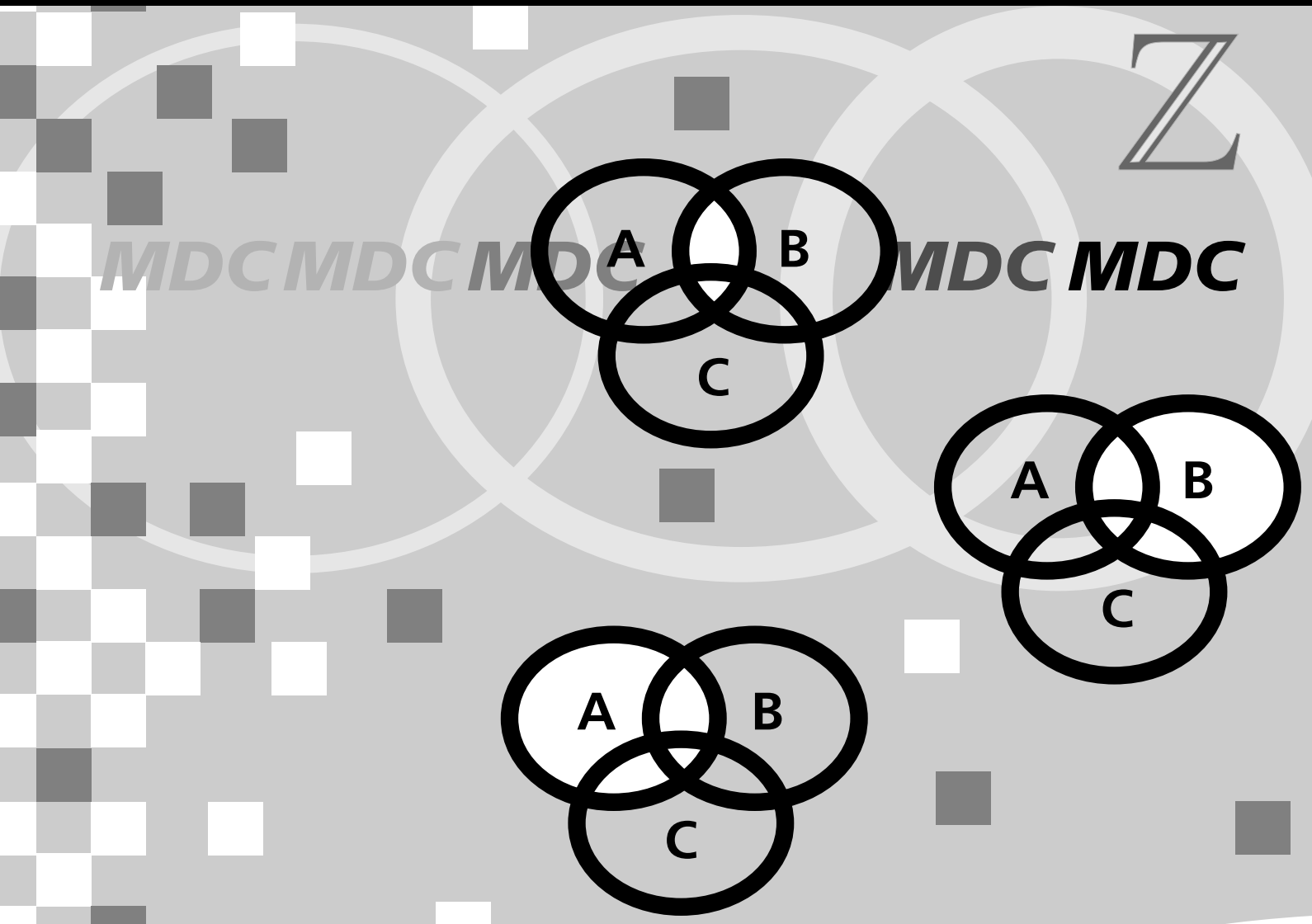
Módulo 1

Volume | 3

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 3 – Módulo 1

Adilson Gonçalves

Luiz Manoel Figueiredo

GOVERNO DO Rio de Janeiro

SECRETARIA DE CIÊNCIA E TECNOLOGIA

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

COORDENAÇÃO DE AVALIAÇÃO DO MATERIAL DIDÁTICO
Débora Barreiros

AVALIAÇÃO DO MATERIAL DIDÁTICO
Letícia Calhau

Departamento de Produção

EDITORA
Tereza Queiroz

COORDENAÇÃO DE PRODUÇÃO
Jorge Moura

CAPA
Eduardo Bordoni

PRODUÇÃO GRÁFICA
Patricia Seabra

Copyright © 2006, Fundação Cecierj / Consórcio Cederj

Nenhuma parte deste material poderá ser reproduzida, transmitida e gravada, por qualquer meio eletrônico, mecânico, por fotocópia e outros, sem a prévia autorização, por escrito, da Fundação.

G635a
Gonçalves, Adilson.
Álgebra I. v. 3 / Adilson Gonçalves; Luiz Manoel Figueiredo. – Rio de Janeiro: Fundação CECIERJ, 2009.
52p.; 21 x 29,7 cm.

ISBN: 85-7648-329-7

1. Álgebra. 2. Teorema de Fermat. 2. Função de Euler. 3. Equações diofantinas. 4. Sistemas lineares. 5. Teorema chinês. I. Figueiredo, Luiz Manoel. II. Título.

CDD: 512

2009/2

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 13 – Pequeno teorema de Fermat _____ **3**
Adilson Gonçalves / Luiz Manoel Figueiredo

Aula 14 – A função ϕ (phi) de Euler _____ **9**
Adilson Gonçalves / Luiz Manoel Figueiredo

Aula 15 – As equações diofantinas lineares _____ **19**
Adilson Gonçalves / Luiz Manoel Figueiredo

Aula 16 – A equação diofantina pitagórica $x^2 + y^2 = z^2$ _____ **25**
Adilson Gonçalves / Luiz Manoel Figueiredo

Aula 17 – Equações de congruências _____ **33**
Adilson Gonçalves / Luiz Manoel Figueiredo

Aula 18 – Sistemas lineares de congruências: o teorema chinês do resto _____ **43**
Adilson Gonçalves / Luiz Manoel Figueiredo

Aula 13 – Pequeno teorema de Fermat

Objetivos

- Apresentar o teorema de Fermat.

Introdução

Nesta aula estudaremos o pequeno teorema de Fermat ou, simplesmente, teorema de Fermat, que essencialmente diz que todo primo ímpar p divide $q^p - q$ onde q é um inteiro qualquer.

Os chineses, desde a antiguidade, já conheciam esta afirmação quando $q = 2$. Por exemplo,

$$\begin{array}{lllllll} p=3 & \longrightarrow & 3 & \text{divide} & 2^3-2= & 8-2= & 6 \\ p=5 & \longrightarrow & 5 & \text{divide} & 2^5-2= & 32-2= & 30 \\ p=7 & \longrightarrow & 7 & \text{divide} & 2^7-2= & 128-2= & 126 \end{array}$$

Não confunda este teorema de Fermat com o chamado "último teorema de Fermat" demonstrado apenas recentemente (1995), de que, a equação $x^n + y^n = z^n$, com $n \geq 3$, não tem solução com x, y, z inteiros não-nulos.

No entanto, foi Fermat quem demonstrou a afirmação $p|q^p - q$, para q inteiro qualquer.

Atividade: Escolha alguns valores de p, primo, e q inteiro qualquer e verifique que p divide $q^p - q$.

Demonstração do teorema de Fermat

Vamos fazer esta demonstração por indução. O teorema diz que p divide $q^p - q$, isto é,

$$q^p \equiv q \pmod{p}$$

para todo primo p e q inteiro.

Vamos usar a seguinte propriedade $P(n)$:

$$P(n) : n^p \equiv n \pmod{p}\,.$$

Claramente $P(1)$ é verdadeira (alguma dúvida?). Vamos mostrar que $P(n) \implies P(n+1)$. Com isto, pelo teorema de indução finita, teremos provado que $P(n)$ é verdadeira para todo $n \in \mathbb{Z}$. A partir daí, provaremos que $q^p \equiv q \pmod{p}$, para todo inteiro q. Vamos então provar a hipótese de indução

$$P(n) \implies P(n+1)\,.$$

Suponha que $P(n)$ seja verdadeiro, isto é,

$$n^p \equiv n \pmod{p}.$$

Para provarmos que $(n+1)^p \equiv n+1 \pmod{p}$, vamos usar o binômio de Newton.

$(n+1)^p = n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + \binom{p}{p-1} n + 1$. Note que cada termo $\binom{p}{i}$, $i = 1, \cdots, p-1$ é um múltiplo de p, portanto:

$$n^p + \underbrace{\binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + \binom{p}{p-1} n}_{\text{múltiplo de } p} + 1 \equiv n^p + 1 \pmod{p}$$

A fórmula de binômio de Newton é:
$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \cdots + \binom{p}{p-1} a^1 b^{p-1} + b^p$. isto é,
$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i}b^i$

logo,

$$(n+1)^p \equiv n^p \pmod{p} \equiv n+1 \pmod{p}$$

onde usamos a hipótese de indução $n^p \equiv n \pmod{p}$.

Portanto, $P(n+1)$ é verdadeiro. Pelo teorema de indução finita, $P(n)$ é verdadeiro para todo n natural, isto é,

$$n^p \equiv n \pmod{p},$$

para todo $n \geq 1$.

Para concluir a demonstração, temos que cuidar do caso $q^p \equiv q \pmod{p}$, com q inteiro negativo.

Bem, se $q < 0$ então, evidentemente, $(-q) > 0$. Assim, $q \in \mathbb{Z}$ e $q < 0$, então o resultado vale para $(-q)$, isto é,

$$(-q)^p \equiv (-q) \pmod{p}.$$

Se p é primo ímpar, então

$$(-q)^p = (-1)^p \cdot q^p = -q^p$$

assim,

$$(-q)^p \equiv (-q) \pmod{p} \Longrightarrow -q^p \equiv -q \pmod{p} \Longrightarrow q^p \equiv q \pmod{p}.$$

Se p é primo par, então $p = 2$. Mas o caso $p = 2$ é bastante simples de ser verificado, pois $\overline{0}$ e $\overline{1}$ são todas as classes $\pmod 2$ e vale que $\overline{0}^2 = \overline{0}$ e $\overline{1}^2 = \overline{1}$.

■

Concluímos a prova do pequeno teorema de Fermat. Em seguida, provaremos uma outra versão, ligeiramente diferente, do mesmo teorema.

Segunda versão do teorema de Fermat

Nossa primeira versão do teorema de Fermat diz que $q^p \equiv q \pmod{p}$, para todo inteiro q. Vamos agora considerar dois casos:

i. Se p divide q então $p \mid q^p$, logo $q^p \equiv q \equiv 0 \pmod{p}$, isto é, a afirmação $q^p \equiv q \pmod{p}$ é, no fundo, trivial, pois diz apenas que $0 \equiv 0 \pmod{p}$.

ii. Se p não divide q então $\text{mdc}(q,p) = 1$, pois p é primo, logo existe inverso de $q \bmod p$, isto é, existe inteiro b tal que $ab \equiv 1 \pmod{p}$. Multiplicando ambos os lados de $q^p \equiv q \pmod{p}$ por b, obtemos

$$q^p b \equiv qb \pmod{p} \Longrightarrow q^{p-1}(qb) \equiv qb \pmod{p}$$

como $qb \equiv 1 \pmod{p}$, então, substituindo na equação acima, resulta

$$q^{p-1} \equiv 1 \pmod{p}.$$

Resumindo, podemos dividir o teorema de Fermat em dois casos, se p divide q então a afirmação $q^p \equiv q \pmod{p}$ é trivial e, se p não divide q então

$$q^p \equiv q \pmod{p} \Longrightarrow q^{p-1} \equiv 1 \pmod{p}.$$

Provamos, portanto, que

Teorema 1 (teorema de Fermat - Segunda versão)
Se p é primo e q é um inteiro que não é divisível por p então

$$q^{p-1} \equiv 1 \pmod{p}.$$

Aplicação do teorema de Fermat

Uma aplicação muito interessante do teorema de Fermat é a determinação da classe de $q^n \bmod p$, onde p é primo e p não divide q.

