotada por + (chamada adição) e de uma operação denotada por $\cdot$ (chamada multiplicação) que satisfazem as condições seguintes:

A.1) A adição é associativa, isto é,

$$\forall x,y,z \in A, \quad (x+y)+z = x+(y+z)$$

A.2) Existe um elemento neutro com respeito à adição, isto é,

$$\exists 0 \in A \qquad \text{tal que, } \forall x \in A, \quad 0+x=x \text{ e } x+0=x,$$

A.3)Todo elemento de A possui um inverso com respeito à adição, isto é,

$$\forall x \in A, \exists z \in A \text{ tal que} \quad x+z=0 \text{ e } z+x=0.$$

A.4) A adição é comutativa, isto é,

$$\forall x, y \in A, \quad x+y=y+x.$$

M.1) A multiplicação é associativa, isto é,

$$\forall x, y, z \in A, \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

M.2) Existe um elemento neutro com respeito à multiplicação,isto é,

$$\exists 1 \in A \text{ tal que, } \forall x \in A, \quad 1 \cdot x = x \text{ e } x.1 = x$$

M.3) A multiplicação é comutativa, isto é,

$$\forall x, y \in A, \quad x \cdot y = y \cdot x.$$

AM) A adição é distributiva relativamente à multiplicação, isto é,

$$\forall x, y, z \in A, \quad x \cdot (y+z) = x \cdot y + x \cdot z.$$

Observação: O elemento neutro com respeito à adição será chamado zero. O inverso de x com respeito à adição será denotado por -x. A definição de anel é um pouco mais geral, sem as propriedades M.2) e M.3), mas como utilizaremos somente anel comutativo com a unidade, preferimos utilizar a definição acima.

Exemplo 3.2. O conjunto $\mathbb{Z}$ dos inteiros com a adição e multiplicação usuais é um anel comutativo com elemento neutro em relação a multiplicação sendo 1. O conjunto dos elementos invertíveis é $\{1,-1\}$.

Definição 3.3 (Subanel)**.** *Seja* $(A,+,\cdot)$ *um anel e B um subconjunto não vazio de A. Suponhamos que B seja fechado para as operações* + *e* $\cdot$ *de A, isto é,*

a) $x,y \in B \Rightarrow x+y \in B$

b) $x,y \in B \Rightarrow x \cdot y \in B$.

Assim podemos também considerar a soma e o produto como operações em B. Se $(B,+,\cdot)$ *for um anel com as operações de A dizemos que B é um subanel de A.*

Definição 3.4. [Ideal] Um subanel I de um anel A é chamado um ideal de A se para todo $a \in A$ e todo $x \in I$ tem-se $xa \in I$ e $ax \in I$. Assim, um subanel de um anel A é um ideal se ele absorve os elementos de A, isto é, $aI \subseteq I$ e $Ia \subseteq I$ para todo a em A. Um ideal I de A é próprio se $I \neq A$.

Exemplo 3.5. $(\mathbb{Z},+,\cdot)$ anel. Todo ideal de $\mathbb{Z}$ é do tipo $m\mathbb{Z} = \{b \in \mathbb{Z} \,/\, b = ma \text{ com } a \in \mathbb{Z}\}$.

Definição 3.6. [Quociente de anel por ideal] Seja I um ideal de um anel A. Para cada $a \in A$, seja $a+I$ a classe de a módulo I, isto é, $a+I = \{b \in A / a-b \in I\}$. As operações naturais

1) $(a+I)+(b+I) = (a+b)+I$

2) $(a+I)\cdot(b+I) = (a\cdot b)+I$

definem uma estrutura de anel no conjunto das classes. Chamamos de anel quociente e denotamos $\overline{A} = A/I$.

Exemplo 3.7. $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p = \{a+p\mathbb{Z} \mid a \in \mathbb{Z}\} = \{\overline{0},\overline{1},\overline{2},\ldots,\overline{p-1}\}$ *onde*
$\overline{a} = \{b \in \mathbb{Z} \mid a-b \in p\mathbb{Z}\} = \{b \in \mathbb{Z} \mid a-b = pc, \text{ para algum } c \in \mathbb{Z}\} = \{b \in \mathbb{Z} \mid b \equiv a \bmod p\}$.

Definindo as operações em $\mathbb{Z}_p$ *por* $\overline{a}+\overline{b} = \overline{a+b}$ *e* $\overline{a}\cdot\overline{b} = \overline{a\cdot b}$ *temos que* $(\mathbb{Z}_p,+,\cdot)$ *é um anel.*

Definição 3.8. [Domínio de Integridade]

Um anel $(D,+,\cdot)$ é chamado domínio ou domínio de integridade se ele satisfaz a seguinte condição:

M.4) O produto de quaisquer dois elementos não nulos de D é um elemento não nulo, isto é,

$$\forall x,y \in D \setminus \{0\}, \quad x \cdot y \neq 0$$

Um anel $(K,+,\cdot)$ é corpo se ele satisfaz a seguinte condição:

M.4') Todo elemento diferente de zero de K possui um inverso com respeito à multiplicação, isto é,

$$\forall x \in K \setminus \{0\}, \quad \exists y \in K \text{ tal que } x \cdot y = 1.$$

Exemplo 3.9. O anel $\mathbb{Z}$ dos inteiros é um domínio de integridade.

Definição 3.10. [Homomorfismos de Anéis]

Sejam $(A,+,\cdot)$ e $(B,\oplus,\odot)$ dois anéis com unidade. Uma aplicação f:$A \to B$ é um homomorfismo se ela é compatível com as estruturas de anéis, isto é, se

(i) $f(x+y) = f(x) \oplus f(y), \forall x,y \in A$.

(ii) $f(x \cdot y) = f(x) \odot f(y), \forall x,y \in A$.

Proposição 3.11. *Sejam $(A,+,\cdot)$ e $(B,\oplus,\odot)$ anéis e $f : (a,+,\cdot) \to (B,\oplus,\odot)$ um homomorfismo de anéis. Então $f(0_A) = 0_B$.*

Exemplo 3.12. $Id : (A,+,\cdot) \to (A,+,\cdot)$, definido por $Id(a) = a, \forall a \in A$, é um homomorfismo chamado identidade.

Exemplo 3.13. E:$(A,+,\cdot) \to (B,\oplus,\odot)$, definido por $E(a) = 0_B$, $\forall a \in A$, é uma aplicação satisfazendo (i) e (ii) mas não (iii).

Exemplo 3.14. Se I é um ideal do anel $(A,+,\cdot)$, então $\varphi : (A,+,\cdot) \to (A/I,\oplus,\odot)$, definido por $\varphi(a) = a+I$, $\forall a \in A$, é um homomorfismo chamado homomorfismo canônico ou projeção canônica.

Exemplo 3.15. Se$(B,\oplus,\odot)$ é um anel, então $\varphi : (\mathbb{Z},+,\cdot) \to (B,\oplus,\odot)$ definido por

$$\begin{cases} \varphi(n) = \underbrace{1_B \oplus 1_B \oplus \cdots \oplus 1_B}_{n \text{ vezes}}, \forall n \geq 0, \\ \varphi(-n) = \underbrace{(-1_B) \oplus (-1_B) \oplus \cdots \oplus (-1_B)}_{n \text{ vezes}}, \forall n \geq 0, \end{cases}$$

é um homomorfismo. Ele é o único homomorfismo de $(\mathbb{Z},+,\cdot)$ em $(B,\oplus,\odot)$.

Exemplo 3.16. Se $f : (A_1,+,\cdot) \to (A_2,+,\cdot)$ e $g : (A_2,+,\cdot) \to (A_3,+,\cdot)$ são homomorfismos, então $g \circ f : (A_1,+,\cdot) \to (A_3,+,\cdot)$ é um homomorfismo.

Propriedades Elementares

Seja $f : (A,+,\cdot) \to (B,+,\cdot)$ um homomorfismo de anéis.

1) Seja $\ker f := \{a \in A; f(a) = 0\} \subseteq A$. Então ker f é um ideal de $(A,+,\cdot)$ chamado núcleo de f.

2) Seja Im $f := \{f(a); a \in A\} \subseteq B$. Então $(Imf, +, \cdot)$ é um anel chamado imagem de f.

3) f é injetivo se, e somente se, ker $f = \{0\}$

Definição 3.17. Um homomorfismo de anéis $f : A \to B$ é um isomorfismo se ele é injetivo e sobrejetivo.

Note que neste caso, a aplicação inversa $f^{-1} : B \to A$ também é um homomorfismo de anéis. Quando existe um isomorfismo entre dois anéis A e B, dizemos que A e B são isomorfos e denotamos por $A \simeq B$.

3.1 CORPO DE FRAÇÕES

Sendo a construção do corpo de frações $\mathbb{Q} = \left\{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\right\}$ a partir do domínio $\mathbb{Z}$, vamos construir um corpo K a partir de um dado domínio D.

Seja D um domínio de integridade qualquer e seja $D^\sharp = D \setminus \{0\}$.

Vamos definir uma relação de equivalência no conjunto,

$\mathscr{A} = D \times D^\sharp = \left\{(a,b) : a \in D, b \in D^\sharp\right\}$. De fato, se $(a,b),(c,d) \in \mathscr{A}$ então

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc,$$

claramente define uma relação de equivalência no conjunto $\mathscr{A}$.

Vamos denotar por $\frac{a}{b}$ (*em vez de* $\overline{(a,b)}$) a classe de equivalência $\frac{a}{b} = \left\{(x,y) \in \mathscr{A} : xb = ya\right\}$.

Assim,

$$\frac{a}{b} = \frac{x}{y} \; em \; \mathscr{A}/\sim \Leftrightarrow bx = ay \; em \; D.$$

Agora vamos definir operações + e $\cdot$ no conjunto quociente

$$\mathscr{A}/\sim = \left\{\frac{a}{b} : a \in D, b \in D^\sharp\right\} = K$$

Sejam (a,b) *e* $(c,d) \in D \times D^\sharp$. Então, soma:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

produto:

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}$$

Observe que se $b,d\in D^{\sharp}$ então $b\cdot d\in D^{\sharp}$ pois D é um domínio de integridade.

Como das vezes anteriores em que definimos operações em conjuntos quocientes, vamos provar que as operações acima estão " bem definidas"em K.

De fato, suponhamos que $\frac{a}{b}=\frac{a'}{b'}$ e $\frac{c}{d}=\frac{c'}{d'}$ então,

1) $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}$

2) $\frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}$

De $\frac{a}{b}=\frac{a'}{b'}$ *e* $\frac{c}{d}=\frac{c'}{d'}$ segue que: $ab'=ba'$ *e* $cd'=dc'$ *em* D.

Agora,

$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}=\frac{a'}{b'}+\frac{c'}{d'}\Leftrightarrow(ad+bc)b'd'=(a'd'+b'c')bd$ *em* $D\Leftrightarrow$
$(ab')(dd')+(cd')(bb')=(a'b)(dd')+(c'd)(bb')$ em D e o item 1) segue das igualdades
$ab'=ba'$ *e* $cd'=c'd$.

Para a demonstração de 2) basta observar que $\frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}\Leftrightarrow(ab')\cdot(cd')=(a'b)(c'd)$ em D e o resultado segue pelas igualdades $ab'=a'b$ *e* $cd'=c'd$.

Vamos denotar por $a^*=\frac{a}{1}$ onde $a\in D$ e 1 é a unidade de D, e denotaremos

$D^*=\left\{a^*=\frac{a}{1}:a\in D\right\}\subset K=\left\{\frac{a}{b}:a\in D,b\in D^{\sharp}\right\}$.

É fácil provar que D^* é um domínio de integridade com unidade $1^*\in D^*$. Aliás 1^* é tal que,

para todo $\frac{a}{b}\in K$ então $\frac{a}{b}\cdot 1^*=1^*\cdot\frac{a}{b}=\frac{a}{b}$ e mais ainda, para todo $\frac{a}{b}\in K$

$$temos\quad \frac{a}{b}+0^*=0^*+\frac{a}{b}=\frac{a}{b}.$$

Consideremos agora a seguinte função:

$\varphi:D\to D^*$.

$a\to a^*$,

É de imediata verificação que:

a) $Im\varphi=D^*$

b) $Ker(\varphi)=\{a\in D:a^*=0^*\}=\{0\}$

c) $\varphi(a+b)=(a+b)^*=a^*+b^*=\varphi(a)+\varphi(b)\ \forall a,b\in D$

d) $\varphi(a\cdot b)=(a\cdot b)^*=a^*\cdot b^*=\varphi(a)\cdot\varphi(b)\ \forall a,b\in D$

Portanto $D\simeq D^*\subset K$.

Observe também que, se $\frac{a}{b}\neq 0^*$ em K, isto é, $a\neq 0$ em D, então $\frac{b}{a}\in K$ e mais, $\frac{a}{b}\cdot\frac{b}{a}=1^*$.

