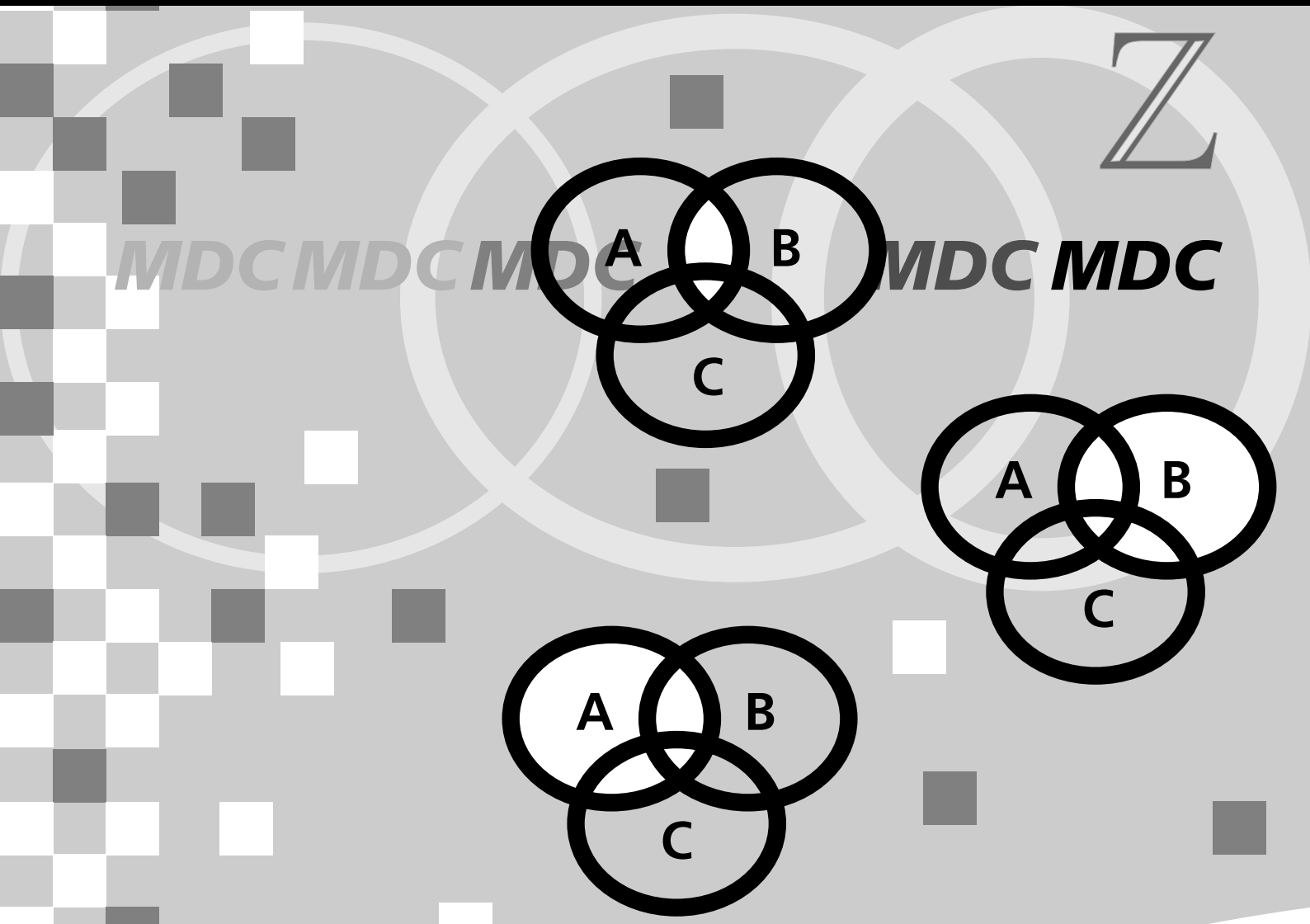
Módulo 2

Volume | 2

Adilson Gonçalves
Luiz Manoel Figueiredo

Álgebra I



Fundação CECIERJ
Consórcio cederj

Fundação CECIERJ

Consórcio cederj

Centro de Educação Superior a Distância do Estado do Rio de Janeiro

Álgebra I

Volume 2 - Módulo 2

Adilson Gonçalves

Luiz Manoel Figueiredo

GOVERNO DO Rio de Janeiro

SECRETARIA DE CIÊNCIA E TECNOLOGIA

UAB UNIVERSIDADE ABERTA DO BRASIL

Ministério da Educação

BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

Apoio:

FAPERJ Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro

Fundação Cecierj / Consórcio Cederj

Rua Visconde de Niterói, 1364 – Mangueira – Rio de Janeiro, RJ – CEP 20943-001
Tel.: (21) 2334-1569 Fax: (21) 2568-0725

Presidente
Masako Oya Masuda

Vice-presidente
Mirian Crapez

Coordenação do Curso de Matemática
UFF - Regina Moreth
UNIRIO - Luiz Pedro San Gil Jutuca

Material Didático

ELABORAÇÃO DE CONTEÚDO
Adilson Gonçalves
Luiz Manoel Figueiredo

COORDENAÇÃO DE DESENVOLVIMENTO INSTRUCIONAL
Cristine Costa Barreto

Departamento de Produção

EDITORA
Tereza Queiroz

COORDENAÇÃO EDITORIAL
Jane Castellani

COORDENAÇÃO DE PRODUÇÃO
Jorge Moura

CAPA
Eduardo Bordoni

PRODUÇÃO GRÁFICA
Oséias Ferraz
Patricia Seabra

G635a
Gonçalves, Adilson.
Álgebra I. v.2 / Adilson Gonçalves. – Rio de Janeiro: Fundação CECIERJ, 2010.
60p.; 21 x 29,7 cm.

ISBN: 85-7648-135-9

1. Ideais. 2. Números primos. 3. Teorema Fundamental da Álgebra. 4. Congruência. 5. Anéis. I. Figueiredo, Luiz Manoel. II. Título.

CDD:512

2010/1

Referências Bibliográficas e catalogação na fonte, de acordo com as normas da ABNT.

Governo do Estado do Rio de Janeiro

Governador
Sérgio Cabral Filho

Secretário de Estado de Ciência e Tecnologia
Alexandre Cardoso

Universidades Consorciadas

UENF - UNIVERSIDADE ESTADUAL DO NORTE FLUMINENSE DARCY RIBEIRO
Reitor: Almy Junior Cordeiro de Carvalho

UERJ - UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
Reitor: Ricardo Vieiralves

UFF - UNIVERSIDADE FEDERAL FLUMINENSE
Reitor: Roberto de Souza Salles

UFRJ - UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
Reitor: Aloísio Teixeira

UFRRJ - UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
Reitor: Ricardo Motta Miranda

UNIRIO - UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
Reitora: Malvina Tania Tuttman

SUMÁRIO

Aula 7 – Ideais maximais e números primos

Metas

Nesta aula definiremos ideais maximais e mostraremos como os números primos estão relacionados com os ideais maximais de $\mathbb{Z}$.

Objetivos

Ao final desta aula você deverá ser capaz de:

- Definir ideais maximais de $\mathbb{Z}$.
- Mostrar que os números primos são os geradores dos ideais maximais em $\mathbb{Z}$;
- Demonstrar a equivalência de três propriedades que definem o conceito de números primos.

Introdução

O inteiro 1 só tem um divisor positivo, que é o próprio. Qualquer outro inteiro positivo $a > 1$ têm pelo menos dois divisores positivos: 1 e a. Um número é chamado primo quando tem exatamente dois divisores positivos.

Os gregos chamavam os números primos de *primeiros* ou *indecomponíveis* e os compostos de *secundários* ou *decomponíveis*. Os romanos traduziram do grego para o latim usando a palavra *primos* para representar esses números "primeiros".

Definição 1 (número primo)
Um número inteiro $a \neq \pm 1$ é um número *primo* quando só tem dois divisores positivos: 1 e $|a|$.

Os números inteiros $a \neq \pm 1$ que não são primos são chamados de números compostos.

Por exemplo, os inteiros $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$ são os 10 primeiros inteiros primos positivos. Os inteiros $-2, -3, -5, -7, -11, -13 \cdots$ são inteiros primos negativos.

Note que ± 1 não são números primos! Os inteiros ficam assim divididos em 3 subconjuntos: $\{\pm 1\}$, os inteiros primos e os inteiros compostos.

Os primos são as unidades básicas em relação as quais podemos expressar todos os números inteiros, no sentido de que qualquer inteiro maior que 1 pode ser escrito como produto de fatores primos. Este é o chamado Teorema Fundamental da Aritmética, que veremos mais tarde.

Nessa aula, que serve de preparação para a demonstração do chamado Teorema Fundamental da Aritmética, mostraremos como os inteiros primos estão relacionados aos geradores dos ideais maximais de $\mathbb{Z}$.

Ideais maximais de $\mathbb{Z}$

Vamos iniciar definindo ideal maximal de $\mathbb{Z}$ e então relacionando estes ideais com os inteiros primos.

Definição 2 (Ideal Maximal de $\mathbb{Z}$)
um ideal $\mathcal{M}$ de $\mathbb{Z}$ é chamado *maximal* se é ideal próprio de $\mathbb{Z}$ (isto é, $\mathcal{M} \subsetneqq \mathbb{Z}$) e $\mathcal{M}$ não está contido propriamente em nenhum outro ideal próprio de $\mathbb{Z}$, ou seja, os únicos ideais de $\mathbb{Z}$ contendo $\mathcal{M}$ são $\mathcal{M}$ e $\mathbb{Z}$.

Lembre-se que $\{0\}$ e $\mathbb{Z}$ são ideais de $\mathbb{Z}$

Em outras palavras, um ideal $\mathcal{M}$ de $\mathbb{Z}$ é maximal se

i. $\mathcal{M} \subsetneqq \mathbb{Z}$ (ideal próprio)

ii. Se I é um ideal de $\mathbb{Z}$, $\mathcal{M} \subset I \subset \mathbb{Z}$, então $I = \mathcal{M}$ ou $I = \mathbb{Z}$.

Exemplo 1
O ideal $\mathbb{Z} \cdot 6$ não é maximal. De fato, temos que $\mathbb{Z} \cdot 6 \subsetneqq \mathbb{Z} \cdot 2 \subsetneqq \mathbb{Z}$, pois

$$x \in \mathbb{Z} \cdot 6 \Rightarrow x = 6q, \text{para algum } q \in \mathbb{Z}$$

$$\Rightarrow x = 2(3q) \Rightarrow x \in \mathbb{Z} \cdot 2$$

Assim, $\mathbb{Z} \cdot 6 \subset \mathbb{Z} \cdot 2$, mas $\mathbb{Z} \cdot 6 \neq \mathbb{Z} \cdot 2$ (por exemplo, $2 \in \mathbb{Z} \cdot 2$, mas $2 \notin \mathbb{Z} \cdot 6$).

Atividades

1. Mostre que
$$\mathbb{Z} \cdot 8 \subsetneqq \mathbb{Z} \cdot 4 \subsetneqq \mathbb{Z} \cdot 2 \subsetneqq \mathbb{Z} \, .$$

2. Mostre que o ideal $\mathbb{Z} \cdot m$, onde m é um inteiro composto, não é maximal.

Relação entre ideais maximais de $\mathbb{Z}$ e inteiros primos

Seja $\mathcal{M} \subset \mathbb{Z}$ um ideal maximal de $\mathbb{Z}$ e seja $p \in \mathcal{M}^+$ tal que $\mathcal{M} = \mathbb{Z} \cdot p$ (existe tal p pelo teorema dos ideais principais).

Lembre-se que $\mathcal{M}^+ = \mathcal{M} \cap \mathbb{Z}^+$

O que podemos dizer a respeito desse número p? A primeira observação é que, como $\mathcal{M} \subsetneqq \mathbb{Z}$ e $p \in \mathcal{M}^+$, temos $p \geq 2$, já que $p = 1$ nos daria $\mathcal{M} = \mathbb{Z}$.

E o que mais poderíamos dizer à respeito desse número $p \geq 2$, gerador de $\mathcal{M}$?

A primeira resposta vem do seguinte resultado:

Proposição 1

Seja $\mathcal{M} = \mathbb{Z} \cdot p$, $p \geq 2$, um ideal maximal de $\mathbb{Z}$. Então $\mathcal{D}(p)^+ = \{1, p\}$, isto é, p é primo.

Demonstração:

Seja $\mathcal{M} = \mathbb{Z} \cdot p$, $p \geq 2$ um ideal maximal de $\mathbb{Z}$ e seja $m \in \mathcal{D}(p)^+$ um divisor positivo de p. Vamos provar que $m = 1$ ou $m = p$.

De fato, $m \in \mathcal{D}(p)^+$ nos diz que $p = m \cdot k$, $k > 0$ e portanto todo múltiplo de p é também múltiplo de m, isto é, $\mathcal{M} = \mathbb{Z} \cdot p \subset \mathbb{Z} \cdot m$. Como $\mathcal{M}$ é ideal maximal de $\mathbb{Z}$ temos duas possibilidades:

(a) $\mathcal{M} = \mathbb{Z} \cdot p = \mathbb{Z} \cdot m$ ou

(b) $\mathbb{Z} \cdot m = \mathbb{Z}$.

Agora

(a) $\mathbb{Z} \cdot p = \mathbb{Z} \cdot m \Longrightarrow m \in \mathbb{Z} \cdot m = \mathbb{Z} \cdot p \Longrightarrow m = s \cdot p$, $s > 0$. Mas $p = m \cdot k$ e daí segue que: $m = (sk)m$ o que implica $sk = 1$, com $k, s > 0$. Portanto $s = k = 1$ e $m = p$.

(b) $\mathbb{Z} \cdot m = \mathbb{Z}$, $m > 0 \Longrightarrow m = 1$.

Assim provamos que $m = 1$ ou $m = p$ e a Proposição 1 está demonstrada. □

Demonstramos então que todo ideal maximal é gerado por um número primo. O próximo teorema afirma que também vale a recíproca: todo ideal gerado por um número primo é maximal.

Teorema 1

Seja $p \geq 2$ um dado número inteiro e seja $\mathcal{M} = \mathbb{Z} \cdot p$ o ideal principal de $\mathbb{Z}$ gerado por p. Então $\mathcal{M} = \mathbb{Z} \cdot p$ é ideal maximal de $\mathbb{Z}$ se, e somente se, p é primo.

Demonstração:

($\Longrightarrow$) Essa parte já foi demonstrada através da proposição 1.

($\Longleftarrow$) Seja $p \geq 2$ um número primo dado, e seja $\mathcal{M} = \mathbb{Z} \cdot p$ o ideal principal gerado por p.

Vamos mostrar que $\mathcal{M} = \mathbb{Z} \cdot p$ é um ideal maximal de $\mathbb{Z}$.

De fato, sabemos que $\mathbb{Z} \cdot n = \mathbb{Z}$ se, e somente se, $n = \pm 1$. Como $p \geq 2$, teremos

(i) $\mathcal{M} = \mathbb{Z} \cdot p \subsetneq \mathbb{Z}$ ($\mathcal{M}$ é o ideal próprio de $\mathbb{Z}$).

Agora, seja I um ideal contendo $\mathcal{M}$, isto é, $\mathbb{Z} \cdot p = \mathcal{M} \subset I \subset \mathbb{Z}$. Vamos provar a condição (ii) da definição de ideal maximal, a saber, que $I = \mathcal{M}$ ou $I = \mathbb{Z}$ (isto é, $\mathcal{M}$ é maximal).

Pelo Teorema do Ideal Principal, existe $m > 0$ tal que $I = \mathbb{Z} \cdot m$. Estamos assumindo $\mathcal{M} = \mathbb{Z} \cdot p \subset I = \mathbb{Z} \cdot m$. Assim, $p \in \mathcal{M}$ implica $p \in I = \mathbb{Z} \cdot m$ o que implica que existe um $k > 0$ tal que $p = k \cdot m$. Assim, $m \in \mathcal{D}(p)^+ = \{1, p\}$ (pois estamos assumindo $p \geq 2$ primo). Portanto $m \in \{1, p\}$.