A idéia aqui é que, se fizermos a divisão do expoente n por $p-1$:

$$n = (p-1)q + r$$

então

$$q^n = q^{q(p-1)+r} = q^r \cdot q^{q(p-1)} = q^r (q^{p-1})^q.$$

Como $q^{p-1} \equiv 1 \pmod{p}$ então

$$q^n = q^r (q^{p-1})^q \equiv q^r \cdot 1^q \equiv q^r \pmod{p}.$$

Mas $0 \leq r < p-1$ (resto da divisão de n por $p-1$). Assim, q^r é uma potência possivelmente muito menor que q^n.

Exemplo **1**

Encontre o resto da divisão de 2^{4514} por 7.

Solução:

Dividindo 4514 por 7-1=6, obtemos

$$4514 = 6 \times 752 + 2\,.$$

Portanto,

$$2^{4514} = 2^{6\times 752+2} = 2^2(2^b)^{752} \equiv 2^2 \pmod 7$$

onde usamos $2^b \equiv 1 \pmod 7$.

Assim, o resto da divisão de 2^{4514} por 7 é $2^2 = 4$.

Exemplo **2**

Vamos mostrar que $2^{70} + 3^{70}$ é divisível por 13.

Solução:

Vamos verificar o resto de 2^{70} e 3^{70} por 13 usando o teorema de Fermat.

$$70 = 5 \times 12 + 10$$

e, logo

$$2^{70} = 2^{5\times 12+10} = 2^{10}(2^{12})^5 \equiv 2^{10} \pmod{13}\,.$$

Analogamente, $3^{70} \equiv 3^{10} \pmod{13}$.

Para calcular 2^{10} mod 13, podemos usar, por exemplo, $2^5 = 32 \equiv b \pmod{13}$. Assim,

$$2^{10} \equiv 2^5 \times 2^5 \equiv b \times b \pmod{13} \equiv 3b \pmod{13} \equiv 10 \pmod{13}\,.$$

Para calcular 3^{10} mod 13 podemos usar $3^3 = 2^7 \equiv 1 \pmod{13}$. Assim,

$$3^{10} = (3^3)^3 \cdot 3^1 \equiv 3 \times 1^3 \equiv 3 \pmod{13}\,.$$

Portanto,

$$2^{70} + 3^{70} \equiv 10 + 3 \equiv 13 \equiv 0 \pmod{13}\,.$$

Logo, 13 divide $2^{70} + 3^{70}$.

p sendo primos de Fermat

Uma outra aplicação muito interessante do teorema de Fermat é como teste de primalidade, isto é, um processo que permite determinar se um dado inteiro é ou não primo.

O processo funciona assim: sabemos que, se p é primo, então $q^{p-1} \equiv 1 \pmod{p}$, onde p não divide q.

Portanto, dado inteiro n se encontrarmos uma base q tal que $q^{n-1} \not\equiv 1 \pmod{n}$ então podemos dizer com certeza que n é composto.

Mas, e se acontecer de $q^{n-1} \equiv 1 \pmod{n}$. Isto prova que n é primo? Leibnitz pensava que sim. Ele usava a base $q = 2$ como teste de primalidade.

Na verdade, o fato de $q^{n-1} \equiv 1 \pmod{n}$ não implica em que n seja primo.

Por exemplo, com $n = 341$ e $q = 2$, temos

$$2^{341-1} = 2^{340} \equiv 1 \pmod{341},$$

mas $341 = 11 \times 31$ não é primo.

Assim, este teste permite identificar números compostos, mesmo que não saibamos fatorá-los, mas não permite provar que um inteiro seja primo. Se é assim, então qual a sua utilidade? Ela é útil porque acerta bem mais do que erra. Vou explicar melhor.

Se $b^{n-1} \equiv 1 \pmod{n}$, mas n não é primo, dizemos que n é pseudoprimo para a base b. Por exemplo, 341 é um pseudoprimo para a base 2.

O teste descrito acima é muito útil porque há muito mais primos que pseudoprimos. Por exemplo, entre 1 e 10^6 existem 78498 números primos, mas somente 245 pseudoprimos para a base 2.

Portanto, se um inteiro n passa no teste para a base 2 então é muito provável que seja primo. O teste pode ser melhorado se testarmos várias bases. Por exemplo, usando bases 2 e 3 podemos aumentar em muito a probabilidade de que um inteiro n que passe no teste seja primo.

Sabe-se que para cada base q existem infinitos inteiros n que são pseudoprimos para a base q.

O problema é que existem inteiros que não são primos e que passam no teste para qualquer base. Estes inteiros são chamados números de carmichael.

R.D. Carmichael foi o primeiro matemático que mostrou que estes números existem.

O menor número de carmichael é 561.

Resumo

Nesta aula vimos o pequeno teorema de Fermat. Na verdade, vimos duas versões bem próximas deste teorema.

Vimos duas aplicações: como um meio de obter a classe $q^n \bmod p$, e como "teste" de primalidade.

Vimos que se um inteiro passa pelo teste com várias bases então é um primo com forte probabilidade. Se falha o teste então certamente é um composto.

Exercícios:

1. Mostre que se p é um primo e a e b são inteiros então

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

2. Calcule o resto da divisão de

   a) 3^{200} por 13

   b) 5^{2530} por 7

3. Use o teorema de Fermat para provar que para todo inteiro n, o número

$$n^3 + (n+1)^3 + (n+2)^3$$

   é divisível por 9.

4. O que são pseudoprimos? mostre que 341 é pseudoprimo para a base 2, mas não é pseudoprimo para a base 3.

Aula 14 – A função ϕ (phi) de Euler

Objetivos

- Escrever a definição da função phi de Euler e calcular $\phi(n)$, para qualquer inteiro n;
- Listar as principais propriedades desta função.

Introdução

Leonhard Euler (1707 - 1783) foi um matemático e físico suíço. Muitos consideram ele e Gauss os maiores matemáticos que existiram.
Euler foi um dos primeiros a aplicar o cálculo à Física.
Seu nome se pronuncia "óiler" e não "euler".

Nesta aula estudaremos a função phi de Euler que recebe este nome em homenagem ao matemático suíço Euler que foi quem primeiro estudou esta função.

Essa função também é conhecida como função totiente.

Definição

Definição 1

Para qualquer inteiro positivo n, definimos $\phi(n)$ como o número de inteiros positivos menores que n e coprimos com n.

Lembre-se que o símbolo # indica a cardinalidade (o número de elementos de) um conjunto.

Em outras palavras,

$$\phi(n) = \#\{x \in \mathbb{Z} \mid 1 \leq x < n \quad \text{e} \quad \text{mdc}(x, n) = 1\}$$

Exemplo 3

Seja $n = 12$. Os inteiros positivos menores que 12 e coprimos com 12 são 1, 5, 7 e 11. Assim, $\phi(12) = 4$.

$$\phi(12) = \#\{1, 5, 7, 11\} = 4\,.$$

Exemplo 4

Seja $n = 15$. Os inteiros positivos menores que 15 e coprimos com 15 são 1, 2, 4, 7, 8, 11, 13 e 14. Assim, $\phi(15) = 8$.

$$\begin{aligned} \phi(15) &= \#\{x \in \mathbb{Z} \mid 1 \leq x < 15 \quad \text{e} \quad \text{mdc}(x, 15) = 1\} \\ &= \#\{1, 2, 4, 7, 8, 11, 13, 14\} = 8\,. \end{aligned}$$

Atividade: Verifique que $\phi(20) = 8$ e $\phi(25) = 20$.

Observe que $\phi(1) = 1$ (segue-se da nossa definição).

A tabela abaixo mostra os valores da função $\phi(n)$ para os 20 primeiros inteiros positivos.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Primeiras propriedades: $\phi(p)$ e $\phi(p^\alpha)$

Vamos demonstrar algumas propriedades que permitirão calcular $\phi(n)$ para qualquer inteiro n, usando-se a decomposição de n em fatores primos.

Vamos começar determinando $\phi(p)$ para p primo.

Lema 1
Se p é um primo então

$$\phi(p) = p - 1\,.$$

Demonstração: Por definição, $\phi(p)$ é o número de inteiros positivos x menores que p e coprimos com p. Mas, como p é primo, todo inteiro x, $1 \leq x < p-1$ é coprimo com p. Assim, $\phi(p) = p - 1$.

■

Observe essa propriedade na tabela acima:

$$\begin{aligned}
\phi(2) &= 2 - 1 = 1 \\
\phi(3) &= 3 - 1 = 2 \\
\phi(5) &= 5 - 1 = 4 \\
\phi(7) &= 7 - 1 = 6 \\
&\vdots
\end{aligned}$$

O próximo passo é generalizar essa propriedade determinando o valor da função em potências de primos, isto é, $\phi(p^\alpha)$.

Proposição 1
Seja p primo. Então vale que

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

onde n é um inteiro positivo qualquer.

Demonstração: Temos que contar quantos inteiros entre 1 e p^α são coprimos com p^α. Faremos isso de uma maneira indireta: contaremos quantos inteiros entre 1 e p^α não são coprimos com p^α.

Teremos:

$$\underbrace{\phi(p^\alpha)}_{\text{coprimos com } p^\alpha} = \underbrace{p^\alpha}_{\text{números de inteiros entre 1 e } p^\alpha} - \#\{\text{não coprimos com } p^\alpha\} \qquad (*)$$

E quem são os inteiros que não são coprimos com p^α? como p é primo, se $\text{mdc}(x, p^\alpha) \neq 1$, então x deve conter o fator primo p, isto é, p divide x. Por outro lado, se $p \mid x$ então, evidentemente, $\text{mdc}(x, p^\alpha) \neq 1$.

Assim, os inteiros não coprimos com p^α são exatamente os múltiplos de p. A questão então é: quantos múltiplos de p existem entre 1 e p^α?

Os múltiplos de p entre 1 e p^α são:

$$1p,\ 2p,\ 3p,\ \cdots,\ p^{\alpha-1} \cdot p = p^\alpha\,.$$

Existem, portanto, $p^{\alpha-1}$ múltiplos de p entre 1 e p^α.

Voltando à equação $(*)$, obtemos

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

■

Exemplo **5**

Temos que $\phi(9) = 6$ pois, os inteiros 1, 2, 4, 5, 7 e 8 são coprimos com 9. Usando o teorema obtemos:

$$\phi(9) = \phi(3^\alpha) = 3^{\alpha-1}(3-1) = 3 \times 2 = 6\,.$$

Exemplo **6**

$$\phi(125) = \phi(5^3) = 5^{3-1}(5-1) = 5^2 \cdot 4 = 100\,.$$

Atividade: Encontre $\phi(16), \phi(25)$ e $\phi(49)$.

Outra propriedade: $\phi(mn)$ com $\text{mdc}(m,n) = 1$

Falta ainda uma propriedade para que passemos calcular $\phi(n)$ a partir da decomposição de n em fatores primos.

Desta vez vamos iniciar com alguns exemplos.

Exemplo **7**

- $\phi(3) = 2$; $\phi(4) = 2$ e

$$\phi(3 \times 4) = \phi(12) = 4 = 2 \times 2 = \phi(3) \times \phi(4)\,.$$

- $\phi(3) = 2$ e $\phi(5) = 4$. Temos que

$$\phi(3 \times 5) = \phi(15) = 8 = 2 \times 4 = \phi(3) \times \phi(5)\,.$$

- $\phi(6) = 2$ e $\phi(2) = 1$ mas,

$$\phi(2 \times 6) = \phi(12) = 4 \neq \phi(6) \times \phi(2)\,.$$

Veja que nos dois primeiros exemplos vale que $\phi(mn) = \phi(m) \times \phi(n)$ mas, isso não se verificou no terceiro. O que deu errado? o que os dois primeiros exemplos têm em comum é que se trata de $\phi(mn)$, com m e n coprimos. Veja:

$$\phi(3 \times 4) = \phi(3) \times \phi(4)$$

onde 3 e 4 são coprimos e

$$\phi(3 \times 5) = \phi(3) \times \phi(5)$$

onde 3 e 5 são coprimos.

No terceiro exemplo, 2 e 6 não são coprimos.

Atividade: Faça você mesmo mais alguns exemplos de $\phi(mn)$, com m e n coprimos. Você encontrará $\phi(mn) = \phi(m) \times \phi(n)$ em todos eles.