Como $D\simeq D^*\subset K$ dizemos que D está imerso em K. Observe também que $b^*\cdot\frac{1}{b}=1^*$ se $b\neq 0,\ b\in D$. Agora é fácil provar que:

$D^*=\{a^*:a\in D\}\subset K=\{a^*\cdot(b^*)^{-1}:a^*\in D^*,b^*\in D^*\ com\ b^*\neq 0^*\}$.

O corpo K construido neste parágrafo recebe o nome de corpo de frações do domínio D.

3.2 ANÉIS DE POLINÔMIOS

Vamos agora definir o principal elemento de nosso trabalho, os anéis de polinômios. Suas propriedades justificam as manipulações que estamos acostumados a utilizar em sala de aula com os alunos.

Definição 3.18. [Anéis de Polinômios]

Seja $(A,+,\cdot)$ um anel comutativo. Um polinômio de uma variável sobre A é uma sequência $(a_0,a_1,...,a_n,...)$, onde $a_i\in A$ para todo índice e onde $a_i\neq 0$ somente para um número finito de índices.

Seja $\mathscr{A}=\{$ polinômios numa variável sobre A $\}$. No conjunto $\mathscr{A}$, definimos as operações seguintes:

$$\begin{aligned}\oplus\colon \mathscr{A}\times\mathscr{A} &\to \mathscr{A}\\ \big((a_o,a_1,...),(b_0,b_1,...)\big) &\mapsto (a_0+b_0,a_1+b_1,...)\\ \odot\colon \mathscr{A}\times\mathscr{A} &\to \mathscr{A}\\ \big((a_o,a_1,...),(b_0,b_1,...)\big) &\mapsto (c_0,c_1,c_2,c_3,c_4,c_5,...)\end{aligned}$$

onde

$$\begin{cases} c_0=a_0b_0\\ c_1=a_0b_1+a_1b_0\\ \vdots\\ c_n=a_0b_n+a_1b_{n-1}+a_2b_{n-2}+\cdots+a_{n-1}b_1+a_nb_0\\ \vdots\end{cases}$$

Afirmo: $(\mathscr{A}, \oplus, \odot)$ é um anel onde:

• o elemento neutro de $\oplus$ é o elemento $(0,0,0,...)$

• o elemento neutro de $\odot$ é o elemento $(1,0,0,...)$

• o oposto de $(a_0, a_1, ..., a_n, ...)$ com respeito à operação $\oplus$ é o elemento $(-a_0, -a_1, ..., -a_n, ...)$.

Observe que a multiplicação de $\mathscr{A}$ é comutativa pois a multiplicação de A é comutativa. Se $(a_0, a_1, ...)$ é um elemento de $\mathscr{A}$, então o símbolo $(a_0, a_1, ...)^n$ designará o elemento

$$\underbrace{(a_0, a_1, ...) \odot (a_0, a_1, ...) \odot \cdots \odot (a_0, a_1, \ldots)}_{n \text{ vezes}}.$$

Usando as definições de $\oplus$ e $\odot$, é fácil ver que

$$(0, ..., 0, a_n, 0, 0, 0, ...) = (a_n, 0, 0, ...) \odot (0, ..., 0, 1, 0, 0, ...)$$

$\overbrace{\text{lugar } n+1}$ $\overbrace{\text{lugar } n+1}$

e que $(0, ..., 0, 1, 0, 0, ...) = (0, 1, 0, 0, ...)^n$.

$\overbrace{\text{lugar } n+1}$

Portanto

$$\begin{aligned}(a_0, a_1, ..., a_n, 0, 0, ...) = (a_0, 0, 0, ...) \\ \oplus[(a_1, 0, 0, ...) \odot (0, 1, 0, 0, ...)] \\ \oplus[(a_2, 0, 0, ...) \odot (0, 1, 0, 0, ...)^2] \\ \oplus \cdots \\ \oplus[(a_n, 0, 0, ...) \odot (0, 1, 0, 0, ...)^n].\end{aligned}$$

Para simplificar, vamos usar as seguintes notações:

$X = (0, 1, \ldots, 0, \ldots)$

$a_i = (a_i, 0, 0, \ldots)$

Assim, o símbolo a_i vai ser usado para indicar duas coisas diferentes: o elemento a_i de A e $(a_i, 0, 0, \ldots)$ de $\mathscr{A}$.

Finalmente, no lugar de escrever $\oplus$ e $\odot$, vamos escrever + e $\cdot$. Assim, o símbolo + (respectivamente o símbolo $\cdot$) será usado para designar duas coisas distintas: a adição de A e a adição de $\mathscr{A}$ (respectivamente a multiplicação de A e a multiplicação de $\mathscr{A}$); Com essas

convenções,

$(a_0, a_1, ..., a_n, 0, ...) = a_0 + a_1X + \cdots + a_nX^n$, onde a_iX^i designa $a_i \cdot X^i$.

Então:

$$\mathscr{A} = \left\{ \sum_{i=0}^{n} a_iX^i; \quad n \in \mathbb{N} \text{ e } a_i \in A \right\}$$

e as operações deste anel são as usuais. Vamos denotar o anel $(\mathscr{A}, +, \cdot)$ por $A[X]$, e chamá-lo de anel de polinômios numa variável sobre A.

Exemplo 3.19. $\mathbb{Z}[X] = \{a_0 + a_1X + a_1X^2 + \ldots + a_nX^n \mid a_i \in \mathbb{Z},\ i = 1, 2, \ldots, n\}$

Definição 3.20. [Coeficiente líder]

Seja $A[x]$ um anel de polinômio e

$$a_kx^k + \cdots + a_1x^1 + a_0, \in A[x]$$

Para o maior i com $a_i \neq 0$ (se houver), a_i é chamado de coeficiente líder ou dominante do polinômio. se o coeficiente líder for igual a 1, dizemos que o polinômio é mônico.

Por exemplo, o coeficiente líder do polinômio $4x^5 + x^3 + 2x^2 \in \mathbb{Z}[x]$ é 4.

Definição 3.21. [Grau de um Polinômio] Sejam A[X] um anel de polinômio e $P(x) = a_kx^k + \cdots + a_1x^1 + a_0 \in A[X]$ não nulo. O grau do polinômio $P(x)$ é dado pelo maior valor de k inteiro, tal que $a_k \neq 0\ e\ a_j = 0$ para todo inteiro $j > k$

Por exemplo, o grau do polinômio $12x^5 + x^4 + 6x^2 \in \mathbb{Z}[x]$ é 5.

O polinômio $x^3 - 2x + 1 \in \mathbb{Z}[X]$ é um polinômio mônico de grau 3.

O grau do polinômio $f(x)$ será denotado por $\partial f(x)$.

Definição 3.22. [Raiz de um polinômio]

Diz-se que $r \in A$ é uma raiz ou zero do polinômio $p(x) \in A[X]$ se $p(r) = 0$.

Definição 3.23. [Domínios Euclidianos]

Um domínio euclidiano $(D, +, \cdot, \varphi)$ é um domínio de integridade $(D, +, \cdot)$ com uma função $\varphi : D \setminus \{0\} \to \mathbb{N} = \{0, 1, 2, ...\}$ que satisfaz as propriedades seguintes:

1) $\forall a, b \in D, b \neq 0$, existem $t, r \in D$ tais que a= bt + r com

$$\begin{cases} \varphi(r) < \varphi(b) \\ ou \quad r = 0 \end{cases}$$

2) $\varphi(a) \leqslant \varphi(ab), \forall a, b \in D \setminus \{0\}$.

Teorema 3.24 (Algorítmo de Euclides para $\mathbb{Z}$)**.** *Seja* $|\ |\colon \mathbb{Z} \to \mathbb{N}$ *a função valor absoluto. Então:*

(i) $(\mathbb{Z},+,\cdot,|\ |)$ *é um domínio euclidiano, isto é,*

- $(\mathbb{Z},+,\cdot)$ *é um domínio,*
- $\forall a, b \in \mathbb{Z}$, $b \neq 0$, *existem* $t,r \in \mathbb{Z}$ *tais que a=bt + r com*

$$\begin{cases} 0 \leqslant r < |b| \\ ou \quad r = 0 \end{cases}$$

- $\forall a, b \in \mathbb{Z} \setminus \{0\}$, $| a | \leq | ab |$.

(ii) Tais elementos t e r podem ser efetivamente calculados.

(iii.1) Em geral, tais inteiros t e r não são únicos.

(iii.2) É sempre possível escolher $r \geq 0$*, e isso de maneira única.*

Demonstração:

(i) e (ii): Que $(\mathbb{Z},+,\cdot)$ é um domínio.

Se $b \in \mathbb{Z} \setminus \{ 0 \}$, temos $| b | \geq 1$, e consequentemente

$| a | \leq | a | | b | = | ab |, \forall a \in \mathbb{Z}$.

Agora, sejam $a,b \in \mathbb{Z}$, $b \neq 0$. Procuramos elementos t e $r \in \mathbb{Z}$ tais que a = bt+r com r "pequeno"e positivo (afim de obter (iii.2)), isto é, procuramos $t \in \mathbb{Z}$ tal que a - bt seja "pequeno"e positivo. Vejamos a ideia da prova no caso $b > 0$ e $a \geqslant 0$.

Neste caso, temos $b \geqslant 1$ e existe um único inteiro t tal que

$$tb \leqslant a \qquad e \qquad (t+1)b > a$$

pela propriedade arquimediana.

Observe que este inteiro t é necessariamente tal que $0 \leqslant t \leqslant a$, de modo que calculando 0b,1b,2b,...,ab, vamos de fato encontrá-lo. Tome r = a - tb (que pode ser efetivamente calculado

pois a e b são dados e t foi calculado).Temos a = bt + r com r $\geqslant$ 0; além disto, de (t+1)b $>$ a, obtemos | a |= r = a-tb $<$ b = | b |. Os outros casos podem ser tratados de maneira similar. Tratamos agora o problema da unicidade. Se existem elementos $t_1, r_1, t_2, r_2 \in \mathbb{Z}$ tais que

$$a = bt_1 + r_1 = bt_2 + r_2 \quad \text{com}$$

$$\begin{cases} 0 \leqslant r_1 < |b| \\ 0 \leqslant r_2 < |b|, \end{cases}$$

então temos $|b||t_1 - t_2| = |b(t_1 - t_2)| = |r_1 - r_2| < |b|$, *logo* $|t_1 - t_2| = 0$ e portanto, $t_1 = t_2$ e $r_1 = r_2$. Falta agora verificar (iii.1). Podemos escrever

3= 2·1 + 1 (t=1,r=1)

3= 2·2 + (-1) (t=2,r=-1),

isto é, temos duas possibilidades para a divisão de 3 por 2.

■

Observação. O algoritmo tem muitas aplicações teóricas e práticas sendo uma ferramenta de porte essencial. Ele pode ser usado para gerar quase todas as aplicações tradicionais usadas em diferentes culturas em todo o mundo. Ele é um elemento-chave dos algarismos de RSA, um método de criptografia de chave pública usado no comércio eletrônico. Ele é usado para resolver as equações diofantinas, utilizado na descoberta de números que sejam convenientes em múltiplas congruências como exemplo o teorema chinês dos restos ou na caracterização do inverso multiplicativo de um número finito.

Vejamos agora um algoritmo para polinômios análogo ao algoritmo de Euclides para $\mathbb{Z}$.

Teorema 3.25. *Seja (K,+,·) um corpo e seja K[X] o anel de polinômios numa variável sobre K. Seja grau: K[X]\ { 0 } $\to \mathbb{N}$ a função grau. Então:*

(i) (K[X],grau) é um domínio euclidiano,isto é:

- *K[X] é um domínio,*
- *$\forall$ f(X),g(X) $\in$ K[X], g(X) $\neq$ 0, existem polinômios t(X),r(X) $\in$ K[X] tais que*

f(X)=g(X)· t(X)+r(X) com

$$\begin{cases} grau\ r(X) < grau\ g(X) \\ ou\ r(X) = 0 \end{cases}$$

• $\forall\ f(X), g(X) \in K[X] \setminus \{0\},\ grau\ f(X) \leq grau(f(X)g(X))$.

(ii) Tais polinômios t(X) e r(X) podem ser efetivamente calculados.

(iii) Tais polinômios t(X) e r(X) são unicamente determinados.

Agora, observando que todo elemento não-nulo de um corpo é invertível, isto é, possui inverso com respeito à multiplicação, obtemos o Teorema 3.25 como consequência do seguinte Teorema.

Teorema 3.26. *Sejam (R,+,·) um anel e R[X] o anel de polinômios numa variável sobre R. Seja g(X)∈ R[X] um polinômio cujo coeficiente líder é invertível em R. Então,*

(i) Existem t(X),r(X) ∈ R[X] tais que

f(X)= g(X)· t(X) + r(X) com

$$\begin{cases} grau\ r(X) < grau\ g(X) \\ ou\ r(X) = 0 \end{cases}$$

(ii) Tais polinômios t(X) e r(X) podem ser efetivamente calculados.

(iii) Tais polinômios t(X) e r(X) são unicamente determinados.