Se $m = 1$ temos $I = \mathbb{Z} \cdot m = \mathbb{Z} \cdot 1 = \mathbb{Z}$. Por outro lado, se $m = p$ temos $I = \mathbb{Z} \cdot m = \mathbb{Z} \cdot p = \mathcal{M}$ e isto completa a demonstração. □

Atividades

1. Mostre que $\mathbb{Z} \cdot 5$ é um ideal maximal de $\mathbb{Z}$.

2. Mostre que $\mathbb{Z} \cdot n = \mathbb{Z} \Leftrightarrow n = \pm 1$.

Propriedades dos números primos

Na aula 6 vimos que se $a, b \in \mathbb{Z}^+$ e $d > 0$ tal que $\mathbb{Z} \cdot a + \mathbb{Z} \cdot b = \mathbb{Z} \cdot d$ então $d = \text{mdc}(a, b)$. Em particular, como $d \in \mathbb{Z} \cdot d$, então $d \in \mathbb{Z} \cdot a + \mathbb{Z} \cdot b$, isto é, existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$. Se o $\text{mdc}(a, b) = 1$, existirão $r, s \in \mathbb{Z}$ tais que $ra + sb = 1$.

Agora vamos demonstrar uma proposição que será usada na demonstração do próximo teorema, que prova a equivalência de três condições para a definição de números primos.

Proposição 2
Seja $p \geq 2$ um número primo e seja $a \in \mathbb{Z}^+$. Se p não é divisor de a então $\text{mdc}(a, p) = 1$. Em particular, nessa situação, existem $r, s \in \mathbb{Z}$ tais que $rp + sa = 1$.

Demonstração:

Seja $p \geq 2$ um número primo. Assim, $\mathcal{D}(p)^+ = \{1, p\}$ e seja $d = \text{mdc}(p, a)$. Pela definição de mdc temos que:

$$d = \max(\mathcal{D}(p)^+ \cap \mathcal{D}(a)^+) .$$

Se p não é divisor de a então $p \notin \mathcal{D}(a)^+$ e daí segue, tendo em vista que $\mathcal{D}(p)^+ = \{1, p\}$, que

$$\mathcal{D}(p)^+ \cap \mathcal{D}(a)^+ = \{1\}$$

e, portanto, $d = \max(\mathcal{D}(p)^+ \cap \mathcal{D}(a)^+) = 1$.

Pela observação feita antes do enunciado dessa proposição, temos que, se $p \geq 2$ primo não é divisor de $a \in \mathbb{Z}^+$, então existem $r, s \in \mathbb{Z}$ tais que $1 = rp + sa$. □

Notação para divisibilidade: Usamos a notação $d \mid a$ quando d é um divisor de a. Caso contrário, escrevemos $d \nmid a$.

Agora mostraremos a equivalência de três propriedades que caracterizam números primos.

Teorema 2
Seja $p \geq 2$ um número inteiro dado. Então as seguintes condições são equivalentes:

(i) p é primo, isto é, $\mathcal{D}(p)^+ = \{1, p\}$

(ii) Para todo $a, b \in \mathbb{Z}^+$ se $p|ab$ então $p|a$ ou $p|b$

(iii) Se $p = mk$ com $m, k \in \mathbb{Z}^+$ então $m = 1$ ou $k = 1$.

Demonstração: (caminho cíclico (i)$\Longrightarrow$(ii)$\Longrightarrow$(iii)$\Longrightarrow$(i)).
(i)$\Longrightarrow$(ii) Suponhamos $p \geq 2$ primo e $a, b \in \mathbb{Z}^+$ com $p|ab$. Vamos mostrar que $p|a$ ou $p|b$.

Se $p|a$ então nada há a provar. Suponha que $p \nmid a$. Pela proposição anterior, temos que $\text{mdc}(p, a) = 1$ e existem $r, s \in \mathbb{Z}$ tais que $rp + sa = 1$.

Multiplicando esta igualdade por b temos $p(rb) + s(ab) = b$, isto é, $b = (rb)p + s(ab)$. Se $p|ab$ temos $ab = pm$, para algum $m \in \mathbb{Z}$, e assim $b = (rb)p + (sm)p = (rb + sm)p$ e isto nos diz que $p|b$. Portanto, se $p \nmid a$, temos $p|b$.
(ii)$\Longrightarrow$(iii) Vamos assumir agora que para todo $a, b \in \mathbb{Z}^+$ se $p|ab$ então $p|a$ ou $p|b$. Vamos provar (iii).

De fato, sejam $m, k \in \mathbb{Z}^+$ tais que $p = mk$. Daí segue que p é divisor de $p = mk$. Portanto, por (ii), temos que $p|m$ ou $p|k$. Mas $p|m$ implica $p \leq m$ e $p = mk \geq m$ implica $p = m$, isto é, $k = 1$.

Mas $p|k$ implica $p \leq k$ e $p = mk \geq k$ implica $p = k$, isto é, $m = 1$ como queríamos demonstrar. Logo (ii)$\Longrightarrow$(iii).

(iii)$\Longrightarrow$(i) Vamos supor $p \geq 2$ tal que, se $p = mk$ com $m, k \in \mathbb{Z}^+$ então $m = 1$ ou $k = 1$. Vamos provar que p é primo.

Seja $r \in \mathcal{D}(p)^+$. Assim $p = rs$ para algum $s \in \mathbb{Z}^+$. Por (iii) temos $r = 1$ ou $s = 1$. Se $s = 1$, $r = p$. Logo $r = 1$ ou $r = p$ e isto nos diz que $\mathcal{D}(p)^+ = \{1, p\}$, isto é, p é primo. □

Definimos anteriormente um inteiro primo como aquele que satisfaz a condição (i) do teorema anterior. A equivalência das 3 condições nos mostra que poderíamos ter usado qualquer uma delas como definição de número primo.

Atividades

1. Dê um exemplo de inteiros m, a e b tais que $m \mid ab$, mas que $m \nmid a$ e $m \nmid b$. Por que este inteiro m deve ser necessariamente um número composto?

Mais sobre o mdc de dois inteiros

Vimos que, se a e b são dois inteiros e $d = \text{mdc}(a, b)$, então existem x e y tais que $xa + yb = d$. O valor de $d = \text{mdc}(a, b)$ pode ser calculado de maneira eficiente usando o algoritmo de Euclides. A questão que colocamos agora é: como calcular estes x e y, dados a e b ?

A resposta é que podemos "inverter" os passos do algoritmo de Euclides para escrevermos d em termos de a e b. Vamos começar com um exemplo.

Exemplo **2**
Calcule, utilizando o algoritmo de Euclides, o mdc de 300 e 135 e e escreva este inteiro em termos de 135 e 300.

Vamos lá. Usando o algoritmo de Euclides temos:

$$\begin{aligned} 300 &= 2 \cdot 135 + 30 \\ 135 &= 4 \cdot 30 + 15 \\ 30 &= 2 \cdot 15 + 0 \end{aligned}$$

Vemos que $15 = \text{mdc}(300, 135)$. Para escrever 15 em função de 300 e 135, começamos com a penúltima equação:

$$135 = 4 \cdot 30 + 15 \Rightarrow 15 = 135 - 4 \cdot 30$$

Agora substituímos 30 pelo valor que podemos obter na primeira equação:

$$15 = 135 - 4 \cdot 30 = 135 - 4(300 - 2 \cdot 135) = -4 \cdot 300 + 9 \cdot 135$$

Atividades

1. Determine inteiros x e y tais que $1 = x \cdot 198 + y \cdot 25$.

Resumo

Nesta aula abordamos os inteiros primos. Todo inteiro pode ser escrito como produto de números primos, o que provaremos na próxima aula.

Há várias maneiras de definirmos números primos. O Teorema 2 apresenta três propriedades equivalentes que caracterizam os inteiros primos. Qualquer uma delas poderia ter sido utilizada como definição.

Os ideais próprios de $\mathbb{Z}$ que não estão contidos em outro ideal próprio de $\mathbb{Z}$ são os ideais maximais de $\mathbb{Z}$. Vimos que estes são exatamente os ideais gerados por primos. Esta é uma outra caracterização de primos em $\mathbb{Z}$, esta mais algébrica. Voltaremos a ela quando estudarmos anéis em geral.

Exercícios

1. Encontre inteiros x e y tais que $xa + yb = \text{mdc}(a, b)$, onde:
   (a) $a = 102$ e $b = 33$.
   (b) $a = -15$ e $c = 50$.
   (c) $a = 20$ e $c = 1$.
2. Prove que inteiros consecutivos devem ser primos entre si.
3. Prove que $2a + 1$ e $4a^2 + 1$ são primos entre si.
4. Sejam $a, b, c \in \mathbb{Z}^+$ inteiros positivos dados. Mostre que
$$a \cdot \text{mdc}(b, c) = \text{mdc}(ab, ac)$$
5. Sejam $a, m, n \in \mathbb{Z}^+$ inteiros positivos dados. Mostre que
$$\text{mdc}(a, m) = \text{mdc}(a, n) = 1 \Longrightarrow \text{mdc}(a, mn) = 1\,.$$
6. Seja $I = \mathbb{Z} \cdot n \subset \mathbb{Z}$ um dado ideal de $\mathbb{Z}$ onde $n \in \mathbb{Z}$. Mostre que
$$I = \mathbb{Z} \cdot n = \mathbb{Z} \Longleftrightarrow n = \pm 1\,.$$
7. Seja $I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset \cdots$ uma cadeia de ideais de $\mathbb{Z}$. Mostre que
$$I = \bigcup_{i=1}^{\infty} I_j$$
é um ideal de $\mathbb{Z}$.
8. Sejam I e J dois dados ideais de $\mathbb{Z}$. Mostre que: se $I \not\subset J$ e $J \not\subset I$ então $I \cup J$ não é um ideal de $\mathbb{Z}$.
9. Seja $p \geq 2$ um dado número primo. Mostre que os únicos múltiplos de p não nulos que são números primos são p e $-p$.

Aula 8 – Fatoração única: o Teorema Fundamental da Aritmética

Metas

Nesta aula apresentaremos o conjunto dos números primos como pilar básico na decomposição de números inteiros como produto de primos.

Objetivos

- Demonstrar o Teorema Fundamental da Aritmética (teorema da fatoração única);
- Demonstrar, usando o teorema da fatoração única, que o conjunto dos números primos é infinito;
- Exprimir e relacionar MDC e MMC, usando a fatoração única.

Introdução

Nesta aula demonstraremos o teorema da fatoração única, também conhecido como o Teorema Fundamental da Aritmética. Nesse Teorema os números primos aparecem como pilar básico, indecomponíveis, e cada inteiro pode se decompor como produto de fatores primos.

O conhecimento da decomposição em fatores primos nos permitirá demonstrar propriedades importantes sobre números inteiros. Essa decomposição é única a menos da ordenação dos fatores primos que entram na decomposição do número.

C.F. Gauss, matemático alemão do século XVIII/XIX, foi o primeiro a desenvolver a aritmética como ciência, de modo sistemático. O enunciado do Teorema Fundamental da Aritmética, como apresentamos aqui, foi publicado em 1801, no famoso livro "Disquisiotores Arithmetcal".

Observe que se considerássemos 1 como primo, não teríamos decomposição única em fatores primos. Por exemplo, $2 = 1{\cdot}2 = (1)^2{\cdot}2 = 1^3{\cdot}2 = \cdots$.

Considerando que $\mathcal{D}(n)^+ = \mathcal{D}(-n)^+$, e que p é primo se, e somente se $-p$ é primo, teríamos, por exemplo, $6 = 2 \cdot 3 = (-2)(-3)$. Para simplificar a nossa abordagem, essencialmente sem perda de generalidade, vamos trabalhar com primos $p \geq 2$ e fatorar, no Teorema Fundamental da Aritmética, números inteiros $n \geq 2$.

Como aplicação do teorema da fatoração única, vamos provar que o conjunto dos números primos é infinito e também explicitar e relacionar MDC e MMC.

Um pouco de história

Antes de enunciarmos o teorema fundamental vamos fazer as observações sobre números primos dando uma idéia de que muitas questões envolvendo números primos ainda estão por ser resolvidas.

Nós vamos provar, usando o Teorema Fundamental da Aritmética (Teorema 1, a seguir), que o conjunto dos números primos é infinito, usando um belo argumento devido a Euclides.

Para se ter uma idéia da importância do tema, podemos citar que vários matemáticos apresentaram, em diferentes épocas, demonstrações sobre a infinitude do conjunto dos números primos.

Por exemplo, *Kummer* (1878), *Pólya* (1924), *Bellman* (1947), *Washington* (1980), entre outros.

Um outro aspecto a se destacar é a dificuldade de decidirmos se um número inteiro N, muito grande é ou não primo. Há algoritmos que indicam se um inteiro é ou não primo, estes algoritmos são conhecidos como testes de primalidade.

Pierre Fermat, matemático francês do século XVII, conjecturou que os números da forma $F_m = 2^m + 1$ com $m = 2^n$ eram todos primos. Os 5 primeiros números de Fermat são, de fato, primos:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257 \text{ e } \quad F_4 = 65.537 \, .$$

No entanto, Euler provou que $F_5 = 641 \times 6700417$. Portanto, F_5 não é primo.

Os primos da forma $F_n = 2^{2^n} + 1$ são conhecidos como primos de Fermat. O maior primo de Fermat conhecido até hoje é F_4. Para se ter uma melhor compreensão das dificuldades aqui envolvidas basta dizer que o número de Fermat F_{23471} possui mais de $(10)^{7000}$ algarismos e foi provado que não é primo por *Keller*, em 1984. O número F_{31} possui mais de 30 bilhões de algarismos.

Uma questão ainda não resolvida é saber se existem infinitos primos de Fermat F_n. Também não é conhecido se os números F_{22}, F_{24}, F_{28} são ou não primos.

Em aulas futuras, voltaremos a fazer mais observações sobre esse tema e

falaremos dos chamados *números de Mersenne*, que são os números da forma $M_n = 2^n - 1$. São de especial interesse os números da forma $M_p = 2^p - 1$ com p primo. Um primo da forma $2^p - 1$ é chamado um primo de Mersenne. $M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127$, são primos mas, $M_{11} = 23 \times 89$ é um número composto.

Boas referências sobre os primos de Mersenne, são http://www.mersenne.org/prime.htm e http://www.utm.edu/research/primes/mersenne/

Muitos dos chamados primos gigantes foram obtidos testando os números de Mersenne. O maior primo conhecido neste momento é um primo de Mersenne. Trata-se do número

$$2^{24036583} - 1$$

Este é o 41^o primo de Mersenne conhecido e tem exatamente 7235733 dígitos! Sua primalidade foi provada em 15 de maio de 2004, parte de um grande esforço de trabalho colaborativo pela Internet chamado GIMPS (Great Internet Mersenne Prime Search).

Marin Mersenne (1588-1648) foi um monge francês, contemporâneo de Fermat. Ele não foi o primeiro a estudar os número da forma $M_n = 2^n - 1$, mas entrou na história por afirmar, em 1644, que os números $2^n - 1$ são primos para

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 \text{ e } 257$$

e compostos para todos os outros inteiros positivos $n < 257$.

Por esta afirmação, aliás incorreta, o nome de Mersenne ficou associado aos primos da forma $2^n - 1$.

Com relação aos números da lista de Mersenne, é fácil ver que para $n = 2, 3, 5, 7, 13$ os números $2^n - 1$ são primos. O fato de que $2^{17} - 1$ e $2^{19} - 1$ são primos era conhecido antes de Mersenne.