Provaremos a seguinte

Proposição 2

Se m e n são coprimos então

$$\phi(mn) = \phi(m) \cdot \phi(n)\,.$$

Demonstração: Sejam m e n inteiros positivos tais que $\text{mdc}(m, n) = 1$ e sejam

$$\begin{aligned} S_m &= \{x \in \mathbb{Z} \mid 1 \leq x < m \text{ e } \text{mdc}(x, m) = 1\} \\ S_n &= \{x \in \mathbb{Z} \mid 1 \leq x < n \text{ e } \text{mdc}(x, n) = 1\} \\ S_{mn} &= \{x \in \mathbb{Z} \mid 1 \leq x < mn \text{ e } \text{mdc}(x, mn) = 1\} \end{aligned}$$

Queremos mostrar que $\#S_{mn} = (\#S_m) \cdot (\#S_n)$, pois $\phi(mn) = \#S_{mn}$, $\phi(m) = \#S_m$ e $\phi(n) = \#S_n$. O que vamos fazer é definir uma função

$$f : S_{mn} \longrightarrow S_m \times S_n\,,$$

isto é, uma função f de S_{mn} no produto cartesiano $S_m \times S_n$. Observe que $\#(S_m \times S_n) = \#S_m \times \#S_n$.

Em seguida, mostraremos que $f : S_{mn} \longrightarrow S_m \times S_n$ é bijetiva quando $\text{mdc}(m, n) = 1$ e, portanto,

$$\#S_{mn} = \#(S_m \times S_n) = (\#S_m) \times (\#S_n) \Longrightarrow \varphi(mn) = \varphi(m) \times \varphi(n)\,,$$

quando $\text{mdc}(m, n) = 1$.

Em resumo, o nosso plano é definir uma função $f : S_{mn} \longrightarrow S_m \times S_n$ e mostra que ela é bijetiva se $\text{mdc}(m, n) = 1$. Vamos em frente então!

- A função f:

  Definimos

  $$\begin{array}{rccc} f: & S_{mn} & \longrightarrow & S_m \times S_n \\ & x & \longmapsto & \left(\overline{x}, \overline{\overline{x}}\right) \end{array}$$

  onde $x \equiv \overline{x} \pmod{m}$ e $x \equiv \overline{\overline{x}} \pmod{n}$.

  Esta definição merece alguns esclarecimentos: se $x \in S_{mn}$ então $\text{mdc}(x, mn) = 1$. Portanto, x não tem fatores primos em comum com mn, logo x não tem fatores comuns com m ou com n, isto é, $\text{mdc}(x, m) = \text{mdc}(x, n) = 1$.

  Pode ser que $x > m$ mas $x \equiv \overline{x}$, com $1 \leq \overline{x} \leq m$. Como $\text{mdc}(x, m) = 1$ então $\text{mdc}(\overline{x}, m) = 1$ (prove isto!), logo $1 \leq \overline{x} \leq m$ e $\text{mdc}(\overline{x}, m) = 1$, isto é, $\overline{x} \in S_{mn}$. Assim, existe $\overline{x} \in S_m$ tal que $x \equiv \overline{x} \pmod{m}$.

  Analogamente, existe $\overline{\overline{x}} \in S_n$ tal que $x \equiv \overline{\overline{x}} \pmod{n}$. Assim, nossa definição da função f faz todo o sentido.

- f é injetiva:

  Vamos mostrar, por contradição, que f é injetiva. Suponha que não seja e suponha que existem $x, y \in S_{mn}$ tais que $f(x) = f(y)$, isto é,

  $$\begin{array}{l} (x \bmod m, x \bmod n) = (y \bmod m, y \bmod n) \Longrightarrow x \equiv y \pmod{m} \\ \text{e } x \equiv y \pmod{n} \ (*) \end{array}$$

  Suponha que $x > y$ (o caso $y > x$ é análogo). Temos

  $$1 \leq y, \ \ x < mn \ (\text{pois } x, y \in S_{mn})\,.$$

  Logo

  $$0 \leq x - y < mn\,.$$

De $(*)$ concluímos que $x - y \equiv 0 \pmod{m}$ e $x - y \equiv 0 \pmod{n}$ o que implica $m \mid x - y$ e $n \mid x - y$, isto é, $x - y$ é múltiplo comum de m e n.

Portanto, $x - y$ é múltiplo de $\text{mmc}(m, n) = mn$. Daí resulta uma contradição, $x - y$ não pode ser múltiplo de mn, uma vez que $0 \leq x - y < mn$.

- f é sobrejetiva:

  Seja $(a, b) \in S_m \times S_n$. Devemos encontrar um $x \in S_{mn}$ tal que $f(x) = (a, b)$, isto é,

$$x \equiv a \pmod{m} \quad \text{e} \quad x \equiv b \pmod{n} \qquad (**)$$

  Note que, caso exista tal x, teremos

$$x \equiv a \pmod{m} \Longrightarrow x = a + km$$

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

$$x \equiv b \pmod{n} \Longrightarrow x = b + ln$$

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

Lembre-se que $\text{mmc}(m, n) \cdot \text{mdc}(m, n) = m \cdot n$. Se m e n são primos entre si então $\text{mdc}(m, n) = 1$, logo $\text{mmc}(m, n) = m \cdot n$.

  Igualando as duas equações temos

$$a + km = b + ln \Longrightarrow a - b = ln = km\,.$$

  Portanto, para encontrarmos x, podemos começar expressando $a - b$ em termos de n e m. Lembre-se que, como $\text{mdc}(m, n) = 1$ então existem $k', k'' \in \mathbb{Z}$ tais que

$$1 = k'm + k''n\,.$$

  Multiplicando por $a - b$:

$$\begin{aligned} a - b &= (a - b)k'n + (a - b)k''n \\ a - \underbrace{(a - b)k''}_{k} m &= b + \underbrace{(a - b)k'}_{l} n\,. \end{aligned}$$

  Logo existem $k, l \in \mathbb{Z}$ tais que

$$a + km = b + ln\,.$$

  Seja $x' = a + km = b + ln$. Então,

$$\begin{aligned} x' = a + km &\Longrightarrow x' \equiv a \pmod{m} \\ x' = b + ln &\Longrightarrow x' \equiv b \pmod{n}\,. \end{aligned}$$

Assim, x' atende às congruências $(**)$.

O único problema é que x' pode ser grande demais para estar em S_{mn}, isto é, poderíamos ter $x' > mn$. Se este for o caso, seja x tal que $x' \equiv x \pmod{mn}$ e $1 \leq x \leq mn$.

Como $x' \equiv x \pmod{mn}$ então $x \equiv x' \equiv a \pmod{m}$. Logo $x \equiv a \pmod{m}$ e $x \equiv b \pmod{n}$ e $x \equiv x' \equiv b \pmod{n}$ e, $1 \leq x \leq mn$. Resta apenas mostrar que $\text{mdc}(x, mn) = 1$.

Como a e m não tem fatores comuns (pois $a \in S_{mn}$) e $x \equiv a \pmod{m}$ então x e m não tem fatores comuns.

Analogamente, como b e n não tem fatores comuns (pois $b \in S_n$) e $x \equiv \pmod{n}$ então x e n não tem fatores comuns.

Portanto, x e mn não tem fatores comuns (porque x não os tem com m e com n), isto é, $\text{mdc}(x, mn) = 1$.

Com isto, conseguimos encontrar um $x \in S_{mn}$ tal que $x \equiv \pmod{m}$ e $x \equiv b \pmod{n}$ o que completa a demonstração de que f é sobrejetiva.

Demonstramos que $f : S_{mn} \longrightarrow S_m \times S_n$ é bijetiva e, portanto, $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ se $\text{mdc}(m, n) = 1$.

■

Exemplo 8

a) $\varphi(20) = \varphi(4 \times 5) = \varphi(4) \cdot \varphi(5) = 2 \times 4 = 8$.

b) $\varphi(30) = \varphi(5 \times 6) = \varphi(5) \cdot \varphi(6) = \varphi(5) \cdot \varphi(2) \cdot \varphi(3) = 4 \times 1 \times 2 = 8$.

Atividade: Encontre $\varphi(100)$ e $\varphi(600)$.

Juntando tudo

Aplicando as propriedades da função $\varphi(m)$ que demonstramos anteriormente, podemos calcular $\varphi(n)$ a partir da decomposição de n em fatores primos.

Provemos que $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ se $\text{mdc}(m, n) = 1$. Podemos facilmente estender este resultado:

Proposição 3

Se $N_1, N_2, \cdots, N_r$ são inteiros positivos dois a dois primos entre si então

$$\varphi(N_1 \cdot N_2 \cdot N_3 \cdot ... \cdot N_r) = \varphi(N_1) \cdot \varphi(N_2) \cdot ... \cdot \varphi(N_r)\,.$$

Demonstração: Basta aplicar a proposição anterior sucessivamente:

$$\begin{aligned}\varphi(N_1 \cdot N_2 \cdot N_3 \cdot ... \cdot N_r) &= \varphi(N_1) \cdot \varphi(N_2 \cdot N_3 \cdot ... \cdot N_r), \text{ pois } \text{mdc}(N_1, N_2, \cdots, N_r) = 1 \\ &= \varphi(N_1) \cdot \varphi(N_2) \cdot \varphi(N_3 \cdot ... \cdot N_r), \text{ pois } \text{mdc}(N_2, N_3, \cdots, N_r) = 1 \\ &\vdots \\ &= \varphi(N_1) \cdot \varphi(N_2) \cdot ... \cdot \varphi(N_r)\,.\end{aligned}$$

Seja agora $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}$, onde $p_1, \cdots, p_r$ são primos distintos. Os termos $p_1^{\alpha_1}, p_2^{\alpha_2}, ..., p_r^{\alpha_r}$ são dois a dois primos entre si. Logo

$$\varphi(N) = \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot ... \cdot \varphi(p_r^{\alpha_r})\,.$$

Mas,

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right).$$

Logo,

$$\varphi(N) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2} \cdot \left(1 - \frac{1}{p_2}\right) \cdot ... \cdot p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right).$$

Reordenando os termos do produto obtemos:

$$\begin{aligned}\varphi(N) &= \underbrace{(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r})}_{=N} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_r}\right) \\ \varphi(N) &= N \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_r}\right).\end{aligned}$$

Podemos escrever esta expressão de uma forma mais sintética como:

$$\varphi(N) = N \cdot \prod_{\substack{p \mid N \\ p \text{ primo}}} \left(1 - \frac{1}{p}\right).$$

O símbolo $\prod$ indica o produto e $p \mid N$, p primo, sob o símbolo, indica que os fatores do produto são os termos $\left(1 - \frac{1}{p}\right)$, onde tomamos todos os primos p divisores de N.

■

Exemplo **9**

Tomemos $N = 120$.

Fatorando 120, obtemos

$$120 = 2^3 \times 3 \times 5\,.$$

Assim,

$$\varphi(120) = 120 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 120 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 32\,.$$

Equivalentemente, poderíamos fazer

$$\varphi(120) = \varphi(2^3 \times 3 \times 5) = \varphi(2^3) \cdot \varphi(3) \cdot \varphi(5) = 2^{3-1}(2-1) \times (3-1) \times (5-1) = 4 \times 2 \times 4 = 32\,.$$

Resumo

Nesta aula definimos a função φ de Euler e obtivemos duas propriedades desta função que permitem calcular rapidamente o valor de $\varphi(N)$ e partir da decomposição de N em fatores primos.

Na próxima aula veremos um teorema muito importante que envolve a função $\varphi(N)$: o teorema de Euler.

Exercícios

1. Calcule $\varphi(N)$ para os seguintes valores de N:

   a) $N = 200$

   b) $N = 500$

   c) $N = 2^2 \times 3^5 \times 7^4$

   d) $N = (20)^5$

2. Verifique, para $N = 12, N = 15$ e $N = 20$, que vale a fórmula

$$\sum_{d|n} \varphi(d) = n\,.$$

   Por exemplo, para $N = 12$, os divisores positivos são $\{1, 2, 3, 4, 6, 12\}$. A fórmula seria:

$$\sum_{d|12} \varphi(d) = n \Longrightarrow \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12$$

   que é uma sentença verdadeira (verifique!).

   Verifique que a fórmula também vale para $N = 15$ e $N = 20$.

   Na verdade, pode-se demonstrar que esta fórmula vale para todo n inteiro positivo.

Aula 15 – As equações diofantinas lineares

Meta:

Apresentar o conceito de equações diofantinas e discutir soluções inteiras das equações diofantinas lineares.

Objetivos

- Definir o conceito de equações diofantinas e equações diofantinas lineares;
- determinar condições necessárias e suficientes para existência das equações diofantinas lineares;
- resolver, quando possível, equações diofantinas lineares em duas variáveis.

Introdução

O estudo das equações polinomiais com coeficientes inteiros e suas possíveis soluções inteiras se reporta aos gregos, no século III d.C.

