Universidade Estadual de Santa Cruz
DEPARTAMENTO DE CIÊNCIAS EXATAS E TECNÓLOGICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

DISSERTAÇÃO DE MESTRADO

Aritmética Modular: noção de congruência da teoria dos números para a teoria de anéis

por

Glauber Paiva Santos †

sob orientação da

Profª. Dra. Fernanda Gonçalves de Paula

†Este trabalho contou com apoio financeiro da Capes - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

Glauber Paiva Santos

Aritmética Modular: noção de congruência da teoria dos números para a teoria de anéis

Ilhéus - Ba
2015

Glauber Paiva Santos

Aritmética Modular: noção de congruência da teoria dos números para a teoria de anéis

Dissertação apresentada ao Departamento de Ciências Exatas e Tecnológicas da Universidade Estadual de Santa Cruz (UESC) para a obtenção do título de Mestre em Matemática, através do PROFMAT - Mestrado Profissional em Matemática em Rede Nacional.

Orientadora: Dra. Fernanda Gonçalves de Paula.

Ilhéus - Ba
2015

S237 Santos, Glauber Paiva
Aritmética Modular: noção de congruência da teoria dos números para a teoria de anéis / Glauber Paiva Santos. – Ilhéus, BA: UESC, 2015.
viii, 41 f.: il.

Orientadora: Fernanda Gonçalves de Paula.
Dissertação (Mestrado) – Universidade Estadual de Santa Cruz. Mestrado Profissional em Matemática em rede Nacional.
Inclui referências.

1. Álgebra. 2. Aritmética – Estudo e ensino (Ensino fundamental). 3. Matemática – (Ensino médio). 4. Anéis (Álgebra). I. Título.

CDD 512

Glauber Paiva Santos

Aritmética Modular: noção de congruência da teoria dos números para a teoria de anéis

Dissertação apresentada ao Departamento de Ciências Exatas e Tecnológicas da Universidade Estadual de Santa Cruz (UESC) para a obtenção do título de Mestre em Matemática, através do PROFMAT - Mestrado Profissional em Matemática em Rede Nacional.

Trabalho aprovado. Eunápolis, 10 de março de 2015:

Prof. Dr. Vinícius Augusto Takahashi Arakawa

Prof. Me. Josaphat Ricardo Gouveia Júnior

Prof. Dra. Fernanda Gonçalves de Paula
Orientadora

Ilhéus - 2015

Dedicatória

Dedico primeiramente a Deus. Depois a minha esposa, meus pais e amigos, pelo apoio e incentivo em mais essa etapa de construção de conhecimento.

Agradecimentos

É de coração que agradeço ...

... A Deus primeiramente, pela força e determinação, por construir os conhecimentos necessários e chegar até aqui.

... A minha esposa, Rejane Ferreira, pela paciência e incentivo, por compreender minhas ausências ao longo de todo esse período de estudo.

... Aos meus pais, Eliete Paiva e Paulino Batista, pelo carinho e apoio prestado, por acreditarem desde o início que eu conseguiria chegar até o fim.

... Aos meus amigos e colegas de turma, pelo apoio, parceria, por tornarem todo o processo mais agradável. Em especial a Carlos Silva, Eduarda Silva e família, que me acolheram em seu lar durante a realização deste curso.

... A todos os professores da Uesc envolvidos nessa formação, especialmente a minha orientadora Dra. Fernanda Gonçalves de Paula.

... À Capes pelo apoio financeiro para realização deste trabalho.

Resumo

Esta dissertação aborda a aritmética modular, uma excelente ferramenta que pode ser inserida no currículo do ensino fundamental e médio, de uma forma mais abstrata. Mostramos a relação entre a Aritmética e a Álgebra, ao definirmos congruência partindo de alguns conceitos da teoria de Anéis e Ideais, e demonstrando o famoso Teorema Chinês dos Restos neste novo ambiente. São apresentadas duas aplicações do cotidiano, que podem ser trabalhadas nas séries finais do ensino fundamental e dois momentos do ensino médio, onde podemos usar Congruência para auxiliar o ensino de outros conteúdos.

Palavras-chaves: Álgebra, Aritmética Modular, Educação Básica.

Abstract

This dissertation addresses the modular arithmetic, an excellent tool that can be inserted into the middle and high school curriculum in a more abstract way. We show the relationship between arithmetic and algebra by defining congruence starting from some concepts of the theory of rings and ideals, and displaying the famous Chinese theorem remains in this new environment. Will have two everyday applications, which can be worked in the final series of elementary school and two high school moments, where we can use congruence to complement the teaching of others contents.

Keywords: Algebra, Modular Arithmetic, Basic Education.

Sumário

Capítulo 1

Introdução

O presente trabalho tem como objetivo principal demonstrar o Teorema Chinês dos Restos, um resultado bem conhecido da Teoria dos Números, a partir de alguns conceitos da Teoria de Anéis, servindo desta forma como aprimoramento na formação continuada do professor de matemática. Aproveitamos também para indicar dois momentos na educação básica onde o tema pode ser inserido, bem como duas de suas interessantes aplicações do cotidiano. Pensamos que através deste trabalho, o professor de matemática do ensino básico possa se sentir motivado a inserir o ensino de Congruências em seu planejamento e aplicá-lo na sala de aula.

É importante observamos que a Aritmética e a Divisibilidade fazem parte do currículo obrigatório do ensino fundamental brasileiro, o que não ocorre especificamente com a Aritmética Modular. A Congruência é um tema que pode ser trabalhado nas classes da educação básica, tanto nas séries finais do ensino fundamental, quanto no ensino médio. Podemos inserir essa ferramenta e suas muitas aplicações no cotidiano das pessoas (que são, por exemplo, sobre os códigos de barras, CPF, CNPJ, ISBN, criptografia, calendários e outros fenômenos periódicos).

Espera-se que à partir deste trabalho, muitos outros possam surgir, completando-o, enriquecendo-o com outras aplicações de Aritmética Modular e mostrando outros momentos do currículo da educação básica onde o tema poderá ser inserido.

Apresentaremos no próximo Capítulo as principais definições, proposições e teoremas da Teoria de Anéis e Ideais, para que, com base nestas, possamos demonstrar o Teorema Chinês dos Restos neste ambiente e definirmos a Congruência módulo Ideal no terceiro capítulo.

Enfim, no terceiro Capítulo, demonstraremos o famoso Teorema Chinês dos Restos no ambiente da Álgebra abstrata, além de apresentarmos a Congruência módulo Ideal e os principais resultados da Teoria dos Números relacionados à Congruência Módulo n e às Congruências Lineares.

No quarto Capítulo são apresentadas duas simples e interessantes aplicações de

Congruência para o ensino básico, a saber os Códigos de Barras e o Cadastro de Pessoas Físicas (CPF) e, indicamos dois momentos no currículo da educação básica brasileira onde o ensino de Congruência pode ser inserido.

Capítulo 2

Introdução à Teoria de Anéis

A Teoria de Anéis é uma subárea de importância fundamental da Àlgebra. A mesma está totalmente conectada com outras grandes áreas como, por exemplo, Teoria dos Números. Por esse motivo, neste capítulo apresentaremos algumas das principais definições, proposições e teoremas da Teoria de Anéis e Ideais, para podermos conceituar e demonstrar resultados relacionados à Congruência no próximo capítulo.

2.1 Primeiras Definições

Definição 2.1.1

Um conjunto não vazio R, juntamente com duas operações binárias + e $\cdot$, é dito ser um **anel** quando:

(i) $(R, +)$ é um grupo abeliano, ou seja:

(a) $a + (b + c) = (a + b) + c$, para todos $a, b, c \in R$;

(b) $\exists\ 0 \in R; a + 0 = 0 + a = a$, para todo $a \in R$;

(c) Para todo $a \in R$, $\exists\ -a \in R$; $a + (-a) = 0 = (-a) + a$;

(d) $a + b = b + a$; para todos $a, b \in R$.

(ii) $\cdot$ é associativa, ou seja,
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todos $a, b, c \in R$.

(iii) valem a leis distributivas:
$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,
$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$, para todos $a, b, c \in R$.

Notação: $(R, +, \cdot)$ denotará um anel R com as operações + e $\cdot$.

□

Observação 2.1.1

Um anel $(R, +, \cdot)$, onde a operação $\cdot$ é comutativa é dito ser um **anel comutativo**. Um anel $(R, +, \cdot)$ onde $\cdot$ tem elemento neutro é dito ser um **anel com elemento identidade** ou simplesmente, um **anel com 1**. Tal elemento neutro sera indicado por 1 ou 1_R.

Definição 2.1.2

Seja $(R, +, \cdot)$ um anel. Um elemento $a \in R$, $a \neq 0$ é um **divisor de zero** de R se existe $b \neq 0$ em R, tal que $a \cdot b = 0$ e $b \cdot a = 0$.