Cerca de 100 anos depois, em 1750, Euler mostrou que $2^{31} - 1$ é primo. Outro século depois, em 1876, Lucas mostrou que $2^{127} - 1$ é primo. Um pouco mais tarde, em 1883, Pervouchine mostrou que $2^{61} - 1$ é primo. Portanto, faltava um inteiro na lista de Mersenne.

No início do século XX, Powers mostrou que os números $2^{89} - 1$ e $2^{107} - 1$ também são primos. Os inteiros 89 e 107 devem então se acrescentados à lista de Mersenne. Por volta de 1947, todos os inteiros $n < 258$ já haviam sido checados. A lista correta de inteiros $n < 258$ tal que $2^n - 1$ é primo é a seguinte:

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \text{ e } 127 \, .$$

Como dissemos, o maior primo conhecido hoje é um primo de Mersenne, o 41^o primo de Mersenne: $2^{24036583} - 1$.

Os testes de primalidade tornaram-se bastante úteis em tempos recentes pela sua aplicação à criptografia. Voltaremos a falar sobre aplicações de teoria dos números à criptografia mais tarde, quando estudarmos o Teorema de Fermat.

A palavra Criptografia deriva do grego "kryptos", que quer dizer escondido. Criptografia quer dizer então algo como "escrita escondida". Criptografia é o estudo das formas de converter uma informação de sua apresentação normal para uma forma em que não possa ser compreendida sem uma informação especial, que pode ser uma "chave" ou "senha". O processo de conversão é chamada "encriptação" Criptografia é amplamente utilizada em transações bancárias e troca de informações pela Internet e envolve processos matemáticos complexos, especialmente da área de Teoria dos Números.

O Teorema Fundamental da Aritmética

Na aula passada, no Teorema 2, vimos que, se $p \geq 2$ é um inteiro, então as três propriedades a seguir são equivalentes:

(i) $\mathcal{D}(p)^+ = \{1, p\}$ (essa foi a nossa definição inicial de números primos)

(ii) Para todo $a, b \in \mathbb{Z}^+$ se $p|ab$ então $p|a$ ou $p|b$

(iii) Se $p = mk$ com $m, k \in \mathbb{Z}^+$ então $m = 1$ ou $k = 1$

Agora vamos enunciar o Teorema da Fatoração Única, também conhecido como Teorema Fundamental da Aritmética.

Teorema 1

(1) Todo inteiro $n \geq 2$ pode ser expresso como produto de números primos (não necessariamente distintos) $n = p_1.p_2.\cdots.p_k$ com $p_i \geq 2$ primos e $1 \leq i \leq k$. Mais ainda,

(2) Essa expressão $n = p_1.p_2.\cdots.p_k$, como produto de primos é única à menos de permutação na ordem dos fatores primos.

Demonstração:

(1) Vamos supor que a afirmação é falsa e chegaremos a uma contradição (absurdo).

Seja $S = \{m \in \mathbb{Z} \mid m \geq 2$ e m não é produto de primos$\}$. Como estamos assumindo que o teorema é falso, temos que $S \subset \mathbb{Z}^+$ é um subconjunto não vazio de $\mathbb{Z}$ limitado inferiormente pelo inteiro 2. Pelo princípio da boa ordenação de $\mathbb{Z}$, S possui um primeiro elemento $m = \min S$, que é o menor inteiro maior ou igual a 2, em S.

Como $m \in S, m \geq 2$ e m não é produto de primos, então, em particular, m não é primo. Assim, $m \in S$ é um número composto $m = rt$ onde $1 < r < m$ e $1 < t < m$. Portanto, $2 \leq r$ e $2 \leq t$ e como m é o menor elemento de S, $r < m$ e $t < m$ temos que $r \notin S$ e $t \notin S$. Pela nossa definição de S segue que

$$r = p_1.p_2.\cdots.p_k \quad \text{e} \quad t = q_1.q_2.\cdots.q_s$$

podem ser expressos como produto de primos. Mas, então,

$$m = rt = p_1.p_2.\cdots.p_k.q_1.q_2.\cdots.q_s$$

também pode ser expresso como produto de primos, logo $m \notin S$. Mas m foi escolhido pertencendo ao conjunto S, como primeiro elemento de S. Assim, temos uma contradição e a primeira parte do teorema está estabelecida.

Agora vamos provar a segunda parte do teorema, a unicidade, à menos de permutação dos fatores primos. Para isto, vamos precisar de um resultado que enunciaremos como um lema. Provaremos o lema e depois voltaremos à demonstração da unicidade.

Lema 1

Sejam $p_1, p_2, \cdots, p_k$ números primos maiores ou iguais a 2. Seja $N = p_1.p_2.\cdots.p_k$ e seja $q, q \geq 2$ primo tal que $q \mid N$, então existe i com $1 \leq i \leq k$ tal que $q = p_i$.

Demonstração do lema:

Vamos usar indução sobre k, o número de primos na lista $p_1, p_2, \cdots, p_k$.

Se $k = 1$, então $N = p_1$ é primo.

$$q \mid N \Rightarrow q \mid p_1 \Rightarrow q = 1 \text{ ou } q = p_1$$

já que p_1 é primo. Como q é primo, então $q \neq 1$ e logo $q = p_1$.

Suponha que $k \geq 2$ e que o lema vale para $k - 1$. Então

$$q \mid N \Rightarrow q \mid p_1 \cdot (p_2 \cdots p_k) \Rightarrow q \mid p_1 \text{ ou } q \mid (p_2 \cdots p_k)\ .$$

Lembre-se que provamos, na aula passada, que p primo e $p \mid ab$ implica em $p \mid a$ ou $p \mid b$ (parte (ii) do Teorema 2 da Aula 7)

Se $q \mid p_1$ então, como p_1 é primo e $q \geq 1$, resulta em $q = p_1$.

Se $q \nmid p_1$ temos $q \mid (p_2 \cdots p_k)$. Nesse caso, pela hipótese de indução sobre k, temos que existe i com $2 \leq i \leq k$ tal que $q = p_i$. Em todas as situações $q \in \{p_1, p_2, \cdots, p_k\}$, como queríamos demonstrar. □

Agora, vamos demonstrar a segunda parte (unicidade) do teorema da fatoração única.

(2) Para mostrar a unicidade, vamos mostrar que, se $n \geq 2, n = p_1.p_2.\cdots.p_k = q_1.q_2\cdots.q_t$ são duas expressões de n como produto de primos, então $k = t$ e a ordenação $q_1, q_2, \cdots, q_{k=t}$ é uma reordenação de $p_1, p_2, \cdots, p_k$.

Vamos demonstrar, por indução sobre t.

Se $t = 1$, temos $N = p_1.p_2.\cdots.p_k = q_1$ com q_1 primo, $q_1 \geq 2$, e $p_1, p_2, \cdots, p_k$ primos maiores ou iguais a dois. Nessa situação temos

$$q_1 \mid N = p_1.p_2.\cdots.p_k \ .$$

Pelo lema, existe i com $1 \leq i \leq k$ tal que $q_1 = p_i$. Daí segue que, $k = t = 1$ e $N = p_i = q$.

Suponha que $t \geq 2$, que o resultado seja válido para $t-1$ e que $N = p_1.p_2.\cdots.p_k = q_1.q_2\cdots.q_t$. Nesse caso, $q_1|N = p_1.p_2.\cdots.p_k$. Pelo lema, temos que existe i com $1 \leq i \leq k$ tal que $q_1 = p_i$.

Como

$$N = p_1.p_2.\cdots.p_{i-1}.p_i.p_{i+1}.\cdots.p_k = q_1.(q_2.\cdots.q_t) \quad \text{e} \quad p_i = q_1 \ ,$$

segue, simplificando, que

$$\underbrace{p_1.p_2.\cdots.p_{i-1}.p_{i+1}.\cdots.p_k}_{k-1 \text{ fatores}} = \underbrace{q_2.q_3.\cdots.q_t}_{t-1 \text{ fatores}} \ .$$

Como temos apenas $(t-1)$ fatores no lado direito da igualdade, podemos aplicar nossa hipótese de indução sobre t e teremos que $k-1 = t-1$, o que implica $k = t$, e que $(q_2, q_3, \cdots, q_k)$ é uma ordenação dos fatores primos $(p_1, p_2, \cdots, p_{i-1}, p_{i+1}, \cdots, p_k)$. Como $p_i = q_1$ temos que $q_1, q_2, q_3, \cdots, q_k$ é uma ordenação de $p_1, p_2, \cdots, p_k$, o que prova a parte (2). □

Exemplo **3**

Podemos escrever o inteiro 12 como produto de fatores primos da seguinte forma:

$$12 = 2 \cdot 2 \cdot 3$$
$$12 = 2 \cdot 3 \cdot 2$$
$$12 = 3 \cdot 2 \cdot 2$$

Para remover este incômodo de haverem várias ordens possíveis para os fatores primos, podemos fixar uma ordenação em especial. Por exemplo, podemos fixar que os fatores primos sejam ordenados em ordem não-decrescente. Desta forma, a fatoração passa a ser única.

No exemplo acima, a única fatoração em que os primos estão em ordem não-decrescente é $12 = 2 \cdot 2 \cdot 3$.

Agora vamos enunciar o teorema da fatoração única em uma versão especial em que fixamos a ordenação dos fatores primos. A demonstração é um corolário do Teorema 1.

Teorema 2

Todo número inteiro $n \leq 2$ pode ser expresso de modo único como produto de primos $n = p_1.p_2.\cdots.p_k$ onde $2 \leq p_1 \leq p_2 \leq \cdots \leq p_k$ são primos.

Demonstração:

Basta observar que existe uma única ordenação $p_1, p_2, \cdots, p_k$ quando $p_1 \leq p_2 \leq \cdots \leq p_k$. □

Atividades

1. É comum agruparmos os primos iguais na fatoração $N = p_1 \cdot p_2 \cdots p_k$ em potências. Por exemplo, escrevemos $12 = 2^2 3$, ao invés de $12 = 2 \cdot 2 \cdot 3$. Escreva uma versão do Teorema Fundamental da Aritmética onde os primos iguais estão agrupados em potência e ordenados em ordem crescente.

A infinitude do conjunto dos números primos

Em seguida provaremos a infinidade do conjunto dos números primos. A demonstração dada é essencialmente um argumento dado por Euclides nos *Elementos*.

Teorema 3

O conjunto dos números primos é infinito.

Demonstração:

Basta demonstrarmos que $\mathcal{P}^+ = \{p \mid p \text{ primo}, \ p \geq 2\}$ é infinito.

Por absurdo, vamos supor que $\mathcal{P}^+ = \{2, 3, \cdots, p_n\}$ é um conjunto finito.

Seja $N = p_1.p_2.\cdots.p_k$ o número obtido pelo produto de todos os elementos de $\mathcal{P}^+$. Agora, o mdc$(N, N+1) = 1$, já que se $m \mid N$ e $m \mid N+1$ então $m \mid (N+1) - N = 1$. Assim, como cada $p_i \mid N$, temos que $p_i \nmid (N+1)$ para todo $1 \leq i \leq k$.

Mas $N + 1 = q_1.q_2.\cdots.q_t$ é produto de primos, pelo teorema da fatoração única e cada primo q_i é divisor de $(N+1)$ e $q_i \notin \{p_1, p_2, \cdots, p_k\}$, contrariando o fato de $\mathcal{P}^+ = \{p_1, p_2, \cdots, p_k\}$ ser o conjunto de todos os primos maiores ou iguais a dois. □

Atividades

1. Dois primos p e q são chamados *primos gêmeos* se sua diferença é 2. Por exemplo 3 e 5 são primos gêmeos. Encontre 6 pares de primos gêmeos.

O conjunto dos primos gêmeos é infinito? Este é um problema em aberto na Matemática! Não se sabe se existem ou não infinitos primos gêmeos.

Números de divisores de um inteiro

Nesta seção, provaremos uma fórmula que permite calcular o número de divisores de um inteiro, a partir da fatoração deste.

Inicialmente, vamos provar um lema.

Lema 2
Se $\text{mdc}(b,c) = 1$ e $d \mid bc$ então existem r, t com $r \in \mathcal{D}(b)^+$, $t \in \mathcal{D}(c)^+$ e $\text{mdc}(r,t) = 1$ tal que $d = rt$.

Demonstração:

Seja $p^m \mid bc$ onde $p \geq 2$ é primo e $m \geq 1$. Assim, $p \mid bc$, p primo implica $p|b$ ou $p|c$. Como $\text{mdc}(b,c) = 1$ então ou $p|b$ ou $p|c$ (exclusivo).

Suponha que $p|b$. Nesse caso $p \not| c$. Portanto $\text{mdc}(p,c) = 1$ e isto implica que $\text{mdc}(p^m, c) = 1$. Portanto $p^m|bc$ e $p|b$ implica $p^m|b$ e $\text{mdc}(p^m, c) = 1$.

No caso $p|c$, teríamos $p \not| b$ e a conclusão seria $p^m|c$ e $\text{mdc}(p^m, b) = 1$.

Assim, partindo de $\text{mdc}(b,c) = 1$ concluímos que cada potência de primos que dividem bc, divide integralmente b ou divide integralmente c (com exclusividade), isto é,

$$p^m \mid bc \Rightarrow (p^m \mid b \text{ e } p \not| c) \text{ ou } (p \not| b \text{ e } p^m \mid c)\,.$$

Como, pelo teorema da fatoração única d é produto de potência de primos, e $d \mid bc$, essas potências de primos divisores de d serão divisores de bc e estarão separadas entre aquelas que dividem b e as demais que dividem c.

Assim,

$$r = p_1^{m_1}.p_2^{m_2}.\cdots.p_k^{m_k},\ p_i^{m_i}|b \quad \text{e} \quad t = q_1^{n_1}.q_2^{n_2}.\cdots.q_l^{n_l},\ q_j^{n_j}|c\,,$$

na fatoração $d = p_1^{m_1}.p_2^{m_2}.\cdots.p_k^{m_k}.q_1^{n_1}.q_2^{n_2}.\cdots.q_l^{n_l} = rt$, onde $\text{mdc}(r,t) = 1$ e o lema está provado. □

Proposição 1

Sejam $a, b, c \in \mathbb{Z}^+$ dados inteiros positivos tais que $a = bc$ e $\text{mdc}(b, c) = 1$. Mostre que

$$|\mathcal{D}(a)^+| = |\mathcal{D}(b)^+| \cdot |\mathcal{D}(c)^+| .$$

Lembre-se que a notação $|X|$ significa a cardinalidade do conjunto X, isto é, o número de elementos do conjunto X

Demonstração:

Pela proposição anterior sabemos que todo $d \in \mathcal{D}(a)^+$ pode ser escrito como um produto $d = rt$, onde $r \in \mathcal{D}(b)^+, t \in \mathcal{D}(c)^+$.

Basta agora mostrar que isto se dá de maneira única: Se $d = rt$ e $d = r't'$, com $r, r' \in \mathcal{D}(b)^+$ e $t, t' \in \mathcal{D}(c)^+$, então $r = r'$ e $t = t'$. Para demonstrar isso, precisaremos da hipótese $\text{mdc}(b, c) = 1$.

Suponhamos $d \mid bc$, onde $\text{mdc}(b, c) = 1$. Suponha também que $d = rt$ e $d = r't'$, com $r, r' \mid b$ e $t, t' \mid c$. Assim, teremos

$$r \mid d = rt = r't' \Longrightarrow r \mid r't .$$

Mas

$$\text{mdc}(b, c) = 1 \Longrightarrow \text{mdc}(r, t') = 1 \Longrightarrow r \mid r'.$$

Reciprocamente,

$$r' \mid d = r't' = rt \Longrightarrow r'|rt \text{ e } \text{mdc}(r', t) = 1$$

nos dá $r' \mid r$. Portanto $r, r' \in \mathbb{Z}^+$ e $r \leq r'$ e $r' \leq r$ implica $r = r'$.