Diophantes de Alexandria foi o primeiro a tratar sistematicamente dessas equações, discutindo existência de suas soluções inteiras e procurando calcular essas soluções. Por isso, essas equações especiais são chamadas de *equações diofantinas*. E entendido que nessas equações estamos interessados em discutir a existência e a possível determinação de suas soluções inteiras (as vezes também soluções racionais). Em geral, esse é um problema que pode ser muito difícil de se atacar com sucesso. Uma dada equação diofantina pode não possuir soluções inteiras, como pode também possuir infinitas soluções inteiras. Por exemplo, $x^2 + y^2 = 3$ não possui soluções inteiras, $x^2+y^2 = 2$ possui quatro soluções inteiras $(\pm 1, \pm 1)$, enquanto que a equação $x^2 + y^2 = z^2$ possui infinitas soluções inteiras (x, y, z).

Nessa aula, discutiremos a existência e, quando possível, calcularemos todas as soluções das equações diofantinas lineares em duas variáveis, $ax + by = c$.

As equações diofantinas lineares

Sejam $a_1, a_2, \cdots, a_n$ inteiros não nulos, e seja c um dado número inteiro.

A equação $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ é chamada *equação diofantina linear em n variáveis* $x_1, x_2, \cdots, x_n$.

O subconjunto $S \subseteq \mathbb{Z}^n = \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{n \text{ vezes}}$ de todas as n-uplas inteiras $(r_1, r_2, \cdots, r_n) \in \mathbb{Z}^n$, que satisfazem a equação $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ (isto é, $a_1r_1 + a_2r_2 + \cdots + a_nr_n = c$) é chamado de *conjunto solução* dessa equação diofantina linear.

Primeiramente estamos interessados em dar condições necessárias e suficientes para que o conjunto S seja não vazio (isto é, exista solução para a dada equação diofantina linear). A seguinte proposição responde a pergunta anterior.

Sejam $a_1, a_2, \cdots, a_n$ inteiros não nulos e seja $d \geq 1$, onde $d = \text{mdc}(a_1, a_2, \cdots, a_n)$ e, seja S o conjunto solução da equação diofantina linear $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$.

Proposição 1

$$S \neq \emptyset \Longleftrightarrow d \text{ é divisor de } c\,.$$

Primeiramente observamos que o Teorema 2, da Aula #6, pode ser generalizado com o seguinte enunciado:

Lema 2 (generalização do Teorema 2 da Aula #6)

$\mathbb{Z}a_1 + \mathbb{Z}a_2 + \cdots + \mathbb{Z}a_n = \mathbb{Z}d\,, (d \geq 1) \Longleftrightarrow d = \text{mdc}(a_1, a_2, \cdots, a_n)$. Em particular, se $\text{mdc}(a_1, a_2, \cdots, a_n) = 1$ então existem inteiros $s_1, s_2, \cdots, s_n$ tais que:

$$s_1a_1' + s_2a_2' + \cdots + s_na_n' = 1\,,$$

e nessa situação, tem-se:

$$\mathbb{Z}a_1' + \mathbb{Z}a_2' + \cdots + \mathbb{Z}a_n' = \mathbb{Z}\,.$$

Assumindo o Lema 1 como verdadeiro, vamos então demonstrar a Proposição 1.

Demonstração:

($\Longrightarrow$) Assume $S \neq \emptyset$. Vamos mostrar que $d \mid c$ (isto é, d é divisor de c).

De $S \neq \emptyset$ segue que existe uma solução $(b_1, b_2, \cdots, b_n)$ para a equação diofantina linear $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$.Assim, $a_1b_1 + a_2b_2 + \cdots + a_nb_n = c$.

Agora, $d \mid a_1, \cdots, a_n \Longrightarrow d \mid c\,.$

($\Longleftarrow$) Assume que $d \mid c$. Vamos provar que $S \neq \emptyset$.

$$d = \text{mdc}(a_1, \cdots, a_n) \Longrightarrow d \mid a_1, \cdots, a_n \,.$$

Sejam $a_1' = \frac{a_1}{d}, a_2' = \frac{a_2}{d}, \cdots, a_n' = \frac{a_n}{d}$ (todos inteiros) e $c' = \frac{c}{d} \in \mathbb{Z}$. Como $d = \text{mdc}(a_1, a_2, \cdots, a_n)$ segue que $\text{mdc}(a_1', a_2', \cdots, a_n') = 1$. Daí segue que:

$$\mathbb{Z}a_1' + \mathbb{Z}a_2' + \cdots + \mathbb{Z}a_n' = \mathbb{Z}\,,$$

e daí segue que existem inteiros $s_1, s_2, \cdots, s_n$ tais que

$$s_1a_1' + s_2a_2' + \cdots + s_na_n' = c'\,.$$

Multiplicando por d, temos:

$$s_1a_1 + s_2a_2 + \cdots + s_na_n = c\,,$$

e, portanto, $(s_1, s_2, \cdots, s_n) \in S$ é uma solução da equação diofantina linear $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$, e $S \neq \emptyset$ completando a demonstração da Proposição 1.

■

Atividade:

1. Defina a noção de $\text{mdc}(a_1, a_2, \cdots, a_n)$ e demonstre o Lema 1, usado na demonstração da Proposição 1.

2. Reescreva a demonstração da Proposição 1 para equações diofantinas lineares $ax + by = c$, em duas variáveis x e y.

As equações diofantinas lineares em duas variáveis

Agora vamos desenvolver os estudos para analisar as equações diofantinas lineares $ax + by = c$, em duas variáveis x e y, com $a, b \neq 0$.

Seja S o conjunto solução (inteiras) de $ax + by = c$. Pela Proposição 1, anteriormente demonstrada, temos que:

"O conjunto solução S de $ax + by = c$ é não vazio
se, e somente se, $d \mid c$ ", onde $d = \text{mdc}(a, b)$.

Em seguida, responderemos a seguinte pergunta, onde $d = \text{mdc}(a, b)$.

Caso S seja não vazio, como descrever todas as soluções inteiras (x, y) da equação diofantina linear $ax + by = c$?

Proposição 2

Seja $(x_0, y_0) \in S$ uma solução particular de $ax + by = c$. Então S possui infinitas soluções $(x, y) \in \mathbb{Z}^2$, e todas as soluções podem ser descritas em equações paramétricas inteiras do seguinte modo:

$$\begin{cases} x = x_0 - \left(\frac{b}{d}\right)t \\ y = y_0 + \left(\frac{a}{d}\right)t \end{cases}$$

com $t \in \mathbb{Z}$.

Demonstração: Primeiramente vamos verificar que os pares $(x, y) \in \mathbb{Z}^2$, descritos por $x = x_0 - \frac{b}{d}\,t$ e $y = y_0 + \frac{a}{d}\,t$ $(t \in \mathbb{Z})$ são soluções de $ax + by = c$. De fato,

$$ax + by = a\left(x_0 - \frac{b}{d}\,t\right) + b\left(y_0 + \frac{a}{d}\,t\right) = (ax_0 + by_0) + \left(-\frac{ab}{d}\,t + \frac{ba}{d}\,t\right) = c + 0 = c\,.$$

Agora, seja $(x, y) \in S$ uma solução genérica de $ax+by = c$e, seja $(x_0, y_0) \in S$ uma dada solução particular de $ax + by = c$. Assim,

$$\begin{cases} ax + by = c \\ ax_0 + by_0 = c \end{cases}$$

Diminuindo essas igualdades temos:

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

ou seja,

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

Seja $a' = \frac{a}{d}$ e $b' = \frac{b}{d}$, onde $d = \text{mdc}(a, b)$.

Portanto teremos:

$$a'(x - x_0) = -b'(y - y_0) = 0\,,$$

onde $\text{mdc}(a', b') = 1$. Assim, $a' \mid (y - y_0)$ e $-b' \mid (x - x_0)$ e temos:

$$\frac{x - x_0}{-b'} = \frac{y - y_0}{a'} = t \in \mathbb{Z}\,.$$

Daí segue que:

$$\begin{cases} x = x_0 + (-b')t = x_0 + \left(-\dfrac{b}{d}\right)t \\ \\ y = y_0 + (a')t = y_0 + \left(\dfrac{a}{d}\right)t \end{cases}$$

com $t \in \mathbb{Z}$ como queríamos demonstrar.

■

Observação

Seja $d = \text{mdc}(a, b)$ e $m = \text{mmc}(a, b)$. Sabemos que $\frac{ab}{d} = m$, daí segue que $\frac{b}{d} = \frac{m}{a}$ e $\frac{a}{d} = \frac{m}{b}$. Portanto, na Proposição 2, anterior, poderíamos descrever as soluções (x, y) de $ax + by = c$ do seguinte modo:

$$\begin{cases} x = x_0 - \dfrac{m}{a}\,t \\ \\ y = y_0 + \dfrac{m}{b}\,t \end{cases}$$

com $t \in \mathbb{Z}$.

Exemplo **10**

Determine o conjunto S de todas as soluções da equação diofantina linear $12x + 18y = 30$.

Solução:

Seja $d = \text{mdc}(12, 18) = 6$. Como $d = 6$ é divisor de $c = 30$, temos que o conjunto solução S é não vazio.

De fato, $(x_0, y_0) = (1, 1) \in S$ é uma solução particular da equação $12x+18y = 30$. Assim, o conjunto S de todas as soluções inteiras de $12x + 18y = 30$ é dado por: $(x, y) \in S$:

$$\begin{cases} x = 1 - \dfrac{18}{6}\,t = 1 - 3t \\ \\ y = 1 + \dfrac{12}{6}\,t = 1 + 2t \end{cases}$$

Atividade:

1. Discuta a existência de soluções inteiras da equação diofantina linear $ax = c$ em uma variável x ($a \neq 0$ e c inteiros).

2. Resolva, se possível, a equação diofantina $10x + 25y = 20$.

3. Interprete graficamente o conjunto $(x, y) \in S$ das soluções inteiras das seguintes equações diofantinas $\begin{cases} \text{(a) } 12x + 18y = 30 \\ \text{(b) } 10x + 25y = 20 \end{cases}$.

4. Em geral, determinar as soluções de equações diofantinas lineares em mais de duas variáveis é mais complicado do que em apenas duas variáveis.

   Por exemplo, mostre que $(x, y, z) \in \mathbb{Z}^3$ descritas parametricamente, em $\mathbb{Z}$, abaixo, são soluções da equação diofantina $2x + 3y + 5z = 0$.

$$\begin{cases} x = \alpha + 5r \\ y = \alpha + 5s \\ z = -\alpha - 2r - 3s \end{cases}$$

   com $\alpha, r, s \in \mathbb{Z}$.

   (Observe que $(\alpha, \alpha, -\alpha)$ é uma solução).

Resumo

Nesta aula, introduzimos métodos que nos permitem discutir existência e cálculo de soluções de equações diofantinas lineares. No caso de duas variáveis, demos a partir de uma solução particular de $ax + by = c$, uma descrição paramétrica inteira de todos as soluções inteiras de $ax + by = c$.

Aula 16 – A equação diofantina pitagórica $x^2 + y^2 = z^2$

Meta:

Apresentar a equação diofantina $x^2+y^2 = z^2$ como um modelo quadrático contendo infinitas soluções.

Objetivos

- Determinar todas as infinitas soluções inteiras da equação quadrática diofantina $x^2 + y^2 = z^2$, em três variáveis x, y e z.

Introdução

As equações diofantinas vem fascinando muitos matemáticos ao longo de muitos séculos e, um desses matemáticos, foi Pierre de Fermat (1601-1665), jurista francês, que dedicava grande parte do seu tempo disponível ao estudo de problemas de Matemática.

Fermat, estudando os escritos de Diophantus, na página onde se tratava das equações pitagóricas $x^2 + y^2 = z^2$ e suas soluções inteiras, anotou na margem da página a seguinte afirmação:

"A equação $x^n + y^n = z^n$, para $n > 2$,
não possui soluções inteiras não nulas x, y e z",

e escrevia em seguida que tinha descoberto *"uma verdadeiramente maravilhosa demonstração para esta afirmação, mas que a margem era demasiadamente estreita para contê-la"*.

É senso comum que, de fato, Fermat não possuía qualquer demonstração daquela afirmação que se convencionou chamar de *"o último teorema de Fermat"*, um dos mais celebrados desafios na Matemática em todos os tempos.

As tentativas para demonstrar esse teorema, foram muitas e, de fato, deram origem a criação de importantes e belas teorias na Matemática como,

por exemplo, a teoria dos anéis e ideais, com destaque para o matemático alemão E.Kummer, no sec XIX.