□

Definição 2.1.3

Um **domínio**, ou um **anel de integridade** é um anel comutativo, com 1, sem divisores de zero.

□

Definição 2.1.4

Um anel $(R, +, \cdot)$ é um **anel com divisão**, ou **quase corpo** se $(R - \{0\}, \cdot)$ é um grupo. Em outras palavras $1 \in R$ e para todo $a \in R$, $a \neq 0$, existe $b \in R$, tal que $a \cdot b = b \cdot a = 1$. Este elemento b é dito ser o inverso de a e é denotado por a^{-1}.

□

Definição 2.1.5

Um **corpo** é um anel com divisão comutativo.

□

Proposição 2.1.1

Seja $(R, +, \cdot)$ um anel. Então:

(i) O elemento neutro da $+$, denotado por 0(ou 0_R), é único.

(ii) Para todo $a \in R$, o **oposto** de a (o inverso com relação a $+$), $-a$, é único.

(iii) Valem as leis do cancelamento para $+$.

(iv) Para todo $a \in R$, $a \cdot 0 = 0 \cdot a = 0$.

(v) Para todos $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ e $(-a) \cdot (-b) = a \cdot b$.

(vi) Se R é um anel com 1, então 1_R é único.

(vii) Se R tem mais que um elemento e R tem 1, então $1 \neq 0$.

(viii) Se R é um anel no qual vale a lei do cancelamento à esquerda (respectivamente, à direita) para o produto, então R não tem divisores de zero à esquerda (respectivamente, à direita).

Demonstração

(i) Se existem 0 e $0'$ em R tais que $a + 0 = 0 + a = a$ e $a + 0' = 0' + a = a$, para todo $a \in R$. Em particular, $0 = 0 + 0' = 0'$, ou seja, o elemento neutro da + é único.

(ii) Para $a \in R$, sejam $b, c \in R$ tais que $0 = a + b = b + a$ e $0 = a + c = c + a$. Então $b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c$, ou seja $b = c$, logo o oposto é único.

(iii) Mostraremos somente que vale a lei do cancelamento à esquerda, o caso à direita é análogo.

Se $a, b, c \in R$ são tais que $a + b = a + c$, então $(-a) + (a + b) = (-a) + (a + c)$, o que implica que $((-a) + a) + b = ((-a) + a) + c$. Logo $0 + b = 0 + c$ e, consequentemente $b = c$.

(iv) Para $a \in R$, temos $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Usando (iii), temos $a \cdot 0 = 0$. Analogamente, $0 \cdot a = 0$, para todo $a \in R$.

(v) Mostremos inicialmente que $a \cdot (-b) = -(a \cdot b)$. Pela unicidade do oposto, é suficiente mostrar que $a \cdot (-b) + a \cdot b = 0 = a \cdot b + a \cdot (-b)$. Mas, $a \cdot (-b) + a \cdot b = a \cdot ((-b) + b) = a \cdot 0 = 0$. A outra igualdade é análoga.

De maneira análoga mostra-se que $(-a) \cdot b = -(a \cdot b)$.

Consequentemente das igualdades acima, temos $(-a) \cdot (-b) = -(a \cdot (-b)) = a \cdot (-(-b)) = a \cdot b$.

(vi) Se 1 e $1'$ são elementos neutros para $\cdot$, então $1 = 1 \cdot 1' = 1'$. Portanto $1 = 1'$.

(vii) Se $1 = 0$ em R, então para todo $a \in R$ temos $a = a \cdot 1 = a \cdot 0 = 0$, ou seja, $R = \{0\}$, o que é uma contradição, portanto $1 \neq 0$ em R.

(viii) Se $a \in R$, $a \neq 0$ e $a \cdot b = 0$, então $a \cdot b = a \cdot 0$ e $a \neq 0$. Por hipótese temos $b = 0$, ou seja, R não possui divisores de zero à esquerda.

■

Definição 2.1.6

Um subconjunto não vazio S de um anel $(R, +, \cdot)$ é dito ser um **subanel** de R se, com as operações induzidas pelas operações de R (restrições), S é um anel.

□

Teorema 2.1.1

Um subconjunto $S \neq \varnothing$ de um anel $(R, +, \cdot)$ é um subanel de R se, e somente se valem as seguintes afirmações:

(i) $0 \in S$;

(ii) Para todos $a, b \in S \Rightarrow a - b = a + (-b) \in S$;

(iii) Para todos $a, b \in S \Rightarrow a \cdot b \in S$.

Demonstração

($\Rightarrow$) Suponhamos que S é um subanel de R, então $S \neq \varnothing$. Assim, existe $x \in S$ e como S é um anel, segue que $-x \in S$, de onde segue que $0 = x + (-x) \in S$, e portanto, a condição (i) é satisfeita. Agora, dados $a, b \in S$, temos que $-b \in S$, como S é anel, temos $a + (-b) = a - b \in S$, mostrando a condição (ii). A condição (iii) é claramente verdadeira, pois S é um anel com as operações de R, logo a multiplicação é fechada em S.

($\Leftarrow$) Reciprocamente, suponhamos que S é um subconjunto de R satisfazendo as três condições do teorema. Então, de (i), temos que $S \neq \varnothing$. A condição (iii) garante que $\cdot$ é um operação em S. Para vermos que $+$ também é uma operação em S, observamos que se $a, b \in S$, segue por (ii), que $-b = 0 - b \in S$ e consequentemente, $a + b = a - (-b) \in S$. Agora é só observar que as propriedades que definem um anel são hereditárias para operações fechadas, exceto o simétrico de $+$, mas se $b \in S$, então $-b = 0 - b \in S$. Portanto, se S satisfaz as condições do teorema, então S é um subanel de R.

■

Definição 2.1.7

Sejam $(R, +, \cdot)$ e $(S, \oplus, \odot)$ anéis. Uma função $\varphi : R \to S$ é um **homomorfismo de anéis** se, para todos $a, b \in R$, tivermos:

(i) $\varphi(a + b) = \varphi(a) \oplus \varphi(b)$, (i.é, φ é um homomorfismo de grupos)

(ii) $\varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$.

Se, além disso, φ for bijetora, diremos que φ é um **isomorfismo de anéis** e, neste caso, diremos também que os anéis R e S são isomorfos e denotamos por $R \cong S$.

Se $(R, +, \cdot) = (S, \oplus, \odot)$, dizemos que φ é um **endomorfismo** de anéis.

Se $\varphi : R \to R$ é um isomorfismo, então φ é um **automorfismo** do anel R.

Teorema 2.1.2

Seja $\varphi : (R, +, \cdot) \to (S, \oplus, \odot)$ um homomorfismo de anéis. Então:

(i) $\varphi(0_R) = 0_S$.

(ii) $\varphi(-a) = -\varphi(a)$, $\forall a \in R$.

(iii) $\varphi(R) = \{\varphi(a); a \in R\}$ é um subanel de S.

(iv) Se R tem 1, então $\varphi(1_R) = 1_{\varphi(R)}$.

(v) Se $a \in R$ é inversível, ou seja, tem inverso multiplicativo, então $\varphi(a^{-1}) = \varphi(a)^{-1}$ em $\varphi(R)$.

Demonstração

(i) Como $\varphi(0_R) \oplus 0_S = \varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) \oplus \varphi(0_R)$, assim, do cancelamento de $\varphi(0_R)$, temos $\varphi(0_R) = 0_S$.

(ii) Para todo $a \in R$, temos $0_S = \varphi(0_R) = \varphi(a + (-a)) = \varphi(a) \oplus \varphi(-a)$, o que implica que $\varphi(-a) = -\varphi(a)$.

(iii) $\varphi(R)$ é um subanel de S, pois por(i), temos que $\varphi(R) \neq \varnothing$ e para todo $\varphi(a), \varphi(b) \in \varphi(R)$, temos:

  (a) $\varphi(a) - \varphi(b) = \varphi(a) \oplus \varphi(-b) = \varphi(a + (-b)) = \varphi(a - b) \in \varphi(R)$.

  (b) $\varphi(a) \odot \varphi(b) = \varphi(a \cdot b) \in \varphi(R)$.

(iv) Para todo $\varphi(a) \in \varphi(R)$, temos que: $\varphi(a) \odot \varphi(1_R) = \varphi(a \cdot 1_R) = \varphi(a) = \varphi(1_R \cdot a) = \varphi(1_R) \odot \varphi(a)$. Logo, $\varphi(1_R) = 1_{\varphi(R)}$.