Por um raciocínio totalmente análogo, podemos concluir que $t = t'$.

Assim, cada divisor d de $a = bc$ com $\text{mdc}(b, c) = 1$ pode ser expresso, de modo único, como produto $d = rt$ com $r \in \mathcal{D}(b)^+, t \in \mathcal{D}(c)^+$. Isto nos diz que

$$|\mathcal{D}(a)^+| = |\mathcal{D}(b)^+| \cdot |\mathcal{D}(c)^+| .$$

2 Seja $a \in \mathbb{Z}^+$ um dado inteiro positivo expresso como produto de potências de primos $p_1, p_2, \cdots, p_k \geq 2$ na forma $a = p_1^{\alpha_1}.p_2^{\alpha_2}.\cdots.p_k^{\alpha_k}$. Mostre que

$$|\mathcal{D}(a)^+| = (1 + \alpha_1)(1 + \alpha_2)\cdots(1 + \alpha_k)$$

(isto nos dá uma fórmula para calcularmos o número de divisores de a).

Demonstração:

Neste exercício, vamos usar indução sobre k.

Se $k = 1$ temos que $a = p_1^{\alpha_1}$. Nesse caso temos

$$\mathcal{D}(a)^+ = \{1, p_1, p_1^2, \cdots, p_1^{\alpha_1} = a\}$$

e

$$|\mathcal{D}(a)^+| = (1 + \alpha_1)\,.$$

Assume verdadeiro para $(k-1)$ fatores primos $a = p_1^{\alpha_1} S$ onde

$$S = p_2^{\alpha_2}.p_3^{\alpha_3}.\cdots.p_k^{\alpha_k}\,.$$

Pelo exercício 1 temos que

$$|\mathcal{D}(a)^+| = |\mathcal{D}(p_1^{\alpha_1})^+| \cdot |\mathcal{D}(S)^+|\,.$$

Mas $|\mathcal{D}(p_1^{\alpha_1})^+| = (1 + \alpha_1)$ e, por indução sobre k,

$$S = p_2^{\alpha_2}.\cdots.p_2^{\alpha_k}, |\mathcal{D}(S)^+| = (1 + \alpha_2)(1 + \alpha_3)\cdots(1 + \alpha_k)\,.$$

Portanto,

$$|\mathcal{D}(a)^+| = (1 + \alpha_1)(1 + \alpha_2)\cdots(1 + \alpha_k)$$

□

Exercícios

1. Sejam $a = p_1^{r_1}.p_2^{r_2}.\cdots.p_s^{r_s}$ e $b = q_1^{t_1}.q_2^{t_2}.\cdots.q_k^{t_k}$ dois inteiros positivos expressos como produto de potências de seus respectivos fatores primos distintos, como na notação acima, com $1 \leq r_i$ para todo i e $1 \leq t_j$ para todo j.

   Mostre que podemos sempre representar os dados números a e b usando o mesmo conjunto de primos:

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

   e

   $$b = p_1^{\beta_1}.p_2^{\beta_2}.\cdots.p_k^{\beta_k},$$

   desde que considerarmos $\alpha_i \geq 0, \beta_i \geq 0$ para todo $i = 1, 2, \cdots, k$.

2. Sejam a e b dois dados inteiros positivos e denotemos (veja exercício 1):

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

   e

   $$b = p_1^{\beta_1}.p_2^{\beta_2}.\cdots.p_k^{\beta_k},$$

   onde $\alpha_i \geq 0, \beta_i \geq 0$ para todo $i = 1, 2, \cdots, k$.

   Seja $\gamma_i = \min\{\alpha_i, \beta_i\} \geq 0, i = 1, 2, \cdots, k$ e seja $\delta_i = \max\{\alpha_i, \beta_i\} \geq \geq 0, i = 1, 2, \cdots, k$.

   (1) Mostre que $\text{mdc}(a, b) = p_1^{\alpha_1}.p_2^{\alpha_2}.\cdots.p_k^{\alpha_k} = D$

   (2) Mostre que $\text{mmc}(a, b) = p_1^{s_1}.p_2^{s_2}.\cdots.p_k^{s_k} = M$

   (3) $M = \dfrac{ab}{D}$, onde $D = \text{mdc}(a, b)$ e $M = \text{mmc}(a, b)$

3. Seja $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ uma cadeia ascendente de ideais de $\mathbb{Z}$. Mostre que existe $k \in \mathbb{Z}^+$ tal que $I_k = I_{k+1} = \cdots = I_{k+m} = \cdots$ (toda cadeia ascendente de ideais de $\mathbb{Z}$, estabiliza).

4. Seja $I_1 = \mathbb{Z} \cdot 2 \supset I_2 = \mathbb{Z} \cdot 4 \supset \cdots \supset I_n = \mathbb{Z} \cdot 2^n \supset \cdots$. Verifique que $\{I\}_{n=1}^{\infty}$ é uma cadeia descendente de ideais de $\mathbb{Z}$ que não estabiliza, isto é, uma cadeia infinita descendente de ideais.

Aula 9 – Os inteiros módulo n: Uma primeira apresentação

Metas

Nesta aula introduziremos, através da relação de congruência, o conjunto $\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{(n-1)}\}$, das classes dos inteiros módulo n.

Objetivos

- Definir a relação de congruência módulo n, em $\mathbb{Z}$, e trabalhar propriedades básicas dessa relação;
- Demonstrar, para inteiro $n \in \mathbb{Z}^+$, que o conjunto $\mathbb{Z}_n$, das classes de congruência módulo n, é finito contendo exatamente n classes;
- Interpretar a definição de congruência módulo n através de Ideais principais em $\mathbb{Z}$.

Introdução

Iniciamos nessa aula o que chamamos de *aritmética modular*, onde em vez de trabalharmos com números inteiros, trabalhamos com classes de inteiros módulo n (também chamadas de *classes resto módulo n*).

Essa aritmética modular está relacionada com fenômenos que se repetem após um certo período fixo, chamado de fenômenos cíclicos ou periódicos. Por exemplo, se você estiver trabalhando com horas, esse período é igual a 24, e um fenômeno ocorrido 20 horas após o meio dia, de um certo dia, terá ocorrido às 8 horas da manhã do dia seguinte, já que $12 + 20 = 32$ e 32, módulo 24, é igual a 8.

Nessa aula faremos uma primeira apresentação da congruência módulo n em $\mathbb{Z}$ (que é uma relação de equivalência), mostrando que o conjunto quociente $\mathbb{Z}_n$ das classes de equivalência módulo n, $n > 0$, contém exatamente n elementos. Apresentaremos ainda, a congruência através das dos ideais principais em $\mathbb{Z}$, isto é, mostraremos que existe uma relação entre classes de congruência módulo n e ideais principais de $\mathbb{Z}$.

A relação de congruência módulo n em $\mathbb{Z}$

Aqui, vale a pena você recordar o conceito de relação de equivalência apresentado na aula 2. Uma relação binária em um conjunto A é uma relação de equivalência nesse conjunto se ela for *Reflexiva, Simétrica e Transitiva*. Introduzimos as notações:

- $a \sim b$ (a é equivalente a b)
- $\overline{a} = \{x \in A \mid x \sim a\}$ (classe de equivalência do elemento A)
- $\overline{A} = A/\sim = \{\overline{a} \mid a \in A\}$ (o conjunto quociente de A pela relação $\sim$)

Mostramos, ainda na aula 2, que $\overline{A} = \{\overline{a} \mid a \in A\}$ define uma partição do conjunto A, isto é, $A = \bigcup\limits_{a \in \mathcal{A}}^{\cdot} \overline{a}$ (cada $\overline{a} \neq \emptyset$, e A é união disjunta de classes de equivalência).

Após recordar esses conceitos vamos definir uma relação de equivalência em $\mathbb{Z}$ especialmente útil, que é a relação de congruência módulo n, em $\mathbb{Z}$.

Definição 1
Seja n um dado inteiro não negativo, e sejam $a, b \in \mathbb{Z}$. Dizemos que a é congruente a b, módulo n, se a diferença $(a - b)$ é múltiplo inteiro de n.

Utilizamos a notação $\equiv \pmod{n}$, para a congruência módulo n. A definição acima pode ser escrita como:

$$a \equiv b \pmod{n} \iff \exists\, k \in \mathbb{Z} \quad \text{tal que} \quad (a - b) = kn\,.$$

Se a não é congruente a b, módulo n, usaremos a notação:

$$a \not\equiv b \pmod{n}\,.$$

Exemplo 4
$27 \equiv 13 \pmod{7}$ mas $27 \not\equiv 13 \pmod{5}$) já que $27 - 13 = 14$ é múltiplo de 7, mas não é múltiplo de 5.

Exemplo 5
$108 \equiv 380 \pmod{17}$, pois $108 - 380 = -(272) = (-16) \times 17$.

Exemplo 6
$100 \equiv 1 \pmod{9}$, pois $99 = (100 - 1) = 11 \times 9$. Observe que, como 9 é múltiplo de 3, então 100 também é congruente a 1, módulo 3.

Exemplo **7**

$100 \equiv 1 \pmod{11}$ e $10 \equiv -1 \pmod{11}$.

Agora vamos provar uma fundamental proposição sobre congruência.

Proposição 1

A relação $\equiv \pmod{n}$, de congruência módulo n, é uma relação de equivalência em $\mathbb{Z}$.

Demonstração:

Sejam $a, b, c \in \mathbb{Z}$, e seja $n \geq 0$ um dado número inteiro. Temos que provar que a relação $\equiv \pmod{n}$ é reflexiva, simétrica e transitiva.

(i) $a \equiv a \pmod{n}$ (reflexiva).

De fato, $(a - a) = 0 = 0 \times n$.

(ii) $a \equiv b \pmod{n} \Longrightarrow b \equiv a \pmod{n}$ (simétrica).

De fato,

$a \equiv b \pmod{n} \Longrightarrow \exists k \in \mathbb{Z}$ tal que $(a - b) = kn \Longrightarrow \exists(-k) \in \mathbb{Z}$ tal que $(b - a) = (-k)n \Longrightarrow b \equiv a \pmod{n}$.

(iii) $a \equiv b \pmod{n}, b \equiv c \pmod{n} \Longrightarrow a \equiv c \pmod{n}$ (transitiva).

Ora, temos que

$$a \equiv b \pmod{n} \Longrightarrow \exists\, k \in \mathbb{Z} \text{ tal que } (a - b) = kn \quad \text{e}$$
$$b \equiv c \pmod{n} \Longrightarrow \exists\, s \in \mathbb{Z} \text{ tal que } (b - c) = sn\,.$$

Portanto, somando essa duas igualdades temos:

$$(a - b) + (b - c) = kn + sn \Longrightarrow a - c = (k + s)n$$

Logo, $(a - c)$ é múltiplo de n.

□

Atividade

Considere a relação de equivalência $\equiv \pmod{5}$ em $\mathbb{Z}$. Mostre que:

1. Os elementos do conjunto $\{\cdots, -10, -5, 0, 5, 10, \cdots\}$ são todos equivalentes $\pmod{5}$.
2. Descreva todas as classes de equivalência $\pmod{5}$. Mostre que existem 5 classes de equivalência no total.

Na próxima seção estudaremos exatamente quais são as classes de $\mathbb{Z} \pmod{n}$.

As classes de equivalência de $\mathbb{Z} \pmod n$

Vamos estudar as classes de equivalência de da relação $\equiv \pmod n$ e, em particular, mostrar que existem exatamente n classes de equivalência da relação de congruência $\equiv \pmod n$.

Inicialmente, vamos ver dois casos especiais: os inteiros 0 e 1. Estes casos serão considerados à parte, como casos excepcionais.

Inteiros $\pmod 0$

Se $n = 0$, a definição de congruência módulo 0, nos diz que:

$$a \equiv b \pmod 0 \Longleftrightarrow \exists\, k \in \mathbb{Z} \text{ tal que } (a-b) = k \times 0 = 0 \Longleftrightarrow a = b\,.$$

Assim, congruência módulo 0 nada mais é do que igualdade entre inteiros.

Nesse caso, as classes $\overline{a}$ são dadas por:

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod 0\} = \{x \in \mathbb{Z} \mid x = a\} = \{a\}\,.$$

Isto é, a classe $\overline{a}$ contém apenas o elemento a. Pode, assim, ser identificada com o conjunto $\{a\}$. O conjunto quociente $\mathbb{Z}/\equiv \pmod 0$ pode ser identificado com $\mathbb{Z}$ e é, portanto, infinito.

Inteiros $\pmod 1$

Se $n = 1$, a definição de congruência módulo 1 nos diz que:

$$a \equiv b \pmod 1 \Longleftrightarrow \exists\, k \in \mathbb{Z} \text{ tal que } (a-b) = k \times 1 = k\,.$$

Isto é, $a \equiv b \pmod 1$ se, e somente se, a diferença $a-b$ é um número inteiro. Mas isto é sempre verdade! Logo

$$a \equiv b \pmod 1, \forall a, b \in \mathbb{Z}\,.$$

Todo inteiro a é congruente a qualquer outro inteiro $b \pmod 1$. As classes $\overline{a}$ são dadas por:

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod 1\} = \mathbb{Z}\,,$$

Assim, só existe uma classe de equivalência, que é o conjunto $\mathbb{Z}$:

$$\overline{0} = \overline{1} = \overline{2} = \cdots = \overline{m} = \cdots = \mathbb{Z}\,.$$

Vimos então dois casos extremos: As classes de $\mathbb{Z} \pmod 0$ são conjuntos unitários: $\overline{a} = \{a\}$, enquanto que a classe de qualquer $a \in \mathbb{Z} \pmod 1$ é o próprio conjunto $\mathbb{Z}$.

Vamos denotar por $\mathbb{Z}_n$ o conjunto quociente de todas as classes de congruência módulo n. Pelo que estudamos acima, temos:

De uma forma mais curta, falamos que $\mathbb{Z}_n$ é o conjunto das classes $\pmod n$

- $\mathbb{Z}_0 = \{\cdots, \{2\}, \{1\}, \{0\}, \{1\}, \{2\}, \cdots\}$
- $\mathbb{Z}_1 = \{\mathbb{Z}\}$

Observe que, no caso $n = 0$, temos que $\mathbb{Z}_0$ é infinito, e no caso $n = 1$ temos que $\mathbb{Z}_1$ é um conjunto unitário.

Agora vamos provar que para $n \geq 2$, $\mathbb{Z}_n$ possui exatamente n elementos.

Proposição 2

Seja $n \geq 2$ um dado número inteiro. Então

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{(n-1)}\} .$$

Em particular, $\mathbb{Z}_n$ possui exatamente n classes.

Demonstração:

Primeiramente, vamos mostrar que as n classes $\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{(n-1)}$ são todas distintas.

Sejam $a, b \in \mathbb{Z}$, com $0 \leq a < b \leq n-1$. Nesse caso $0 < (b-a) < n$ e, portanto, $b \not\equiv a \pmod n$.

Como $\overline{a} = \overline{b} \iff a \equiv b \pmod n \iff b \equiv a \pmod n$, então temos que $\overline{b} \neq \overline{a}$, como queríamos demonstrar. Assim, as classes

$$\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{(n-1)}$$

são todas distintas.

Vamos agora provar que estas são todas as classes $\pmod n$, isto é,

$$x \in \mathbb{Z}_n \Rightarrow x \in \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{(n-1)}\} .$$

Seja $\overline{x} \in \mathbb{Z}_n$.

Caso 1: $x \geq 0$.

Se $x \leq (n-1)$ então $\overline{x} \in \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{(n-1)}\}$.

Assuma $x \geq n$. Pelo Teorema da Divisão de Euclides, existe $q, r \in \mathbb{Z}$ tais que

$$x = qn + r, \qquad 0 \leq r \leq n-1 .$$

Assim, $x - r = qn$, o que implica em $x \equiv r \pmod{n}$.