Demonstração:

(i) e (ii). Se f(X)=0 ou se grau f(X)<grau g(X), acabou: tome $t(X) = 0$ e $r(X) = f(X)$. Se grau f(X)≥ grau $g(X) = m$, escreva $f(X) = a_nX^n + \cdots + a_0$ com n≥ m e $a_n \neq 0$, e escreva $g(X) = b_mX^m + \cdots + b_0$. Pela hipótese, o coeficiente líder b_m de g(X) é invertível em R, logo $\frac{1}{b_m} \in R$ e ,portanto, $\frac{1}{b_m}a_nX^{n-m} \in R[X]$. Observe que $\frac{1}{b_m}a_nX^{n-m}$ é exatamente o polinômio pelo qual se precisa multiplicar o primeiro termo de g(X) para se obter o primeiro termo de f(X). Temos então:

$$f(X) - \tfrac{1}{b_m}a_nX^{n-m}g(X) = \underbrace{\left(a_{n-1} - \frac{a_nb_{m-1}}{b_m}\right)X^{n-1} + \cdots + \left(a_{n-m} - \frac{a_nb_0}{b_m}\right)X^{n-m} + \cdots}_{chame\ isso\ de\ f_1(X) \in R[X]}$$

e $f(X) = g(X)\frac{1}{b_m}a_nX^{n-m} + f_1(X)$. Observe que $\frac{1}{b_m}a_n$ e $f_1(X)$ foram efetivamente calculados. Se $f_1 = 0$ ou se grau $f_1(X)$ <grau $g(X) = m$, acabou: tome $t(X) = \frac{1}{b_m}a_nX^{n-m}$ e $r(X) = f_1(X)$. Se p=grau $f_1(X) \geq m$, repita o processo com $f_1(X) = c_pX^p + \cdots + c_0$ com

$n-1 \geq p \geq m$ e $c_p \neq 0$, e tome $f_2(X) = f_1(X) - \frac{1}{b_m} c_p X^{p-m} g(X)$; temos então:

$$f(X) = g(X)\left[\frac{1}{b_m} a_n X^{n-m} + \frac{1}{b_m} c_p X^{p-m}\right] + f_2(X),$$

com $\frac{1}{b_m} a_n, \frac{1}{b_m} c_p, f_2(X)$ efetivamente calculáveis.

Se $f_2(X) = 0$ ou se grau $f_2(X) < m$, acabou: tome

$$t(X) = \frac{1}{b_m} a_n X^{n-m} + \frac{1}{b_m} c_p X^{p-m} \; e \; r(X) = f_2(X)$$

.

Se grau $f_2(X) \geq m$, repita o processo. Como grau $f(X) > grau f_1(X) > grau f_2(X) > \cdots$, obtemos depois de um número finito de passos um polinômio $f_i(X)$ nulo ou de grau menor que m. Tome $r(X) = f_i(X)$.

(iii) Se existem polinômios $t_1(X), r_1(X), t_2(X), r_2(X) \in R[X]$ tais que

$$f = gt_1 + r_1 = gt_2 + r_2 \quad \text{com}$$
$$\begin{cases} grau\ r_1 < grau\ g\ (ou\ r_1 = 0) \\ grau\ r_2 < grau\ g\ (ou\ r_2 = 0), \end{cases}$$

então $g(X) \cdot [t_1(X) - t_2(X)] = r_2(X) - r_1(X)$. Suponha que o polinômio $t_1(X) - t_2(X)$ seja não-nulo; temos então

$$grau(r_2(X) - r_1(X)) = grau(g(X) \cdot [t_1(X) - t_2(X)]) = grau\ g(X) + grau(t_1(X) - t_2(X)),$$

onde a última igualdade acima decorre da hipótese que o coeficiente do termo de maior grau de g(X) é invertível em R. Assim, $grau\ (r_2(X) - r_1(X)) \geq grau\ g(X)$, o que é absurdo pois temos grau $(r_2(X) - r_1(X)) \leq max\ \{grau\ (r_1(X)), grau\ r_2(X)\} < grau\ g(X)$.

■

A demonstração acima generaliza o processo usual da divisão de polinômios que exibimos no seguinte exemplo concreto em $\mathbb{Z}[X]$.

Resolução:

$$\begin{array}{ll} \text{f(X)} = 2X^4+3X^3+0X^2+2X+1 & \underline{\mid -X^2-5 \qquad = g(X)} \\ \underline{-(2X^4+0X^3+10X^2)} & -2X^2-3X+10 = t(X) \\ f_1(X) = \ 3X^3-10X^2+2X+1 & \\ \quad \underline{-(3X^3+0X^2+15X)} & \\ f_2(X) = \quad -10X^2-13X+1 & \\ \quad \underline{-(-10X^2+0X-50)} & \\ r(X) = \quad -13X+51 & \end{array}$$

Assim obtemos que

$2X^4+3X^3+2X+1 = (-X^2-5)(-2X^2-3X+10)+(-13X+51)$,onde

$grau(-13X+51) = 1 < 2 = grau(-X^2-5)$.

O algoritmo da divisão é uma ferramenta importante, possui diversas aplicações.

O Teorema a seguir é uma aplicação do algoritmo da divisão e nos dá uma fatoração de um polinômio de modo que fica fácil verificar as raízes do polinômio.

Teorema 3.27. *Sejam A um anel, $f(X) \in A[X]$ e $\alpha \in A$. Então $f(\alpha) = 0$ se, e somente se, existe um polinômio $t(X) \in A[X]$ tal que $f(X) = (X-\alpha)t(X)$.*

Demonstração:

Pela proposição 3.26, sabemos que existem t(X), $r(X) \in A[X]$ tais que

$f(X) = (X-\alpha)t(X)+r(X)$ com grau $r(X) < grau(X-\alpha) = 1$ *ou* $r(X) = 0$, isto é, com r(X) uma constante. Então $f(\alpha) = (\alpha-\alpha)t(\alpha)+r(\alpha) = r(\alpha) = r(X)$ e, portanto,

$$f(\alpha) = 0 \Longleftrightarrow f(X) = (X-\alpha)t(X).$$

■

Definição 3.28. Sejam A um anel, $f(X) \in A[X]$, $\alpha \in A$, e um inteiro $s \geqslant 1$. Dizemos que α é uma raiz de f(X) de multiplicidade s se $(X-\alpha)^s$ divide f(X) mas $(X-\alpha)^{s+1}$ não divide f(X).

Teorema 3.29. *Sejam A um anel, $f(X) \in A[X]$, $\alpha \in A$, e seja $s \geqslant 1$ um inteiro. Então as afirmações seguintes são equivalentes:*

(i) α é uma raiz de f(X) de multiplicidade s.

(ii) Existe $h(X) \in A[X]$ *tal que* $f(X) = (X-\alpha)^s h(X)$ *com* $h(\alpha) \neq 0$

Demonstração.

$(i) \Rightarrow (ii)$. Aplique o Teorema 3.27. $(ii) \Rightarrow (i)$. Devemos mostrar que $(X-\alpha)^{s+1}$ não divide f(X). Suponha que $(X-\alpha)^{s+1}$ divida f(X). Temos então

$(X-\alpha)^s h(X) = f(X) = (X-\alpha)^{s+1} l(X)$ para algum polinômio $l(X) \in A[X]$, logo $(X-\alpha)^s [h(X) - (X-\alpha) l(X)] = 0$. Como $(X-\alpha)^s$ é um polinômio mônico, obtemos $h(X) - (X-\alpha) l(X) = 0$. Então $h(X) = (X-\alpha) l(X)$ e portanto $h(\alpha) = 0$, o que contradiz nossa hipótese.

■

Definição 3.30. [Irredutível] Seja A um anel comutativo. Um elemento $a \in A$ é dito irredutível se $a \neq 0$, se $a \notin A^* = \{x \in A \mid xy = yx = 1 \text{ para algum } y \in A\}$ e se $a = bc$ com $b, c \in A$, então $b \in A^*$ *ou* $c \in A^*$

Vamos definir uma série de conceitos necessários para um importante resultado sobre fatoração de polinômios.

Definição 3.31. [Polinômios irredutíveis] Seja R um domínio de integridade. Dizemos que o polinômio não constante p(x) é irredutível em R[x] (ou irredutível sobre R) se é impossível expressar p(x) como um produto a(x)b(x) de dois polinômios a(x) e b(x) em R[x] cujos graus são ambos maiores ou iguais a 1.

Definição 3.32. [Elemento Associado] Seja D um anel. Dois elementos $a, b \in D$ são associados (em D) se existe $u \in D$, u invertível em D, tal que $a = ub$.

Definição 3.33. Em teoria dos anéis, um domínio de integridade D é chamado domínio de fatoração única (denotado de DFU) ou fatorial se:

1. $\forall a \in D$, se $a \notin D^*$ e $a \neq 0$ temos que $\exists c_i \in D$ irredutíveis $\forall i \in I_n = \{1, 2, 3, \ldots, n\}$ tal que $a = \prod_{i=1}^{n} c_i$

2. Seja $a = \prod_{i=1}^{n} c_i \quad e \quad a = \prod_{j=1}^{m} d_j$ com c_i, d_j irredutíveis $\forall i \in I_n$ e $\forall j \in I_m$ Então $m = n$ e Existe $\sigma : I_n \to I_n$ bijeção, tal que c_i é associado a $d_{\sigma(i)}$

Teorema 3.34. *Sejam D um domínio e* $0 \neq f(X) \in D[X]$. *Então:*

1) Número de raízes de f(X) em D[X] (contando as multiplicidades) é menor ou igual ao grau de f(X).

2) Chamando $\alpha_1, \ldots, \alpha_r$ *essas raízes e denotando por* $e_1, \ldots, e_r$ *as suas multiplicidades, temos* $f(X) = (X-\alpha_1)^{e_1} \ldots (X-\alpha_r)^{e_r} t(X)$*, onde* $t(X) \in D[X]$ *é um polinômio que não tem raiz em D.*

Demonstração.

• Se $f(X)$ não tem raiz em D, acabou.

• Se $f(X)$ tem uma raiz α_1 em D de multiplicidade e_1, então

$$f(X) = (X-\alpha_1)^{e_1} t_1(X)$$

com $t_1(X) \in D[X]$ e $t_1(\alpha_1) \neq 0$. Se $f(X)$ não tem outra raiz em D, então acabou, pois:

$\sharp\{\text{raízes de } f(X) \text{ em } D\} = e_1 \leqslant e_1 + grau\, t_1(X) = grau\, f(X)$.

• Se $f(X)$ tem uma outra raiz α_2 em D de multiplicidade e_2, então

$$(*)\ f(X) = (X-\alpha_1)^{e_1} t_1(X) = (X-\alpha_2)^{e_2} h_1(X)$$

com $h_1(X) \in D[X]$ e $h_1(\alpha_2) \neq 0$. Se K denota o corpo de frações de D, então K[X] é um domínio fatorial e $f(X)$ tem uma única fatoração em polinômios irredutíveis em K[X]. Como $X-\alpha_1$ e $X-\alpha_2$ são irredutíveis e não são associados, então em vista da igualdade (*), existe $t_2(X) \in K[X]$ tal que

$$t_1(X) = (X-\alpha_2)^{e_2} t_2(X).$$

Por outro lado, já que $t_1(X)$ e $(X-\alpha_2)^{e_2} \in D[X]$ e que $(X-\alpha_2)^{e_2}$ é mônico, temos $t_2(X) \in D[X]$ e portanto

$$f(X) = (X-\alpha_1)^{e_1} (X-\alpha_2)^{e_2}\, t_2(X)$$

com $t_2(X) \in D[X]$, $t_2(\alpha_1) \neq 0$ e $t_2(\alpha_2) \neq 0$. Se $f(X)$ não tem outra raiz em D, então acabou pois:

$\sharp\{\text{raízes de } f(X) \text{ em } D\} = e_1 + e_2 \leqslant grau f(X)$.

• Se f(X) tem uma outra raiz α_3 em D de multiplicidade e_3, então temos:

$$f(X) = (X-\alpha_1)^{e_1}(X-\alpha_2)^{e_2}t_2(X) = (X-\alpha_3)^{e_3}h_2(X)$$

com $h_2(X) \in D[X]$ e $h_2(\alpha_3) \neq 0$, e obteremos

$$t_2(X) = (X-\alpha_3)^{e_3}t_3(X) \text{ com } t_3(X) \in D[X].$$

O processo tem que terminar pois grau $f(X) > grau\, t_1(X) > grau\, t_2(X) > \ldots$.

■

Esse teorema é importante e nos dá a quantidade máxima de raízes de um polinômio num anel. Além disso, se são dadas as raízes podemos fatorar o polinômio como no item 2 do teorema. É claro que se o polinômio está fatorado como produto de polinômios mônicos de grau 1, então facilmente encontramos as raízes. Encontrar raízes é um problema antigo e não há um método geral para este problema. Para polinômios de grau 1 e 2 são fáceis. Para os de grau 3 e 4 existem métodos de resolução por radicais mas não é prático e não é muito utilizado. Vamos estudar quando certos polinômios são irredutíveis, assim reduzimos alguns casos na busca de raízes de polinômios.