Algumas soluções particulares desse teorema foram apresentadas, como por exemplo, para $n = 3$ (Euler), $n = 4$ (Fermat, Leibnitz e Euler) e $n = 5$ (Dirichilet e Legendre) e para alguns valores de n (primos regulares), por E.Kummer.

Em 1993, quase 300 anos após a formulação de Fermat, e após a contribuição de muitos matemáticos, o matemático inglês Andrew Wiles, anunciou a demonstração do chamado *"último teorema de Fermat"*.

Em 1993, aos 40 anos de idade, Andrew Wiles relatou o que sentiu ao ter tomado conhecimento do grande desafio legado por Fermat: *"Parecia tão simples e, no entanto, nenhum dos grandes matemáticos da história conseguira resolvê-lo. Ali estava um problema que eu, menino de 10 anos, podia entender e a partir daquele momento nunca o deixaria escapar"*.

Nessa aula trataremos da equação diofantina pitagórica $x^2 + y^2 = z^2$ e suas infinitas soluções inteiras.

A equação diofantina $x^2 + y^2 = z^2$

Estamos interessados em descrever o conjunto S de todas as soluções inteiras $S = (a, b, c)$ da equação $x^2 + y^2 = z^2$.

Assim, S pode ser descrito por:

$$S = \{(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \mid a^2 + b^2 = c^2\}.$$

Observação

É fácil verificar as seguintes afirmações:

a. $(0, \pm b, \pm b)$ e $(\pm a, 0, \pm a) \in S, \forall a, b \in \mathbb{Z}$

b. Se $(a, b, c) \in S$ então $(\pm a, \pm b, \pm c) \in S$

c. Se $k \in \mathbb{Z}$ e $(a, b, c) \in S$ então $(\pm ka, \pm kb, \pm kc)$

Definição 1

Seja $(a, b, c) \in S$. Dizemos que $(a, b, c) \in S$ é uma solução reduzida se $\text{mdc}(a, b) = 1$ com a, b, c positivos.

Pelas observações anteriores temos que se $(a, b, c) \in S$ é uma solução reduzida então $(\pm ka, \pm kb, \pm kc) \in S, \forall\ k \in \mathbb{Z}$.

Em seguida provaremos que todas as soluções $(a, b, c) \in \mathbb{Z}^3$ de $x^2 +$

$y^2 = z^2$ com $ab \neq 0$ são expressas da forma acima, em função das soluções reduzidas.

Proposição 1

Seja $(a, b, c) \in S$, com $ab \neq 0$. Então existe solução reduzida (a', b', c') e existe $k \in \mathbb{Z}$ tal que (a, b, c) é uma das soluções descritas por $(\pm ka', \pm kb', \pm kc')$.

Demonstração: Seja $(a, b, c) \in S$, com $ab \neq 0$. Assim, $a^2 + b^2 = c^2$ com a e b não nulos. Como $(s)^2 = (-s)^2$ para todo $s \in \mathbb{Z}$ temos que $|a|^2 + |b|^2 = |c|^2$ e $(|a|, |b|, |c|) \in S$ com $|a|, |b| > 0$.

Seja $d = \text{mdc}(|a|, |b|)$. Assim, $d \geq 1$. Se $d = 1$, temos que $(|a|, |b|, |c|) \in S$ é uma solução reduzida e, nesse caso, (a, b, c) é uma das soluções $(\pm a, \pm b, \pm c)$ e a Proposição 2 é verdadeira tomando $k = 1$. Assim, podemos assumir $d \geq 2$.

Sejam a' e b' definidos por $a' = \frac{|a|}{d}$ e $b' = \frac{|b|}{d}$. Sabemos que a' e b' são inteiros positivos e que $\text{mdc}(a', b') = 1$.

Agora,

$$|a|^2 + |b|^2 = |c|^2 \Longrightarrow d^2((a')^2 + (b')^2) = |c|^2$$

e, portanto, $d^2 \mid |c|^2$.

Como $d^2 \mid |c|^2$, segue, pelo teorema fundamental da aritmética, que d também divide $|c|$. Seja c' o inteiro positivo definido por $c' = \frac{|c|}{d}$. Assim, $d^2((a')^2 + (b')^2) = d^2(c')^2$, $(a')^2 + (b')^2 = (c')^2$ e (a', b', c') é solução reduzida.

Portanto, (a, b, c) é uma das soluções $(\pm|a|, \pm|b|, \pm|c|)$ e como $|a| = da', |b| = db'$ e $|c| = dc'$ temos que existe $k = d$ tal que (a, b, c) é uma das soluções $(\pm da', \pm db', \pm dc')$ e isto demonstra a Proposição 2 com (a', b', c') solução reduzida.

■

Proposição 2

Seja $(a, b, c) \in S$ uma solução reduzida. Então

$$\text{mdc}(a, b) = \text{mdc}(a, c) = \text{mdc}(b, c) = 1\,.$$

Demonstração: Pela definição de solução reduzida, temos $a, b, c > 0$ e $\text{mdc}(a, b) = 1$.

Sejam $d_1 = \text{mdc}(a, c)$ e $d_2 = \text{mdc}(b, c)$. Vamos provar que $d_1 = d_2 = = 1$.

Seja $p_1 \geq 2$ um primo dividindo d_1. Assim, $p_1 \mid a$ e $p_1 \mid c$. Agora,

$$a^2 + b^2 = c^2 \Longrightarrow b^2 = c^2 - a^2 \, .$$

Como $p_1 \mid a$ e $p_1 \mid c$ temos que $p_1^2 \mid b^2$ e daí segue que $p_1 \mid b$ e, portanto, $p_1 \mid \text{mdc}(a, b) = 1$, uma contradição. Daí, segue que $d_1 = 1$. Analogamente temos que $d_2 = 1$.

■

Agora, vamos calcular todas as soluções reduzidas (a, b, c) de $x^2 + y^2 = = z^2$. A partir dessas soluções reduzidas, temos que o conjunto de todas as soluções inteiras de $x^2 + y^2 = z^2$ será a união de todas as soluções dos tipos

$$(\pm a, 0, \pm a), (0, \pm b, \pm b), \ \forall \, a, b \in \mathbb{Z} \, .$$

e $(\pm ka, \pm kb, \pm kc)$, com (a, b, c) solução reduzida e para todo $k \in \mathbb{Z}$.

Teorema 1
O conjunto de todas as soluções reduzidas (a, b, c) de $x^2 + y^2 = z^2$ pode ser descrito do seguinte modo:

$$\begin{cases} a = rs \\ b = \dfrac{s^2 - r^2}{2} \\ c = \dfrac{s^2 + r^2}{2} \end{cases} \qquad \text{ou} \qquad \begin{cases} a = \dfrac{s^2 - r^2}{2} \\ b = rs \\ c = \dfrac{s^2 + r^2}{2} \end{cases}$$

com $r < s$ inteiros positivos ímpares.

Demonstração: Sejam $a, b, c > 0$ inteiros e (a, b, c) uma solução reduzida $x^2 + y^2 = z^2$.

Inicialmente, vamos provar o seguinte:

Lema 3
c deve ser ímpar, e temos duas possibilidades?

(i) a ímpar, b par e c ímpar ou,

(ii) a par, b ímpar e c ímpar.

Demonstração: Primeiramente, vamos demonstrar que c deve ser ímpar.

Assume, por contradição, que $c = 2t$ é um inteiro par. Portanto, $c^2 = 4t^2 \equiv 0 \pmod 4$ é um par, múltiplo de 4.

Como a solução é reduzida temos, pela Proposição 3, que $\text{mdc}(a, c) = \text{mdc}(b, c) = 1$. Daí, segue que teríamos $a = 2k + 1$ e $b = 2s + 1$ ímpares. Agora $a^2 + b^2 = c^2$ nos diz que:

$$(2k + 1)^2 + (2s + 1)^2 = 4t^4 \equiv 0 \pmod 4 .$$

Mas,

$$4k^2 + 4k + 1 + 4s^2 + 4s + 1 \equiv 2 \pmod 4 .$$

Uma contradição. Portanto c é ímpar, em qualquer solução reduzida (a, b, c).

Como a soma de dois números inteiros ímpares (ou dois inteiros pares) é sempre par, temos que em uma solução reduzida (a, b, c) uma das duas vale:

(i) (a, b, c), com $\begin{cases} a = \text{ímpar} \\ b = \text{par} \\ c = \text{ímpar} \end{cases}$

ou

(ii) (a, b, c), com $\begin{cases} a = \text{par} \\ b = \text{ímpar} \\ c = \text{ímpar} \end{cases}$.

Como na situação (ii) apenas trocamos os papéis de a e b, vamos resolver calculando todas as soluções reduzidas (a, b, c), com a ímpar, b par e c ímpar. Depois trocamos os papéis de a e b.

A partir de agora, seja (a, b, c) uma solução reduzida de $x^2 + y^2 = z^2$, com a ímpar, b par e c ímpar.

Agora vamos provar um lema:

Lema 4

$$\text{mdc}(c - b, c + b) = 1 .$$

Demonstração: Assume $d = \text{mdc}(c - b, c + b)$ e suponhamos $d \geq 2$. Seja $p \geq 2$ um primo tal que $p \mid d$.

Agora, $(c - b)$ e $(c + b)$ ímpares nos diz que $p \geq 3$ é ímpar.

$$a^2 + b^2 = c^2 \Longrightarrow a^2 = c^2 - b^2 = (c - b)(c + b) .$$

Como $p \mid (c-b)$ e $p \mid (c+b)$ temos que $p \mid a^2$. Agora, p primo nos diz que $p \mid a$.

Agora,

$$\begin{cases} c - b = rp \\ c + b = sp \end{cases}$$

nos dá $2c = (r+s)p$. Como $p \geq 3$ é ímpar, segue que $p \mid c$.

Portanto, $p \mid a$ e $p \mid c$. Uma contradição pois, pela Proposição 3, temos $\text{mdc}(a, c) = 1$.

Portanto $d = \text{mdc}(c-b, c+b) = 1$. Daí segue que $a^2 = c^2 - b^2 = = (c-b)(c+b)$ com $\text{mdc}(c-b, c+b) = 1$.

Como a é ímpar, temos pelo teorema fundamental da aritmética que $(c-b)$ e $(c+b)$ são inteiros quadrados ímpares.

Digamos que existem r, s inteiros ímpares tais que $c-b = r^2$ e $c+b = s^2$ com $|s| > |r|$.

Portanto, temos que existem r, s inteiros ímpares tais que

$$b = \frac{s^2 - r^2}{2} > 0 \quad \text{e} \quad c = \frac{s^2 + r^2}{2} > 0 \quad (s^2 > r^2).$$

Como $a^2 = (c-b)(c+b) = r^2 s^2$ temos que $a = |r| \cdot |s| > 0$ com r, s ímpares.

Assim, as soluções reduzidas com a ímpar são as seguintes:

$$\begin{cases} a = |r| \cdot |s| \\ b = \dfrac{|s|^2 - |r|^2}{2} \\ c = \dfrac{|s|^2 + |r|^2}{2} \end{cases}$$

com $|r| > 0, |s| > 0$ inteiros ímpares com $|s| > |r|$.

As soluções reduzidas com a par e b ímpar são dadas por:

$$\begin{cases} a = \dfrac{|s|^2 - |r|^2}{2} \\ b = |r| \cdot |s| \\ c = \dfrac{|s|^2 + |r|^2}{2} \end{cases}$$

com $|r| > 0, |s| > 0$ inteiros ímpares com $|s| > |r|$ e isto demonstra o teorema 1.

■

Observação

As soluções reduzidas $(a, b, c) \in S$ da equação pitagórica $x^2 + y^2 = z^2$ poderiam ainda ser apresentadas de uma outra forma. Vamos ver como podemos apresentar essa nova forma das soluções reduzidas.

Como $0 < r < s$ são números ímpares na descrição paramétrica (inteira) apresentada no teorema 1, podemos então introduzir os inteiros m e n tais que:

$$(*) \quad \begin{cases} s + r = 2m \\ s - r = 2n \end{cases}$$

(observe que $s \pm r$ é par).

Daí, segue que $(s + r)(s - r) = 4mn$, ou seja,

$$\frac{s^2 - r^2}{2} = 2mn \tag{1}$$

Mas resolvendo o sistema $(*)$ temos $s = m+n$ e $r = m-n$, com $m > n$.