Portanto $\overline{x} = \overline{r} \in \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{(n-1)}\}$, pois $0 \leq r \leq n-1$.

Caso 2: $x < 0$.

Nesse caso sabemos que existe inteiro positivo k tal que $x + kn = y \geq 0$. Como $y - x = kn$ temos que

$$y \equiv x \pmod{n}$$

e $\overline{y} = \overline{x}$.

Como $y \geq 0$, pelo caso 1, $\overline{y} \in \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{(n-1)}\}$. Como $\overline{x} = \overline{y}$ então $\overline{x} \in \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{(n-1)}\}$, como queríamos demonstrar.

Portanto, acabamos de provar que $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{(n-1)}\}$ possui exatamente n classes de congruência módulo n. □

Atividades

Volte à atividade proposta na seção passada, descrever o conjunto $\mathbb{Z}_5$ e mostrar que ele tem 5 elementos. Pela Proposição 2, temos que

$$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} .$$

Você pode descrever cada uma destas classes?

Propriedades da congruência

Agora vamos provar algumas propriedades de congruência que nos serão úteis na demonstração de critérios de divisibilidade por 3, 5, 9 e 11, que apresentaremos na próxima aula.

Proposição 3

(*i*) $(10)^s \equiv 0 \pmod 5, \forall s \geq 1$, inteiro;

(*ii*) $(10)^s \equiv 1 \pmod 9, \forall s \geq 1$ inteiro. Em particular temos também que $(10)^s \equiv 1 \pmod 3$;

(*iii*) $(10)^s \equiv -1 \pmod{11}, \forall s = 2k+1 \geq 1$, inteiro ímpar

(*iv*) $(10)^s \equiv 1 \pmod 1 1, \forall s = 2m \geq 2$, inteiro par.

Demonstração:

(*i*) $(10)^s = (5 \cdot 2)^s = 5(2^s 5^{s-1})$, que é um múltiplo de 5 para todo $s \in \mathbb{Z}$ com $s \geq 1$. Então $(10)^s \equiv 0 \pmod 5$.

(*ii*) $(10)^s - 1 = (10-1)[(10)^{s-1} + (10)^{s-2} + \cdots + (10)^2 + (10) + 1]$.

Portanto $(10)^{s-1}$ é múltiplo de 9 (e em particular também é múltiplo de 3).

Assim, $(10)^s \equiv 1 \pmod 9$ e $(10)^s \equiv 1 \pmod 3$ para todo $s \geq 1$.

(*iii*) Vamos provar que $(10)^{2k+1} \equiv -1 \pmod{11}$ por indução sobre k.

Se $k = 0$ temos:

$$(10)^{2k+1} = 10 = -1 + (11) \equiv -1 \pmod{11}.$$

Agora assumimos $(10)^{2k+1} \equiv -1 \pmod{11}$ como sendo verdadeira e vamos provar que $(10)^{2(k+1)+1} = (10)^{2k+3} \equiv -1 \pmod{11}$.

Ora temos que $(10)^{2k+3} = (10)^2 \times (10^{2k+1})$, mas $(10)^2 = 1 + 9 \times 11$ e $(10)^{2k+1} = -1 + 11s$, para algum $s \in \mathbb{Z}$, pela hipótese de indução. Assim,

$(10)^{2k+3} = (10)^2 \times 10^{2k+1} = (1 + 9 \times 11)(-1 + s \times 11) =$
$-1 + (s \times 11 - 9 \times 11 + (99)s \times 11) = -1 + (100s - 9) \times 11 \equiv -1 \pmod{11}$.

(*iv*) Análogo à demonstração de (*iii*), $(10)^{2m} \equiv 1 \, (mod \, 11)$, por indução sobre m.

□

Atividade

Mostre que $(10)^{2m} \equiv 1\,(mod\,11), \forall m \in \mathbb{Z}^+$. (Sugestão: use indução sobre m.)

Congruências via ideais principais em $\mathbb{Z}$

Trabalhamos nessa aula com o conceito de congruência módulo n, mostrando que o conjunto quociente das classes de congruência é dado por

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{(n-1)}\}\,.$$

onde cada classe é dada por:

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\} = \{a + kn \mid k \in \mathbb{Z}\}\,.$$

Seja $J = \mathbb{Z}n$ a sub-estrutura de ideal principal do domínio $\mathbb{Z}$. Podemos reescrever a classe $\overline{a}$, através de:

$$\overline{a} = \{kn + a \mid k \in \mathbb{Z}\} = (\mathbb{Z}n) + a = J + a, \quad \text{onde } J = \mathbb{Z}n\,.$$

Portanto, nessa linguagem, temos:

$$x \equiv a \pmod{n} \Longleftrightarrow x \in J + a \Longleftrightarrow (x - a) \in J = \mathbb{Z}n\,.$$

Exemplo 1

Tome $n = 5$. Temos

$$\begin{aligned} J = \mathbb{Z}5 &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} & \overline{0} &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\ \overline{1} &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} & \overline{2} &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\ \overline{3} &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} & \overline{4} &= \{\ldots, -6, -1, 4, 9, 14, \ldots\} \end{aligned}$$

Note que temos

$$\overline{0} = J \quad \overline{1} = 1 + J \quad \overline{2} = 2 + J \quad \overline{3} = 3 + J \quad \overline{4} = 4 + J$$

Atividades

1. Seja $J \subset \mathbb{Z}$ uma sub-estrutura ideal de $\mathbb{Z}$, isto é, J satisfazendo as três seguintes propriedades:

   (a) $0 \in J$

(b) $J - J \subseteq J$

(c) $\mathbb{Z}J \subseteq J$.

Defina uma relação binária $\sim$ em $\mathbb{Z}$ do seguinte modo: $x, y \in \mathbb{Z}$,

$$x \sim y \Longleftrightarrow (x - y) \in J\,.$$

(a) Utilize as três propriedades que definem ideal para mostrar que $\sim$ é uma relação de equivalência em $\mathbb{Z}$.

(b) Verifique que se $J = \mathbb{Z}n, n \in \mathbb{Z}^+$, a relação de equivalência $\sim$, acima definida, é exatamente a relação de congruência módulo n, em $\mathbb{Z}$.

2. Determine a congruência de $6m + 5$, módulo 4, sabendo-se que $m \equiv 1 \pmod 4$.

3. Sabendo-se que $x \equiv y\,(mod\,n)$, mostre que $x^2 + y^2 \equiv 2(xy) \pmod{n^2}$.

4. Determine a classe $\overline{2}$ em $\mathbb{Z}_3$ e em $\mathbb{Z}_5$.

Na próxima aula definiremos soma e produto entre classes e voltaremos a falar em critério de divisibilidade.

Resumo

Nessa aula destacamos, mais uma vez, a importância de se trabalhar com o conceito de relação de equivalência, e apresentamos a especial relação de congruência módulo n, no conjunto $\mathbb{Z}$ dos números inteiros. Esse conceito será mais explorado nas próximas aulas. Apresentamos alguns exemplos de congruências que serão importantes na demonstração de critérios de divisibilidade. Por fim, Mostramos a relação entre congruência módulo n e ideais maximais de $\mathbb{Z}$.

Aula 10 – Propriedades de congruência e critérios de divisibilidade

Metas

Nesta aula apresentaremos propriedades fundamentais de congruência.

Objetivos

- Discutir criticamente as propriedades básicas de congruência;
- Operar com congruência e demonstrar critérios de divisibilidade e cálculos de resto em divisão nos inteiros.

Introdução

Nesta aula demonstraremos propriedades básicas de congruência que nos permitirão, nas próximas aulas, definir soma e produto entre classes, e aplicar esse conceito de congruência para mostrar critérios de divisibilidade nos inteiros e cálculos de restos de divisão em $\mathbb{Z}$.

Propriedades básicas de congruência

Vamos iniciar demonstrando algumas propriedades básicas importantes da congruência.

Proposição 1
Seja $n \in \mathbb{Z}^+$ um dado número inteiro e sejam a e b inteiros tais que $a \equiv r \pmod{n}$ e $b \equiv s \pmod{n}$. Então

(i) $(a+b) \equiv (r+s) \pmod{n}$

(ii) $a \cdot b \equiv r \cdot s \pmod{n}$

Demonstração:

Temos que

$$a \equiv r \pmod{n} \Longrightarrow a = r + k_1 n, \quad k_1 \in \mathbb{Z}$$
$$b \equiv s \pmod{n} \Longrightarrow b = s + k_2 n, \quad k_2 \in \mathbb{Z}$$

Assim,

$$(a+b) = (r+k_1n)+(s+k_2n) = (r+s)+(k_1+k_2)n \Rightarrow (a+b) \equiv (r+s) \pmod{n} .$$

e

$$ab = rs + (rk_2)n + (sk_1)n + (k_1k_2)n^2 \Rightarrow ab = rs + tn ,$$

onde $t = (rk_2 + sk_1 + (k_1k_2)n)$. Assim,

$$a \cdot b \equiv r \cdot s \pmod{n}$$

□

Corolário 1
Seja $n \in \mathbb{Z}^+$ um dado inteiro e sejam $a, b \in \mathbb{Z}$. Então

(i) $a \equiv 1 \,(\mathrm{mod}\, n) \Longrightarrow a \cdot b \equiv b \,(\mathrm{mod}\, n)$

(ii) $a \equiv -1 \,(\mathrm{mod}\, n) \Longrightarrow a \cdot b \equiv -b \,(\mathrm{mod}\, n)$

(iii) $a \equiv r \,(\mathrm{mod}\, n) \Longrightarrow a^k \equiv r^k \,(\mathrm{mod}\, n), \forall\, k \in \mathbb{Z}^+$

Demonstração:

$(i), (ii)$ e (iii) são conseqüências imediatas Proposição 1, ítem (ii). A demonstração de (iii) é feita através de indução sobre k. □

Atividade

Demonstre, usando indução sobre k, o ítem (iii) do Corolário 1

Cálculo do resto da divisão de um inteiro por 7 e 11

Vamos agora aplicar as propriedades de congruência que já estudamos para o cálculo do resto da divisão de um inteiro por outro número. O que é fantástico é que podemos calcular o resto sem efetuar a divisão, melhor ainda, sem ter que calcular o número que devemos dividir.

No exemplo a seguir, calculamos o resto da divisão de $N = 2^{123509}$ por 7 e 11. Não precisamos calcular explicitamente 2^{123509}, que, aliás, é um inteiro enorme com 37180 dígitos!

Exemplo 8
Seja N o (gigantesco) número inteiro dado por $N = 2^{123509}$. Vamos calcular o resto da divisão de N por 7 e por 11.

1. Resto da divisão de N por 7.

   Observe que 2^3 é a menor potência de 2 tal que $2^3 \equiv 1 \pmod 7$. Dividindo 123509 por 3 obtemos

   $$123509 = (41169) \times 3 + 2\,.$$

   Daí segue que

   $$N = 2^{123509} = 2^{3\times 41169+2} = 2^{3\times 41169}2^2 = (2^3)^{41169}(2^2)\,.$$

   Mas, $2^3 = 8 \equiv 1 \pmod 7$. Pelo corolário anterior, ítem (iii), temos que

   $$\begin{aligned} 2^3 \equiv 1 \pmod 7 \Longrightarrow (2^3)^{41169} &\equiv 1^{41169} \pmod 7 \\ \Rightarrow (2^3)^{41169} &\equiv 1 \pmod 7\,. \end{aligned}$$

   Pelo mesmo corolário, ítem (ii), temos que

   $$\begin{aligned} (2^3)^{41169} \equiv 1 \pmod 7 \text{ e } 4 \equiv 4 \pmod 7 \Rightarrow N &= (2^3)^{41169}2^2 \\ &\equiv 1 \times 4 = 4 \pmod 7\,. \end{aligned}$$

   Portanto, $N \equiv 4 \pmod 7$, isto é, o resto da divisão de N por 7 é 4.

2. Resto da divisão de N por 11.

   Basta observar que $2^5 = 32 \equiv -1 \pmod{11}$, e nesse caso

   $$2^{10} = 2^5 \cdot 2^5 \equiv (-1)\cdot(-1) = 1 \pmod{11}\,.$$

   Como $123509 = 12350 \cdot 10 + 9$ temos

   $$N = 2^{123509} = 2^{12350\times 10+9} = (2^{10})^{12350}(2^9)\,.$$

   Como $2^{10} \equiv 1 \pmod{11}$, temos pelo corolário anterior que

   $$N \equiv 1 \times 2^9 \pmod{11}\,.$$

   Mas, $2^9 = 2^5 \cdot 2^4$, $2^5 \equiv -1 \pmod{11}$ e $2^4 = 16 \equiv 5 \pmod{11}$.

   Daí segue que

   $$\begin{aligned} N \equiv 2^9 \pmod{11} \Rightarrow N \equiv 2^4 2^5 \pmod{11} &\Rightarrow N \equiv (-1)(5) \pmod{11} \\ \Rightarrow N \equiv -5 \pmod{11} &\Rightarrow N \equiv 6 \pmod{11}\,. \end{aligned}$$

   A resposta é o resto da divisão de N por 11 que é, portanto, igual a 6.

Note que nos dois exemplos anteriores usamos o truque de encontrar a menor potência 2^n tal que 2^n seja congruente a ± 1 (módulo o inteiro em questão). O problema é que nem sempre esta potência existe e nem sempre ela é pequena. Nestes casos é mais fácil reduzir o problema para um problema mais fácil e resolvê-lo, como no exemplo a seguir.

Exemplo **9**

Calcule o resto da divisão de 3^{1300} por 23.

Solução: As primeiras potências de 3 são:

$$3^1 = 3, 3^2 = 9, 3^3 = 27 \equiv 4 \pmod{23}, 3^4 = 81 \equiv 12 \pmod{23}, \cdots$$

Para obter ± 1 teríamos que até o expoente 11: $3^{11} \equiv 1 \pmod 3$

Pois é, não obtivemos ± 1 nestas primeiras potências. Aqui, ao invés de continuar procurando, podemos usar o $3^3 \equiv 4 \pmod{23}$, para reduzir o problema a um mais fácil.

Como $1300 = 3 \cdot 433 + 1$, então

$$3^{1300} = 3^{3\cdot 433+1} = (3^3)^{433}3^1 \equiv 4^{433}\dot{3} = 3 \cdot (2^2)^{433} = 3 \cdot 2^{866}$$

Não resolvemos o problema, mas caímos em problema menor. Podemos agora usar $2^5 = 32 \equiv 9 \pmod{23}$. Como $866 = 5 \cdot 173 + 1$, temos

$$N \equiv 3 \cdot 2^{866} = 3 \cdot 2^{5\cdot 173+1} = 3 \cdot 2 \cdot (2^5)^{173} \equiv 2 \cdot 3 \cdot 9^{173} = 2 \cdot 3 \cdot (3^2)^{173} = 2 \cdot 3^{347}$$

Aplicamos novamente o $3^3 \equiv 4 \pmod{23}$. Como $347 = 3 \cdot 115 + 2$ então

$$N \equiv 2\cdot 3^{3\cdot 115+2} = 2\cdot 3^2\cdot (3^3)^{115} \equiv 2\cdot 3^2\cdot 4^{115} = 2\cdot 3^2\cdot (2^2)^{115} = 3^2\cdot 2^{231} \pmod{23}$$

Aplicando sucessivamente $2^5 \equiv 9 \pmod{23}$ e $3^3 \equiv 4 \pmod{23}$ obtemos

$$\begin{aligned}
N &\equiv 3^2 \cdot 2^{231} = 3^2 \cdot 2^{5\cdot 46+1} = 3^2 \cdot 2 \cdot (2^5)^{46} \equiv 2 \cdot 3^2 \cdot 9^{46} = 2 \cdot 3^2 \cdot 3^{92} = 2 \cdot 3^{94} \\
&= 2 \cdot 3 \cdot (3^3)^{31} \equiv 2 \cdot 3 \cdot 4^{31} = 3 \cdot 2 \cdot (2^2)^{31} = 3 \cdot 2^{63} = 3 \cdot 2^{5\cdot 12+3} = 3 \cdot 2^3 \cdot (2^5)^{12} \\
&\equiv 3 \cdot 2^3 \cdot 9^{12} = 2^3 \cdot 3^{25} = 2^3 \cdot 3^{3\cdot 8+1} = 2^3 \cdot 3 \cdot (3^3)^8 \equiv 2^3 \cdot 3 \cdot 4^8 = 2^3 \cdot 3 \cdot 2^{16} \\
&= 3 \cdot 2^{19} = 3 \cdot 2^{3\cdot 5+4} = 3 \cdot 2^4 \cdot (2^5)^3 \equiv 2^4 \cdot 3 \cdot 9^3 = 2^4 \cdot 3^7 = 2^4 \cdot 3^{3\cdot 2+1} \\
&= 2^4 \cdot 3 \cdot (3^3)^2 \equiv 2^4 \cdot 3 \cdot 4^2 = 3 \cdot 2^8 = 3 \cdot 2^{5+3} = 3 \cdot 2^3 \cdot 2^5 \equiv 3 \cdot 8 \cdot 9 = 8 \cdot 3^3 \\
&\equiv 8 \cdot 4 = 32 \equiv 9 \pmod{23}
\end{aligned}$$

Portanto, o resto de 3^{1300} por 23 é 9.