Definição 3.35. Seja $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in A[X]$ um polinômio não nulo. Chamamos de conteúdo de f(X), e denotaremos por C(f), o MDC dos coeficientes $a_0, a_1, a_2 \ldots, a_m$ *de* $f(X)$. Repare que dado $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ vamos ter para cada $0 \leqslant i \leqslant n, b_i \in A$ *tal que* $a_i = C(f)b_i$. Definindo-se $f_1(X) = b_0 + b_1X + b_2X^2 + \cdots + b_nX^n$ temos que $f(X) = C(f)f_1(X)$ *e* $C(f_1(X)) = 1$.

Quando um polinômio tem conteúdo igual a 1 dizemos esse polinômio é primitivo. No caso acima $f_1(X)$ é primitivo e acabamos de ver que todo polinômio f(X) satisfaz $f(X) = C(f)f_1(X)$, com $f_1(X)$ primitivo.

Teorema 3.36 (Gauss)**.** *Sejam D um domínio fatorial e K seu corpo de frações.*

Se $g(X) \in D[X]$ *tem grau* $\geqslant 1$*, então g(X) é irredutível em D[X] se, e somente se, g(X) é primitivo em D[X] e irredutível em K[X].*

Demonstração

" $\Leftarrow$ " é claro.

" $\Rightarrow$ " Suponha por absurdo que $g(X) = h(X)l(X)$ *com* $h(X), l(X) \in K[X]$ de grau $\geqslant 1$. Podemos escrever $h(X) = (\frac{a}{b})h_1(X)$ e $l(X) = (\frac{a'}{b'})l_1(X)$ com $a, b, a', b' \in D, b \neq$

$0,\ b' \neq 0,\ h_1(X),\ l_1(X) \in D[X]$ polinômios primitivos de grau $\geqslant 1$ e, portanto, $g(X) = (\frac{aa'}{bb'})h_1(X)l_1(X)$ ou também, $bb'g(X) = aa'h_1(X)l_1(X)$. Vemos que $bb'C(g(X)) = C(bb'g(X)) = C(aa'h_1(X)l_1(X)) = aa'C(h_1(X)l_1(X)) = aa'$.

Portanto $(\frac{aa'}{bb'}) = C(g(X)) \in D$. Assim, $g(X) = (\frac{aa'}{bb'})h_1(X)l_1(X)$; com $\frac{aa'}{bb'}h_1(X) \in D[X]$ de *grau* $\geqslant 1$, e com $l_1(X) \in D[X]$ de grau ≥ 1, isto é, g(X) é produto de dois fatores de *grau* $\geqslant 1$ *em* $D[X]$; absurdo.

■

Teorema 3.37 (Teorema de Bezout)**.** *Dados inteiros a e b, ambos não nulos, existem inteiros m e n tais que am + bn = mdc(a, b).*

Observação: Como consequência imediata da identidade de Bézout, temos que se c é um inteiro que divide a e b, então c também divide $mdc(a,b)$. Ora, se m, n são inteiros tais que $am+bn = mdc\ (a,b)$ e q_1, q_2 inteiros tais que $a = q_1c$ e $b = q_2c$, então $(q_1m+q_2n)c = mdc(a,b)$, ou seja, c divide $mdc(a,b)$. Um outro corolário da identidade de Bézout afirma que a equação diofantina linear $ax+by = c$ tem solução se $mdc(a,b)$ divide c. Realmente, tem-se pela identidade de Bézout que existem inteiros m, n tais que $am+bn = mdc(a,b)$ e, assim, desde que $c = q\ mdc(a,b)$, $q(am+bn) = a(qm)+b(qn) = q\ mdc(a,b) = c$, isto é, (qm,qn) é solução da equação diofantina linear.

A demonstração do teorema de Bézout para polinômios é feita de maneira análoga a demonstração para números inteiros. Em matemática, particularmente em teoria dos números, a identidade de Bézout, também é chamada como lema de Bézout, teorema de Bézout ou ainda teorema de Bachet-Bézout. O matemático francês Étienne Bézout (1730 - 1783), cujo nome do lema está associado, provou o análogo do resultado para polinômios. Foi Claude Gaspard Bachet de Méziriac (1581 - 1638), outro matemático francês, quem provou a identidade para números inteiros.

Definição 3.38. Sejam $f(X)$ e $g(X)$ pertencentes a $K[X]$ dois polinômios não simultaneamente nulos. Um polinômio $d(X)$ pertencente a $K[X]$ é chamado de máximo divisor comum de $f(X)$ e $g(X)$, com a notação mdc $(f(X),g(X))$ se satisfaz as seguintes condições:

(i) $d(X) \mid f(X)$ *e* $d(X) \mid g(X)$

(ii) Para todo polinômio $d'(X)$ pertencente ao corpo $K[X]$, se $d'(X) \mid f(X)$ e $d'(X) \mid g(X)$ então $d'(X) \mid d(X)$.

Teorema 3.39. *Seja K um corpo e p(x) um polinômio irredutível em K[x]. Se* $a(x), b(x) \in K[x]$ *são tais que p(x) divide a(x)b(x), então p(x) divide a(x) ou p(x) divide b(x).*

Demonstração:

Suponha que p(x) não divide a(x), e seja d(x) = mdc(p(x), a(x)). Como p(x) é irredutível e não divide a(x), o grau de d(x) não pode ser maior do que zero. Logo d(x) = 1. Pelo Teorema de Bézout, existem $r(x)$ e $s(x)$ tais que $a(x)r(x)+p(x)s(x)=1$. Multiplicando a igualdade acima por b(x) e observando que $p(x) \mid a(x)b(x)$obtemos:

$$a(x)b(x)r(x)+p(x)b(x)s(x)=b(x) \Longleftrightarrow p(x)(q(x)r(x)+b(x)s(x))=b(x),$$

isto é, $p(x)|b(x)$.

■

Observe que o principal na demonstração acima é observar que $mdc(p(x),a(x))=1$. Assim, temos o seguinte resultado: se $p(x)|a(x)b(x)$ *e* $mdc(p(x),a(x))=1$, então $p(x)|b(x)$, com a mesma demonstração dada acima.

Teorema 3.40. *Todo polinômio não nulo em K[x], considerando K um corpo, pode ser fatorado em K[x] como um produto de polinômios irredutíveis. Esta fatoração é única, a menos da ordem dos fatores e da multiplicação por constantes não nulas de K.*

Demonstração:

Seja $f(x) \in K[x]-0$.

Vamos provar por indução sobre $\partial f(x)=n$. Se $n=0$ então $f(x)=u$ é uma constante não nula. Assim, podemos assumir que $\partial f(x)=n \geq 1$. Vamos supor pela hipótese de indução que todo polinômio não nulo de grau menor que n pode ser escrito na expressão desejada.

Suponha que $f(x)$ é um polinômio redutível sobre K. Assim,

$\exists\, g(x),h(x) \in K[x], 1 \leqslant \partial g(x) < n, 1 \leqslant \partial h(x) < n$ *tais que* $f(x)=g(x)\cdot h(x)$.

Agora, por indução temos,

$g(x)=a\cdot p_1(x)\cdots p_r(x), a \in K\setminus\{0\}$ e $p_1(x),\ldots,p_r(x)$ polinômios irredutíveis sobre K. Analogamente, $h(x)=b\cdot p_{r+1}(x)\cdots p_m(x), b \in K\setminus\{0\}$ e $p_{r+1}(x),\ldots,p_m(x)$ polinômios irredutíveis sobre K. Assim, $f(x)=u\cdot p_1(x)\cdots p_m(x)$, onde $u=ab \in K\setminus\{0\}$ *e* $p_1(x),\ldots,p_m(x)$ polinômios irredutíveis sobre K.

Vamos agora demonstrar a unicidade da expressão.

Suponhamos $f(x)=u\cdot p_1(x)\cdots p_m(x)=u'\cdot p'_1(x)\cdots p'_s(x)$ onde $u,u' \in K\setminus\{0\}$ *e* $p_1(x)\ldots p_m(x), p'_1$ são polinômios irredutíveis sobre K. Assim, temos, $p_1(x) \mid p'_1(x)\ldots p'_s(x)$ e daí segue que

$\exists\, u_i' \in K \setminus \{0\}$ 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 $K[x]$).

Agora 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 $K[x]$. Suponhamos $m > 1$. De $p_i'(x) = u_i' \cdot p_1(x)$ e sendo $K[x]$ um domínio temos que: $u \cdot p_2(x) \cdots p_m(x) = u' \cdot u_i \cdot p_1'(x) \cdots p_{i-1}(x) \cdot p_{i+1}(x) \cdots p_s(x)$ 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, e isto termina a demonstração do teorema.

■

Corolário 3.41. *Seja D um domínio. Sejam f(X),* $g(X) \in D[X]$ *dois polinômios de grau menor ou igual à n tais que* $f(\alpha) = g(\alpha)$ *para* $(n+1)$ *elementos* α *distintos de D. Então* $f(X) = g(X)$.

Demonstração. Basta aplicar o Teorema 3.34 e o Teorema anterior ao polinômio $f(X) - g(X)$.

■

3.3 CRITÉRIOS DE IRREDUTIBILIDADE

Mesmo se D for um domínio fatorial (ou até um corpo), pode não existir um algorítmo que determine se um polinômio qualquer $f(X) \in D[X]$ é irredutível ou não. Mesmo que tal algorítmo exista (é o caso por exemplo em $\mathbb{Z}[X]$), ele pode ser tão ”brando”que na prática não seja utilizável. Vamos estabelecer algumas maneiras para que um polinômio $f(X) \in D[X]$ seja irredutível. Primeiro, lembramos que no caso de D ser um domínio fatorial com corpo de frações K, a irredutibilidade de f(X) em D[X] está relacionada com a irredutibilidade de f(X) em K[X]. Na maior parte das vezes vai ser mais fácil procurar os fatores em D[X] pois D sendo um conjunto menor que K, há menos fatores que valem para serem testados em D[x]. Mostraremos isto com alguns exemplos.

Exemplo 3.42. Seja $f(X) = X^4 - X^2 + 1 \in \mathbb{Z}[X]$. Vamos mostrar que $f(X)$ é irredutível em $\mathbb{Z}[X]$, ou seja, que f(X) não é um produto de dois fatores de grau $\geqslant 1 em\, \mathbb{Z}[X]$.

• $f(X)$ não tem um fator de grau 1 em $\mathbb{Z}[X]$. Com efeito, se ele tivesse, este fator (que tem que ser mônico pois $f(X)$ é mônico) seria do tipo $X - a$ com a $\in \mathbb{Z}$, isto é, teríamos $X^4 - X^2 + 1 = (X-a)g(X)$ com $g(X) \in \mathbb{Z}[X]$. Olhando para o termo constante, teríamos $1 = am$

com $m \in \mathbb{Z}$, logo $a = \pm 1$, isto é, ± 1 seria raiz de $X^4 - X^2 + 1$. No entanto, é imediato verificar que nem 1, nem -1, são raízes de $X^4 - X^2 + 1$.(Observe que se tivéssemos trabalhado em $\mathbb{Q}[X]$ no lugar de $\mathbb{Z}[X]$, a priori a poderia ser qualquer elemento diferente de zero de $\mathbb{Q}$ e logo não daria para verificar, um por um, que nenhum a de $\mathbb{Q}$ é raiz de $f(X)$).

• $f(X)$ não tem fator $g(X)$ de grau 3 em $\mathbb{Z}[X]$. Com efeito, se ele tivesse, teríamos $f(X) = g(X)h(X)$, onde $h(X) \in \mathbb{Z}[X]$ teria necessariamente grau 1, mas isto é impossível pelo caso precedente.

• $f(X)$ não tem fator de grau 2 em $\mathbb{Z}[X]$. Com efeito, se ele tivesse, teríamos

$X^4 - X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d)$ com a,b,c,d $\in \mathbb{Z}$

(termo constante) $\quad 1 = bd, \quad$ logo $b = d = \pm 1$;

(termo em X) $\quad 0 = ad + bc = b(a + c) \quad logo \quad a = -c$;

(termo em X^2) $\quad -1 = 2b - a^2, \quad$ logo $\quad a^2 - 1 = 2b = \pm 2$;

assim $a^2 = 3$ ou $a^2 = -1$, o que é impossível. Logo $f(x)$ é irredutível em $\mathbb{Z}[X]$.

Vejamos agora um critério de irredutibilidade, se A é um anel e I é um ideal de A, já sabemos que a aplicação

$A[X] \to (A/I)[X]$

$f(X) := \sum a_i X^i \mapsto \overline{f}(X) := \sum \overline{a_i} X^i$

é um homomorfismo de anéis.

Escolhendo o ideal I de maneira adequada, pode-se esperar que o anel A/I seja relativamente simples para a análise do polinômio reduzido $\overline{f}(X)$. Conseguindo informações sobre o reduzido, podemos esperar traduzí-las em informações sobre o polinômio f(X).

Teorema 3.43. *Seja A um anel, I um ideal e $f(X) \in A[X]$ um polinômio mônico. Se $\overline{f}(X)$ é irredutível em $(A/I)[X]$, então $f(X)$ é irredutível em $A[X]$.*

Demonstração.

