Universidade Federal de Sergipe
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT

Congruências modulares: construindo um conceito e as suas aplicações no ensino médio

Por

José Hélio Barbosa Junior

Mestrado Profissional em Matemática - São Cristóvão - SE

Orientador: Prof. Dr. Kalasas Vasconcelos de Araújo

Abril de 2013

Universidade Federal de Sergipe
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT

José Hélio Barbosa Junior

Congruências modulares: construindo um conceito e as suas aplicações no ensino médio

Trabalho apresentado ao Departamento de Matemática da Universidade Federal de Sergipe como requisito final para a obtenção do título de Mestre em Matemática pelo PROFMAT

Orientador: Prof.Dr. Kalasas Vasconcelos de Araújo

São Cristóvão - Sergipe
Abril de 2013

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Barbosa Junior, José Hélio
B238c Congruências modulares: construindo um conceito e as suas aplicações no ensino médio / José Hélio Barbosa Junior; orientador Kalasas Vasconcelos de Araújo. – São Cristóvão, 2013.
51 f.: il.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional – Profmat) – Universidade Federal de Sergipe, 2013.

1. Matemática – Estudo e ensino. 2. Ensino médio. 3. Números naturais. 4. Aritmética. 5. Divisão Euclidiana. 6. Congruência modular. I. Araújo, Kalasas Vasconcelos de, orient. II. Título

CDU 512:37

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe ,como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Congruência modular: construindo um conceito e suas aplicações no ensino médio

por

José Hélio Barbosa Júnior

Aprovada pela Banca Examinadora:

Prof. Dr. Kalasas Vasconcelos de Araújo - UFS
Orientador

Prof. Dr. Rodrigo Gondim Neves - UFRPE
Primeiro Examinador

Prof. Dr. Zaqueu Alves Ramos - UFS
Segundo Examinador

São Cristóvão, 11 de abril de 2013

Cidade Universitária "Prof. José Aloísio de Campos" – Av. Marechal Rondon, s/no - Jardim Rosa Elze – Campus de São Critóvão. Tel. (00 55 79) 2105-6986 – Fax (0 xx 55 79) 2105-6566
CEP: 49100-000 - São Cristóvão – Sergipe - Brasil – E-mail: promat_ufs@yahoo.com.br

Sumário

Agradecimentos **iii**

Resumo **iv**

Abstract **v**

Introdução **vi**

1 Divisibilidade **1**

1.1 Propriedades da divisibilidade. 1

1.2 Números naturais primos e números naturais compostos. 2

1.3 O Crivo de Eratóstenes. 3

1.4 Teorema Fundamental da Aritmética. 4

1.5 Estendendo a divisibilidade ao conjunto dos números interios 5

2 Divisão Euclidiana **7**

2.1 Algoritmo da Divisão Euclidiana 7

3 O Mínimo Múltiplo Comum e O Máximo Divisor Comum entre dois números inteiros **10**

3.1 Mínimo Múltiplo Comum (m.m.c) 10

3.2 Máximo Divisor Comum(m.d.c) 13

3.2.1 Relação de Bézout 17

3.3 Equações Diofantinas Lineares 18

4 Fazendo contas com restos **21**

4.1 O resto da soma é a soma dos restos? 22

4.2 O resto do produto é o produto dos restos? 24

5 Congruência Modular **26**

5.1 Propriedades da congruência modular. 28

5.2 Propriedades operatórias da congruência modular. 28

5.3 Congruências Lineares. 30

6 Aplicações das congruências modulares. **33**
6.1 Teorema Chinês dos Restos (TCR) 34
6.2 Partilha de senhas 37
6.2.1 Como funciona a Partilha de senhas? 37

Referências Bibliográficas **41**

Agradecimentos

Agradeço a Deus por ter me concedido a oportunidade de concretizar mais um sonho.

À minha esposa, Aline Gusmão, pelo apoio e dedicação nesses dois anos em que estive me dedicando a esse projeto.

Às minhas filhas, Larissa e Heloísa, que sempre serão motivo de inspiração nesta minha caminhada.

Aos meus pais, José Hélio e Maria Aldinete, que sempre foram compreensivos com a minha ausência em alguns momentos.