(v) Se $a \in R$ tem inverso, então $1_R = a \cdot a^{-1} = a^{-1} \cdot a$, o que implica que $1_{\varphi(R)} = \varphi(1_R) = \varphi(a \cdot a^{-1}) = \varphi(a) \odot \varphi(a^{-1}) = \varphi(a^{-1}) \odot \varphi(a)$. Logo $\varphi(a^{-1}) = \varphi(a)^{-1}$.

■

Teorema 2.1.3

Se $\varphi : (R, +, \cdot) \to (S, \oplus, \odot)$ é um homomorfismo de anéis e S' é um subanel de S, então $\varphi^{-1}(S')$ é um subanel de R, ou seja, a imagem inversa, por homomorfismo, de subanel é subanel.

Demonstração

De fato:

(i) $\varphi^{-1}(S') \neq \varnothing$, pois como $\varphi(0_R) = 0_S \in S'$, então $0_R \in \varphi^{-1}(S')$;

(ii) Para todos $a, b \in \varphi^{-1}(S')$, temos $\varphi(a), \varphi(b) \in S'$.

Como S' é subanel, $\varphi(a) - \varphi(b) \in S'$ e portanto, $\varphi(a - b) \in S'$. Daí, $a - b \in \varphi^{-1}(S')$. Analogamente, como S' é subanel, $\varphi(a) \odot \varphi(b) \in S'$ e consequentemente $\varphi(a \cdot b) \in S'$. Logo, $a \cdot b \in \varphi^{-1}(S')$. Portanto, $\varphi^{-1}(S')$ é um subanel de R.

■

Corolário 2.1.1

Se $\varphi : R \to S$ é um homomorfismo de anéis, então $Ker(\varphi) = \varphi^{-1}(\{0_S\})$ é um subanel de R, chamado o **núcleo do homomorfismo** φ. Note que $Ker(\varphi) = \{a \in R; \varphi(a) = 0_S\}$.

Teorema 2.1.4

Se $\varphi : R \to S$ é um homomorfismo de anéis e $a \in Ker(\varphi)$ então $a \cdot r \in Ker(\varphi)$ e $r \cdot a \in Ker(\varphi)$, para todo $r \in R$.

Demonstração

Se $a \in Ker(\varphi)$ e $r \in R$, então temos $\varphi(a \cdot r) = \varphi(a) \odot \varphi(r) = 0_S \odot \varphi(r) = 0_S$. Logo, $a \cdot r \in Ker(\varphi)$. Analogamente, temos que $r \cdot a \in Ker(\varphi)$.

■

2.2 Ideais e Anel Quociente

Definição 2.2.1

Um subanel I de um anel R é:

(i) um **ideal** de R, se $\forall a \in I$ e $r \in R \Rightarrow a \cdot r \in I$ e $r \cdot a \in I$.

(ii) um **ideal à direita** de R, se $\forall a \in I$ e $r \in R \Rightarrow a \cdot r \in I$.

(iii) um **ideal à esquerda** de R, se $\forall a \in I$ e $r \in R \Rightarrow r \cdot a \in I$.

□

Observação 2.2.1

Os conjuntos $\{0\}$ e R são chamados **ideais triviais** de R.

Teorema 2.2.1

Sejam R um anel e $I \neq \varnothing$ um subconjunto de R. I é um ideal de R se, e somente se para todo $a, b \in I$ e $r \in R$, temos:

(i) $0 \in I$;

(ii) $a - b \in I$

(iii) $a \cdot r \in I$ e $r \cdot a \in I$

Demontração

($\Rightarrow$)Imediata.

($\Leftarrow$) Suponhamos que I é um subconjunto de R satisfazendo as três condições do teorema. Então, de (i), temos que $I \neq \varnothing$. A condição (iii) garante que $\cdot$ é um operação em I. Para vermos que + também é uma operação em I, observamos que se $a, b \in I$, segue por (ii), que $-b = 0 - b \in I$ e consequentemente, $a + b = a - (-b) \in I$. Agora é só observar que as propriedades que definem um anel são hereditárias para operações fechadas, exceto o simétrico de +, mas se $b \in S$, então $-b = 0 - b \in I$. Portanto, se I satisfaz as condições do teorema, então I é um Ideal de R.

■

Definição 2.2.2

Uma relação E sobre um conjunto R não vazio é chamada **relação de equivalência** sobre R se, E é reflexiva, simétrica e transitiva, isto é, se são verdadeiras as sentenças:

(i) $a \in R \Rightarrow aEa$, para todo a (reflexiva);

(ii) $aEb \Rightarrow bEa$, para todo $a, b \in R$(simétrica);

(iii) $aEb\ e\ bEc \Rightarrow aEc$, para todo $a, b, c \in R$ (transitiva);

□

Definição 2.2.3

Sejam R um anel e I um ideal. Definimos a relação $\sim$ em R por:

$$x \sim y \Leftrightarrow x - y \in I$$

para todo $x, y \in R$.

□

É fácil ver que $\sim$ define uma relação de equivalência em R:

(i) $x \sim x$ pois $x - x = 0 \in I$

(ii) Se $x \sim y$ então $y \sim x$ pois $x - y \in I$ implica em $y - x = -(x - y) \in I$ porque I é um ideal.

(iii) Se $x \sim y$ e $y \sim z$ então $x \sim z$ pois se $x - y \in I$ e $y - z \in I$, e por I ser Ideal, somando-os temos que $x - z \in I$.

■

Mais ainda, para todo $a \in R$, definamos $\overline{a} = \{x \in R; x - a \in I\} = a + I$.

Seja R/I o conjunto das classes de equivalência de $\sim$, ou seja,

$$R/I = \{a + I; a \in R\}$$

Observe que $a + I = b + I$ se, e somente se $a - b \in I$. Em R/I definimos as operações $+$ e $\cdot$ por:

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

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

para todo $a, b \in R$. Vejamos que $+$ e $\cdot$ estão bem definidas, ou seja, não depemdem da escolha dos representantes das classes de equivalência.

Se $a + I = a' + I$ e $b + I = b' + I$, então existem $x_1, x_2 \in I$ tais que $a = a' + x_1$ e $b = b' + x_2$. Asssim,

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+I = ((a'+x_1)+(b'+x_2))+I = \\ &= (a'+b')+(x_1+x_2)+I = (a'+b')+(x_1+x_2)+I = \\ &= (a'+b')+0+I = (a'+b'+0)+I = \\ &= (a'+I)+(b'+I)\end{aligned}$$

e

$$\begin{aligned}(a+I)\cdot(b+I) &= a\cdot b+I = (a'+x_1)(b'+x_2)+I = \\ &= (a'b'+a'x_2+x_1b'+x_1x_2)+I = \\ &= (a'b'+I)+((a'x_2+x_1b'+x_1x_2)+I) = \\ &= (a'b'+I)+(0+I) = \\ &= (a'b'+0)+I = a'b'+I = (a'+I)\cdot(b'+I)\end{aligned}$$

Teorema 2.2.2

O conjunto R/I, juntamente com as operações

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

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

é um anel.

Demonstração

É fácil verificar que $(R/I, +)$ é um grupo abeliano e, decorre imediatamente do fato de R ser anel que a operação $\cdot$ de R/I é associativa e é distribuitiva em relação à adição.

Para provar por exemplo, que a relação $\cdot$ em R/I é associativa, usamos o fato de que a multiplicação em R é associativa. De fato, para todos $a, b, c \in R$, temos:

$$\begin{aligned}(a+I)\cdot[(b+I)\cdot(c+I)] &= (a+I)[(bc)+I] \\ &= a(bc)+I \\ &= (ab)c+I \\ &= [(ab)+I](c+I) \\ &= [(a+I)\cdot(b+I)]\cdot(c+I)\end{aligned}$$

■

O anel $(R/I, +, \cdot)$ chama-se **anel quociente** de R por I.

Corolário 2.2.1

Seja $(R/I, +, \cdot)$ um anel. Então:

(i) $0 + I = I$ é o elemento neutro de $+$;

(ii) $(-x) + I$ é o elemento oposto (inverso com relação a $+$) de $x + I$, $\forall x \in R$.

Além disso,

(iii) Se R é um anel com unidade 1, então R/I é um anel com unidade $1 + I$;

(iv) Se R é um anel comutativo, então R/I é também comutativo.

■

Em muitos textos, o próximo resultado é conhecido como o Primeiro Teorema do Isomorfismo.

Corolário 2.2.2

Se $\varphi : R \to S$ é um homomorfismo de anéis, então

$$R/Ker(\varphi) \cong \varphi(R) = Im(\varphi)$$

Corolário 2.2.3

Um homomorfismo sobrejetor de anéis $\varphi : R \to S$ é um isomorfismo se, e somente se $Ker(\varphi) = \{0_R\}$.

■

Capítulo 3

Congruências

Em Álgebra Abstrata, entende-se relação de congruência como uma relação de equivalência em um conjunto compatível com algumas operações algébricas, ou seja, é uma relação binária entre elementos de um dado conjunto, que satisfaz as propriedades de reflexividade, simetria e transitividade.