Seja $f(x) = a_0 + a_1 X + a_2 X^2 + \ldots + X^n$ com $a_0, a_1, \ldots, a_{n-1} \in A$ polinômio mônico em $A[X]$

Suponha que $f(X) = h(X)g(X)$ onde $grau(h) < grau(f)$ e $grau(g) < grau(f)$. Podemos supor

$$h(X) = 1X^r + b_{r-1}X^{r-1} + \ldots + b_1X + b_0$$

e

$$g(X) = 1X^s + c_{s-1}X^{s-1} + \ldots + c_1X + c_0$$

onde $r+s = n$.

$h(X)$ e $g(X)$ são mônicos pois $f(X)$ é mônico, logo $\overline{h}(X)$ e $\overline{g}(X)$ são mônicos em $(A/I)[X]$,

grau $\overline{h}(X) = grau\, h(X)$ e $grau\, \overline{g}(X) = grau\, g(X)$

Assim $\overline{h}(X)$ *e* $\overline{g}(X)$ não são constantes. Logo $\overline{f}$ é redutível em $\big(A/I\big)[X]$.

■

Observação: Ressaltamos aqui a hipótese do polinômio ser mônico é crucial, pois caso não seja, o teorema não vale. Vejamos um exemplo: Seja $f(x) = 3x^3 + x \in \mathbb{Z}[X]$. Então $f(X) = x(3x^2+1)$ é redutível em $\mathbb{Z}[X]$. No entanto, $\overline{f}(x) = x$ é irredutível em $(\mathbb{Z}/3\mathbb{Z})[X] = \mathbb{Z}_3[X]$. Ou seja, o teorema anterior não é válido.

Teorema 3.44. *Seja* $f(X) \in \mathbb{Z}[X]$ *um polinômio mônico.*

Seja p um número primo.

a) Sejam $\overline{\gamma_1}, \ldots, \overline{\gamma_r}$ *as raízes de* $\overline{f}(X)$ *em* $\mathbb{Z}/p\mathbb{Z}$*. Caso f(X) tenha uma raíz* $\alpha \in \mathbb{Z}$*, então existe um índice* $i \in \{1, \ldots, r\}$ *tal que* $\alpha \equiv \gamma_i (mod\, p)$.

b) Suponha que grau $\big(f(X)\big) \geqslant 3$ *e que* $\overline{f}(X) = (X - \overline{\gamma})\varphi(X)$ *com* $\varphi(X)$ *irredutível em* $(\mathbb{Z}/p\mathbb{Z})[X]$*. Então f(X) é irredutível em* $\mathbb{Z}[X]$*, ou f(X) possui uma raíz* $\alpha \in \mathbb{Z}$ *tal que*

$\alpha \equiv \gamma (mod\, p)$.

Demonstração.

a) Como p é um número primo, então $\mathbb{Z}/p\mathbb{Z}$ é um corpo, logo $\mathbb{Z}/p\mathbb{Z}[X]$ é um domínio fatorial e $X - \overline{\gamma}_1, \ldots, X - \overline{\gamma}_r$ são os fatores irredutíveis de grau 1 de $\overline{f}(X)$. Caso f(X) tenha uma raíz α *em* $\mathbb{Z}$, então $X - \alpha$ é um fator de f(X) em $\mathbb{Z}[X]$, logo existe um índice $i \in 1, \ldots, r$ tal que $\overline{\alpha} = \overline{\gamma}_i, i.e., \quad tal\ que \quad \alpha \equiv \gamma_i (mod\, p)$.

b) Suponha que f(X) não seja irredutível em $\mathbb{Z}[X]$, logo $f(X) = g(X)h(X)$ com $g(X), h(X) \in \mathbb{Z}[X]$ mônicos de grau maior ou igual a 1.

Temos então $\overline{f}(X) = \overline{g}(X)\overline{h}(X) \quad em \quad (\mathbb{Z}/p\mathbb{Z})[X]$.

Pela hipótese, $\overline{f}(X) = (X - \overline{\gamma})\varphi(X)$ é uma fatoração em elementos irredutíveis em $(\mathbb{Z}/p\mathbb{Z})[X]$. Como $(\mathbb{Z}/p\mathbb{Z})[X]$ é um domínio fatorial, concluímos que $\overline{g}(X) = X - \overline{\gamma}$ ou $\overline{h}(X) = X - \overline{\gamma}$, e portanto que $g(X) = X - \alpha$ *ou* $h(X) = X - \alpha$ *com* $\alpha \in \mathbb{Z}$ *e* $\alpha \equiv \gamma \, mod \, p$.

■

Exemplo 3.45. Seja $f(X) = X^3 + (1329!)X^2 + 3002X + 12.001 \in \mathbb{Z}[X]$. Olhando módulo 3, temos

$$\overline{f}(X) = X^3 + \overline{2}X + \overline{1} \in (\mathbb{Z}/3\mathbb{Z})[X]$$

Este polinômio $\overline{f}(X)$ é irredutível em $(\mathbb{Z}/3\mathbb{Z})[X]$ pois, se ele fosse redutível em $(\mathbb{Z}/3\mathbb{Z})[X]$, então ele teria um fator de grau 1, logo possuiria uma raiz em $(\mathbb{Z}/3\mathbb{Z})$, o que é absurdo pois $\overline{f}(\overline{0}) = \overline{1} \neq \overline{0}$, $\overline{f}(\overline{1}) = \overline{1} \neq \overline{0}$, $\overline{f}(\overline{2}) = \overline{1} \neq \overline{0}$. Logo pelo item b do teorema anterior temos que f(X) é irredutível em $\mathbb{Z}[X]$.

Exemplo 3.46. Seja $f(X) = X^3 - 15X^2 + 10X - 83 \in \mathbb{Z}[X]$. Olhando módulo 2, temos $\overline{f}(X) = X^3 + X^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$, que é irredutível em $(\mathbb{Z}/2\mathbb{Z})[X]$. Logo $f(X)$ é irredutível em $\mathbb{Z}[X]$.

Exemplo 3.47. O polinômio $f(X) = X^3 - 15X^2 + 10X - 84$ é irredutível em $\mathbb{Z}[X]$.

Basta mostrar que $f(X)$ não tem raízes em $\mathbb{Z}$. Uma raiz em $\mathbb{Z}$ tem que ser um divisor de 84. Como $x^3 - 15x^2 + 10x - 84 = (x^2 + bx + c) \cdot (x + d)$, então o termo independente $c \cdot d = -84$. Assim d divide 84 , portanto, basta verificar que:

$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 7, \pm 12, \pm 14, \pm 21, \pm 28, \pm 42 \text{ e } \pm 84\}$ não são raízes de $f(X)$.

Vamos utilizar o teorema anterior para diminuir o número destas verificações.

Mod $3\mathbb{Z}$, temos

$$\overline{f}(X) = X(X^2 + \overline{1}) \text{ em } (\mathbb{Z}/3\mathbb{Z})[X]$$

e, claramente, $X^2 + \overline{1}$ é irredutível em $(\mathbb{Z}/3\mathbb{Z})[X]$. Logo se α é raiz de $f(X)$ em $\mathbb{Z}$, então $\alpha \equiv 0(mod 3)$. Portanto bastaria verificar que $\pm 3, \pm 6, \pm 12, \pm 21, \pm 42$ e ± 84 não são raízes de $f(X)$.

Queremos limitar ainda mais o número destas verificações. Mod $5\mathbb{Z}$, temos

$$\overline{f}(X) = (X - \overline{4})(X^2 + \overline{4}X + \overline{1}) \text{ em } (\mathbb{Z}/5\mathbb{Z})[X]$$

e, claramente, $X^2 + \overline{4}X + \overline{1}$ é irredutível em $(\mathbb{Z}/5\mathbb{Z})[X]$. Logo se α é raiz em $\mathbb{Z}/5\mathbb{Z}$ de $f(X)$, então $\alpha \equiv 4(mod 5)$. Portanto bastaria verificar que -6,-21 e 84 não são raízes de $f(X)$.

Facilmente verifica-se que os números inteiros negativos β não são raízes de $f(X)$, pois $f(\beta) < 0$. Verifica-se finalmente diretamente que $f(84) \neq 0$. Concluimos então que $f(X)$ é irredutível em $\mathbb{Z}[X]$.

Observação: O método do exemplo anterior foi fazer considerações $(mod p)$, para diversos primos p em $\mathbb{Z}$, acumulando então informações que nos permitiram concluir algo sobre o polinômio original $f(X)$ de $\mathbb{Z}[X]$.

A seguir, estabelecemos um critério que se destaca pela facilidade de seu uso quando se conhece os elementos irredutíveis de um domínio fatorial.

Teorema 3.48. *(Critério de Eisenstein). Sejam D um domínio fatorial e*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in D[X]$$

um polinômio de grau $\geqslant 1$.

Se existe um elemento irredutível $p \in D$ *tal que* $\forall i \leqslant n-1$,

$$\begin{cases} p \nmid a_n \\ p \mid a_i, \\ p^2 \nmid a_0, \end{cases}$$

então f(X) não é o produto de dois fatores de grau $\geqslant 1$ *em D[X] (equivalentemente, o polinômio f(X) é irredutível em K[X], onde K é o corpo de frações de D).*

Demonstração.

Suponha que a afirmação seja falsa, isto é suponha que $f(X) = g(X)h(X)$ com

$$\begin{cases} g(X) = \alpha_s X^s + \cdots + \alpha_1 X + \alpha_0 \in D[X], \alpha_s \neq 0, \\ h(X) = \beta_t X^t + \cdots + \beta_1 X + \beta_0 \in D[X], \beta_t \neq 0, \\ s,t \geqslant 1 (equivalentemente, s,t \leqslant n-1). \end{cases}$$

Temos

$$\begin{cases} a_0 = \alpha_0\beta_0 \\ \\ p \mid a_0, \\ \\ p^2 \nmid a_0, \end{cases} \quad \Longrightarrow \quad \begin{cases} p \mid \alpha_0 \quad e \quad p \nmid \beta_0 \\ ou \\ p \mid \beta_0 \quad e \quad p \nmid \alpha_0. \end{cases}$$

pois D é fatorial

Digamos que seja o caso $p \mid \alpha_0$ e $p \nmid \beta_0$ (o outro caso é análogo à esse). Temos

$$\begin{cases} a_n = \alpha_s\beta_t \\ \\ p \nmid a_n \end{cases} \quad \Longrightarrow p \nmid \alpha_s \; e \; p \nmid \beta_t.$$

Seja α_u, $u \leqslant s \leqslant n-1$, o coeficiente do termo de mais baixo grau de g(X) que p não divida e considere o coeficiente a_u em f(X).

Temos

$$a_u = \underbrace{\alpha_0\beta_u + \alpha_1\beta_{u-1} + \cdots + \alpha_{u-1}\beta_1}_{\text{p divide}} + \underbrace{\alpha_u\beta_0}_{\text{p não divide}}$$

e, portanto, p não divide a_u. Isto contradiz a hipótese que p divide a_i, $\forall_i \leqslant n-1$.

■

Observação. Na demonstração do Teorema 3.48 a hipótese de que D fatorial somente foi usada para concluir que o elemento irredutível $p \in D$ é um elemento primo (ie., se $a, b \in D$ e $p \mid ab$, então $p \mid a$ ou $p \mid b$). O Critério de Eisenstein poderia então ter sido enunciado com as hipóteses de D ser um domínio qualquer e $p \in D$ ser um elemento primo.

Este critério foi elaborado pelo matemático alemão Gotthold Eisensten, estabelecendo uma regra que permite classificar alguns polinômios com coeficientes inteiros como irredutíveis.

O critério de Eisenstein pode ser utilizado em sala de aula para mostrar quando um polinômio com coeficientes inteiros não possui raiz inteira. O método utilizando o Teorema 3.44 não seria para aplicar em sala de aula mas é uma ferramenta interessante para o professor, uma vez que este deve sempre possuir uma fundamentação teórica além do que é repassado aos alunos.

4 CONGRUÊNCIAS POLINOMIAIS

Neste capítulo iremos estudar conceitos envolvendo congruência e polinômios. Apesar do assunto congruência não ser um assunto visto no ensino fundamental e médio, vamos dedicar este capítulo a um conceito mais avançado, aplicando resultados dos capítulos anteriores. Vamos estudar congruência do tipo $f(x) \equiv 0\ (mod\ n)$, $n \in \mathbb{N}$ com $f(x) \in \mathbb{Z}[X]$. O Teorema Chinês do Resto e o Lema de Hensel serão os resultados mais importantes para este capítulo, uma vez que podemos justificar a resolução de uma congruência polinomial com estes resultados.

Teorema 4.1. *Seja $f(x) = a_0 + a_1x + \ldots + a_kx^k$ um polinômio com coeficientes $a_i's$ inteiros. Então vale a implicação $a \equiv b\ (mod\ m) \Longrightarrow f(a) \equiv f(b)\ (mod\ m)$, para quaisquer inteiros a,b.*

Demonstração.