Às minhas irmãs, Jamilly e Julianna, que sempre vibraram muito com as minhas conquistas.

Aos meus tios e tias, sempre preocupoados com a minha formação, em especial ao meu tio Rozevaldo, "Tio zé", que sempre me motivou a uma formação continuada, reconhecendo sempre o meu potencial.

Aos familiares, Hebert Rocha, Camila Gusmão, Deni Gusmão, Erivaldo Lima.

A todos os meus amigos. Não quero aqui citar nomes, pois faltariam linhas para falar de todos eles.

Aos meus colegas de trabalho das escolas: Liceu de Estudos Integrados, Dinâmico e Presidente Costa e Silva.

Aos meus colegas de mestrado, hoje considerados amigos: Anselmo Vasconcelos, Davi Dantas, Wellington Luz, Sérgio Ricardo. Só Deus sabe as noites de estudos que enfrentamos.

A todos os meus professores do PROFMAT, em especial ao meu orientador Kalasas Vasconcelos, que sempre se mostrou uma pessoa motivadora, não só na preparação desse TCC, mas também nas disciplinas que lecionou durante o mestrado; ao amigo e professor Almir Rogério e ao coordenador do programa PROFMAT em Sergipe, Fábio dos Santos.

Abril de 2013

Resumo

A presente dissertação tem como objetivo apresentar aos alunos do ensino básico uma poderosa ferramenta na resolução de problemas aritméticos, que é a **Congruência modular**.

Para tanto, iniciamos nosso estudo abordando conceitos básicos da teoria dos números: divisibilidade, divisão euclidiana, máximo divisor comum, mínimo múltiplo comum, analise de restos, culminando com a congruência modular e algumas de suas aplicações: Teorema Chinês dos restos e Partilha de senhas.

Palavras Chaves: Divisibilidade, divisor, restos, aritmética modular, partilha de senhas.

Abstract

The purpose of this dissertation is to present to the students of basic education a powerful tool in the resolution of Arithmetic such as Modular Congruence.

We initiate our study by approaching the main basics concepts of Number Theory: Divisibility, Eucledian Division, Greatest Common Divisor, Remainder modular arytmetics, culminating with Modular Congruence and its applications: Chinese Remainder Theorem and Intergers.
Keywords: Divisibilidade, Divisor, Remainders, Modular Arytmetics, Intergers.

Introdução

Desde a antiguidade, os gregos se dedicavam à Matemática e, dada a atitude filosófica e especulativa que os mesmos tinham face à vida, deram a esta ciência um caráter científico.

Pitágoras de Samos (580? – 500? a.C) e a sua escola, chamada escola Pitagórica, difundiram a Matemática pela Grécia e suas colônias. Os mesmos atribuíam aos números um poder místico, adotando a *Aritmética* como fundamento de seu sistema filosófico. O filosófo Platão (429 – 348 a.C), apesar de não ser matemático, tinha preferência pelos aspectos mais teóricos e conceituais, e fazia uma clara diferenciação entre a ciência dos números, que ele chamava *Aritmética*, e a arte de calcular, que ele chamava *Logística*, a qual desprezava por ser "infantil e vulgar".

Tratada de maneira tão significativa pelos Gregos, a Matemática, em especial a *Aritmética*, ganha ainda mais notoriedade, com o surgimento de um importante tratado "Os Elementos de Euclides". Foi Euclides que estabeleceu um padrão de apresentação e rigor na Matemática, que passou a ser seguido nos milênios que se sucederam. A obra de Euclides é composta por treze livros, sendo que três desses, os Livros VII, VIII e IX, eram dedicados à *Aritmética*. Neles, encontram-se temas relacionados à: Divisibilidade, Divisão com Resto, Máximo Divisor Comum, Números Primos, Progressões Geométricas, dentre outros.

Após Euclides, a *Aritmética* passou por um longo período de estagnação, cerca de 500 anos, até ressurgir com os trabalhos de Diofanto de Alexandria, que viveu por volta de 250 d.C. Diofanto escreveu uma obra em treze volumes, chamada **Aritmética**.