O conceito de congruência, apresentado nesta parte do trabalho, será de extrema importância para o desenvolvimento das aplicações contidas no próximo capítulo. Na primeira seção apresentamos a definição e as propriedades de Congruência módulo n, conhecida no anel dos inteiros, em seguida, na próxima seção, mostraremos o conceito de Congruência Linear e demonstramos alguns dos seus resultados neste ambiente. Já na terceira seção é apresentada a definição de Congruência Módulo I, no campo da teoria de anéis e ideais, para enfim, na última seção, apresentarmos o famoso Teorema Chinês dos Restos e prová-lo com algumas ferramentas da Álgebra.

3.1 Congruência Módulo n

O conceito de congruência módulo n pode ser identificado em diversas situações, tais como: nos diferentes códigos numéricos de identificação (código de barras, CPF, CNPJ, ISBN), na segurança de informação (criptografia), nos calendários e em outros fenômenos periódicos.

Foi apresentada, da forma que conhecemos hoje, por Johann Carl Friedrich Gauss e publicada no seu livro Disquisitiones Arithmeticae (Pesquisas Aritméticas), de 1801, a Congruência Módulo n trata-se da realização de uma aritmética com restos da divisão euclidiana por um número fixado. Gauss definiu a congruência módulo n da seguinte maneira: ″Se um número **n** divide a diferença de dois números **a** e **b**, **a** e **b** são chamados congruentes relativos a **n**. O número **n** é chamado modulus. Se **a** e **b** são congruentes, cada um é chamado resíduo do outro. Designaremos congruência pelo símbolo ≡ e colocaremos em parênteses o modulus...″. Mas formalmente, temos a seguinte definição:

Definição 3.1.1

Em $\mathbb{Z}$ dizemos que a é côngruo a b módulo n e escrevemos $a \equiv b \ mod \ n$ se n divide $(b-a)$, isto é, se existe $q \in \mathbb{Z}$ tal que $b - a = nq$.

□

Pela definição 2.2.2, apresentada no capítulo anterior, vamos mostrar que a relação acima definida, é de fato uma relação de equivalência, ou seja, satisfaz as propriedades de reflexividade, simetria e transitividade.

De fato:

(i) $a \equiv a \ mod \ n$ pois $n|[(a-a) = 0]$

(ii) Se $a \equiv b \ mod \ n$ então $b \equiv a \ mod \ n$ pois se $n|(a-b)$ então $n|(b-a)$

(iii) Se $a \equiv b \ mod \ n$ e $b \equiv c \ mod \ n$ temos que $n|(a-b)$ e $n|(b-c)$ e então $n|(a-b)+(b-c)$, ou seja, $n|(a-c)$. Isto mostra que $a \equiv c \ mod \ n$

Definição 3.1.2 (Algoritmo da Divisão Euclidiana)

Sejam a e n dois números inteiros. Existem únicos $q, r \in \mathbb{Z}$ tal que $a = qn + r$ com $0 \leq r < n$.

□

As classes de equivalência de $\mathbb{Z}$ $mod \ n$ serão as classes dos restos da divisão por n. Com efeito, dados $a, n \in \mathbb{Z}$ com $n \neq 0$ pelo algorítmo da divisão euclidiana, existem únicos $q, r \in \mathbb{Z}$ tal que $a = qn + r$ com $0 \leq r < n$. Isto mostra que $a \equiv r \ mod \ n$.

Denotaremos por $\mathbb{Z}_n$ o conjunto das classes de equivalência de $\mathbb{Z}$ módulo n.

Para todos $\overline{a}, \overline{b} \in \mathbb{Z}_n$, temos: $\overline{a} = \overline{b} \Leftrightarrow a \equiv b \ mod \ n$.

□

Exemplo 3.1.1

Sejam $R = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, $n \geq 0$, $+$ e $\cdot$ operações em $\mathbb{Z}_n$, definidas por:

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

(ii) $\overline{a} \cdot \overline{b} = \overline{ab}$,

para todo $\overline{a}, \overline{b} \in \mathbb{Z}_n$.

É fácil verificar que $(\mathbb{Z}_n, +, \cdot)$ é um anel, onde a operação $\cdot$ é comutativa e tem elemento neutro $\overline{1}$. Este anel é chamado o **anel dos inteiros módulo n**.

Exemplo 3.1.2

Como $25 = 6 \cdot 4 + 1$ e $-25 = 6 \cdot (-5) + 5$, tem-se que: $25 \equiv 1 \ mod \ 6$ e $-25 \equiv 5 \ mod \ 6$

Observação 3.1.1

Quando a não é congruente a b módulo n, representamos $a \not\equiv b \ mod \ n$.

Proposição 3.1.1

Dados $a, b, n \in \mathbb{Z}$ com $n > 1$, tem-se que $a \equiv b \ mod \ n$ se, e somente se, a e b deixam mesmo resto quando divididos por n

Demonstração

Sejam $a = nq_1 + r_1$ com $r_1 < n$ e $b = nq_2 + r_2$ com $r_2 < n$, as divisões euclidianas de a e b por n, respectivamente. Logo,

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

Portanto, pela definição 3.1.1, temos que $a \equiv b \ mod \ n$ se, e somente se $n|(b-a)$, o que, em vista da igualdade acima, é equivalente a dizer que $r_2 - r_1 = 0$, já que $|r_1 - r_2| < n$.

■

Proposição 3.1.2

Sejam a, b, c, d, n e r, números inteiros, com $n > 1$ e $r \geq 1$. Então:

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

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

(iii) Se $a \equiv b \ mod \ n$, então $a^r \equiv b^r \ mod \ n$.

(iv) $(a + c) \equiv (b + c) \ mod \ n$ se, e somente se $a \equiv b \ mod \ n$.

(v) Se $ab \equiv ac \ mod \ n$ e $mdc(a, n) = 1$, então $b \equiv c \ mod \ n$.

Demonstração

(i) Tem-se que $n|(b - a)$ e $n|(d - c)$, donde $n|[(b - a) + (d - c)] = (b + d) - (a + c)$. Portanto, $(a + c) \equiv (b + d) \ mod \ n$.

(ii) Suponha que $a \equiv b \ mod \ n$ e $c \equiv d \ mod \ n$. Tem-se que $n|(b-a)$ e $n|(d-c)$, donde $n|d(b-a)$ e $n|a(d-c)$. Daí, $n|[d(b-a)+a(d-c)]$, ou seja, $n|(bd-ac)$. Portanto, $ac \equiv bd \ mod \ n$.

(iii) Suponha que $a \equiv b \ mod \ n$. Aplicando o item (v) desta proposição $r-1$ vezes:

$$r \ congruencias \begin{cases} a \equiv b \ mod \ n \\ a \equiv b \ mod \ n \\ \vdots \\ a \equiv b \ mod \ n \end{cases} \Rightarrow a^r \equiv b^r \ mod \ n$$

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

(v) Suponha que $ab \equiv ac \ mod \ n$. Então, $n|(ac-ab) \Rightarrow n|a(c-b)$. Como $mdc(a,n) = 1$, tem-se necessariamente que $n|(c-b)$. Portanto, $b \equiv c \ mod \ n$.

■

Proposição 3.1.3

Sejam $a, b, c, n \in \mathbb{Z}$, com $c \neq 0$ e $n > 1$. Temos que:

$$ab \equiv ac \ mod \ n \Leftrightarrow b \equiv c \ mod \ \frac{n}{mdc(a,n)}$$

Demonstração

Como $\frac{n}{mdc(a,n)}$ e $\frac{a}{mdc(a,n)}$ são coprimos, temos que

$$ab \equiv ac \ mod \ n \Leftrightarrow n|(c-b)a \Leftrightarrow \frac{n}{mdc(a,n)}|(c-b)\frac{a}{mdc(a,n)} \Leftrightarrow$$

$$\Leftrightarrow \frac{n}{mdc(a,n)}|(c-b) \Leftrightarrow b \equiv c \ mod \ \frac{n}{mdc(a,n)}$$

■

3.2 Congruências Lineares

Denomina-se congruência linear, toda congruência da forma $ax \equiv b \ mod \ n$, com $a, b, n \in \mathbb{Z}$ e $n > 0$, onde x representa as soluções a serem encontradas.

Lema 3.2.1

Sejam $a, b \in \mathbb{Z} \setminus \{0\}$ e $c \in \mathbb{Z}$. A equação $ax + by = c$ admite solução em números inteiros se, e somente se, $mdc(a, b)|c$.

Proposição 3.2.1

Dados $a, b, n \in \mathbb{Z}$ com $n > 0$, a congruência $ax \equiv b \ mod \ n$ possui solução se, e somente se, $mdc(a, n)|b$.