$f(a) - f(b) = (a_0 + a_1a + \ldots + a_ka^k) - (a_0 + a_1b + \ldots + a_kb^k) =$
$a_1(a-b) + a_2(a^2 - b^2) + \ldots + a_k(a^k - b^k)$.

Em vista da fatoração $a^i - b^i = (a^{i-1} + a^{i-2}b + \ldots + b^{i-1}) \cdot (a-b)$, que é válida para qualquer inteiro $i \geq 1$, concluímos que $(a-b) \mid f(a) - f(b)$. Então se $m \mid a-b$, evidentemente $m \mid f(a) - f(b)$.

■

Exemplo 4.2. Seja $a = (72)^6 + (72)^5 + 2$.

Mostraremos que $7 \mid a$

Seja $f(x) = x^6 + x^5 + 2$. Dado o fato que $72 \equiv 2\ (mod\ 7)$, calculemos f(2):

$$f(2) = 2^6 + 2^5 + 2 = 64 + 32 + 2 = 98 = 14 \cdot 7$$

Teorema 4.3. *Sejam $f(x) = a_0 + a_1x + \ldots + a_kx^k$ e $g(x) = b_0 + b_1x + \ldots + b_lx^l$ dois polinômios com coeficientes inteiros. Dados $a, b \in \mathbb{Z}$, vale a implicação*

$$a \equiv b \ (mod\ m) \qquad \Longrightarrow \qquad \begin{cases} f(a)+g(a) \equiv f(b)+g(b) \ (mod\ m) \\ \\ f(a)g(a) \equiv f(b)g(b) \ (mod\ m). \end{cases}$$

Demonstração.

Seja $a \equiv b \ (mod\ m)$. Então, pelo teorema anterior, $f(a) \equiv f(b) \ (mod\ m)$, $g(a) \equiv g(b) \ (mod\ m)$. Como a congruência preserva as operações + e $\cdot$, obtemos

$$f(a)+g(a) \equiv f(b)+g(b) \ (mod\ m), \quad f(a)g(a) \equiv f(b)g(b) \ (mod\ m)$$

■

Teorema 4.4. *Dado um número inteiro a, então a congruência* $ax \equiv 1 \ (mod\ m)$ *admite solução se, e somente se,* $mdc(a,m) = 1$.

Demonstração.

Sejam a,b inteiros. Então $ab \equiv 1 \ (mod\ m)$ equivale a $ab - cm = 1$ para algum inteiro c, ou seja $mdc(a,m) = 1$, então a existência de b está garantida pelo algoritmo Euclideano.

■

Observação: O inverso b de a módulo m, foi determinado módulo m; os outros são todos congruentes entre si. Assim por abuso de linguagem falaremos do inverso de *a mod m* , ou da solução de $ax \equiv 1 \ (mod\ m)$, e o indicaremos por $(\frac{1}{a})_m$ ou $(a^{-1})_m$.

Teorema 4.5. *A congruência* $ax \equiv b \ (mod\ m)$ *é solúvel se, e somente se,* $mdc(a,m) \mid b$. *Quaisquer duas soluções (se existirem) são congruentes módulo m.*

Demonstração.

Seja d o máximo divisor comum de a e m . Se existir uma solução c da congruência $ax \equiv b \ (mod\ m)$, então $m \mid ac - b$, e daí, necessariamente, $d \mid b$. Por outro lado, se $d \mid b$, então resolver $ax \equiv b \ (mod\ m)$ equivale a resolução de $a'x \equiv b' \ (mod\ m')$, onde $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ e $m' = \frac{m}{d}$. Pois, se x_0 fosse uma solução da primeira congruência, ele seria também uma solução da segunda e vice versa. A solução da segunda é $\alpha = (\frac{1}{a'})_{m'}b'$ e é facilmente verificável, e que $x_0 = \alpha$ é uma solução de $ax \equiv b \ (mod\ m)$. Considerando x_0 como solução da congruência solúvel $ax \equiv b \ (mod\ m)$, suas soluções são do tipo: $x \equiv x_0 \ (mod\ m)$ ou escrita de uma maneira equivalente $x = x_0 + tm \ \ com \ \ t \in \mathbb{Z}$.

■

Teorema 4.6. *Seja f(x) um polinômio com coeficientes inteiros. Sejam $r_1, r_2, \ldots, r_k$ uma coleção de inteiros positivos primos entre si e $m = r_1 r_2 \ldots r_k$. Então, resolver $f(x) \equiv 0 \ (mod\ m)$ equivale resolver o sistema simultâneo das congruências $f(x) \equiv 0 \ (mod\ r_i)$, $i = 1, 2, \ldots, k$.*

Demonstração.

Seja x_0 uma solução de $f(x) \equiv 0 \ (mod\ m)$. Então, $m \mid f(x_0)$ e obviamente $r_i \mid f(x_0)$ para todo i; ou seja, $f(x_0) \equiv 0 \ (mod\ r_i)$ para todo i, então $m = m.m.c.(r_1, \ldots, r_k) \mid f(x_0)$, e assim $f(x_0) \equiv 0 \ (mod\ m)$.

■

Exemplo 4.7. Consideremos a congruência $35x \equiv 1 \ (mod\ 51)$.

Tendo em vista que $51 = 3 \cdot 17$, então pelo teorema anterior basta-nos resolver o sistema simultâneo,

$$35x \equiv 1 \ (mod\ 3),\ 35x \equiv 1 \ (mod\ 17).$$

Estes em si reduzem-se a $x \equiv -1 \ (mod\ 3)$ e $x \equiv 1 \ (mod\ 17)$.

As soluções da primeira congruência são $x_0 = -1 + 3k$ para qualquer inteiro k, e dessas procuramos aquelas que satisfazem a segunda congruência. Logo, k deve satisfazer

$-1 + 3k \equiv 1 \ (mod\ 17)$, i.e, $3k \equiv 2 \ (mod\ 17)$.

Dado o fato que $(\frac{1}{3})_{17} = 6$, obtemos $k_0 = 2 \cdot (\frac{1}{3})_{17} = 12$ que é uma solução da última congruência. Então $x_0 = -1 + 3k_0 = 35$ é uma solução da congruência original.

Sejam, $r_1, r_2, \ldots, r_k$ uma coleção de inteiros positivos primos entre si e seja $m = r_1 r_2 \ldots r_k$. Para cada i, $mdc(\frac{m}{r_i}, r_i) = 1$ e, portanto, $((\frac{m}{r_i})^{-1})_{r_i}$ existe. Para cada i, escolhamos o menor inverso positivo e denotaremos $((\frac{m}{r_i})^{-1})_{r_i} \cdot \frac{m}{r_i}$ por ε_i.

Evidentemente, $\varepsilon_i \equiv 1 \ (mod\ r_i)$ e $\varepsilon_i \equiv 0 \ (mod\ r_j)$ *se* $i \neq j$. Os inteiros $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$ satisfazem as seguintes propriedades de "ortogonalidade"

Teorema 4.8. *(i)* $\varepsilon_i \varepsilon_j \equiv 0 \ (mod\ m) \Longleftrightarrow i \neq j$.

(ii) $\sum_{i=1}^{k} a_i \varepsilon_i \equiv \sum_{i=1}^{k} b_i \varepsilon_i \ (mod\ m) \Longleftrightarrow a_i \equiv b_i \ (mod\ r_i)$ *para todo i*;

(iii) $\sum_{i=1}^{k} \varepsilon_i \equiv 1 \ (mod\ m)$.

Demonstração

A demonstração é de fácil verificação utilizando as definições de ε_i e congruência.

■

Teorema 4.9 (Teorema Chinês do Resto)**.** *Sejam $a_1, a_2, \ldots, a_k$ uma coleção de inteiros. O sistema simultâneo de equações $x \equiv a_i \ (mod\ r_i)$, $i = 1, 2, \ldots, k$ tem a solução $x_0 = \sum_{i=1}^{k} a_i \varepsilon_i$. Além do mais, todas as soluções são congruentes entre si módulo m.*

Demonstração.

Para cada j , tendo em vista que $\varepsilon_j \equiv 1 \ (mod\ r_j)$, $x_0 \varepsilon_j \equiv x_0 \ (mod\ r_j)$. Por outro lado, $x_0 \varepsilon_j = \sum_{i=1}^{k} a_i \varepsilon_i \varepsilon_j \equiv a_j \varepsilon_j^2 \ (mod\ m)$ (ii). Então, para cada j, $x_0 \equiv x_0 \varepsilon_j \equiv a_j \ (mod\ r_j)$.
A última afirmação é uma simples aplicação da parte (ii) do teorema anterior.

■

Exemplo 4.10. Se de uma cesta com ovos retirarmos três unidades por vez, sobra um ovo. O mesmo acontece se os ovos são retirados 4 a 4 ou 5 a 5. Mas não resta nenhum ovo se retirarmos 7 unidades por vez. Encontrar o menor número possível de ovos.

Sejam:

$$\begin{cases} x \equiv 1 \ mod\ 3 \\ x \equiv 1 \ mod\ 4 \\ x \equiv 1 \ mod\ 5 \\ x \equiv 0 \ mod\ 7 \end{cases}$$

$a_i = 1 \quad e \quad i = 1, 2, 3 \ e \ a_4 = 0$

$r_1 = 3, \quad r_2 = 4, \quad r_3 = 5, \quad r_4 = 7$

$x_0 = \sum a_i \varepsilon_i = 1 \cdot \varepsilon_1 + 1 \cdot \varepsilon_2 + 1 \cdot \varepsilon_3 + 0 \cdot \varepsilon_4$

$m = 3 \cdot 4 \cdot 5 \cdot 7$

$m_1 = 140$

$m_2 = 105$

$m_3 = 84$

$m_4 = 60$

$\varepsilon_i = ((\frac{m}{r_i})^{-1})_{r_i} \cdot \frac{m}{r_i}$

$\varepsilon_1 = ((140)^{-1})_3 \cdot 140 = 2 \cdot 140 = 280$

$\varepsilon_2 = ((105)^{-1})_4 \cdot 105 = 1 \cdot 105 = 105$

$\varepsilon_3 = ((84)^{-1})_5 \cdot 84 = 4 \cdot 84 = 336$

$\varepsilon_4 = ((60)^{-1})_7 \cdot 60 = 2 \cdot 60 = 120$

Logo: $x_0 = 280 + 105 + 336 = 721 \equiv 301 \ (mod\ 420)$, que é solução do sistema de congruência.

Teorema 4.11. *Seja f(x) um polinômio com coeficientes inteiros. Para cada* $i, 1 \leq i \leq k$, *seja* a_i *uma solução de* $f(x) \equiv 0 \ (mod\ r_i)$. *Então* $x_o = \sum_{i=1}^{k} a_i \varepsilon_i$ *é uma solução de* $f(x) \equiv 0 \ (mod\ m)$.

Demonstração.

O Teorema Chinês do Resto afirma que $x_0 \equiv a_i \ (mod\ r_i)$ para todo i. Daí,
$f(x_0) \equiv f(a_i) \equiv 0 \ (mod\ r_i)$ para todo i. Como $r_i \mid f(x_0)$ para $i = 1, 2, \ldots, k$,
m = m.m.c. $(r_1, r_2, \ldots, r_k) \mid f(x_0)$; ou seja, $f(x_0) \equiv 0 \ (mod\ m)$

■

Corolário 4.12. *Sejam f(x) um polinômio com coeficientes inteiros, e m um inteiro positivo tendo a fatoração canônica* $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. *Então,* $f(x_0) \equiv 0 \ (mod\ m)$ *tem solução, se e somente se,* $f(x_0) \equiv 0 \ (mod\ p_i^{\alpha_i})$ *tem solução para cada i.*

Exemplo 4.13. Encontrar todas as soluções de $f(x) = x^2 + 5x + 9 \equiv 0 \ (mod\ 15)$. Consideremos o sistema

$f(x) \equiv x^2 - x \equiv 0 \ (mod\ 3)$

$f(x) \equiv x^2 - 1 \equiv 0 \ (mod\ 5)$

As soluções não congruentes módulo 3 da primeira são $a_1 = 0$, $a_2 = 1$ e da segunda que são não congruentes módulo 5, $b_1 = -1$, $b_2 = 1$.

Então pelo Teorema Chinês do Resto, $f(x) \equiv 0 \ (mod\ 15)$ admite quatro soluções não congruentes módulo 15. Elas são

$c_{ij} = (\frac{1}{5})_3 \cdot 5 \cdot a_i + (\frac{1}{3})_5 \cdot 3 \cdot b_j \; i,j = 1,2$. Logo, $c_{11} = -6,\ c_{12} = 6,\ c_{21} = 4,\ c_{22} = 16$.

4.1 CONGRUÊNCIAS DE GRAUS GERAIS (MÉTODOS DE REDUÇÃO)

Sejam $m \in \mathbb{Z}, m > 0$ *e* $f(X) \in \mathbb{Z}[X]$. Estamos interessados em encontrar valores de X $(mod\ m)$ que satisfazem a congruência polinomial $f(X) \equiv 0\ (mod\ m)$. Pelo colorário 4.12 podemos reduzir nosso estudo ao caso $m = p^\alpha$, isto é quando m é potência de primo.