Uma observação importante sobre este exemplo é que há uma maneira muito mais simples de achar o mesmo resultado! Aprenderemos mais tarde que $3^{22} \equiv 1 \pmod{23}$, o que simplifica muito as coisas!

Veremos que $a^{p-1} \equiv 1 \pmod p$ para todo p primo e a inteiro tal que $p \nmid a$. Este é o Pequeno Teorema de Fermat

Atividades

Calcule a resto da divisão de $N = 3^{345678}$ por 7, 11 e 13.

Sugestão: use o seguinte:

$$3^3 = 27 \equiv -1 \pmod 7,\ 3^5 = 243 \equiv 1 \pmod{11} \text{ e } 3^3 \equiv 1 \pmod{13}\ .$$

Critérios de divisibilidade

Nesta seção vamos estudar os critérios de divisibilidade. Estes são regras simples que permitem determinar rapidamente se um inteiro N é divisível por outro. Provavelmente você viu no ensino fundamental alguns critérios de divisibilidade. Talvez você ainda não conheça a prova de que estes critérios funcionam.

Seja $N = a_r a_{r-1} a_i a_1 a_0$ um número inteiro positivo, escrito na base decimal, onde $a_0, a_1, \cdots, a_r$ são os algarismos que compõem o número $(0 \leq a_i \leq 9,\ i = 0, \cdots, r)$. Então

$$N = (10)^r \cdot a_r + (10)^{r-1} \cdot a_{r-1} + \cdots + (10)^i \cdot a_i + \cdots + (10) \cdot a_1 + a_0\ .$$

A chave para estes critérios é ver o resto de 10 pelo inteiro que queremos estabelecer o critério.

Os casos $2, 5$ e 10 são particularmente simples, pois estes são divisores de 10. Como $10 \equiv 0 \pmod 2$ então

$$\begin{aligned} N &= (10)^r \cdot a_r + (10)^{r-1} \cdot a_{r-1} + \cdots + (10)^i \cdot a_i + \cdots + (10) \cdot a_1 + a_0 \\ &\equiv 0 \cdot a_r + 0 \cdot a_{r-1} + \cdots + 0 \cdot a_1 + a_0 = a_0 \pmod 2 \end{aligned}$$

Assim, $N \equiv a_0 \pmod 2$. Portanto

$$N \equiv 0 \pmod 2 \Leftrightarrow a_0 \equiv 0 \pmod 2$$

isto é, quando $a_0 = 0, 2, 4, 6$ ou 8 (lembre-se que $0 \leq a_0 \leq 9$).

Analogamente, como $10 \equiv 0 \pmod 5$ então

$$\begin{aligned} N &= (10)^r \cdot a_r + (10)^{r-1} \cdot a_{r-1} + \cdots + (10)^i \cdot a_i + \cdots + (10) \cdot a_1 + a_0 \\ &\equiv 0 \cdot a_r + 0 \cdot a_{r-1} + \cdots + 0 \cdot a_1 + a_0 = a_0 \pmod 5 \end{aligned}$$

Assim, $N \equiv a_0 \pmod 5$. Portanto,

$$N \equiv 0 \pmod 5 \Leftrightarrow a_0 \equiv 0 \pmod 5$$

isto é, quando $a_0 = 0$ ou 5.

Como $10 \equiv 0 \pmod{10}$ então, de maneira inteiramente análoga, $N \equiv a_0 \pmod{10}$. Assim,

$$N \equiv 0 \pmod{10} \Leftrightarrow a_0 \equiv 0 \pmod{10}$$

isto é, quando $a_0 = 0$.

Em resumo, provamos que um inteiro N é divisível por 2 quanto termina em $0, 2, 4, 6$ ou 8; divisível por 5 quando termina em 0 ou 5 e divisível por 10 quando termina em 0. Como observamos, estes critérios são fáceis de serem determinados porque $2, 5$ e 10 são divisores de 10. Em um grau de dificuldade maior estão os inteiros $3, 9$ e 11. Temos que:

$$\begin{aligned} 10 &\equiv 1 \pmod{3} \\ 10 &\equiv 1 \pmod{9} \\ 10 &\equiv -1 \pmod{11} \end{aligned}$$

Usaremos estas congruências para demonstrar os conhecidos critérios de divisibilidade por 3 e por 11 (deixaremos o 9 como exercício).

Critério de divisibilidade por 3

Proposição 2 (Divisibilidade por 3)
N é divisível por 3 se, e somente se, a soma $\sum_{i=0}^{r} a_i$ dos algarismos que compõe o número N, em sua expressão decimal, é um múltiplo de 3.

Demonstração:

Escrevemos $N = a_r \cdot a_{r-1} \cdots a_i \cdots a_1 a_0$ em expressão decimal. Assim,

$$N = (10)^r \cdot a_r + (10)^{r-1} \cdot a_{r-1} + \cdots + (10)^i \cdot a_i + \cdots + (10) \cdot a_1 + a_0 = \sum_{i=0}^{r} a_i 10^i \, .$$

Utilizando as propriedades de congruência provadas anteriormente, temos:

$$10 \equiv 1 \pmod{3} \Rightarrow 10^s \equiv 1 \pmod{3}, \forall\ s \geq 1 \text{ inteiro}$$

Logo,

$$(10)^i \cdot a_i \equiv a_i \times 1 = a_i \pmod{3}, \forall i \text{ inteiro}$$

e assim

$$N = \sum_{i=0}^{r} a_i 10^i \equiv \sum_{i=0}^{r} a_i \times 1 = \sum_{i=0}^{r} a_i \pmod{3} \Longrightarrow N \equiv \sum_{i=0}^{r} a_i \pmod{3} \, .$$

Assim

$$N \text{ é múltiplo de } 3 \iff N \equiv 0 \pmod 3 \iff \sum_{i=0}^{r} a_i \equiv 0 \pmod 3$$
$$\iff \sum_{i=0}^{r} a_i \text{ é múltiplo de } 3,$$

demonstrando o critério de divisibilidade por 3. □

Exemplo **10**
O inteiro 349803 é divisível por 3, pois $3 + 4 + 9 + 8 + 0 + 3 = 27$ que é múltiplo de 3.

Atividade

Enuncie e demonstre o critério de divisibilidade por 9.

Sugestão: Siga os mesmos passos da demonstração do critério da divisão por 3.

Critério de divisibilidade por 11

O critério de divisibilidade por 11 é o seguinte:

Proposição 3 (Divisibilidade por 11)
$N = a_r \cdot a_{r-1} \cdots a_i \cdots a_1 a_0$ é divisível por 11 se, e somente se, a soma alternada $\sum_{i=0}^{r} (-1)^i \cdot a_i$ é um múltiplo de 11.

Exemplo **11**
O inteiro 37196791709 é um múltiplo de 11, pois

$$3 - 7 + 1 - 9 + 6 - 7 + 9 - 1 + 7 - 0 + 9 = 11$$

é múltiplo de 11.

Demonstração da proposição:

Seja $N = a_r \cdot a_{r-1} \cdots a_i \cdots a_1 + a_0$ a expressão decimal de N. Assim,

$$N = (10)^r \cdot a_r + (10)^{r-1} \cdot a_{r-1} + \cdots + (10)^i \cdot a_i + \cdots + (10) \cdot a_1 + a_0 \,.$$

Como $10 \equiv -1 \pmod{11}$, então

$$10^i \equiv (-1)^i = \begin{cases} 1, \text{ se i é par} \\ -1, \text{ se i é ímpar} \end{cases}$$

Assim,

$$\begin{aligned} N &= a_r \cdot a_{r-1} \cdots a_i \cdots a_1 + a_0 \\ &\equiv a_0 + a_1(-1) + a_2.1 + a_3(-1) + a_4.1 + a_5(-1) + \cdots + (-1)^r \cdot a_r \pmod{11} \\ &= a_0 - a_1 + a_2 - a_3 + a_4 - a_5 \cdots \end{aligned}$$

Portanto,

$$N \text{ é múltiplo de } 11 \iff N \equiv 0 \pmod{11} \iff \sum_{i=0}^{r} (-1)^i \cdot a_i \equiv 0 \pmod{11}$$

$$\iff \text{a soma alternada } \sum_{i=0}^{r} (-1)^i \cdot a_i \text{ é múltiplo de } 11\,.$$

o que demonstra o critério de divisibilidade por 11. □

Atividade

Elabore um exemplo para o critério de divisibilidade acima. Por exemplo, multiplique 11 por algum inteiro n e verifique que $11n$ satisfaz o critério de divisibilidade por 11.

Um pouco mais sobre divisibilidade

É possível combinar critérios de divisibilidade. Por exemplo, um inteiro é múltiplo de 55 se, e somente se, é múltiplo de 5 e 11 simultaneamente. O que garante isso é o seguinte lema simples:

Lema 3
Sejam, p e q primos distintos, o inteiro N é múltiplo de pq se, e somente se, N é múltiplo de p e q.

Demonstração: Se N é múltiplo de pq, então $N = k(pq)$ para algum $k \in \mathbb{Z}$, logo

$$N = (kq)p = (kq)p$$

ou seja, N é múltiplo de p e de q.

Assuma agora que $p \mid N$ e $q \mid N$. Então estes primos estão presentes na expressão de N como produto de fatores primos, isto é,

$$N = p^i.q^j.\cdots, \text{ com } i, j \geq 1\,.$$

Portanto $pq \mid N$. □

É fácil ver que o mesmo acontece para um número qualquer de primos distintos: um inteiro N é divisível por $p_1, p_2, p_3, \cdots$ se, e somente se, N é simultaneamente divisível por $p_1, p_2, p_3, \cdots$.

Como aplicação deste lema vejamos o seguinte exemplo.

Exemplo **12**

Mostre que 98275320 é múltiplo de 55.

Solução: Como $55 = 5.11$, basta mostrar que 55 é múltiplo de 5 e 11 simultaneamente.

Como o último algarismo de 98275320 é 0 então é múltiplo de 5. Com relação ao 11, temos que a soma alternada dos algarismos de 98275320 é $9 - 8 + 2 - 7 + 5 - 3 + 2 - 0 = 0$, o que mostra que 98275320 é múltiplo de 11.

Atividades

Mostre que um inteiro N é divisível por primos distintos $p_1, p_2, p_3, \cdots$ se, e somente se, N é simultaneamente divisível por cada um dos primos $p_1, p_2, p_3, \cdots$.

Resumo

Nesta aula estabelecemos mais algumas propriedades de congruência e abordamos os critérios de divisibilidade por 3 e 11. Podemos testar a divisibilidade por produto de primos distintos $p_1.p_2.p_3 \ldots$ testando a divisibilidade por cada um deles.

Exercícios

1. Calcule:

   (a) $2^{6736730} \pmod 7$

   (b) $3^{123400} \pmod{11}$

   (c) $13^{234500} \pmod{19}$

2. Mostre que o inteiro $N = a_r a_{r-1} \cdots a_1 a_0$ é múltiplo de 4 se, e somente se, o inteiro $a_1 a_0$ é múltiplo de 4.

   Sugestão: Note que $10^r \equiv 0 \pmod 4$ para $r \geq 2$.

3. Generalize o resultado anterior para qualquer potência de 2.

4. Sejam $N = a_r a_{r-1} \cdots a_1 a_0$ e $N_1 = a_r a_{r-1} \cdots a_1$. Mostre que N é divisível por 7 se, e somente se, $N_1 - 2a_0$ é divisível por 7.

   Exemplo: Se $N = 3507$ então $N_1 = 350$ e $N_1 - 2a_0 = 350 - 2 \cdot 7 = 350 - 14 = 336$. Tanto 336 quanto 3507 são divisíveis por 7.

   Embora o resultado acima seja um critério de divisibilidade por 7, não é nada prático, uma vez que determinar se $N_1 - 2a_0$ é divisível por 7 é quase tão difícil quanto determinar se N é divisível por 7.

Aula 11 – O anel dos inteiros módulo n

Metas

Nesta aula introduziremos operações de soma e produto de classes de congruência munindo $\mathbb{Z}_n$ de uma estrutura de anel comutativo com unidade multiplicativa 1.

Objetivos

- Definir e operar com soma e produto de classes de congruência;
- definir a noção de anel comutativo com unidade (multiplicativa) apresentando $\mathbb{Z}_n, +, \cdot$ como um desses modelos de anéis.

Introdução

Nesta aula usaremos propriedades básicas essenciais de congruência para definir soma e produto de classes de congruência em $\mathbb{Z}_n$, e apresentar $\mathbb{Z}_n, +, \cdot$ como um modelo de anel comutativo com unidade.

O anel $\mathbb{Z}_n$ dos inteiros módulo n

Agora vamos introduzir operações de soma e produto de classes de congruências, mostrando que as definições são "boas", no sentido de que não dependem da escolha de representantes das classes de congruência.

Seja $n \in \mathbb{Z}^+$ um dado inteiro, e sejam $\overline{a}, \overline{b}$ duas classes de congruência módulo n. Nosso objetivo é definir uma *soma e produto de classes*.

A definição mais natural é

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{e} \quad \overline{a} \cdot \overline{b} = \overline{ab}\,.$$

O problema é que uma classe tem vários (infinitos, na verdade) representantes possíveis. Qualquer definição que envolva representantes de uma classe só é interessante se não depender do representante utilizado. É o que teremos que garantir para nossas definições de soma e produto.

Observe que se $a \equiv a' \pmod{n}$ e $b \equiv b \pmod{n}$ então

$$\begin{cases} a+b & \equiv & (a'+b') \pmod{n} \\ a \cdot b & \equiv & (a' \cdot b') \pmod{n} \end{cases}$$

Assim, $\overline{(a+b)} = \overline{(a'+b')}$ e $\overline{(a \cdot b)} = \overline{(a' \cdot b')}$ e temos igualdades de classes com representantes distintos.

Portanto a classe da soma e a classe do produto não depende da escolha dos representantes que escolhemos para as respectivas classes. Definimos então:

Definição 1 (Soma e produto de classes)
Sejam $\overline{a}$ e $\overline{b}$ classes em $\mathbb{Z}_n$. definimos

$$\overline{a+b} = \overline{a} + \overline{b}$$
$$\overline{(a \cdot b)} = \overline{a} \cdot \overline{b}$$

Como mostramos que

$$\overline{a} = \overline{a'} \quad e \quad \overline{b} = \overline{b'} \Rightarrow \overline{(a+b)} = \overline{(a'+b')} \quad \text{e} \quad \overline{(a \cdot b)} = \overline{(a' \cdot b')}$$

então o resultado das operações, soma e produto, com classes não muda se mudarmos os representantes das classes.