Demonstraçâo

($\Rightarrow$) Suponhamos que a congruência $ax \equiv b \ mod \ n$ tenha uma solução x; logo, temos que $n|(ax - b)$, o que equivale à existência de y tal que $ax - b = ny$. Portanto, a equação $ax - ny = b$ admite solução, o que implica, pelo lema 3.2.1, que $mdc(a, n)|b$.

($\Leftarrow$) Reciprocamente, suponha que $mdc(a, n)|b$. Logo, pelo lema 3.2.1, a equação $ax - ny = b$ admite uma solução (x, y). Portanto, $ax = b + ny$ e, consequentemente, x é solução da congruência, pois $ax \equiv b \ mod \ n$.

Teorema 3.2.1

Sejam $a, b, n \in \mathbb{Z}$ com $n > 0$ e $mdc(a, n)|b$. Se x_0 é uma solução da congruência $ax \equiv b \ mod \ n$, então

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d}$$

onde $d = mdc(a, n)|b$, formam um sistema completo de soluções 2 a 2 incongruentes da congruência.

Demonstração

Pela Proposição 3.2.1, sabemos que a congruência admite solução. Vamos mostrar que os números $x_0 + i\frac{n}{d}$, com $i \in \mathbb{N}$, são soluções. De fato,

$$a\left(x_0 + i\frac{n}{d}\right) = ax_0 + i\frac{an}{d} \equiv ax_0 \equiv b \ mod \ n$$

Além disso, esses números são dois a dois incongruentes módulo n. De fato, se, para $i, j < d$,

$$x_0 + i\frac{n}{d} \equiv x_0 + j\frac{n}{d} \ mod \ n$$

então

$$i\frac{n}{d} \equiv j\frac{n}{d} \ mod \ n$$

Pela Proposição 3.1.3 e pelo fato de

$$\frac{n}{mdc\left(\frac{n}{d}, n\right)} = d$$

segue-se que $i \equiv j \ mod \ d$, implicando que $i = j$.

Finalmente, mostraremos que toda solução x da congruência $ax \equiv b \ mod \ n$ é congruente, módulo n, a $x_0 + i\frac{n}{d}$ para algum $i < d$. De fato, seja x uma solução qualquer da congruência; logo,

$$ax \equiv ax_0 \ mod \ n$$

e, portanto, pela Proposição 3.1.3,

$$x \equiv x_0 \ mod \ n$$

Logo, $x - x_0 = kn/d$. Pelo Algoritmo da Divisão Euclidiana, existe $i < d$ tal que $k = qd + i$ e, portanto,

$$x = x_0 + qn + i\frac{n}{d} \equiv x_0 + i\frac{n}{d} \ mod \ n$$

como queríamos.

■

Exemplo 3.2.1

Resolva a congruência $8x \equiv 4 \ mod \ 12$.

Temos que, como $d = mdc(8, 12) = 4$ divide 4, pelo teorema anterior, a congruência tem $d = 4$ soluções módulo 12.

Por tentativa e erro, obtemos a solução $x_0 = 2$. Portanto, as soluções módulo 12 são

$$2, 2 + 3, 2 + 6, 2 + 9$$

Corolário 3.2.1

Se $mdc(a, n) = 1$, então a congruência $ax \equiv b \ mod \ n$ possui uma única solução módulo n.

■

3.3 Congruência Módulo I

Nesta seção mostraremos que é possível generalizar o conceito de congruência módulo n, estudada na primeira seção. À partir da definição de Ideal, apresentada no capítulo anterior, definiremos Congruência Módulo I. Para tanto, primeiramente observe que, se considerarmos $I = n\mathbb{Z}$, então, para $a, b \in \mathbb{Z}$, temos que $a \equiv b \ mod \ n$ se, e somente se $a - b \in n\mathbb{Z}$. Assim, se $a \equiv b \ mod \ n$, então $a - b = nk$ para algum $k \in \mathbb{Z}$, mas $nk \in n\mathbb{Z}$, logo, $a - b \in n\mathbb{Z}$. Por outro lado, se $a - b \in n\mathbb{Z}$, então $a - b = nk$ para algum $k \in \mathbb{Z}$, o que significa que $a \equiv b \ mod \ n$.

No que se segue, será feita a generalização desta idéia para um anel qualquer.

Definição 3.3.1

Sejam R um anel, I um ideal de R e $a, b \in R$. Dizemos que a é côngruo à b módulo I quando $a - b \in I$.

□

Usaremos a notação $a \equiv b \ mod \ I$ para indicar que a é côngruo a b módulo I. Quando $R = \mathbb{Z}$ e $I = n\mathbb{Z}$, escrevemos simplesmente $a \equiv b \ mod \ n$.

Definição 3.3.2

Sejam R um anel e I um ideal de R. Denota-se por $\overline{a} = \{x \in R; x \equiv a \ mod \ I\}$ a qual chama-se de **classe de equivalência** do elemento $a \in R$ relativamente à relação $\equiv mod \ I$.

□

Observação 3.3.1

O anel quociente $\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}\}$ é o próprio anel comutativo $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Sendo assim, pode-se utilizar qualquer uma das notações $\mathbb{Z}_n$ ou $\mathbb{Z}/n\mathbb{Z}$ para esse anel quociente.

Embora estes conjuntos sejam matematicamente iguais, suas construções requerem conceitos matemáticos diferentes; enquanto para construir os elementos de $\mathbb{Z}_n$, que são classes de congruência módulo n, os conceitos envolvidos são divisibilidade, ou

resto da divisão, para construir os elementos de $\mathbb{Z}/n\mathbb{Z}$, que são classes de equivalência da congruência módulo ideal, as noções envolvidas são anel, subanel, operação entre elementos do anel e do ideal.

Exemplo 3.3.1

Mostre que $\mathbb{Z}_n$ é corpo $\Leftrightarrow$ n é primo.

De fato,

($\Rightarrow$) Suponha que n não é primo. Se $n = 1$ então $\mathbb{Z}_n = \mathbb{Z}/\mathbb{Z}$ que tem apenas um elemento e então não pode ser um corpo. Se $n > 1$ então $n = rs$ com r e s inteiros menores que n. Colocando $I = n\mathbb{Z}$ temos:

$$(I + r)(I + s) = I + rs = I$$

Mas I é o elemento neutro de $\mathbb{Z}/I$, enquanto $I + r$ e $I + s$ não o são. Como em um corpo o conjunto dos divisores de zero é vazio, segue que $\mathbb{Z}/I$ não é um corpo. Em ambos os casos obtemos uma contradição, pois estamos supondo que $\mathbb{Z}_n$ é corpo; logo n é primo.
($\Leftarrow$) Agora suponha que n é primo. Seja $I + r$ um elemento não-nulo de $\mathbb{Z}_n = \mathbb{Z}/I$, onde $I = n\mathbb{Z}$. Ora, podemos supor que $1 \leq r < n$. Assim, como n é primo, r e n são coprimos e portanto existem inteiros a e b tais que $ar + bn = 1$. Daí, temos que

$$(I + a)(I + r) = (I + 1) - (I + n)(I + b) = (I + 1)$$

e de modo análogo

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

Agora, como $I + 1$ é o elemento identidade de $\mathbb{Z}/I$, encontramos um inverso multiplicativo para um dado elemento $I + 1$. Como cada elemento não nulo de $\mathbb{Z}$ tem inverso, e $\mathbb{Z}$ é comutativo, segue que $\mathbb{Z}$ é corpo.

■

Exemplo 3.3.2

A função $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, definida por $\varphi(a) = \overline{a}$ é um homomorfismo de anéis, para todo $a \in \mathbb{Z}$.

De fato, para todo $a, b \in \mathbb{Z}$, temos:

(i) $\varphi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \varphi(a) \oplus \varphi(b)$

(ii) $\varphi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \varphi(a) \odot \varphi(b)$.

φ é sobrejetor mas não é injetor, pois $\varphi(a) = \varphi(a+n)$, para todo $a \in \mathbb{Z}$.

Exemplo 3.3.3

Para $R = \mathbb{Z}$, temos que $I = n\mathbb{Z}$, com $n \geq 0$ são todos os ideais de $\mathbb{Z}$. Mas ainda, todos são núcleos de homomorfismo de anéis. De fato, $n\mathbb{Z} = Ker(\varphi)$, onde $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ é o homomorfismo canônico dado por $\varphi(a) = \overline{a}$, para todo $a \in \mathbb{Z}$, e, neste caso, $Ker(\varphi) = \{a \in \mathbb{Z}; \overline{a} = \overline{0}\} = n\mathbb{Z}$.