Daí segue que

$$\frac{s^2 + r^2}{2} = \frac{(m+n)^2 + (m-n)^2}{2} = m^2 + n^2 \tag{2}$$

e

$$rs = (m + n)(m - n) = m^2 - n^2 \tag{3}$$

Portanto, utilizando essa nova parametrização inteira, teremos a descrição de todas as soluções reduzidas $(a, b, c) \in S$ da equação pitagórica através de

$$\begin{cases} a = m^2 - n^2 \\ b = 2mn \\ c = m^2 + n^2 \end{cases}$$

com $m > n$ inteiros, onde m e n são distintas paridades, pois a e c são ímpares ou

$$\begin{cases} a = 2mn \\ b = m^2 - n^2 \\ c = m^2 + n^2 \end{cases}$$

com m e n inteiros de distintas paridades.

Atividades:

1. Seja $a = pq$, onde p e q são primos ímpares com $q > p$. Mostre que:

   (i) $a = pq$, $b = \frac{q^2 - p^2}{2}$ e $c = \frac{q^2 + p^2}{2}$ é uma solução inteira reduzida de $x^2 + y^2 = z^2$.

   (ii) Aplique a fórmula acima para os seguintes valores de p e q:

   a) $p = 3 < 5 = q$

   b) $p = 5 < 7 = q$

2. Sejam d e c inteiros positivos tais que $d^2 \mid c^2$. Mostre que $d \mid c$.

3. Mostre que: dado um número inteiro positivo $a \geq 3$ sempre existe inteiros positivos b e c tais que $a^2 + b^2 = c^2$.

Resumo

Nessa aula, apresentamos as equações diofantinas pitagóricas $x^2 + y^2 = z^2$ correlacionadas com o mais famoso desafio da Matemática: *"o último teorema de Fermat"*, e apresentamos uma forma de apresentar todas as soluções inteiras (a, b, c) dessa equação.

Aula 17 – Equações de congruências

Meta:

Apresentar as equações de congruências do tipo $ax \equiv b \pmod{n}$.

Objetivos

- Discutir a existência de soluções inteiras das equações de congruências $ax \equiv b \pmod{n}$;
- resolver, quando possível, equações de congruências;
- utilizar congruências para discutir a existência de certas equações diofantinas.

Introdução

Equações de congruências são equações onde o símbolo = de igualdade é substituído pelo símbolo $\equiv \pmod{n}$, de congruência módulo n.

Equações de congruências são muitas vezes utilizadas para discussão e determinação de soluções inteiras de equações diofantinas.

Estudaremos nessa aula as equações de congruências lineares do tipo $ax \equiv b \pmod{n}$.

Estamos interessados em descrever todos os inteiros $x \in \mathbb{Z}$, se existirem, que satisfaçam a equação de congruência $ax \equiv b \pmod{n}$. Assim, resolver uma equação de congruência é descrever todas as suas soluções inteiras.

As equações de congruências $ax \equiv b \pmod{n}$

Seja $n > 0$ um dado inteiro e sejam $a, b \in \mathbb{Z}$ com $a \neq 0$. Vamos discutir a existência de soluções inteiras $x \in \mathbb{Z}$ que satisfazem a congruência $ax \equiv b \pmod{n}$.

Observe que $x \in \mathbb{Z}$ satisfaz a congruência $ax \equiv b \pmod{n}$ se, e somente se, existir $t \in \mathbb{Z}$ tal que

$$(ax - b) = tn \Longleftrightarrow \exists\ t \in \mathbb{Z} \quad \text{tal que} \quad ax = b + tn\ .$$

Assim, a congruência pode ser vista como uma igualdade mais um múltiplo de n

Nas equações usuais (estudadas no ensino médio) do tipo $ax = b$, com $a, b \in \mathbb{Z}$ e $a \neq 0$, nem sempre possui soluções inteiras. De fato, a solução $x = \frac{b}{a}$ será inteira (e única) apenas se *"a for divisível por b"*. Se *"a não for divisível por b"* então não existe solução inteira da equação $ax = b$.

Quando trabalhamos com a congruência $\equiv \pmod{n}$, em vez da igualdade $=$, na equação $ax \equiv b \pmod{n}$ o contexto é diferente. Nessa última situação, pode não existir solução (inteira) de $ax \equiv b \pmod{n}$, como também pode existir infinitas soluções inteiras. De fato, vamos ver mais adiante que : *"se a congruência* $ax \equiv b \pmod{n}$ *possui uma solução* $x = x_0 \in \mathbb{Z}$ *então possui infinitas soluções do tipo* $x = x_0 + tn$ *para todo* $t \in \mathbb{Z}$*"* .

Antes de demonstrarmos algumas proposições vamos analisar dois exemplos.

Exemplo **11**

A equação de congruência $2x \equiv 1 \pmod{4}$ não possui soluções inteiras.

Solução:

De fato, suponhamos que $x_0 \in \mathbb{Z}$ é uma solução. Assim, $2x_0 \equiv 1 \pmod{4}$, o que nos diz que: existe $t \in \mathbb{Z}$ tal que $(2x_0 - 1) = 4t$. Mas isto é um absurdo pois, $(2x_0 - 1)$ é ímpar e é igual a $4t$ que é um inteiro par.

Exemplo **12**

A equação $2x \equiv 1 \pmod{7}$ possui infinitas soluções inteiras.

Solução:

Seja $S \subset \mathbb{Z}$ o conjunto de todas as soluções inteiras da equação de congruência $2x \equiv 1 \pmod{7}$. Vamos determinar S, mostrando que S é um conjunto infinito.

De fato, como $4 \times 2 = 8 \equiv 1 \pmod{7}$ temos que: resolver $2x \equiv 1 \pmod{7}$, multiplicando por 4, temos

$$8x \equiv x \equiv 4 \pmod{7},$$

e, assim,

$$S = \{x \in \mathbb{Z} \mid x \equiv 4 \pmod{7}\}.$$

Mas, $x \equiv 4 \pmod{7}$ se, e somente se, existe $t \in \mathbb{Z}$ tal que

$$x = 4 + 7t \iff x \in \mathbb{Z}.7 + 4.$$

Portanto, nesse caso, o conjunto S de todas as soluções inteiras de $2x \equiv 1 \pmod 7$ é dado por:

$$S = \mathbb{Z}.7 + 4 = \{x = 4 + 7k \mid k \in \mathbb{Z}\}\,.$$

Em particular, vemos que S é um conjunto com infinitas soluções inteiras.

Atividades:

1. Verifique que as seguintes equações de congruências não possuem soluções inteiras:

   (i) $4x \equiv 5 \pmod 6$

   (ii) $6x \equiv 8 \pmod 9$

2. Determine o conjunto $S \subset \mathbb{Z}$ de todas as soluções das seguintes congruências:

   (i) $3x \equiv 2 \pmod 5$

   (ii) $5x \equiv 4 \pmod 7$

   (iii) $4x + 7 \equiv 10 \pmod 9$

3. Você conseguiria descobrir por que razão as equações de congruências do ítem 1 não possuem soluções?

Observação

No exemplo 2 vimos que mesmo que a equação usual $2x = 1$ não possua solução inteira, a equação de congruência $2x \equiv 1 \pmod 7$ possui infinitas soluções dadas por

$$S = \mathbb{Z}.7 + 4 = \{4 + 7k \mid k \in \mathbb{Z}\}\,.$$

No contexto geral se uma equação de congruência $ax \equiv b \pmod n$ possui uma solução particular $x_0 \in \mathbb{Z}$ então $x = x_0 + kn$ para todo $k \in \mathbb{Z}$, também será solução da equação. Para isso, basta substituir:

$$ax = a(x_0 + kn) = ax_0 + akn\,.$$

Mas x_0, sendo solução particular, satisfaz a congruência $ax \equiv b \pmod n$ e portanto, existe $t \in \mathbb{Z}$ tal que $ax_0 = b + tn$.

Substituindo, teremos

$$ax = ax_0 + akn = (b + tn) + akn = b + (t + ak)n \Longrightarrow ax \equiv b \pmod{n}.$$

Agora seja dada a equação de congruência $ax \equiv b \pmod{n}$ com $a \neq 0$ e seja S o subconjunto de $\mathbb{Z}$ de todas as soluções inteiras dessa equação.

Definição 1
$S \subset \mathbb{Z}$ é chamado de o conjunto solução da equação $ax \equiv b \pmod{n}$.

O conjunto S pode ser $\emptyset$, como vimos no exemplo 1, ou pode ser infinito como vimos no exemplo 2.

É natural perguntarmos: Quando é que $S \neq \emptyset$? A seguinte proposição faz a primeira abordagem sobre essa questão.

Proposição 1
Seja $d = \text{mdc}(a, n)$. Então $S \neq \emptyset$ se, e somente se, $d \mid b$ (d é também divisor de b).

Demonstração: Seja $d = \text{mdc}(a, n)$.

($\Longrightarrow$) Assumir primeiramente que o conjunto solução S, da equação de congruência $ax \equiv b \pmod{n}$ seja não vazio.

Assim, existe $x_0 \in S$, uma solução inteira da equação $ax \equiv b \pmod{n}$. Portanto, existe $t \in \mathbb{Z}$ tal que $ax_0 = b + tn$. Como $d \mid a$ e $d \mid n$, segue que d deve também dividir $b = ax_0 + (-t)n$.

($\Longleftarrow$) Agora vamos assumir que $d \mid b$ e vamos exibir uma solução $x_0 \in S$ (portanto $S \neq \emptyset$).

Como $d \mid a, d \mid b$ e $d \mid n$, podemos definir os números inteiros $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ e $n' = \frac{n}{d}$.

Agora, pode-se verificar diretamente dividindo a, b e n por d, que:

$$ax \equiv b \pmod{n} \Longleftrightarrow a'x \equiv b' \pmod{n'}.$$

Assim, resolver a equação de congruência, módulo n, $ax \equiv b \pmod{n}$ é equivalente a resolver a equação de congruência módulo n', $a'x \equiv b' \pmod{n'}$ de equação de congruência reduzida.

Como resolver $ax \equiv b \pmod{n}$ é equivalente a resolver a equação reduzida $a'x \equiv b' \pmod{n'}$, vamos apresentar uma metodologia de exigir uma solução x_0 dessa última equação reduzida. Mais ainda, após apresentar uma

solução particular x_0 da equação reduzida, vamos provar que $S = \mathbb{Z}.n' + x_0$, isto é, o conjunto solução de $ax \equiv b \pmod{n}$ que é o mesmo de $a'x \equiv b' \pmod{n'}$ é infinito e expresso por $S = \mathbb{Z}.n' + x_0$.

Como $\text{mdc}(a', n') = 1$ sabemos que existem inteiros r e s tais que $ra' + sn' = 1$. Determinado o inteiro r, vamos provar que $x_0 = rb'$ é uma solução particular de $a'x \equiv b' \pmod{n'}$.

De fato, de $ra' + sn' = 1$, multiplicando por b' temos:

$$ra'b' + sn'b' = b' .$$

Assim, $a'(rb')b' + (-sb')n'$ e isto nos diz que $a'(x_0) \equiv b' \pmod{n'}$ onde $x_0 = rb'$ é solução particular de $a'x \equiv b' \pmod{n'}$.

Portanto, achando r, como acima, temos $x_0 = rb'$, solução particular, e portanto, existe $t \in \mathbb{Z}$ tal que $a'x_0 = b' + tn'$.

Agora, seja $x \in S$ uma solução geral de $a'x \equiv b' \pmod{n'}$. Assim, existe $k \in \mathbb{Z}$ tal que $a'x = b' + kn'$. Mas, $a'x_0 = b' + tn'$, daí segue que

$$a'(x - x_0) = (k - t)n' .$$

Portanto, n' é um divisor de $a'(x - x_0)$. Como $\text{mdc}(a', n') = 1$, segue, pelo teorema fundamental da aritmética, que n' deve ser divisor de $(x - x_0)$. Portanto, $(x - x_0)$ é múltiplo de n' e temos que $x \in \mathbb{Z}.n' + x_0$.

Como $\mathbb{Z}.n' + x_0 \subset S$, por verificação direta, vemos que o conjunto solução S é igual ao conjunto $\mathbb{Z}.n' + x_0$ como queríamos demonstrar.

■

Agora vamos ver um exemplo.

Exemplo **13**

Determinar o conjunto solução S da equação de congruência

$$12x \equiv 18 \pmod{21} .$$

Solução:

Primeiramente vamos testar se S é não vazio.

Temos que $d = \text{mdc}(a, n) = 3$. Como $d = 3$ divide $18 = b$, temos pela proposição anterior que $S \neq \emptyset$.