Entre os séculos XVI e XVII, vários matemáticos se dedicaram à *Aritmética*, destacando-se Pierre de Fermat e Leonhard Euler, sendo fundamentais no desenvolvimento da Teoria dos Números.

Entre os séculos XVIII e XIX, surge um dos maiores matemáticos de todos os tempos, o Alemão Carl Frederich Gauss (1777 – 1855), que de forma precoce, aos 17 anos de idade, decide incursionar na Aritmética, com o proposito de esclarecer, completar e desenvolver o que os seus predecessores haviam realizado e, aos 21 anos, Gauss produz uma das obras primas de toda a matemática, o livro *Disquisitiones Arithmeticae*, trazendo nesta obra a noção de congruência modular e aritmética dos restos, sendo de grande aplicação no cotidiano. A exemplo, podemos citar os sistemas de criptografia e segurança de dados.

Diante de notória importância da *Aritmética* ao longo da história e, observando a

carência dos alunos do ensino básico bem como a dos livros didáticos nessa importante área do conhecimento, o presente trabalho tem como objetivo, de forma gradativa e numa linguagem acessível ao aluno, revisar os vários tópicos relacionados à teoria dos números, a fim de construir o conceito de congruência modular, e as suas aplicações, e será estruturado da seguinte forma:

No capítulo 1, faz-se uma revisão do conceito de divisibilidade, bem como as suas propriedades. Aqui, o aluno terá a oportunidade de rever importantes conceitos como: números naturais primos, o importante teorema fundamental da aritmética, e estender a ideia de divisibilidade ao conjunto dos números inteiros, com exemplos de aplicação diferenciados daqueles encontrados nos livros didáticos.

No capítulo 2, destaca-se a divisão entre números inteiros com resto, a chamada divisão euclidiana, que fundamentará teoricamente os capítulos subsequentes.

No capítulo 3, utilizando as deficinições de multiplicidade e divisibilidade, define-se o mínimo múltiplo comum(mmc) e o máximo divisor comum(mdc) entre números inteiros, onde é enfatizado o importante algoritmo de Euclides para determinar o mdc de números inteiros e a relação de Bézout, que servem de base para a resolução das equações diofantinas lineares.

No capítulo 4, desenvolve-se a ideia de fazer contas com restos, utilizando exemplos de aplicação em olimpíadas e desafios matemáticos, evidenciando a ideia de periodicidade, repetição.

No capítulo 5, a ideia de fazer contas com restos é formalizada num importante conceito da aritmética, a congruência modular, que junto com as suas propriedades operatórias, dão base a resolução de congruências lineares, e fundamentam o último capítulo deste trabalho, que são as aplicações da congruência modular: o Teorema Chinês dos Restos, concluindo com a partilha de senhas, que dá uma ideia dessa poderosa ferramenta matemática nos sistemas de segurança de dados.

Capítulo 1

Divisibilidade

Consideremos o conjunto dos números naturais, $\mathbb{N} = \{1, 2, 3, 4, ...\}$.Vejamos um importante conceito, a *divisibilidade*. Dados dois números naturais a e b, com com $a \neq 0$, diz-se que a divide b, quando existir um número natural k, tal que $b = a \cdot k$. Neste caso, podemos dizer:

i) a é um divisor de b ou a divide b;

ii) a é um fator de b;

iii) b é um múltiplo de a. Sendo todas essas proposições equivalentes.

Observação 1.1 *: As proposições acima, também são válidas para o natural k, substituindo-o no lugar de a.*

Exemplo 1.1 *:*

a) 8 é um divisor de 72, pois 72=8· 9.

b) 12 não é um divisor de 135, pois o mesmo não é um fator de 135.

c) 3 é um divisor de 3^8, pois o mesmo é um fator de 3^8.

1.1 Propriedades da divisibilidade.

Consideremos os números naturais a, b e c, com a$\neq$0. Temos:

i) 1 é divisor de a;

ii) a é divisor de a;

iii) a é divisor de 0.

iv) Se a é divisor de b, e b é divisor de c, então a é divisor de c.

Vejamos a demonstração de (iv).

Se a é divisor de b então, existe um número natural k, tal que $b = a \cdot k$. Da mesma forma, se b é divisor de c então, existe um natural q, tal que $c = b \cdot q$. Logo, $c = b \cdot q \Rightarrow c = a \cdot k \cdot q \Rightarrow c = a \cdot (k \cdot q)$, ou seja, a é divisor de c.