3.4 Teorema Chinês dos Restos

Uma formulação simples do Teorema Chinês dos Restos assegura que dados $p_1, \ldots, p_n$ primos distintos e $a_1, \ldots, a_n$ inteiros, existe um inteiro x tal que p_i divide $x - a_i$, para $i = 1, \ldots, n$. De outra forma, a_i é o resto da divisão de x por p_i para cada $i \in \{1, \ldots, n\}$.

Acredita-se que os chineses anteriores à era cristã já tinham conhecimento deste fato, que possivelmente estava relacionado com um problema prático da época. Contudo, o matemático chinês Sun Tsu (século I d.C.) teve seu nome fortemente associado ao Teorema Chinês dos Restos, sendo considerado o divulgador deste resultado. O problema específico abordado por Sun Tsu foi obter o menor inteiro positivo que dividido por 3, 5 e 7 tivesse restos 2, 3 e 2 , respectivamente. No final desta seção, resolveremos esse problema.

Como consequência de um isomorfismo de anéis, obteremos o Teorema Chinês dos Restos, uma importante aplicação da congruência modular.

Lembremos que:

Lema 3.4.1 (Identidade de Bezout)

Se $a, b \in \mathbb{Z}$ e $d = mdc(a, b)$ então existem $r, s \in \mathbb{Z}$, tais que $d = a \cdot r + b \cdot s$.

Usando este resultado mostraremos que:

Lema 3.4.2

Se $a, b \in \mathbb{Z}$ são primos entre si, isto é, $mdc(a, b) = 1$, então $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab}$.

Demonstração

Desde que $\mathbb{Z}_{ab} \cong \dfrac{\mathbb{Z}}{(ab)\mathbb{Z}}$ e $\mathbb{Z}_a \times \mathbb{Z}_b \cong \dfrac{\mathbb{Z}}{a\mathbb{Z}} \times \dfrac{\mathbb{Z}}{b\mathbb{Z}}$, é suficiente mostrarmos que $\dfrac{\mathbb{Z}}{(ab)\mathbb{Z}} \cong \dfrac{\mathbb{Z}}{a\mathbb{Z}} \times \dfrac{\mathbb{Z}}{b\mathbb{Z}}$.

Seja $\varphi : \mathbb{Z} \to \dfrac{\mathbb{Z}}{a\mathbb{Z}} \times \dfrac{\mathbb{Z}}{b\mathbb{Z}}$, definida por $\varphi(x) = (x + a\mathbb{Z},\ x + b\mathbb{Z})$, para todo $x \in \mathbb{Z}$. Claramente temos que φ é um homomorfismo de anéis. Mais ainda, $Ker(\varphi) = \{x \in \mathbb{Z};\ \varphi(x) = 0\} = \{x \in \mathbb{Z};\ \varphi(x) = (a\mathbb{Z},\ b\mathbb{Z})\}$.

Se $x \in Ker(\varphi)$, então $x \in a\mathbb{Z}$ e $x \in b\mathbb{Z}$. Logo, $a \mid x$ e $b \mid x$, o que implica que $mmc(a, b) \mid x$.

Mas, $mmc(a, b) = \dfrac{a \cdot b}{mdc(a, b)} = a \cdot b$. Assim, $x \in (ab)\mathbb{Z}$, ou seja $Ker(\varphi) \subseteq (ab)\mathbb{Z}$. A inclusão contrária é imediata.

Logo, pelo corolário 2.2.2, temos $\dfrac{\mathbb{Z}}{(ab)\mathbb{Z}} \cong Im(\varphi) \subseteq \mathbb{Z}_a \times \mathbb{Z}_b$ e $\#(\mathbb{Z}_{ab}) = ab = \#(\mathbb{Z}_a \times \mathbb{Z}_b)$, o que implica que φ é sobrejetora.

■

Teorema 3.4.1

Se $n \in \mathbb{Z}$, $n > 0$ e $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, com p_i's primos distintos, então $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$.

Demonstração

Segue diretamente do lema anterior e por técnicas de indução.

■

Observemos que na demonstração do lema 3.4.2, mostramos que φ é sobrejetora sem exibirmos a pré-imagem de um elemento genérico. Assim cabe a seguinte pergunta:

Se $(c + a\mathbb{Z},\ d + b\mathbb{Z}) \in \mathbb{Z}_a \times \mathbb{Z}_b$, então qual é o $x \in \mathbb{Z}$ tal que $\varphi(x) = (c + a\mathbb{Z},\ d + b\mathbb{Z})$?

Observe que

$$\begin{cases} x + a\mathbb{Z} = c + a\mathbb{Z} \\ x + b\mathbb{Z} = d + b\mathbb{Z} \end{cases} \Rightarrow \begin{cases} x \equiv c\ mod\ a \\ x \equiv d\ mod\ b \end{cases} \Rightarrow \begin{cases} x = c + a \cdot n_1,\ n_1 \in \mathbb{Z} \\ x = d + b \cdot n_2,\ n_2 \in \mathbb{Z} \end{cases}$$

Por exemplo $\mathbb{Z}_{15} = \mathbb{Z}_3 \times \mathbb{Z}_5$, qual é o elemento $x \in \mathbb{Z}$, tal que $\varphi(x) = (\overline{2}, \overline{4})$?

Temos:

$$\begin{cases} x \equiv 2 \ mod \ 3 \\ x \equiv 4 \ mod \ 5 \end{cases}$$

Assim, substituindo $x = 2 + 3 \cdot n_1$, com $n_1 \in \mathbb{Z}$ em $x \equiv 4 \ mod \ 5$, obtemos:

$$2 + 3 \cdot n_1 \equiv 4 \ mod \ 5$$

$$3 \cdot n_1 \equiv 2 \ mod \ 5$$

$$2 \cdot 3 \cdot n_1 \equiv \cdot 2 \ mod \ 5$$

$$n_1 \equiv 4 \ mod \ 5$$

daí, $n_1 = 4 + 5n_2$, para algum $n_2 \in \mathbb{Z}$. Então, $x = 2 + 3(4 + 5n_2) = 14 + 15n_2$, ou seja $x = 14 \ mod \ 15$.

Corolário 3.4.1 (Teorema Chinês dos Restos)

Seja $\{m_i\}_{i=1}^{k}$ um conjunto de k inteiros 2 a 2 primos entre si, ou seja, $mdc(m_i, m_j) = 1$, para todo $i \neq j$. Então o sistema de congruências lineares:

$$\begin{cases} x \equiv a_1 \ mod \ m_1 \\ \vdots \\ x \equiv a_k \ mod \ m_k \end{cases}$$

onde $a_i \in \mathbb{Z}$, possui uma única solução módulo $n = m_1 m_2 \cdots m_k$.

Demonstração

Como $m_1, \ldots, m_k$ são números inteiros 2 a 2 primos entre si e $n = m_1 m_2 \cdots m_k$, pelo lema 3.4.2, temos que $\mathbb{Z}_n \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$, ou seja, existe um isomorfismo φ entre $\mathbb{Z}_n$ e $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$. Logo, φ é bijetora. Temos da sobrejetividade de φ que, para qualquer $(a_1 + m_1\mathbb{Z}, \ldots, \ a_k + m_k\mathbb{Z}) \in \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ com $a_1, \ldots, a_k \in \mathbb{Z}$, existe $(x + n\mathbb{Z}) \in \mathbb{Z}_n$ com $x \in \mathbb{Z}$ tal que $\varphi(x + n\mathbb{Z}) = (a_1 + m_1\mathbb{Z}, \ldots, \ a_k + m_k\mathbb{Z})$. O que implica que o sistema:

$$\begin{cases} x \equiv a_1 \ mod \ m_1 \\ \vdots \\ x \equiv a_k \ mod \ m_k \end{cases}$$

tem solução e, o fato de φ ser injetora, nos garante a unicidade desta solução módulo n.

■

Observação 3.4.1

O Teorema Chinês dos Restos como visto acima, não mostra como obter a solução do sistema, sugere apenas uma forma diferente e elegante de demonstrar esta famosa ferramenta. Em Teoria dos Números vemos que tal solução módulo n, pode ser obtida como segue:

$$x = n_1x_1a_1 + n_2x_2a_2 + \cdots + n_kx_ka_k$$

onde $n_i = \dfrac{n}{m_i}$ e x_i é solução de $n_ix \equiv 1 \ mod \ m_i$, $i = 1, 2, \ldots, k$.

Exemplo 3.4.1

Um camponês tem certo número de ovos; quando os divide por 3, sobra-lhe 1; quando os divide por 4, sobram 2 ovos; e quando os divide por 5, sobram 3. Quantos ovos tem o camponês, sabendo que a quantidade de ovos é um número inteiro entre 100 e 200?

Solução

Observe que podemos escrever um sistema de congruências para resolver este problema:

$$\begin{cases} x \equiv 1 \ mod \ 3 \\ x \equiv 2 \ mod \ 4 \\ x \equiv 3 \ mod \ 5 \end{cases}$$

onde x representa o número de ovos do camponês.