Agora vamos determinar S. A equação reduzida $a'x \equiv b' \pmod{n'}$ é a seguinte: $a' = \frac{12}{3} = 4$, $b' = \frac{18}{3} = 6$ e $n' = \frac{21}{3} = 7$. Então $4x \equiv 6 \pmod{7}$.

Como $\text{mdc}(a', n') = \text{mdc}(4, 7) = 1$ então existem $r = 2$ e $s = 1$ tal que

$$ra' + sb' = 2 \times +(-1) \times 7 = 1\,.$$

Pela Proposição 1, $x_0 = rb' = 2 \times 6 = 12$ é uma solução particular de congruência $12x \equiv 18 \pmod{21}$ ou, equivalentemente, de $4x \equiv 6 \pmod{7}$. Como $12 \equiv 5 \pmod{7}$, podemos escolher $x_0 = 5$ como solução particular da nossa equação de congruência módulo $n' = 7$.

Pela Proposição 1, o conjunto solução S pode ser descrito por:

$$S = \mathbb{Z}.n' + x_0 = \mathbb{Z}.7 + 5 = \{x = 5 + 7k \mid k \in \mathbb{Z}\}\,.$$

Portanto, a solução da equação de congruência módulo 21 está dada, em função da congruência módulo 7: $S = \mathbb{Z}.7 + 5$.

E se quiséssemos dar uma outra resposta usando congruências módulo 21, como poderíamos descrever o conjunto S?

As soluções x dadas acima são da forma $x = 5+7t$. Como $21 = 7 \times d = = 7 \times 3$, podemos demonstrar $t \in \mathbb{Z}$ em $d = 3$ categorias: $t = 3k$ (múltiplo de $d = 3$); $t = 3k + 1$ ou $t = 3k + 2$. Substituindo em $x = 5 + 7t$ obtemos as respostas módulo 21:

$$x = 5 + 7t = \begin{cases} 5 + 21k & \text{se} \quad t = 3k \\ 5 + 7(3k + 1) = 12 + 21k & \text{se} \quad t = 3k + 1 \\ 5 + 7(3k + 2) = 19 + 21k & \text{se} \quad t = 3k + 2 \end{cases}$$

Portanto, podemos dar uma descrição, alternativa, para o conjunto solução S, em função da congruência original módulo 21.

$$S = \mathbb{Z}.21 + 5 \cup \mathbb{Z}.21 + 12 \cup \mathbb{Z}.21 + 19\,.$$

Enquanto, que descrevendo, na forma reduzida, temos uma única classe solução módulo 5, $S = \mathbb{Z}.7 + 5$, temos descrevendo o mesmo conjunto S três distintas classes soluções módulo 21, com representantes $x_0 = 5, x_1 = 12$ e $x_2 = 19$.

Observe que

$$\mathbb{Z}.7 + 5 = \mathbb{Z}.21 + 5 \cup \mathbb{Z}.21 + 12 \cup \mathbb{Z}.21 + 19$$

(união disjunta de três classes).

Inversão modular e solução da equação $ax \equiv b \pmod{n}$ em $\mathbb{Z}_n$

Seja $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}, +, \cdot$ o Anel comutativo com unidade $\overline{1}$ dos inteiros módulo n.

A equação modular $ax \equiv b \pmod{n}$ em $\mathbb{Z}$, pode ser interpretada como uma equação (usual) em $\mathbb{Z}_n$. Para isso, basta observar que:

$$\underbrace{ax \equiv b \pmod{n}}_{\text{em } \mathbb{Z}} \Longleftrightarrow \underbrace{\overline{a} \cdot \overline{x} = \overline{b}}_{\text{em } \mathbb{Z}_n} .$$

Assim, resolver $ax \equiv b \pmod{n}$ é equivalente a resolver (achar $\overline{x}$) a equação $\overline{a} \cdot \overline{x} = \overline{b}$ em $\mathbb{Z}_n$.

Na Aula 12, vimos pela Proposição 2 que $\overline{a} \neq \overline{0}$ possui inverso multiplicativo, $\overline{r} \neq \overline{0}$, em $\mathbb{Z}_n$, se, e somente se, $\text{mdc}(a, n) = 1$.

Portanto, se $ax \equiv b \pmod{n}$ for uma equação de congruência reduzida, isto é, $\text{mdc}(a, n) = 1$, temos que $\overline{a} \neq \overline{0}$ possui inverso multiplicativo e $\overline{r} \neq \overline{0}$ em $\mathbb{Z}_n$. Assim, $\overline{r} \cdot \overline{a} = \overline{1}$.

Agora, para resolver $\overline{a} \cdot \overline{x} = \overline{b}$, basta multiplicar por $\overline{r} = (\overline{a})^{-1}$ ambos os membros dessa igualdade. De fato,

$$\overline{x} = \overline{r}(\overline{a} \cdot \overline{x}) = \overline{r} \cdot \overline{b} = \overline{rb}$$

e $\overline{x} = \overline{rb}$ é a única solução em $\mathbb{Z}_n$. Voltando para trabalhar com $\equiv \pmod{n}$, em $\mathbb{Z}_n$, isto significa que $x_0 = rb$ é uma solução particular da congruência $ax \equiv b \pmod{n}$ e o conjunto solução $S \subset \mathbb{Z}$ dessa equação reduzida é dado por

$$S = \overline{x} = \overline{x_0} = \mathbb{Z}.n + x_0 ,$$

como já tínhamos visto anteriormente na resolução de equações de congruências reduzidas.

Observação

Essa metodologia de resolver a equação de congruência reduzida através de $\overline{a} \cdot \overline{x} = \overline{b}$ é equivalente aquela desenvolvida na demonstração da Proposição 1. As dificuldades que aparecem em ambas são essencialmente de mesmo grau. Na Proposição 1, se $\text{mdc}(a, n) = 1$, temos que achar inteiros $r, s \in \mathbb{Z}$ tais que $ar + sn = 1$ e $x_0 = rb$ é uma solução particular com $S = \mathbb{Z}.n + x_0$. Olhando como uma equação (usual) $\overline{a} \cdot \overline{x} = \overline{b}$, em $\mathbb{Z}_n$, temos que achar $\overline{r} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{r} = \overline{1}$ e aí, $x_0 = rb \in \mathbb{Z}$ é uma solução particular sendo $\overline{x} = \overline{x_0} = \mathbb{Z}.n + x_0$ a única solução em $\mathbb{Z}_n$.

Exemplo **14**

Resolver a equação de congruência $243x \equiv 5 \pmod{725}$.

Solução:

Temos que $a = 243, b = 5$ e $n = 725$ com $\text{mdc}(a, n) = \text{mdc}(243, 725) = 1$. Pode-se calcular, usando a metodologia usada no exemplo 16 da Aula 12 utilizando o algoritmo da divisão de Euclides.

Os valores $r = 182$ e $s = -61$ tais que

$$ra + sn = 182 \times 243 + (-61) \times 725 = 1\,.$$

Portanto, $x_0 = rb = 182 \times 5 = 910$ é uma solução particular módulo 725.

Mas, módulo 725, podemos escolher $x_0 = 910 - 725 = 185$ é uma solução particular da congruência $243x \equiv 5 \pmod{725}$ e a solução geral dessa equação de congruência reduzida é

$$S = \mathbb{Z}.725 + 185 = \{x = 185 + 725k \mid k \in \mathbb{Z}\}\,.$$

Observe que $(\overline{234})^{-1} = \overline{182}$, em $\mathbb{Z}_{725}$ e não seria mais fácil seguir o caminho de resolver $\overline{a} \cdot \overline{x} = \overline{b}$ com $a = 243, b = 5$, módulo 725.

Atividade:

1. Calcule os inversos multiplicativos de $\overline{a}$ nos seguintes casos:

   (i) $\overline{a} = \overline{3}$, $\mathbb{Z}_n = \mathbb{Z}_{10}$

   (ii) $\overline{a} = \overline{4}$, $\mathbb{Z}_n = \mathbb{Z}_{21}$

   (iii) $\overline{a} = \overline{6}$, $\mathbb{Z}_n = \mathbb{Z}_{35}$

2. Use o exemplo 1 acima para resolver as seguintes equações de congruências reduzidas?

   (i) $3x \equiv 7 \pmod{10}$

   (ii) $4x \equiv 15 \pmod{21}$

   (iii) $6x - 2 \equiv 11 \pmod{35}$

3. Sejam a e n os seguintes pares de números dados. Para cada um deles use o algoritmo de Euclides, utilizado no exercício 16 da Aula 12, para determinar inteiros r e s tal que $ar + ns = 1$.

   (i) $a = 26, n = 14$

(ii) $a = 243, n = 725$

4. Seja $10x \equiv 15 \pmod{20}$ a equação de congruência dada.

   (i) Determine a solução módulo $n' = \frac{n}{d} = 4$ da equação reduzida $2x \equiv 3 \pmod{4}$.

   (ii) Escreva as soluções dessa equação módulo 21.

Resumo

Nessa aula apresentamos metodologia para solucionar as equações de congruências do tipo $ax \equiv b \pmod{n}$, em $\mathbb{Z}$. Se $d = \text{mdc}(a, n)$ divide b, o conjunto solução S é não vazio e através da equação de congruência reduzida $a'x \equiv b' \pmod{n}'$ encontramos as soluções módulo n' (única) e em seguida expressamos essas soluções módulo n (d soluções módulo n). Apresentamos ainda a forma alternativa de se considerar a equação de congruência $ax \equiv b \pmod{n}$, em $\mathbb{Z}$, como uma equação (usual) $\overline{a} \cdot \overline{x} = \overline{b}$, em $\mathbb{Z}_n$ onde pretendemos determinar $\overline{x}$.

Aula 18 – Sistemas lineares de congruências: o teorema chinês do resto

Meta:

Apresentar sistemas lineares de congruências e o teorema chinês do resto.

Objetivos

- Resolver sistemas lineares de congruências simples do tipo $\begin{cases} x \equiv a \pmod{m} \\ x \equiv a \pmod{n} \end{cases}$;
- resolver sistemas lineares do tipo $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$,usando uma primeira versão do teorema chinês do resto;
- resolver sistemas lineares, com n equações e uma incógnita, utilizando o teorema chinês do resto (versão geral).

Introdução

Sistemas de congruências é um conjunto de equações de congruências onde se procura soluções inteiras que satisfaçam simultaneamente todas as equações de congruências do sistema.

Estudaremos nessa aula sistemas lineares de congruência em uma variável x, do tipo

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \quad \vdots \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

O instrumento principal utilizado na resolução desses sistemas é o famoso teorema chinês do resto, assim chamado por ter sido utilizado pelos chineses desde o início da era cristã e aparecendo no livro - Manual de Aritmética - do mestre Sun, escrito por volta do sec IV, da nossa era. Esse teorema tem várias aplicações computacionais aritméticas com grandes números, utilizando-se várias congruências escolhidas dentro das condições de aplicabilidade do teorema.

Os sistemas lineares

Os sistemas lineares mais simples de congruência são do tipo

$$(*) \quad \begin{cases} x \equiv b \pmod{m} \\ x \equiv b \pmod{n} \end{cases} .$$

Como resolver esse sistema descrevendo todas as suas soluções inteiras?

Solução:

De $x \equiv b \pmod{m}$ segue que $(x-b) \in \mathbb{Z}.m$ e de $x \equiv b \pmod{n}$ segue que $(x-b) \in \mathbb{Z}.n$. Assim, $(x-b) \in \mathbb{Z}.m \cap \mathbb{Z}.n$.

Pelo teorema 6 da Aula 3, temos que:

$$(x-b) \in \mathbb{Z}.m \cap \mathbb{Z}.n = \mathbb{Z}.M, \quad M = \text{mmc}(m,n)\,.$$

Portanto, $x \equiv b \pmod{M}$ com $M = \text{mmc}(m,n)$ nos dão todas as infinitas soluções do sistema $(*)$:

$$S = \mathbb{Z}.M + b\,.$$

Observação

Se $\text{mdc}(m,n) = 1$, temos que, nesse caso, $M = mn$ e as soluções inteiras do sistema $(*)$ são dadas por:

$$x \equiv b \pmod{mn}\,.$$

A dificuldade é bem maior se considerarmos o sistema de congruência do tipo

$$(**) \quad \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

(se $a = b$ caímos no caso anterior cuja solução já foi explicitada).

Como resolver esse sistema $(**)$? Antes de fazermos uma consideração geral sobre as soluções do sistema $(**)$, vamos dar um exemplo.