A resolução de $f(x) \equiv 0\ (mod\ p^\alpha)$ onde $\alpha \geq 2$, pode ser reduzida à de $f(x) \equiv 0\ (mod\ p)$. Aliás, tendo em vista que $f(x) \equiv 0\ (mod\ p^\alpha)$ implica em $f(x) \equiv 0\ (mod\ p^{\alpha-1})$, o método para achar as soluções da primeira seria encontrar as soluções $a_1, a_2, \ldots, a_s$, não congruentes módulo $p^{\alpha-1}$, da segunda e depois voltar para a primeira e testar $x = a_i + tp^{\alpha-1}$ onde $0 \leq t \leq p$.

Então o método geral consiste na construção a partir das soluções de $f(x) \equiv 0 (mod p)$ as de $f(x) \equiv 0\ (mod\ p^2)$, e com essas subir gradativamente até chegar as de $f(x) \equiv 0\ (\ mod p^\alpha)$. Esta subida será facilitada pelos resultados seguintes.

Seja $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_kx^k$ um polinômio com coeficientes inteiros. Consideremos $f(x+y)$.

$$f(x+y) = a_0 + a_1(x+y) + a_2(x+y)^2 + a_3(x+y)^3 \ldots + a_k(x+y)^k$$

$$= a_0 + a_1(x+y) + a_2(x^2 + 2xy + y^2) + a_3(x^3 + 3x^2y + 3xy^2 + y^3) + \ldots$$

$$= a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots$$

$$+y(a_1 + 2a_2x + 3a_3x^2 + \ldots)$$

$$+y^2(a_2 + 3a_3x + \ldots) + y^3(a_3 + \ldots) + \ldots$$

Esta expansão sugere que

$$f(x+y) = f(x) + yf'(x) + y^2\frac{f''(x)}{2!} + y^3\frac{f^{(3)}(x)}{3!} + \ldots$$

que nada mais é que a expansão de Taylor!

Teorema 4.14. *Se f(x) é um polinômio com coeficientes inteiros então* $f(x+y) = f(x) + yf'(x) + \ldots + y^i\frac{f^{(i)}(x)}{i!} + \ldots + y^k\frac{f^{(k)}(x)}{k!}$ *e, para cada i,* $\frac{f^{(i)}(x)}{i!}$ *é um polinômio com coeficientes inteiros.*

Lema 4.15 (Lema de Hensel)**.** *Seja p um número primo ,* $f(x) \in \mathbb{Z}[x]$, *e* $m, a \in \mathbb{Z}$ *tais que* $m > 0$ *e* $f(a) \equiv 0\ (mod\ p^m)$. *Então:*

1) se $f'(a) \not\equiv 0\ (mod\ p)$ *e* $f(a) \not\equiv 0\ (mod\ p^{m+1})$, *então existe um único inteiro t tal que* $1 \leq$

$t \leq p-1$ *e* $f(a+tp^m) \equiv 0 \ (mod\ p^{m+1})$. *Especificamente, t é determinado pela equação* $tf'(a) \equiv -\dfrac{f(a)}{p^m} \ (mod\ p)$;

2) *Se* $f'(a) \equiv 0 \ (mod\ p)$ *e* $f(a) \equiv 0 \ (mod\ p^{m+1})$, *então para todo t tal que* $1 \leq t \leq p-1$, $f(a+tp^m) \equiv 0 \ (mod\ p^{m+1})$;

3) *Se* $f'(a) \equiv 0 \ (mod\ p)$ *e* $f(a) \not\equiv 0 \ (mod\ p^{m+1})$, *então não existe* $1 \leq t \leq p-1$ *tal que* $f(a+tp^m) \equiv 0 \ (mod\ p^{m+1})$.

Demonstração:

Observe inicialmente que se $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, então, para qualquer inteiro t temos

$$f(x+tp^m) \equiv f(x) + tp^m f'(x) \ (\text{mod } p^{m+1}).$$

Vamos analisar cada um dos casos:

1) Seja a um inteiro tal que $f(a) \equiv 0 \ (\text{mod } p^m)$ e $f(a) \not\equiv 0 \ (\text{mod } p^{m+1})$. Isto implica que $p^m \mid f(a)$ e $\dfrac{f(a)}{p^m} \not\equiv 0 \ (\text{mod } p)$. Como $f'(a) \not\equiv 0 \ (\text{mod } p)$, então existe um único t, módulo p, tal que $tf'(a) + \dfrac{f(a)}{p^m} \equiv 0 \ (\text{mod } p)$, ou seja, $tf'(a) = -\dfrac{f(a)}{p^m} + kp$, para algum inteiro k. Assim,

$$\begin{aligned} f(a+tp^m) \equiv f(a) + tp^m f'(a) &= f(a) + p^m \left(-\frac{f(a)}{p^m} + kp \right) \\ &= f(a) - f(a) + kp^{m+1} \equiv 0 \ (\text{mod } p^{m+1}). \end{aligned}$$

Portanto, existe exatamente um único $a' (\text{mod } p^{m+1})$ tal que $f(a') \equiv 0 \ (\text{mod } p^{m+1})$ e $a' \equiv a \ (\text{mod } p^m)$, isto é, $a' \equiv a + tp^m (\text{mod } p^{m+1})$. Além disso, $t \equiv -\dfrac{f(a)}{p^m} (f'(a))^{-1} \ (\text{mod } p)$.

2) Suponha agora $f'(a) \equiv 0 \ (\text{mod } p)$ e $f(a) \equiv 0 \ (\text{mod } p^{m+1})$. Assim $f'(a) = kp$, e agora, para qualquer inteiro t temos

$$f(a+tp^m) \equiv f(a) + tp^m f'(a) = f(a) + tkp^{m+1} = f(a) \equiv 0 \ (\text{mod } p^{m+1}).$$

Portanto, existem p elementos $a' \ (\text{mod } p^{m+1})$ tais que $f(a') \equiv 0 \ (\text{mod } p^{m+1})$ e $a' \equiv a \ (\text{mod } p^m)$.

3) Se $f'(a) \equiv 0 \pmod{p}$ e $f(a) \not\equiv 0 \pmod{p^{m+1}}$, então $f'(a) = kp$ e para qualquer inteiro t temos

$$f(a+tp^m) \equiv f(a)+tp^m f'(a) = f(a)+tkp^{m+1} = f(a) \not\equiv 0 \pmod{p^{m+1}}.$$

Portanto, não existe a' tal que $f(a') \equiv 0 \pmod{p^{m+1}}$ e $a' \equiv a \pmod{p^m}$. ■

Observação: Pelo item 2) do Lema de Hensel, numa congruência polinomial, o número de soluções pode ser maior que o grau do polinômio, caso a congruência polinomial seja módulo um número composto. No caso módulo p, com p primo, o Teorema de Lagrange garante que o número de soluções é no máximo igual ao grau do polinômio.

Teorema 4.16. *Seja* $f(a) \equiv 0 \ (mod\ p^\beta)$. *Então para* $a' = a + tp^\beta$, $f(a') \equiv 0 \ (mod\ p^{\beta+1}) \Longleftrightarrow tf'(a) \equiv -\frac{f(a)}{p^\beta} \ (mod\ p)$

$$\Longleftrightarrow \quad \begin{cases} f'(a) \equiv \frac{f(a)}{p^\beta} \equiv 0 \ (mod\ p) \\ ou \\ (f'(a), p) = 1. \end{cases}$$

Demonstração.

Seja $a' = a + tp^\beta$, onde t será determinado para que $f(a') \equiv 0 \ (mod\ p^{\beta+1})$. Pela expansão de Taylor,

$$f(a') = f(a+tp^\beta) = f(a) + (tp^\beta)f'(a) + (tp^\beta)^2\frac{f''(a)}{2!} + \ldots$$

Então, de $f(a') \equiv 0 \ (mod\ p^{\beta+1})$, obtem-se $0 \equiv f(a) + (tp^\beta)f'(a) \ (mod\ p^{\beta+1})$.

Tendo em vista que $p^\beta \mid f(a)$, esta congruência pode ser posta na forma

$tf'(a) \equiv -\frac{f(a)}{p^\beta} \ (mod\ p)$, e ela possui soluções se e somente se
$(f'(a), p) = 1$ *ou*, $p \mid f'(a)$ e $p \mid \frac{f(a)}{p^\beta}$.

■

Exemplo 4.17. Seja $f(x) = x^2 + 5x - 9$; então, $f'(x) = 2x + 5$.

Desejamos encontrar todas as soluções de $f(x) \equiv 0 \ (mod\ 25)$.

As soluções de $f(x) \equiv x^2 + 1 \equiv 0 \ (mod\ 5)$ são $x \equiv \pm 2 \ (mod\ 5)$.

Sejam $a_1 = -2$, $a_2 = 2$. Então, $f(a_1) = -15$, $f(a_2) = 5$, $f'(a_1) = 1$, $f'(a_2) = 9$.

Resolvemos

$$t_1 f'(a_1) \equiv -\frac{f(a_1)}{5} \ (mod\ 5)$$

$$t_2 f'(a_2) \equiv -\frac{f(a_2)}{5} \ (mod\ 5)$$

Então, $t_1 \equiv 3$ *e* $t_2 \equiv 1\ (mod\ 5)$; daí as soluções de $f(x) \equiv 0\ (mod\ 5^2)$ são congruentes com $a_1' = -2+3\cdot 5 = 13,\ a_2' = 2+5 = 7,$ módulo 25.

Exemplo 4.18. Seja $f(X) = X^3 + 3X^2 + 23$ e consideremos a congruência
$f(X) \equiv 0\ (mod\ 3\times 5^2)$

(i) Primeiramente vamos calcular as soluções de $f(X) \equiv 0\ (mod\ 3)$ e de $f(X) \equiv 0\ (mod\ 5)$. Por tentativas obtemos $X \equiv 1\ (mod\ 3)$ e $X \equiv 4\ (mod\ 5)$, respectivamente;

(ii) Para calcular as soluções de $f(X) \equiv 0\ (mod\ 5^2)$ precisamos encontrar os valores de t tais que $f(4+5t) \equiv 0\ (mod\ 5^2)$.

Temos:

$f(4+5t) \equiv 0\ (mod\ 5^2)$

$(4+5t)^3 + 3(4+5t)^2 + 23 \equiv 0\ (mod\ 5^2)$

$4^3 + (3\cdot 4^2\cdot 5t) + 3(4^2 + 2\cdot 4\cdot 5t) + 23 \equiv 0\ (mod\ 5^2)$

$10t + 10 \equiv 0\ (mod\ 5^2)$

$2t + 2 \equiv 0\ (mod\ 5)$

$t \equiv 4\ (mod\ 5)$

$t = 4+5k,\ para\ algum\ k \in \mathbb{Z}$

As soluções de $f(X) \equiv 0\ (mod\ 5^2)$ são $X = 4+5t = 4+5(4+5k) = 24+25k$, ou seja, $X \equiv 24\ (mod\ 25)$

(iii) As soluções de $f(X) \equiv 0\ (mod\ 3\times 5^2)$ são as soluções do sistema

$$\begin{cases} X \equiv 1\ (mod\ 3) \\ X \equiv 24\ (mod\ 25) \end{cases}$$

Pelo Teorema Chinês do Resto, este sistema admite uma única solução módulo 3×5^2. Feitos os cálculos obtemos: $X \equiv 49\ (mod\ 3\times 25)$.

Exemplo 4.19. Seja $f(X) = X^4 - 11X^3 + 26X^2 - 22X + 123$ e consideremos a congruência $f(X) \equiv 0 \ (mod\ 13 \times 5^3)$

Utilizando o mesmo processo que no exemplo anterior.

(i) As soluções de $f(X) \equiv 0 \ (mod\ 13)$ e de $f(X) \equiv 0 \ (mod\ 5)$ são respectivamente $X \equiv 1 \ (mod\ 13)$ e $X \equiv 3 \ (mod\ 5)$;

(ii) Para calcular as soluções de $f(X) \equiv 0 \ (mod\ 5^2)$, procuraremos valores de t tais que $f(3+5t) \equiv 0 \ (mod\ 5^2)$

Assim,

$f(3+5t) \equiv 0 \ (mod\ 5^2) \iff$
$(3+5t)^4 - 11(3+5t)^3 + 26(3+5t)^2 - 22(3+5t) + 123 \equiv 0 \ (mod\ 5^2)$

$\iff (3^4 + 4 \times 3^3 \times 5t) - 11(3^3 + 3 \times 3^2 \times 5t) + 26(3^2 + 2 \times 3 \times 5t) - 22(3+5t) + 123 \equiv 0 \ (mod\ 5^2)$

$\iff -275t + 75 \equiv 0 \ (mod\ 5^2)$

$\iff 0 \equiv 0 \ (mod\ 25)$

Temos assim, que t é qualquer e portanto existem 5 soluções incongruentes módulo 25: 3,8,13,18 e 23;

(iii) Para o cálculo das soluções de $f(X) \equiv 0 (mod 5^3)$ precisamos resolver 5 congruências:

- $f(3+5^2t) \equiv 0 \ (mod\ 5^3)$;
- $f(8+5^2t) \equiv 0 \ (mod\ 5^3)$;
- $f(13+5^2t) \equiv 0 \ (mod\ 5^3)$;
- $f(18+5^2t) \equiv 0 \ (mod\ 5^3)$;
- $f(23+5^2t) \equiv 0 \ (mod\ 5^3)$.