Como $mdc(3, 4) = mdc(3, 5) = mdc(4, 5) = 1$, temos, pelo Teorema Chinês dos Restos, que:

$n = 3 \cdot 4 \cdot 5 = 60$, $n_1 = 20$, $n_2 = 15$ e $n_3 = 12$. Devemos resolver as congruências:

$$20x_1 \equiv 1 \ mod \ 3 \Leftrightarrow 2x_1 \equiv 1 \ mod \ 3 \Rightarrow x_1 = 2$$

$$15x_2 \equiv 1 \ mod \ 4 \Leftrightarrow 3x_2 \equiv 1 \ mod \ 4 \Rightarrow x_2 = 3$$

$$12x_3 \equiv 1 \ mod \ 5 \Leftrightarrow 2x_3 \equiv 1 \ mod \ 5 \Rightarrow x_3 = 3$$

Assim, $x \equiv 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 \ mod \ 60 \Rightarrow x \equiv 238 \ mod \ 60 \Rightarrow x \equiv 58 \ mod \ 60$. As soluções desse sistema são da forma $58 + 60k$, com $k \in \mathbb{Z}$. Tomando $k = 2$, temos que o número de ovos do camponês é 178.

Exemplo 3.4.2 (Problema estudado por Sun-Tsu)

Obtenha o menor inteiro positivo, que dividido por 3, 5 e 7, deixe restos 2, 3 e 2, respectivamente.

Solução

Observe que podemos escrever um sistema de congruências para resolver este problema:

$$\begin{cases} x \equiv 2 \ mod \ 3 \\ x \equiv 3 \ mod \ 5 \\ x \equiv 2 \ mod \ 7 \end{cases}$$

Como $mdc(3,5) = mdc(3,7) = mdc(5,7) = 1$, temos, pelo Teorema Chinês dos Restos:

$n = 3 \cdot 5 \cdot 7 = 105$, $n_1 = 35$, $n_2 = 21$ e $n_3 = 15$. Devemos resolver as congruências:

$$35x_1 \equiv 1 \ mod \ 3 \Leftrightarrow 2x_1 \equiv 1 \ mod \ 3 \Rightarrow x_1 = 2$$

$$21x_2 \equiv 1 \ mod \ 5 \Leftrightarrow x_2 \equiv 1 \ mod \ 5 \Rightarrow x_2 = 1$$

$$15x_3 \equiv 1 \ mod \ 7 \Leftrightarrow x_3 \equiv 1 \ mod \ 7 \Rightarrow x_3 = 1$$

Assim, $x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \ mod \ 105 \Rightarrow x \equiv 233 \ mod \ 105 \Rightarrow x \equiv 23 \ mod \ 105$. As soluções desse sistema são da forma $23 + 105k$, com $k \in \mathbb{Z}$. Logo, o menor inteiro que satisfaz o problema é 23.

Capítulo 4

Aplicações para o Ensino Básico

Congruência é um tema bastante atual e que pode ser trabalhado na educação básica, sendo um gerador de excelentes oportunidades de contextualização no processo de ensino/aprendizagem da Matemática. Neste capítulo, usaremos essa ferramenta, definida no capítulo anterior, mostrando duas belas e simples aplicações no cotidiano, que poderão ser utilizadas por professores de matemática em determinadas etapas do seu planejamento. Para aqueles que atuam no ensino médio, mostraremos também dois momentos do currículo, onde o tema pode ser usado para auxiliar o ensino de outros conteúdos.

4.1 Código de Barras

Uma das aplicações mais importantes e interessantes da Aritmética Modular é aquela que explica os códigos de barras, que são hoje utilizados no mundo todo e servem para fazer identificações em diversas áreas, tais como, indústria, comércio, bancos, bibliotecas, hospitais, bancos de sangue, correios, transportes, controles de acesso entre outros.

Numa definição técnica, o código de barras é uma representação gráfica de dados. Ele permite uma rápida captação de dados, proporciona velocidade nas transações, precisão nas informações e admite atualização em tempo real e tudo isso implica em maior controle, diminuição de erros, gerenciamento remoto, garantindo velocidade no atendimento de pedidos e clientes, além da significativa redução nos custos.

Tendo em vista todas as vantagens proporcionadas pela inserção dos códigos de barras, principalmente na área comercial, fica evidente a motivação para trabalhar tal assunto em sala de aula, pois é um bom exemplo da aplicação de Aritmética Modular.

Um dos códigos de barras mais usados no mundo todo é o $EAN-13$, constituído de 13 algarismos, sendo que os três primeiros dígitos do código representam o país de registro do produto (verifique que para produtos filiados no Brasil teremos sempre os dígitos 7, 8 e 9); os quatro dígitos seguintes identificam o fabricante; os próximos cinco dígitos identificam o produto e o último é o dígito verificador ou de controle, que se pode calcular através da congruência, módulo 10.

Vejamos agora como calcular o dígito verificador ou de controle:

Seja $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}$ a sequência formada pelos 12 primeros dígitos, devemos multiplicá-los, nessa ordem, pela base $\{1,3,1,3,1,3,1,3,1,3,1,3\}$ e somar os produtos obtidos. Vamos representar por S a soma obtida. O dígito que está faltando, que vamos representar por a_{13} deve ser tal que ao ser somado com S, deve gerar um múltiplo de 10, isto é, o número $S + a_{13}$ deve ser múltiplo de 10, ou seja, $S + a_{13} \equiv 0 \ mod\ 10$.

Vejamos, por exemplo, como foi calculado o dígito verificador do código de barras apresentado na figura abaixo:

Temos que,

$$S = 4 \cdot 1 + 8 \cdot 3 + 9 \cdot 1 + 1 \cdot 3 + 6 \cdot 1 + 6 \cdot 3 + 8 \cdot 1 + 3 \cdot 3 + 2 \cdot 1 + 6 \cdot 3 + 6 \cdot 1 + 8 \cdot 3$$

$$S = 4 + 24 + 9 + 3 + 6 + 18 + 8 + 9 + 2 + 18 + 6 + 24 = 131$$

Logo, $131 + a_{13} \equiv 0 \ mod\ 10 \Leftrightarrow a_{13} \equiv -131 \ mod\ 10 \Leftrightarrow a_{13} \equiv 9 \ mod\ 10$, ou seja, a_{13} é de fato igual a 9 conforme ilustrado na figura acima.

4.2 Cadastro de Pessoas Físicas - CPF

O **cadastro de pessoas físicas** (CPF) é o registro de um cidadão na Receita Federal Brasileira no qual devem estar todos os contribuintes (pessoas físicas nacionais e estrangeiras com negócios no Brasil). O CPF armazena informações fornecidas pelo próprio contribuinte e por outros sistemas da Receita Federal.

O número de CPF de uma pessoa no Brasil é constituído de 11 dígitos, sendo um primeiro bloco com 9 algarismos e um segundo, com mais dois algarismos, que são, como nos códigos de barra, dígitos de controle ou de verificação, criados para evitar erros de digitação. A determinação desses dois dígitos de controle é mais um caso de

aplicação da noção de congruência.

Vejamos agora como calcular o dígito verificador ou de controle:

Seja $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ a sequência formada pelos 9 primeros dígitos, devemos multiplicá-los, nessa ordem, pela base $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e somar os produtos obtidos. Vamos representar por S_1 essa soma obtida. O primeiro dígito de controle, que vamos representar por a_{10} deve ser tal que ao ser subtraído da soma S_1, deve gerar um múltiplo de 11, ou seja, $S - a_{10} \equiv 0 \ mod \ 11$. Note que tal número será o próprio resto da divisão por 11 da soma S_1.

A determinação do segundo dígito de controle é feita de modo similar, sendo que agora acrescentamos o décimo dígito (que é o que acabamos de calcular) e usamos uma base de multiplicação de 0 a 9, assim, se chamarmos a soma dos produtos obtidos de S_2, o segundo dígito de controle a_{11} é o resto da divisão por 11 da soma S_2.

Observação: Se o resto da divisão for 10, ou seja, se o número obtido fosse congruente ao 10, módulo 11, usaríamos, nesse caso, o dígito zero.