Exemplo 1.2 *: Tem-se que 4 é divisor de 16, e 16 é divisor de 80 logo, 4 é divisor de 80. Observe:* $16 = 4 \cdot 4$ *,* $80 = 16 \cdot 5 \Rightarrow 80 = 4 \cdot 4 \cdot 5$*, evidenciando que 4 é um fator de 80.*

v) Sejam a, b, c e d, números naturais, com $a \neq 0$ e $c \neq 0$, então, se a divide b e c divide d, então $(a \cdot c)$ divide $(b \cdot d)$.

Demonstração: Se a divide b, então existe um número natural k, tal que $b = a \cdot k$. Da mesma forma, se c divide d, então existe um número natural q, tal que $d = c \cdot q$. Temos que $b \cdot d = (a \cdot k) \cdot (c \cdot q) = (a \cdot c) \cdot (k \cdot q)$, ou seja,$(a \cdot c)$ é um fator de $(b \cdot d)$, demonstrando a preposição.

Exemplo 1.3 *: 5 divide 20, e 6 divide 12, logo,* $30 = 5 \cdot 6$ *divide* $240 = 20 \cdot 12$*. Observe:* $20 = 5 \cdot 4$ *e* $12 = 6 \cdot 2$*, assim,* $240 = 20 \cdot 12 = 5 \cdot 4 \cdot 6 \cdot 2 = 5 \cdot 6 \cdot 4 \cdot 2 = 30 \cdot 4 \cdot 2$.

vi) Sejam a, b e c números naturais, com $a \neq 0$, tais que a divide $(b + c)$ ou a divide$(b - c)$, então a divide b se, e somente se, a divide c.

vii) Sejam a, b e c números naturais, com $a \neq 0$, e x e y números naturais tais que a divide b e a divide c, então a divide $(xb + yc)$; e se $xb \geq yc$, então a divide $(xb - yc)$.

viii) Sejam a e b números naturais, ambos diferentes de zero, tem-se que se a divide b, então $a \leq b$.

Exemplo 1.4 *: O número* $2^{10} \cdot 5$ *é divisível por* 2^4*?*

Solução: Como $2^{10} = 2^4 \cdot 2^6$, temos $2^{10} \cdot 5 = 2^4 \cdot 2^6 \cdot 5$, ou seja, 2^4 é um fator de $2^{10} \cdot 5$. Portanto a resposta é sim.

Exemplo 1.5 *: O número* $2^9 \cdot 3$ *é divisível por 9?*

Solução: Observe que $9 = 3 \cdot 3$, e que o número $2^9 \cdot 3$, apresenta apenas um fator 3, logo, 9 não é divisor de $2^9 \cdot 3$.

1.2 Números naturais primos e números naturais compostos.

Definição 1.1 *: Um número natural diferente de* 0 *e de* 1 *e que é apenas divisível por* 1 *e por si próprio é chamado número primo. Um número natural diferente de* 0 *e de* 1 *que não é primo é chamado de número composto. Desta maneira, excetuando-se os números* 0 *e* 1*, qualquer outro número natural ou é primo ou é composto.*

Exemplo 1.6 *: Os números 2, 3, 5, 11 são números primos, enquanto* $8 = 2 \cdot 4$ *e* $36 = 4 \cdot 9$ *são números compostos.*

Verificar se um número natural é primo ou composto, não é uma tarefa muito simples. O fato é que os números naturais compostos são infinitos. ***Euclides de Alexandria***, em 300 a.C, demonstrou que também são infinitos os números primos.

1.3 O Crivo de Eratóstenes.

Eratóstenes (?276 a.C. – ?196 a.C.) foi criado em Cirene, cidade grega ao norte da África. Estudou em Alexandria, no Egito, e depois em Atenas, retornando a Alexandria em 255 a.C., onde se estabeleceu. Eratóstenes escreveu sobre matemática, astronomia, geografia, história e fez críticas literárias. É atribuído a Eratóstenes o cálculo do tamanho da terra e, dentre outras descobertas, o chamado Crivo de Eratóstenes, um método bastante eficiente para obter de forma sistemática números primos.