Desenvolvendo e simplificando obtemos,

- $3+70t \equiv 0 \ (mod\ 5)$, que não tem solução;
- $3+80t \equiv 0 \ (mod\ 5)$, que não tem solução;
- $95-10t \equiv 0 \ (mod\ 5)$, qualquer valor de t é solução;
- $84+50t \equiv 0 \ (mod\ 5)$, que não tem solução;
- $0+10t \equiv 0 \ (mod\ 5)$, qualquer valor de t é solução;

Assim as soluções da congruência $f(X) \equiv 0 \ (mod\ 125)$ são: $13+25s$ com $s \in \{0,1,2,3,4\}$ e $23+25t$ *com* $t \in \{0,1,2,3,4\}$;

(iiii) O método para encontrar as soluções de $f(X) \equiv 0(mod 13 \times 5^3)$ é o seguinte: para cada solução a da congruência $f(X) \equiv 0\ (mod\ 5^3)$, e cada solução b da congruência $f(X) \equiv 0\ (mod\ 13)$, resolveremos o sistema

$$\begin{cases} X \equiv a\ (mod\ 5^3) \\ X \equiv b\ (mod\ 13). \end{cases}$$

Ficamos assim com 10 sistemas para resolver. Pelo Teorema Chinês dos restos cada um deles tem uma única solução módulo 13×5^3. Feitas as contas, as 10 soluções são: 248, 313, 573, 638, 898, 963, 1223, 1288, 1548 e 1613.

Embora não tenhamos meios de resolver $f(x) \equiv 0\ (mod\ p)$ para um polinômio f de grau geral, é ainda possível reduzir f para um outro de grau menor que p.

Teorema 4.20. *Seja p um primo. Então todo inteiro satisfaz a congruência* $x^p \equiv x\ (mod\ p)$

Demonstração.

O que temos aqui nada mais é que a variação do Teorema de Fermat.

Corolário 4.21. *Seja p um primo. Dado um polinômio* $f(x)$ *com coeficientes inteiros, existe* $g(x)$ *um polinômio com coeficientes inteiros e de grau menor que p tal que*

$f(a) \equiv g(a)\ (mod\ p)$ *para qualquer inteiro a.*

Demonstração.

Pelo teorema anterior, $x^p \cdot x^i = x^{p+i} \equiv x \cdot x^i = x^{i+1}\ (mod\ p)$

está satisfeita para todos os inteiros. Então g(x) obtem-se trocando x^{p+i} *por* x^{i+1}no polinômio $f(x)$.

■

Exemplo 4.22. Seja $p = 5$ e $f(x) = 2x^7 + x^6 + 3x^3 + 1$. Então a congruência

$$\begin{aligned} f(x) &\equiv 2x^3 + x^2 + 3x^3 + 1 \\ &\equiv 5x^3 + x^2 + 1 \equiv x^2 + 1\ (mod\ 5) \end{aligned}$$

Está satisfeita para todos os inteiros.

Os próximos dois resultados serão utilizados para a demonstração do Teorema de Lagrange, nosso último resultado.

Teorema 4.23. *Sejam a, b inteiros positivos e mdc* $(a,b) = d$. *Se d não divide c então a equação* $a \cdot x + b \cdot y = c$ *não possui nenhuma solução inteira. Se* $d \mid c$ *ela possui infinitas soluções e se* $x = x_0$ *e* $y = y_0$ *é uma solução particular então todas as soluções são dadas por;*

$x = x_0 + (\frac{b}{d}) \cdot k$

$y = y_0 - (\frac{a}{d}) \cdot k$

Onde k é um inteiro.

Demonstração.

Se d não divide c, então a equação $a \cdot x + b \cdot y = c$ não possui solução, pois como o $mdc(a,b) = d$ implica que $d \mid a$ e $d \mid b$. Assim d deveria dividir c, já que c está escrito como combinação linear de a e b.

Suponha que $d \mid c$ pelo Teorema de Bezout existem inteiros n_0 *e* m_0 tais que

$$a \cdot n_0 + b \cdot m_0 = d$$

De $d \mid c$ existe um inteiro k tal que $c = k \cdot d$. Multiplicando ambos os membros da igualdade acima por k obtemos:

$$a \cdot (n_0 \cdot k) + b \cdot (m_0 \cdot k) = k \cdot d = c$$

Assim o par (x_0, y_0), sendo $x_0 = n_0 k$ *e* $y_0 = m_0 k$ é uma solução de $a \cdot x + b \cdot y = c$. Note que é fácil verificar que os pares da solução da equação $a \cdot x + b \cdot y = c$ são da forma

$$x = x_0 + (\frac{b}{d}) \cdot k$$

$$y = y_0 - (\frac{a}{d}) \cdot k$$

Veja que

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

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

$= a \cdot x_0 + b \cdot y_0$

Note que acabamos de mostrar que a partir de uma solução particular (x_0, y_0) podemos gerar

infinitas soluções.

Agora só basta mostrar que toda solução da equação $a \cdot x + b \cdot y = c$ é da forma

$$x = x_0 + (\frac{b}{d}) \cdot k$$

$$y = y_0 - (\frac{a}{d}) \cdot k$$

Vamos supor que (x,y) é a solução de $a \cdot x + b \cdot y = c$ *e ainda* (x_0, y_0) é uma solução particular $a \cdot x_0 + b \cdot y_0 = c$. Subtraindo as duas últimas igualdades temos:

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

O que implica em $a \cdot (x - x_0) = -b \cdot (y - y_0)$. Como o $mdc\ (a,b) = d$ podemos escrever

que mdc $(\frac{a}{d}, \frac{b}{d}) = 1$. Dividindo a igualdade acima por d.

$\frac{a}{d} \cdot (x - x_0) = -\frac{b}{d} \cdot (y - y_0) \Rightarrow \frac{b}{d} \mid \frac{a}{d} \cdot (x - x_0)$

Usando o Lema de Euclides $\frac{b}{d} \mid (x - x_0)$, portanto existe um k inteiro tal que;

$$x - x_0 = k \cdot \frac{b}{d} \Rightarrow x = x_0 + \frac{b}{d} \cdot k.$$

Substituindo x na equação acima obtemos;

$$y = y_0 - \frac{b}{d} \cdot k$$

■

Proposição 4.24. *Sejam a, b, m inteiros tais que* $m > 0$ *e* $mdc(a,m) = d$. *No caso em que d não divide b a congruência* $a \cdot x \equiv b \bmod m$ *não possui nenhuma solução e quando d divide b possui exatamente d solução incongruente módulo m.*

Demonstração.

Sabemos que o inteiro x é solução de $a \cdot x \equiv b \bmod m$ se, e somente se, existe um inteiro y tal que $a \cdot x = b + m \cdot y$, ou seja, $a \cdot x - m \cdot y = b$. Sabemos que de acordo o Teorema 4.23 esta equação não possui nenhuma solução caso d não divide b e se $d \mid b$ então a dita equação possui infinitas soluções dadas por:

$$x = x_0 - (\frac{m}{d}) \cdot k$$

$$y = y_0 - (\frac{a}{d}) \cdot k$$

onde (x_0, y_0) é uma solução particular de $a \cdot x - m \cdot y = b$. Assim a congruência $a \cdot x \equiv b \ mod \ m$ possuem infinitas soluções dadas por

$$x = x_0 - (\frac{m}{d}) \cdot k$$

Estamos interessados em saber o número de soluções incongruentes. Tome x_1, x_2 soluções congruente módulo m. Então $x_1 = x_0 - (\frac{m}{d}) \cdot k_1 \equiv x_0 - (\frac{m}{d}) \cdot k_2 = x_2 \ mod \ m$. O que implica $(\frac{m}{d}) \cdot k_1 \equiv (\frac{m}{d}) \cdot k_2 \ mod \ m$. E como $(\frac{m}{d}) \mid m \ e \ ((\frac{m}{d}), m) = \frac{m}{d}$ temos pela lei do cancelamento que:

$k_1 \equiv k_2 \ mod \ m$

Assim concluímos que as soluções incongruentes serão obtidas ao tomarmos

$x = x_0 - (\frac{m}{d}) \cdot k$, com k englobando todos os restos possíveis na divisão por d.

■

Vamos finalizar este capítulo com o Teorema de Lagrange que nos diz quantas raízes podemos ter numa equação do tipo $f(x) \equiv 0 \ (mod p)$

Teorema 4.25 (Lagrange)**.** *Se p é primo e f é um polinômio de grau m com coeficientes inteiros, a congruência $f(x) \equiv 0 \ (mod \ p)$ admite no máximo m soluções.*

Demonstração.

A demonstração deste resultado pode ser feita por indução no grau m do polinômio f. De fato, quando $m = 1$ obtém-se uma congruência do tipo $ax \equiv b \ mod \ p$, a qual, como sabemos, admite soluções se e só se $mdc(a, p) = 1$. Neste caso, de acordo com a Proposição 4.24 existe uma única solução, e portanto o resultado verifica-se trivialmente. Supondo então que este resultado é válido para qualquer polinômio de grau menor que m, e que a congruência $f(x) \equiv 0 \ mod \ p$ admite pelo menos uma solução, digamos a, podemos escrever a referida congruência na forma

$f(x) \equiv (x - a)g(x) \ mod \ p$,

onde g denota um polinômio de grau $m-1$ com coeficientes inteiros. Ora, naturalmente, todas as soluções de $f(x) \equiv 0 \, mod \, p$ incongruentes módulo p com a são obrigatoriamente também soluções de $g(x) \; mod \; p$. No entanto, esta última congruência tem, necessariamente, grau maior ou igual a 1 e menor ou igual a $m-1$. Assim, aplicando a hipótese de indução conclui-se que esta admite no máximo $m-1$ soluções, o que, como a é raiz de $f(x) \equiv 0 \, mod \, p$, implica naturalmente que $f(x) \equiv 0 \, mod \, p$ tem, no máximo, m soluções.

■

5 CONCLUSÃO

O trabalho buscou ajudar professores no que diz respeito aos polinômios.

O trabalho auxilia no caráter de verificar alguns critérios de decomposição de um polinômio em fatores irredutíveis, influencia no desenvolvimento de equações polinomiais, no teorema do resto, aborda os principais conceitos envolvidos no ensino médio quanto ao tópico de polinômios de uma maneira ou de outra já que observa o polinômio como elemento de um anel, no caso, um anel de polinômio. Já para acadêmicos de matemática o trabalho visa uma leitura que pode aprofundar conceitos de anel de polinômios dentre outros conceitos que são abordados para que a leitura fique ainda mais rica e aprofundada nos alicerces que geram a fatoração de um polinômio.

As congruências entram no papel de explorar os critérios de divisibilidade de números inteiros com uma forma distinta de observação.

São vistos teoremas clássicos, lembrando que há um capítulo inteiro de congruências polinomiais, ou seja, o trabalho avança para conceitos que podem até não ser vistos na graduação talvez só na pós-graduação.

REFERÊNCIAS

FILHO, E.de A. ***Teoria Elementar dos Números.*** *3.ed.São Paulo: Editora Nobel,1985.*

FONSECA, R.V. ***Introdução à Teoria dos Números.*** *Belém: Universidade do Estado do Pará,2011.*

GONÇALVES, A. ***Introdução à Álgebra.*** *4. ed. Rio de Janeiro: Instituto de Matemática Pura e aplicada, 1999. (Projeto Euclides, CPM13).*

HEFEZ, A. ***Elementos de Aritmética.*** *2. ed. Rio de Janeiro: Instituto de Matemática Pura e aplicada, 2011. (Coleção do Professor de matemática, CPM13).*

IEZZI, G. ***Fundamentos da Matemática Elementar.*** *2. ed. São Paulo: Editora Atual, 1977.*

IEZZI,G. e HYGINO H. D. ***Álgebra Moderna.*** *4. ed. São Paulo: Editora Atual, 2003.*

LEQUAIN, Y. e GARCIA, A. ***Elementos de Álgebra.*** *1. ed. Rio de Janeiro: Instituto de Matemática Pura e aplicada, 2002. (Projeto Euclides, CPM13).*

LIMA, E.L. ***Análise Real*** *8. ed. Rio de Janeiro: Instituto de Matemática Pura e aplicada, 2006. (Coleção Matemática Universitária, v.1).*

MONTEIRO, L. ***Elementos de Álgebra, Elementos de Matemática.*** *4. ed. Rio de Janeiro: Instituto de Matemática Pura e aplicada, 1969.*

SIDKI, S. ***Introdução à Teoria dos Números.*** *Rio de Janeiro: Instituto de Matemática Pura e aplicada, 1975.*