Vejamos, por exemplo, quais devem ser os dígitos de controle do CPF ilustrado na figura abaixo:

Temos que,

$$S_1 = 4 \cdot 1 + 9 \cdot 2 + 3 \cdot 3 + 4 \cdot 4 + 9 \cdot 5 + 3 \cdot 6 + 4 \cdot 7 + 9 \cdot 8 + 3 \cdot 9$$

$$S = 4 + 18 + 9 + 16 + 45 + 18 + 28 + 72 + 27 = 237$$

Logo, $237 - a_{10} \equiv 0 \ mod \ 11 \Leftrightarrow a_{10} \equiv 237 \ mod \ 11 \Leftrightarrow a_{10} \equiv 6 \ mod \ 11$. Assim, $a_{10} = 6$. Daí,

$$S_2 = 4 \cdot 0 + 9 \cdot 1 + 3 \cdot 2 + 4 \cdot 3 + 9 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + 9 \cdot 7 + 3 \cdot 8 + 6 \cdot 9$$

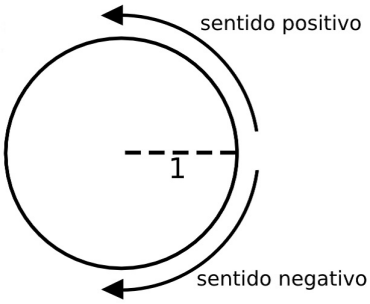
$$S = 0 + 9 + 6 + 12 + 36 + 15 + 24 + 63 + 24 + 54 = 243$$

Logo, $243 - a_{11} \equiv 0 \ mod \ 11 \Leftrightarrow a_{11} \equiv 243 \ mod \ 11 \Leftrightarrow a_{11} \equiv 1 \ mod \ 11$. Assim, $a_{11} = 1$. Portanto, o número do CPF é 493.493.493 – 61.

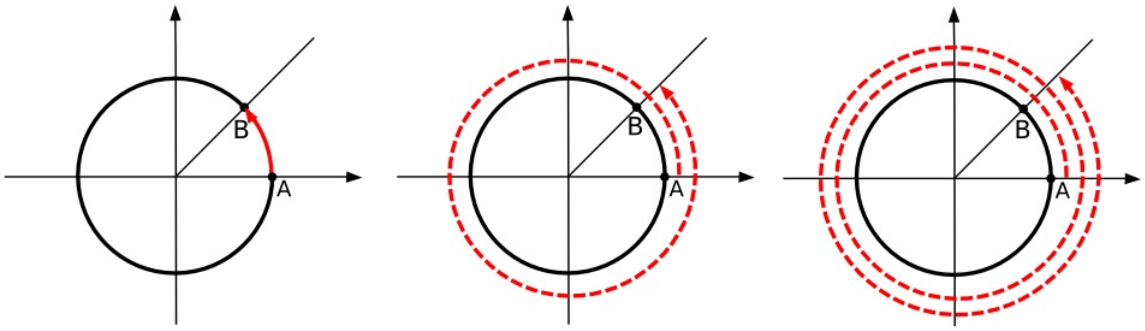
A seguir apresentaremos dois momentos onde o conceito de congruência pode ser usado como apoio à compreensão de outros conceitos no Ensino Básico.

4.3 Trigonometria

Na exposição dos conceitos básicos da trigonometria, um elemento importante é a circunferência unitária ou circunferência trigonométrica:



Observando a figura abaixo, veja que, tomando um ângulo $\alpha = med(A\widehat{O}B)$ e dando uma volta ou n voltas completas sobre o circulo, não se altera a posição final do ângulo, neste caso, esses ângulos são chamados de côngruos.



Portanto dado um ângulo qualquer α (com a notação de graus), os ângulos da forma $\alpha + 360° \cdot k$, com $k \in \mathbb{Z}$ são os chamados ângulos congruentes a α, e suas representações na circunferência coincidem.

Observe que a notação de congruência $\equiv$ pode ser abertamente utilizada pelo professor no momento em que definir arcos côngruos, por exemplo, o arco de 500° é côngruo (e, portanto está representado pelo mesmo ponto do círculo unitário) que o arco de 140°, podendo escrever $500° \equiv 140°$.

4.4 Números Complexos

Quando se estuda o conceito de números complexos, $\mathbb{C}$, o cálculo das potências naturais da chamada unidade imaginária $i = \sqrt{(-1)}$, é um momento oportuno para aplicação dos conceitos de congruência.

Considerando as operações usuais dos números complexos, vamos analisar as seguintes potências: $i^0, i^1, i^2, i^3, i^4, i^5, i^6, i^7, i^8$.

Temos que:

$$i^0 = 1$$

$$i^1 = i$$

$$i^2 = -1$$

$$i^3 = i^2 i = (-1)i = -i$$

$$i^4 = (i^2)^2 = (-1)^2 = 1$$

$$i^5 = i^4 i = 1i = i$$

$$i^6 = i^4 i^2 = 1(-1) = -1$$

$$i^7 = i^4 i^3 = 1(-i) = -i$$

$$i^8 = i^4 i^4 = (1)(1) = 1$$

Continuando as potencias de i, percebemos que trata-se de um problema cíclico, onde as potencias se repetem a cada ciclo de 4, conforme abaixo:

$$i^{4n} = (i^4)^n = (1)^n = 1$$

$$i^{4n+1} = (i^4)^n i = (1)^n i = i$$

$$i^{4n+2} = (i^4)^n (i^2) = (1)^n (-1) = -1$$

$$i^{4n+3} = (i^4)^n (i^3) = (1)^n (-i) = -i$$

Desse modo pode-se usar as seguintes congruências sobre o expoente das potências de i e então determinar quais valores do conjunto $\{1, i, -1, -i\}$ vale a potência, assim:

Expoente de $i \equiv 0 \ mod \ 4 \Rightarrow$ a potência de i é 1.
Expoente de $i \equiv 1 \ mod \ 4 \Rightarrow$ a potência de i é i.
Expoente de $i \equiv 2 \ mod \ 4 \Rightarrow$ a potência de i é -1.
Expoente de $i \equiv 3 \ mod \ 4 \Rightarrow$ a potência de i é $-i$.

Assim, com esses exemplos que mostramos, podemos observar que em nosso cotidiano existem inúmeras situações onde se faz presente a noção de congruência.

Capítulo 5

Considerações Finais

Conclui-se que, a Aritmética Modular, que envolve o estudo das congruências, é uma ferramenta eficaz na resolução de certos problemas de matemática e possui aplicações interessantes do cotidiano. Percebe-se que é possível inserí-la no ensino básico e os professores de matemática, podem incluí-la em seu planejamento, pois além de proporcionar aos alunos a possibilidade de aprofundar o significado de resto e manipulá-lo, é capaz de gerar ótimas oportunidades de contextualização no processo de ensino/aprendizagem.

O Teorema Chinês dos Restos é, sem duvida, uma das mais eficazes aplicações da congruência, ao demonstrá-lo no ambiente da álgebra abstrata, observarmos uma elegante ligação entre um resultado bem conhecido da Teoria dos Números e a Teoria de Anéis.

Apresentados como aplicações da Aritmética Modular, no contexto social, os código de barras e o CPF despertam o interesse no aluno em aprender tal teoria. Apresentados como momentos do currículo da educação básica em que a congruência módulo n pode ser inserida, no ensino médio, no momento em que se estuda arcos côngruos e as potências naturais do número complexo $i = \sqrt{-1}$, promovem uma ótima oportunidade de mostrar as conexões entre temas matemáticos interessantes.

Professores de matemática, que atuam principalmente no ensino básico, poderão utilizar este trabalho em nível de formação continuada e aplicá-lo na sala de aula. Acredita-se também que, motivados por este, outros trabalhos nessa linha possam surgir, com outras aplicações interessantes de congruência, que poderão ser aplicadas na Educação Básica.

Referências

[1] DOMINGUES, Hygino H. e IEZZI, Gelson. ***Álgebra Moderna***. *São Paulo: Editora Atual, 1982.*

[2] LIMA, Elon Lages; et al. ***A Matemática do Ensino Médio:*** *Volume* 1. 9.*ed. Rio de Janeiro: IMPA, 2006.* Coleção do Professor de Matemática.

[3] HEFEZ, Abramo. ***Elementos de Aritmética***. *2 ed. Rio de Janeiro: SBM, 2011.*

[4] SANTOS, José Plínio de Oliveira. ***Introdução à Teoria dos Números***. 3.*ed. Rio de Janeiro: IMPA, 2012.*

[5] DANTE, Luiz Roberto. ***Matemática***. *volume* 2. *São Paulo: Ática, 2004.*

[6] DANTE, Luiz Roberto. ***Matemática***. *volume* 3. *São Paulo: Ática, 2004.*

[7] GARBI, Gilberto G. ***O romance das equações algébricas***. *3 ed. rev. e ampl. São Paulo: Editora Livraria da Física, 2009.*

[8] DE SÁ, IIydio Pereira. ***Aritmética modular e algumas de suas aplicações***, *p.* 1 *a* 16. *Disponível em: <http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf> Acesso em: 20/12/2014.*

[9] <http://msdn.microsoft.com/pt-br/library/cc580676.aspx> Acessado em: 20/12/2014.