A palavra Crivo, significa peneira. Sendo assim, o método consiste em peneirar números naturais, em um conjunto limitado de tais números, eliminando-os, restando assim, apenas números primos.

Para construir o Crivo, Eratóstenes baseou-se no seguinte resultado, devido ao próprio.

Proposição 1.1 *: Se um número natural* $a > 1$ *é composto, então ele é múltiplo de algum número primo* p *tal que* $p^2 \leq a$*. Equivalentemente, é primo todo número* a *que não é múltiplo de nenhum primo* p *tal que* $p^2 \leq a$*.*

Demonstração: Para demonstrar esse resultado, utilizaremos o fato de que se um número natural a é múltiplo de b e b é múltiplo de c, então a é múltiplo de c.

Vejamos um exemplo prático: 20 é múltiplo de 4 e 4 é múltiplo de 2, logo, 20 é múltiplo de 2.

Sendo assim, se a é um natural composto e p é o menor número primo do qual a é múltiplo, então $a = p \cdot b$, com p e b naturais menores do que a. Sendo b primo ou composto, ele será múltiplo de um primo q, pois ele será o próprio q, se for primo, ou será $b = n \cdot q$, caso seja composto.

Desta forma, a é múltiplo de b e b é múltiplo de q, então a é múltiplo de q e sendo p o menor primo do qual a é múltiplo, temos $p \leq q$. Segue,$p^2 \leq p \cdot q \leq a$ e que o menor divisor de um número natural é um número primo.

Exemplo 1.7 *: Verificar se o número 167 é primo ou composto.*

Solução: Utilizando o mesmo critério adotado por Eratóstenes, basta verificar se 167 é múltiplo dos primos 2, 3, 5, 7 ou 11, já que o próximo primo 13, é tal que $13^2 = 169 > 167$. Como 167 não é múltiplo de 2, 3, 5, 7 ou 11, temos que o mesmo é primo.

Exemplo 1.8 *: Identifique todos os números primos menores que 90.*

Solução: Consideremos, inicialmente, o primeiro número primo, o número 2. A seguir, grifamos todos os múltiplos de 2 existentes na tabela.
Em seguida, observamos o primeiro número não grifado na tabela, o número 3, que é primo, pois não é múltiplo de nenhum número anterior diferente de 1. Grifamos todos os seus múltiplos.

Continuamos esse procedimento, tomando o próximo número não grifado na tabela, o número 5, que é primo. Grifamos todos os seus múltiplos.

Continuando esse procedimento e, levando em consideração que o mesmo terminará assim que chegarmos ao número primo 11, pois $11^2 = 121 > 90$. Tem-se:

	2	**3**	4	**5**	6	**7**	8	9	10	**11**	12	**13**	14	15
16	**17**	18	**19**	20	21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40	**41**	42	**43**	44	45
46	**47**	48	49	50	51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70	**71**	72	**73**	74	75
76	77	78	**79**	80	81	82	**83**	84	85	86	87	88	**89**	90

Assim, os números destacados em negrito, são todos primos.

Observação 1.2 *: Fatorar um número natural, significa escrever esse número como um produto de dois ou mais fatores, diferentes de 1. Sendo assim, observe as várias formas de fatorar o número 480.*

$480 = 2 \cdot 240$
$480 = 4 \cdot 120$
$480 = 10 \cdot 48$
$480 = 2^5 \cdot 3 \cdot 5$
Essa última forma de escrever um número natural na forma fatorada é devida a um importante teorema, conhecido como *Teorema Fundamental da Aritmética*, e é destacado por ***Euclides de Alexandria*** no livro *Os Elementos*.

1.4 Teorema Fundamental da Aritmética.

Teorema 1 *: Todo número natural maior do que 1 ou é primo ou se escreve de modo único como um produto de números primos.*

Exemplo 1.9 *: Vejamos alguns números naturais e as suas respectivas fatorações completas, ou seja, aquelas em que só aparecem fatores primos na sua decomposição.*

a) $72 = 2^3 \cdot 3^2$

b) $144 = 2^4 \cdot 3^2$

c) $2700 = 2^3 \cdot 3^3 \cdot 5^3$

Exemplo 1.10 *: O número* $2 \cdot 3^6$ *é divisível por 6?*

Solução: Observe que $6 = 2 \cdot 3$, como o número$2 \cdot 3^6$ apresenta os fatores 2 e 3, portanto o mesmo é divisível por 6.