Agora o conjunto $\mathbb{Z}_n$ está munido de operações soma e produto de classes. Vamos escrever esse modelo como $\mathbb{Z}_n, +, \cdot$.

As propriedades básicas de $\mathbb{Z}_n, +, \cdot$

Vamos ver aqui que várias propriedades do anel dos inteiros $\mathbb{Z}, +, \cdot$, com a soma e produto usuais, se transferem para $\mathbb{Z}_n, +, \cdot$. Mostraremos, em particular, que $\mathbb{Z}_n, +, \cdot$ é um anel.

No entanto, há diferenças entre $\mathbb{Z}$ e $\mathbb{Z}_n$. Para começar, $\mathbb{Z}, +, \cdot$ é um anel infinito, enquanto que $\mathbb{Z}_n, +, \cdot$ é sempre um anel finito. Veremos também, na próxima aula, diferenças bastante importantes no que se refere aos chamados "divisores de zero".

Propriedades de soma de classes

(1) A soma de classes é associativa, isto é,

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c}), \forall\, \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$$

(2) Existe uma classe $\overline{0}$ tal que

$$\overline{a}+\overline{0}=\overline{0}+\overline{a}=\overline{a},\ \forall\,\overline{a}\in\mathbb{Z}_n$$

(3) Para toda classe $\overline{a}\in\mathbb{Z}_n$ existe uma classe $\overline{b}=\overline{(-a)}$ tal que

$\overline{a}+\overline{b}=\overline{b}+\overline{a}=\overline{0}$, (isto é, toda classe $\overline{a}$ possui uma classe *inverso aditivo* de $\overline{a}$)

(4) A soma de classes é comutativa, isto é,

$$\overline{a}+\overline{b}=\overline{b}+\overline{a},\ \forall\,\overline{a},\overline{b}\in\mathbb{Z}_n$$

Demonstração:

Vamos fazer a demonstração das propriedades em relação à soma. Sejam $\overline{a},\overline{b},\overline{c}\in\mathbb{Z}_n$.

(1)

$$\overline{a}+\overline{b}=\overline{(a+b)}\Longrightarrow(\overline{a}+\overline{b})+\overline{c}=\overline{(a+b)}+\overline{c}=\overline{[(a+b)+c]}$$

Mas $(a+b)+c=a+(b+c)$ com $a,b,c\in\mathbb{Z}$. Logo,

$$\overline{[(a+b)+c]}=\overline{[a+(b+c)]}=\overline{a}+\overline{(b+c)}=\overline{a}+(\overline{b}+\overline{c})\,.$$

(2)

$$\begin{aligned}\overline{a}+\overline{0} &= \overline{[(a+0)]}=\overline{a}\\ \overline{0}+\overline{a} &= \overline{[(0+a)]}=\overline{a}\,.\end{aligned}$$

(3)

Seja $\overline{y}=\overline{(-a)}$ onde $-a$ é o inverso aditivo de a em $\mathbb{Z}$. Assim,

$$\begin{aligned}\overline{a}+\overline{y} &= \overline{(a+y)}=\overline{(a+(-a))}=\overline{0}\\ \overline{y}+\overline{a} &= \overline{(y+a)}=\overline{((-a)+a)}=\overline{0}\,.\end{aligned}$$

(4)

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

já que $a+b=b+a$ em $\mathbb{Z}$.

■

Propriedades básicas de produto de classes

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

(5) O produto de classes é associativo, isto é,

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

(6) Existe $\overline{1} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{1} = \overline{1} \cdot \overline{a} = \overline{a}$ (existe unidade multiplicativa $\overline{1}$ em $\mathbb{Z}_n$)

(7) O produto de classes é comutativo, isto é,

$$\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$$

Leis distributivas

(8)

$$\begin{cases} \overline{a} \cdot (\overline{b} + \overline{c}) &= \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c} \\ (\overline{a} + \overline{b}) \cdot \overline{c} &= \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c} \end{cases}$$

Demonstração:

(5)

$$\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{(b \cdot c)} = \overline{[a \cdot (b \cdot c)]} = \overline{(a \cdot b) \cdot c} = \overline{(a \cdot b)} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$$

(aqui usamos a associatividade $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ em $\mathbb{Z}$).

(6)

$$\begin{aligned} \overline{a} \cdot \overline{1} &= \overline{(a \cdot 1)} = \overline{a} \\ \overline{1} \cdot \overline{a} &= \overline{(1 \cdot a)} = \overline{a}\,. \end{aligned}$$

(7)

$$\overline{a} \cdot \overline{b} = \overline{(a \cdot b)} = \overline{(b \cdot a)} = \overline{b} \cdot \overline{a}$$

(aqui usamos a comutatividade $a \cdot b = b \cdot a$ em $\mathbb{Z}$).

(8)

$$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{(b + c)} = \overline{[a \cdot (b + c)]} = \overline{(a \cdot b + a \cdot c)} = \overline{(a \cdot b)} + \overline{(a \cdot c)} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$$

(aqui usamos a distributividade $a \cdot (b + c) = a \cdot b + a \cdot c$ em $\mathbb{Z}$).

Também temos que:

$$(\overline{a}+\overline{b})\cdot\overline{c} = \overline{(a+b)}\cdot\overline{c} = \overline{[(a+b)\cdot c]} = \overline{[a\cdot c + b\cdot c]} = \overline{a}\cdot\overline{c} + \overline{b}\cdot\overline{c}$$

(aqui usamos a distributividade $(a+b)\cdot c = a\cdot c + b\cdot c$ em $\mathbb{Z}$).

Tendo em vista que $\mathbb{Z}_n, +, \cdot$ satisfaz as 8 propriedades ele é chamado de um modelo de anel comutativo com unidade (multiplicativa) $\overline{1}$.

Observe que $\mathbb{Z}, +, \cdot$ é também um modelo de anel comutativo com unidade $1 \in \mathbb{Z}$, mas que satisfaz ainda uma nova propriedade:

(9) $\mathbb{Z}$ não possui divisores de zero, isto é, para todo $a, b \in \mathbb{Z}$, a e b diferentes de zero, tem-se $a \cdot b \neq 0$.

O modelo $\mathbb{Z}_n, +, \cdot$ nem sempre satisfaz essa nova propriedade. Vamos mostrar que apenas se $n = p$ é um número primo o modelo $\mathbb{Z}_p$ satisfaz a propriedade 9 e uma propriedade 10 mais forte que a 9.

(10) Seja $p \geq 2$ primo. Para todo $\overline{a} \in \mathbb{Z}_p$ existe uma classe $\overline{b} \in \mathbb{Z}_p$ tal que $\overline{a}\overline{b} = \overline{1}$.

Isto é, todo elemento não-nulo possui um inverso multiplicativo.

De maneira geral, um conjunto $A, +, \cdot$ com operações de soma $+$ e multiplicação $\cdot$ é chamado **Anel comutativo com unidade** quando satisfaz as propriedades (1) a (8) listadas anteriormente.

O modelo $\mathbb{Z}, +, \cdot$ é um anel e provamos acima que $\mathbb{Z}_n, +\cdot$ é um anel para qualquer $n > 1$.

Se, além disso, o anel satisfizer a propriedade (9) então é chamado **Domínio de Integridade**. Temos que $\mathbb{Z}$ é um domínio de integridade, mas, como mostraremos na próxima aula, $\mathbb{Z}_n$ é domínio de integridade se, e somente se, n é primo.

Se o anel satisfizer a propriedade (10) então é chamado **Corpo**. O domínio de integridade $\mathbb{Z}$ não é corpo, mas $\mathbb{Z}_n$ é corpo sempre que n é primo. Tudo isto será demonstrado na próxima aula.

Tabelas de operações em $\mathbb{Z}_n$

Vamos construir algumas tabelas se soma e multiplicação das classes em $\mathbb{Z}_n$. Estas tabelas dispõe as classes de $\mathbb{Z}_n$ nas primeiras linha e coluna e o resultado das operações do interior da tabela.

Vamos aos exemplos.

Exemplo **13**
Tabelas de soma e produto de $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Soma em $\mathbb{Z}_3$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Produto em $\mathbb{Z}_3$

Vamos fazer um outro exemplo deste tipo.

Exemplo **14**
Tabelas de soma e produto de $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Soma em $\mathbb{Z}_6$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Produto em $\mathbb{Z}_6$

Resumo

Nessa aula apresentamos as definições de soma e produto em $\mathbb{Z}_n$. Estas foram induzidas a partir das definições de soma e produto em $\mathbb{Z}$.

As oito produtos básicas das operações de soma e produto em $\mathbb{Z}$ se transferiram para soma e produto em $\mathbb{Z}_n$, o que torna $\mathbb{Z}_n$ um anel comutativo com unidade, tal como $\mathbb{Z}$.

O que diferencia a estrutura algébrica de $\mathbb{Z}$ e $\mathbb{Z}_n$ são as propriedades (9) e (10) descritas anteriormente. O anel $\mathbb{Z}$ satisfaz a propriedade (9) e é,

portanto, um Domínio de Integridade, mas não satisfaz a propriedade (10), isto é, não é corpo.

Para $\mathbb{Z}_n$ temos duas situações diferentes, dependendo de n. Se n não é primo, então $\mathbb{Z}_n$ não é Domínio de Integridade e se n é primo então $\mathbb{Z}_n$ é um corpo. Tudo isto será demonstrado na próxima aula.

Veremos que todo corpo é domínio de integridade. Por isto dizer que $\mathbb{Z}_n$ é corpo para n primo implica que $\mathbb{Z}_n$ também é domínio

Atividades

1. Escreva as tabelas de operações de soma e multiplicação de $\mathbb{Z}_n$, para os seguintes valores de n.

   (a) $n = 2$

   (b) $n = 5$

   (c) $n = 7$

   (d) $n = 12$

2. Seja $f\colon \mathbb{Z}_6 \to \mathbb{Z}_6$ a função definida por $f(x) = 2x + \overline{1}$. Determine

$$\mathrm{Im}(f) = \{f(\overline{a}) \mid \overline{a} \in \mathbb{Z}_6\} \subset \mathbb{Z}_6 \ .$$

   A função é sobrejetiva? É injetiva?

3. Responda as mesmas perguntas do exercício anterior para a função $f\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ definida por $f(x) = 2x + \overline{1}$.

Aula 12 – inversos multiplicativos e divisores de zero em $\mathbb{Z}_n$

Metas

Apresentar $\mathbb{Z}_n, +, .$, com propriedades específicas que dependem da escolha de n.

Objetivos

Ao final desta aula você deve ser capaz de:

- Determinar para que valores de n existem divisores de zero em $\mathbb{Z}_n$.
- Determinar quais elementos em $\mathbb{Z}_n$ possuem inverso multiplicativo e quais são divisores de zero.

Introdução

Vimos na aula passada que $\mathbb{Z}_n, +, .$ é um anel comutativo com unidade $\overline{1}$. Para resolvermos equações envolvendo congruências necessitamos de algumas propriedades específicas que nos permitam explicitar as soluções dessas congruências.

Nessa aula vamos dar continuidade ao estudo da estrutura algébrica de $(\mathbb{Z}_n, +, \cdot)$. Vamos estudar propriedades e situações especiais envolvendo o produto em $\mathbb{Z}_n$.

Os dois conceitos fundamentais introduzidos nesta aula são os de *divisor de zero* e o de *inverso multiplicativo*. Vamos a eles!

Divisores de zero

Vimos estudando divisores de inteiros desde o 1^o grau: d é divisor de n se existe algum inteiro k tal que $n = d.k$. Se $n = 0$ então qualquer inteiro d é divisor de zero no sentido usual da palavra divisor, pois $n = d.0$.

Em $\mathbb{Z}_n$ também vale que o produto de qualquer classe $\overline{a}$ pela classe nula é a classe nula: $\overline{a}.\overline{0} = \overline{0}$.

Mas aqui existe uma diferença fundamental entre $\mathbb{Z}$ e $\mathbb{Z}_n$: nos inteiros o produto de dois números diferentes de zero é um número diferente de zero.

O mesmo pode não acontecer em $\mathbb{Z}_n$. Para certos valores de n existem classes $\overline{a} \neq \overline{0}$ e $\overline{b} \neq \overline{0}$ tais que $\overline{a}.\overline{b} = \overline{0}$.

Vamos estudar agora exatamente este tipo de situação. Para começar, vamos dar uma definição para a expressão "divisor de zero" que se aplica exatamente a estas situações.

Definição 1 (Divisor de zero)
Uma classe $\overline{a} \neq \overline{0}$ é chamada divisor de zero em $\mathbb{Z}_n$ quando existe uma classe $\overline{b} \neq \overline{0}$ tal que $\overline{ab} = \overline{0}$

Observe que, no sentido dado pela definição acima, *não há divisores de zero em* $\mathbb{Z}$, pois o produto de inteiros não-nulos é sempre um inteiro não-nulo.

Agora daremos um exemplo mostrando que existem divisores de zero em $\mathbb{Z}_6$.

Exemplo **15**
Observe a tabela de multiplicação de $\mathbb{Z}_6$.

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Como $\overline{2}.\overline{3} = \overline{3}.\overline{2} = \overline{0}$ então $\overline{2}$ e $\overline{3}$ são divisores de zero em $\mathbb{Z}_6$. Da mesma forma, $\overline{3}.\overline{4} = \overline{0}$ mostra que $\overline{4}$ também é divisor de zero. Assim as classes $\overline{2}$, $\overline{3}$ e $\overline{4}$ são divisores de zero em $\mathbb{Z}_6$.

Atividades

1. Encontre os divisores de zero em $\mathbb{Z}_8$.

2. Mostre que $\mathbb{Z}_7$ não tem divisores de zero.

3. Mostre que a classe $\overline{5}$ é um divisor de zero em $\mathbb{Z}_{10}$, mas a classe $\overline{5}$ não é um divisor de zero em $\mathbb{Z}_6$.

Quando $\mathbb{Z}_n$ tem divisores de zero?

Vimos que $\mathbb{Z}_6$ possui 3 divisores de zero: as classes $\overline{2}$, $\overline{3}$ e $\overline{4}$. Por outro lado, $\mathbb{Z}_7$ não possui divisores de zero. A pergunta natural aqui é a seguinte: para que valores de $n \geq 2$ o anel $\mathbb{Z}_n$ possui divisores de zero? A próxima proposição responde a esta pergunta.

Proposição 1
Seja $n \geq 2$, um dado número inteiro. O anel $\mathbb{Z}_n$ possui divisores de zero se, e somente se, n não é um número primo.

Demonstração.

($\Rightarrow$) Vamos iniciar provando que $\mathbb{Z}_n$ possui divisores de zero então n é composto.

Suponha que $\mathbb{Z}_n$ possua divisores de zero. Sejam $\overline{a}, \overline{b} \in \mathbb{Z}_n$ tais que $\overline{a}\overline{b} = \overline{0}$. Então

$$\overline{a}\overline{b} = \overline{0} \Rightarrow ab \equiv 0 \pmod{n} \Rightarrow n \mid ab$$

Note que as classes $\overline{a}, \overline{b}$ não são necessariamente distintas. Por exemplo, $\mathbb{Z}_4$ possui um único divisor de zero, que é a classe $\overline{2}$. Neste caso, $\overline{2} \cdot \overline{2} = \overline{0}$.

Se n fosse um primo, então $n \mid ab$ implicaria em $n \mid a$ ou $n \mid b$, isto é, $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, o que contraria a hipótese de que $\overline{a} \neq 0$ e $\overline{b} \neq 0$.

Assim, se existirem divisores de zero em $\mathbb{Z}_n$ então n não é um número primo.

($\Leftarrow$)

Vamos agora provar que se n não é um primo então $\mathbb{Z}_n$ tem divisores de zero.

Suponha que $n = ab$, onde $1 < a, b < n$.