Exemplo **15**

Resolva o sistema de congruência

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{8} \end{cases}$$

Solução:

Se $x \equiv 2 \pmod 5$ então existe $y \in \mathbb{Z}$ tal que

$$x = 2 + 5y \tag{4}$$

Substituindo na segunda congruência do sistema temos que $x = 2 + 5y \equiv 4 \pmod 8$ implica

$$5y \equiv 2 \pmod 8 . \tag{5}$$

Portanto os valores de x são da forma $x = 2 + 5y$ onde y é solução da congruência (5). Como $\text{mdc}(5, 8) = 1$, essa equação (5) é uma equação de congruência reduzida e, portanto, teremos soluções $y = y_0 + 8k$ onde $y_0 = rb = r2 = -6$, onde $r = -3, s = 2$ e $-3 \times 5 + 2 \times 8 = 1$. Logo as soluções y são $y \equiv -6 \pmod 8$, ou seja, $y \equiv 2 \pmod 8$ o que implica $y = 2 + 8k$ com $k \in \mathbb{Z}$.

As soluções x do sistema serão:

$$x = 2 + 5y = 2 + 5(2 + 8k) = 12 + 40k ,$$

isto é,

$$x \equiv 12 \pmod{40} .$$

Assim, $S = \mathbb{Z}.40 + 12 \subset \mathbb{Z}$ é o conjunto de todas as soluções inteiras do sistema.

Observação

Observe que foi importante, para a solução de congruência, em y, que $\text{mdc}(m, n) = 1$ e daí então construímos a solução de congruência módulo $mn = 40$, para o sistema dado.

Agora vamos mostrar que existe solução do sistema $\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$ quando $\text{mdc}(m, n) = 1$.

Teorema 1

Sejam m e n inteiros positivos tal que $\text{mdc}(m, n) = 1$. Então

(i) o sistema de congruência $\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$ possui solução x_0 com $0 \leq x_0 < mn$

(ii) as soluções do sistema são dadas por $x \equiv x_0 \pmod{mn}$.

Observação

A solução x_0 com $0 \leq x_0 < mn$ é a menor solução não negativa do sistema.

Demonstração: Se $x \equiv a \pmod{m}$ então existe $y \in \mathbb{Z}$ tal que

$$x = a + my \tag{6}$$

Substituindo (6) na segunda equação do sistema de congruência temos $x = a + my \equiv b \pmod{n}$. Daí,

$$my \equiv (b - a) \pmod{n} \tag{7}$$

Como $\text{mdc}(m, n) = 1$ essa equação de congruência reduzida possui solução y_0 e as soluções de (7) são dadas por:

$$y = y_0 + nk \tag{8}$$

com $k \in \mathbb{Z}$. Substituindo (8) em (6) temos:

$$x = a + my = a + m(y_0 + nk) = (a + my_0) + (mn)k\,,$$

com $k \in \mathbb{Z}$ o que implica

$$x \equiv (a + my_0) \pmod{mn}\,.$$

A solução particular $a + my_0$ pode ser escolhida módulo mn, como um valor x_0, com $0 \leq x_0 < mn$, e teremos $x \equiv x_0 \pmod{mn}$, como todas as soluções do sistema de congruência.

■

Exemplo **16**

Vamos resolver agora um sistema linear de congruência com três equações. "Resolva o seguinte":

$$(*) \quad \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{14} \end{cases}$$

Solução:

A nossa estratégia poderia ser:

Primeiramente vamos resolver o sistema com as duas primeiras equações.

$$(**) \quad \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \end{cases}$$

Então temos:

$$x \equiv 1 \pmod{3} \Longrightarrow x = 1 + 3y, y \in \mathbb{Z}$$

e

$$x = 1 + 3y \equiv 2 \pmod 5 \Longrightarrow 3y \equiv 1 \pmod 5 .$$

Daí segue as soluções $y \equiv 2 \pmod 5$ (verifique isto, como na atividade proposta).

Assim, $y = 2 + 5k$, com $k \in \mathbb{Z}$ daí,

$$x = 1 + 3y = 1 + 3(2 + 5k) = 7 + 15k \Longrightarrow x \equiv 7 \pmod{15}$$

nos dá todas as soluções do sistema $(**)$.

Para resolver o sistema $(*)$, basta agora resolver o sistema

$$\begin{cases} x \equiv 7 \pmod{15} \\ x \equiv 3 \pmod{14} \end{cases}$$

Então

$$x \equiv 7 \pmod{15} \Longrightarrow x = 7 + 15y ,$$

com $y \in \mathbb{Z}$. Substituindo em $x \equiv 3 \pmod{14}$ temos:

$$x = 7 + 15y \equiv 3 \pmod{14} \Longrightarrow 15y \equiv -4 \pmod{14} \equiv 10 \pmod{14} ,$$

isto é, $15y \equiv 10 \pmod{14}$.

Como $1 \times 15 + (-1) \times 14 = 1$, temos $r = 1$ e $s = -1$ e, como solução para esta última equação de congruência reduzida:

$$y_0 = 1 \times 10 = 10 \quad \text{e} \quad y \equiv 10 \pmod{14}$$

o que implica $y = 10 + 14k$. Substituindo em $x = 7 + 15y$ temos:

$$x = 7 + 15y = 7 + 15(10 + 14k) = 157 + (14 \times 15)k$$

Assim, $x_0 = 157$ é o menor inteiro não negativo que satisfaz simultaneamente as três equações de congruência do sistema e o conjunto de todas as soluções do sistema é dado por

$$x \equiv x_0 \pmod{3 \times 5 \times 14} \equiv 157 \pmod{210} .$$

Agora vamos apresentar a versão mais geral do teorema chinês do resto, para um sistema com n equações de congruências.

Teorema 2 (Teorema chinês do resto)
Sejam $m_1, m_2, \cdots, m_n$ inteiros positivos tal que $\text{mdc}(m_i, m_j) = 1$ para todo $i \neq j$. Então

(i) o sistema de congruência

$$(*) \quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \quad \vdots \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

possui uma solução x_0, com $0 \leq x_0 < (m_1.m_2.\ldots.m_n)$

(ii) as soluções do sistema são dadas por

$$x \equiv x_0 \pmod{m_1.m_2.\ldots.m_n}\,.$$

Demonstração: Vamos usar indução sobre n. Se $n = 1$ o sistema possui uma única equação e portanto, a equação já nos dá as soluções do sistema.

Agora, vamos assumir $n \geq 2$ e vamos supor que o teorema é válido para qualquer sistema com as hipóteses relativamente primos dos $m_i's$, contando com $(n-1)$ equações. A partir daí, provaremos o teorema para o nosso sistema com n equações de congruências.

Portanto, estamos assumindo que o sistema

$$(**) \quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \quad \vdots \quad \vdots \\ x \equiv a_{n-1} \pmod{m_{n-1}} \end{cases}$$

com $\text{mdc}(m_i, m_j) = 1$ se $i \neq j$, possui uma solução a e que todas as soluções de $(**)$ são da forma $x \equiv a \pmod{t}$, onde $t = m_1 m_2 \cdots m_{n-1}$.

Agora, escrevemos um sistema $(***)$ com duas equações, cujas soluções são as mesmas do sistema original $(*)$:

$$(***) \quad \begin{cases} x \equiv a \pmod{t} \\ x \equiv a_n \pmod{m_n} \end{cases}$$

com $\text{mdc}(t, m_n) = 1$.

Como $\text{mdc}(t, m_n) = 1$, temos pelo Teorema 1 (Teorema chinês dos restos para duas equações), que $(***)$ admite uma solução x_0, com $0 \leq x_0 < tm_n = m_1 m_2 \cdots m_n$ e todas as soluções x desse sistema é dada por

$$x \equiv x_0 \pmod{tm_n} \equiv x_0 \pmod{m}$$

onde $m = tm_n = m_1 m_2 \cdots m_n$.

Como as soluções de $(*)$ e $(***)$ são as mesmas, o teorema está demonstrado.

Atividades:

1. Determine todas as soluções do sistema linear de congruência

$$\begin{cases} x \equiv 1 \pmod{13} \\ x \equiv 4 \pmod{15} \\ x \equiv 8 \pmod{19} \end{cases}$$

   Determine ainda, a menor solução x_0 (não negativa) disse sistema.

2. (i) Observe que o sistema de congruência

$$\begin{cases} x \equiv 5 \pmod{12} \\ x \equiv 21 \pmod{8} \end{cases}$$

   possui soluções embora $\text{mdc}(12, 8) = 4 \neq 1$.

   (ii) Calcule essas soluções, e entenda criticamente porque alguns sistemas sem a hipótese do mdc $= 1$ ainda podem ter soluções.

3. Verifique que a menor solução positiva do sistema

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

   é 79.

4. Calcule o resto da divisão de $N = 2^{6754}$ por 105 (relacione com o exercício 3).

Uma aplicação: computação aritmética com grandes números

Vamos supor que a capacidade máxima de nossa máquina computacional é 100 e que gostaríamos dar condições para que ele calculasse o produto X dos números $N_1 = 3456$ e $N_2 = 7982$.

Vamos escolher os seguintes números, dois a dois relativamente primos, $m_1 = 89, m_2 = 95, m_3 = 97, m_4 = 98, m_5 = 99$ para, através de congruências módulo m_k, $(k = 1, 2, 3, 4, 5)$ operarmos dentro da capacidade da nossa máquina que é $C = 100$.

Calculo restos de divisão

$$\begin{array}{l|l} 3456 \equiv 74 \pmod{89} & 7982 \equiv 61 \pmod{89} \\ 3456 \equiv 36 \pmod{95} & 7982 \equiv 2 \pmod{95} \\ 3456 \equiv 61 \pmod{97} & 7982 \equiv 28 \pmod{97} \\ 3456 \equiv 26 \pmod{98} & 7982 \equiv 44 \pmod{98} \\ 3456 \equiv 90 \pmod{99} & 7982 \equiv 62 \pmod{99} \end{array}$$

Multiplicando essas congruências teremos que $X = 3456 \times 7982$ satisfaz as seguintes congruências:

$$(*) \quad \begin{cases} x \equiv 74 \times 61 \equiv 64 \pmod{89} \\ x \equiv 36 \times 2 \equiv 72 \pmod{95} \\ x \equiv 61 \times 28 \equiv 59 \pmod{97} \\ x \equiv 26 \times 44 \equiv 66 \pmod{98} \\ x \equiv 90 \times 62 \equiv 36 \pmod{99} \end{cases}$$

Usando o teorema do resto chinês, pode-se resolver o sistema $(*)$ cuja solução geral

$$X \equiv X_0 \pmod{m},$$

com $m = 89 \times 95 \times 97 \times 98 \times 99$ e

$$X_0 = 27.585.792,$$

com $0 \leq X_0 < m$.

O valor de m é $m = 7.956.949.770$, e X_0 é a menor solução positiva $0 < X_0 < m$. Como $0 < (3456) \times (7982) < 10^8 < m$ temos que

$$X_0 = 3456 \times 7982 = 27.585.792.$$

Atividades:

1. Resolva, usando o teorema do resto chinês, o seguinte sistema:

$$\begin{cases} x \equiv 10 \pmod{13} \\ x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod{6} \\ x \equiv 1 \pmod{5} \end{cases}$$

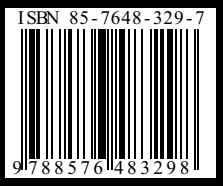
2. Mostre que a menor solução inteira de X no exemplo 1 é também solução do seguinte problema:

"Um grupo de 13 ladrões assaltaram um cofre com x moedas de ouro. Quando eles fizeram a divisão, equitativamente de todas as moedas entre eles, sobraram 10 moedas. Isso deu motivo a uma briga entre eles e dois dos ladrões morreram. Eles tornaram a dividir, equitativamente entre eles, todas as moedas e sobraram 5 moedas de ouro. Brigaram outra vez e cinco ladrões morreram. Dividiram, equitativamente todas as moedas e sobraram 3 moedas. Mais uma última briga e morreu mais um ladrão. Repetiram a divisão de todas as x moedas, equitativamente entre eles, e sobrou apenas uma moeda. Sabendo-se que $x < m = 5 \times 6 \times 11 \times 13$, calcule x".

Resumo

Nesta aula apresentamos métodos que nos permite resolver alguns sistemas de congruências lineares, através do famoso teorema do resto chinês. Esse teorema, conhecido há mais de dois mil anos, nos ajuda a fazer operações com grandes números, através de adequadas congruências que se ajustam dentro das hipóteses do teorema chinês dos restos.

ISBN 85-7648-329-7



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

Ministério
da Educação

BRASIL
UM PAÍS DE TODOS
GOVERNO FEDERAL