Como $1, a, b < n$ então $\overline{a} \neq \overline{0}$ e $\overline{b} \neq \overline{0}$. Como

$$n = ab \Rightarrow \overline{a} \cdot \overline{b} = \overline{n} = \overline{0}$$

e, assim, $\mathbb{Z}_n$ tem divisores de zero. □

Uma outra maneira de escrever a Proposição 1 é a seguinte: $\mathbb{Z}_n$ não possui divisores de zero se, e somente se, n é um número primo.

Atividades

Reveja todos os exemplos de $\mathbb{Z}_n$ com os quais já trabalhamos e verifique que a Proposição 1 se aplica.

Inversos multiplicativos em $\mathbb{Z}_n$

Nesta seção vamos estudar uma outra propriedade importante com relação a multiplicação das classes em $\mathbb{Z}_n$: a de terem ou não inverso multiplicativo.

Vamos voltar a tabela de multiplicação de $\mathbb{Z}_6$. Para a classe $\overline{2}$, não há uma outra classe $\overline{b}$ tal que $\overline{2} \cdot \overline{b} = \overline{1}$. O mesmo vale para as classes $\overline{3}$ e $\overline{4}$.

Por outro lado, observe as classes $\overline{1}$ e $\overline{5}$. Temos

$$\overline{1} \cdot \overline{1} = \overline{1} \quad \text{e} \quad \overline{5} \cdot \overline{5} = \overline{1}$$

As classes $\overline{1}$ e $\overline{5}$ são o que se poderia chamar de "divisores de um", mas não é essa a expressão mais usada. É mais comum falarmos que uma classe possui "inverso multiplicativo". Vamos escrever a definição exata e depois voltamos ao $\mathbb{Z}_6$.

Definição 2 (Inverso multiplicativo)
Seja $\overline{a} \neq \overline{0}$ em $\mathbb{Z}_n$. Dizemos que $\overline{a}$ possui inverso multiplicativo em $\mathbb{Z}_n$ se existe uma classe $\overline{b} \in \mathbb{Z}_n$ tal que

$$\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} = 1$$

Uma classe $\overline{a}$ que possui inverso multiplicativo em $\mathbb{Z}_n$ é chamada *invertível*.

Voltando ao $\mathbb{Z}_6$, vimos que as classes $\{\overline{1}, \overline{5}\}$ possuem inverso multiplicativo, ao passo que as classes $\{\overline{2}, \overline{3}, \overline{4}\}$ não possuem inverso multiplicativo.

Neste ponto você deve ter percebido que os elementos de $\mathbb{Z}_6 \backslash \{\overline{0}\}$ que não possuem inverso multiplicativo são exatamente os 3 divisores de zero de $\mathbb{Z}_6$. Mostraremos, no próximo Lema, que este é sempre o caso: um divisor de zero em $\mathbb{Z}_n$ nunca possui inverso multiplicativo.

Lema 4
Seja $\overline{a} \in \mathbb{Z}_n$ um divisor de zero. A classe $\overline{a}$ não possui inverso multiplicativo.

Demonstração.

Suponha que $\overline{a}$ possua algum inverso multiplicativo $\overline{b} \in \mathbb{Z}_n$, isto é $\overline{a} \cdot \overline{b} = \overline{1}$.

Como $\overline{a}$ é divisor de zero em $\mathbb{Z}_n$, então existe algum $\overline{c} \neq \overline{0}$ em $\mathbb{Z}_n$, com tal que

$$\overline{a} \cdot \overline{c} = \overline{0}\,.$$

Multiplicando ambos os lados desta equação por $\overline{b}$, obtemos:

$$\overline{a}\cdot\overline{c}\cdot\overline{b}=\overline{0}\cdot\overline{b}\Rightarrow\left(\overline{a}\cdot\overline{b}\right)\cdot\overline{c}=\overline{0}\Rightarrow\overline{1}\cdot\overline{c}=\overline{0}\Rightarrow\overline{c}=\overline{0}\,,$$

o que contradiz o fato de que $\overline{c}\neq\overline{0}$. □

Muito bem, agora sabemos que os divisores de zero não são inversíveis. Mas quem são os inversíveis? No caso de $\mathbb{Z}_6$, todos os não divisores de zero (as classes $\{\overline{1},\overline{5}\}$) são inversíveis. Será que este é sempre o caso?

A próxima proposição dá uma caracterização de todos os elementos inversíveis em $\mathbb{Z}_n$.

Proposição 2
Seja $n\geq 2$. Uma classe $\overline{a}\in\mathbb{Z}_n$ possui inverso multiplicativo se, e somente se, $\text{mdc}(a,n)=1$.

Demonstração.

($\Rightarrow$)

Suponhamos que $\overline{a}\neq\overline{0}$ possua um inverso multiplicativo $\overline{b}\neq\overline{0}$ em $\mathbb{Z}_n$. Assim, $\overline{a}\cdot\overline{b}=\overline{1}$. segue que

$$\overline{a}\cdot\overline{b}=\overline{1}\Rightarrow\overline{ab}=\overline{1}\Rightarrow ab\equiv 1\pmod{n}\Rightarrow ab-1=kn\Rightarrow ab-kn=1\,,$$

para algum $k\in\mathbb{Z}$.

Seja $d\geq 1$ um divisor comum de n e a. Então $d\mid a$ e $d\mid n$, logo

$$\left.\begin{array}{l} d\mid a\Rightarrow d\mid ab\\ d\mid n\Rightarrow d\mid kn\end{array}\right\}\Rightarrow d\mid(ab-kn)\Rightarrow d\mid 1\Rightarrow d=1$$

Concluímos então que $\text{mdc}(a,n)=1$.

($\Leftarrow$)

Suponha agora que $\text{mdc}(a,n)=1$. Vamos mostrar que $\overline{a}$ possui inverso multiplicativo em $\mathbb{Z}_n$.

Como $\text{mdc}(a,n)=1$ então existem $r,s\in\mathbb{Z}$ tais que $ra+sn=1$. Segue-se que

$$\overline{1}=\overline{ra+sn}\Rightarrow\overline{1}=\overline{r}\cdot\overline{a}+\overline{s}\cdot\overline{n}=\overline{r}\cdot\overline{a}+\overline{s}\cdot\overline{0}=\overline{r}\cdot\overline{a}+\overline{0}=\overline{r}\cdot\overline{a}\,,$$

onde usamos o fato de que $\overline{n}=\overline{0}$. De $\overline{r}\cdot\overline{a}=\overline{1}$ resulta que $\overline{a}$ possui inverso multiplicativo em $\mathbb{Z}_n$. □

Atividades

Construa a tabela de multiplicação de $\mathbb{Z}_{12}$. Verifique as classes invertíveis são as classes $\overline{a}$, com $1 \leq a \leq 11$, tais que $\text{mdc}(a, 12) = 1$.

Inversíveis e divisores de zero em $\mathbb{Z}_n$

Já vimos que os divisores de zero em $\mathbb{Z}_n$ não são inversíveis e vimos que os inversíveis em $\mathbb{Z}_n$ são exatamente as classes $\overline{a}$ tais que $\text{mdc}(a, n) = 1$.

Mostraremos agora que os elementos não-nulos de $\mathbb{Z}_n$ que não são inversíveis são divisores de zero. Já havíamos observado isto para o anel $\mathbb{Z}_6$. Nele, temos:

$$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\} = \{\overline{0}\} \cup \underbrace{\{\overline{1}, \overline{5}\}}_{\text{inversíveis}} \cup \underbrace{\{\overline{2}, \overline{3}, \overline{4}\}}_{\text{divisores de zero}}$$

Proposição 3
Os elementos não-nulos de $\mathbb{Z}_n$ que não são inversíveis são divisores de zero.

Demonstração.

Seja $\overline{a} \in \mathbb{Z}_n$ não nulo e não invertível. Pela Proposição 2, temos que, como $\overline{a}$ não é invertível,

$$\text{mdc}(a, n) = d > 1 \, .$$

Como $d \mid a$ e $d \mid n$, existem inteiros e e f tais que $a = d.e$ e $n = d.f$. Multiplicando a por f temos

$$af = def = (df)e = ne \Rightarrow \overline{af} = \overline{ne} \Rightarrow \overline{a} \cdot \overline{f} = \overline{e} \cdot \overline{n} = \overline{e} \cdot \overline{0} = \overline{0}$$

Como $n = df$ e $d > 1$, então $1 \leq f < n$ e assim $\overline{f} \neq \overline{0}$. De $\overline{a} \cdot \overline{f} = \overline{0}$, resulta que $\overline{a}$ é divisor de zero. $\square$.

Comparando as Proposições 2 e 3 vemos que os divisores de zero em $\mathbb{Z}_n$ são exatamente as classes $\overline{a}$ tais que $\overline{a} \neq \overline{0}$ e $\text{mdc}(a, n) > 1$.

Assim, provamos que para qualquer n, temos:

$$\mathbb{Z}_n = \{\overline{0}\} \quad \cup \quad \underbrace{\{\overline{a} \mid \text{mdc}(a, n) = d > 1\}}_{\text{divisores de zero}} \quad \cup \quad \underbrace{\{\overline{a} \mid \text{mdc}(a, n) = 1\}}_{\text{inversíveis}}$$

Atividades

Determine todos os divisores de zero e todos os elementos inversíveis em $\mathbb{Z}_n$ para os seguintes inteiros n:

1. $n = 8$
2. $n = 10$
3. $n = 12$

O corpo $\mathbb{Z}_p$

No caso do anel $\mathbb{Z}_p$, com p um primo, todos os elementos não-nulos são inversíveis, isto é, não há divisores de zero, como mostra o seguinte corolário da Proposição 2.

Corolário 2
Se $p \geq 2$ é um número primo, então todo elemento $\overline{a} \neq \overline{0}$ em $\mathbb{Z}_p$ possui inverso multiplicativo.

Demonstração.

Seja $p \geq 2$ um número primo e seja $\overline{a} \neq \overline{0}$. Temos que

$$\overline{a} \neq \overline{0} \Rightarrow p \not| a \, .$$

Como p é primo e $p \not| a$ então $\text{mdc}(a, p) = 1$. Pela Proposição 2 segue-se que $\overline{a}$ possui inverso multiplicativo. □

Encontramos aqui um anel com uma propriedade especial muito importante: a de que todo elemento não-nulo possui inverso multiplicativo. Anéis deste tipo são chamados *corpos* e possuem grande importância na Álgebra.

Definição 3 (Corpo)
Um anel comutativo com unidade tal que todo elemento não-nulo possui inverso multiplicativo é chamado um *corpo*.

Portanto, o anel $\mathbb{Z}_p, +, \cdot$, com $p \geq 2$ primo, é um corpo. Este é um corpo com exatamente p elementos:

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\} \, .$$

Este é, portanto, um corpo com um número finito de elementos, ou seja, um *corpo finito*.

O anel $\mathbb{Z}$ não é um corpo. Os únicos inteiros não-nulos que possuem inverso multiplicativo são os inteiros $\{+1, -1\}$. Os outros inteiros não possuem inverso multiplicativo.

Já o anel $\mathbb{Q}$, dos números racionais, é um corpo. Todo número $\frac{m}{n}$, com $m, n \neq 0$, possui inverso multiplicativo, a saber, o inteiro $\frac{n}{m}$,pois

$$\frac{m}{n} \times \frac{n}{m} = 1$$

Calculando o inverso multiplicativo de $\overline{a}$ em $\mathbb{Z}_n$

Se $\text{mdc}(a, n) = 1$ então a classe $\overline{a}$ possui inversa multiplicativa. Mas como calcular esta inversa?

Vimos que

$$\text{mdc}(a, n) = 1 \Rightarrow \text{Existem } r, s \in \mathbb{Z} \text{ tais que } ra + sn = 1$$

Mas

$$ra + sn = 1 \Rightarrow \overline{r} \cdot \overline{a} + \overline{s} \cdot \overline{n} = \overline{r} \cdot \overline{a} + \overline{0} = \overline{1} \Rightarrow \overline{r} \cdot \overline{a} = \overline{1}$$

Assim, $\overline{r}$ é o inverso multiplicativo de $\overline{a}$.

Exemplo **16**
Calcule o inverso multiplicativo de 23 em $\mathbb{Z}_{61}$.

É fácil ver que $\text{mdc}(23, 61) = 1$ porque 23 é primo e $23 \not| 61$. Usaremos o algoritmo de Euclides para determinar os inteiros r, s tais que $23r+61s = 1$. Temos que

$$\begin{array}{rcll} 61 & = & 2 \times 23 + 15 & \Longrightarrow \quad 15 = 61 - 2 \times 23 \\ 23 & = & 1 \times 15 + 8 & \Longrightarrow \quad 8 = 23 - 1 \times 15 \\ 15 & = & 1 \times 8 + 7 & \Longrightarrow \quad 7 = 15 - 1 \times 8 \\ 8 & = & 1 \times 7 + 1 & \Longrightarrow \quad 1 = 8 - 1 \times 7 \end{array}$$

Os números em negrito são os substituídos a cada passo pelos valores obtidos nas divisões sucessivas acima

Invertendo os passos temos:

$$\begin{aligned} 1 &= 8 - 1 \times \mathbf{7} = 8 - 1 \times (15 - 1 \times 8) = (-1) \times 15 + 2 \times \mathbf{8} \\ &= (-1) \times 15 + 2(23 - 1 \times 15) = 2 \times 23 - 3 \times \mathbf{15} = 2 \times 23 - 3 \times (61 - 2 \times 23) \\ &= 8 \times 23 - 3 \times 61 \end{aligned}$$

Portanto, 8 é o inverso multiplicativo de 23 em $\mathbb{Z}_{61}$. Escrevemos também

$$8 \equiv 23^{-1} \pmod{61} .$$

Resumo

Nesta aula estudamos duas propriedades relacionadas à multiplicação de elementos de $\mathbb{Z}_n$. Estudamos os divisores de zero e os elementos inversíveis em $\mathbb{Z}_n$. Aprendemos a reconhecer estes elementos: dado $\overline{a} \in \mathbb{Z}_n$, com $\overline{a} \neq \overline{0}$, temos que

$$\begin{array}{lll} \text{mdc}(a,n) = 1 & \Rightarrow & \overline{a} \text{ é invertível em } \mathbb{Z}_n \\ \text{mdc}(a,n) = d > 1 & \Rightarrow & \overline{a} \text{ é divisor de zero em } \mathbb{Z}_n \end{array}$$

Por fim, aprendemos a calcular efetivamente o inverso multiplicativo de uma classe $\overline{a} \in \mathbb{Z}_n$, com $\text{mdc}(a,n) = 1$, utilizando o algoritmo de Euclides.

Atividades

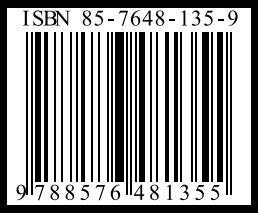
1. Mostre que se $\overline{a} \neq \overline{0}$ possui inverso multiplicativo em $\mathbb{Z}_n$, então esse inverso é único.

2. Encontre o inverso multiplicativo de:

   (a) 29 em $\mathbb{Z}_{121}$

   (b) 15 em $\mathbb{Z}_{67}$.

ISBN 85-7648-135-9



UENF
Universidade Estadual
do Norte Fluminense

UERJ
UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO

Universidade Federal Fluminense
uff

UNIVERSIDADE DO BRASIL

Universidade Federal Rural
do Rio de Janeiro

UNIRIO

FAPERJ
Fundação Carlos Chagas Filho de Amparo
à Pesquisa do Estado do Rio de Janeiro

GOVERNO DO
Rio de Janeiro
SECRETARIA DE
CIÊNCIA E TECNOLOGIA

UAB
UNIVERSIDADE
ABERTA DO BRASIL

Ministério
da Educação

BRASIL
UM PAÍS DE TODOS
GOVERNO FEDERAL