Exemplo 1.11 *: No exemplo* 1.6*, verificamos que 6 000 era múltiplo de 240. Vejamos uma outra forma de evidenciar tal fato.*

Solução: Temos que $6000 = 2^4 \cdot 3 \cdot 5^3$ e $240 = 2^4 \cdot 3 \cdot 5$. Observe que um número para ser múltiplo de 240, deve possuir pelo menos quatro fatores iguais a 2, um fator igual a 3 e um fator igual a 5. Logo, como o número 6 000 satisfaz tais condições, o mesmo é múltiplo de 240.

Exemplo 1.12 *: É verdade que se um número for divisível por 4 e por 5, então ele tem que ser divisível por* $4 \cdot 5 = 20$*?*

Solução: Um número natural que é divisível por 4, deve possuir pelo menos dois fatores iguais a 2. Como o número é divisível por 5, a sua decomposição deverá ter pelo menos um fator 5. Portanto, esse número deverá ser divisível por $2 \cdot 2 \cdot 5$. Logo, a resposta é sim. Observe que este último exercício nos dá um interessante critério de divisibilidade de um número natural por 20.

1.5 Estendendo a divisibilidade ao conjunto dos números interios

Assim como vimos a *divisibilidade* no conjunto dos números naturais, podemos verificá-la no conjunto dos números inteiros.

O conjunto dos números inteiros $\mathbb{Z}$, que é uma ampliação do conjunto dos números naturais, surgiu da necessidade de efetuar a operação $b–a$, em que a e b são números naturais e $b < a$. Escrevendo os seus elementos em ordem crescente, temos:
$\mathbb{Z} = \{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}$.Trate-se de um conjunto com infinitos elementos, com as seguintes características:

i) Os números à esquerda do zero são denominados negativos;

ii) Os números á direita do zero são denominados positivos;

iii) O zero não é positivo e nem negativo;

iv) Dado um número inteiro a, o número inteiro $-a$ é denominado oposto ou simétrico de a.

v) A distância de um número inteiro a ao zero é denominado módulo ou valor absoluto do número inteiro a, representado por $|a|$.

Dados dois números inteiros a e b, com $a \neq 0$, dizemos que a é um divisor de b, ou que a divide b, se e somente se, existir um número inteiro k, tal que $b = ak$. Desta maneira, define-se a divisibilidade em $\mathbb{Z}$, que é similar a divisibilidade em $\mathbb{N}$, valendo também as propriedades da seção 1.1, levando em consideração algumas características:

1ª) Se o inteiro a divide o inteiro b, então $-a$ divide b; a divide $-b$; $-a$ divide $-b$.

2ª) Se o inteiro a é divisor de 1, então $a = \pm 1$.

3ª) Se a divide b e b divide a, então $a = \pm b$.

4ª) Se a divide b com $b = b \neq 0$, então $|a| \leq |b|$.

Exemplo 1.13 *: -72 é divisivel por 8, pois $8 \cdot (-9) = -72$.*

Exemplo 1.14 *: 45 não é divisível por -4, pois -4 não é um fator de 45.*

Capítulo 2

Divisão Euclidiana

Considere a situação-problema: Deseja-se dividir 58 bolas de gude entre 4 crianças. Quanto caberá a cada uma delas? Observe que neste caso, 58 não é múltiplo de 4, ou seja, 4 não divide 58. O valor mais próximo que caberia a cada uma delas, seriam 14 bolinhas, porém ainda restariam 2 bolinhas. Observa-se, assim, que na divisão entre inteiros, podemos trabalhar com a ideia de "resto".

Para realizar divisões com esta característica, o grande matemático *Euclides* utilizava um algoritmo, que aparece na sua obra *Os elementos*, e que por essa razão ficou conhecida como *Divisão Euclidiana*.

2.1 Algoritmo da Divisão Euclidiana

Dados os números inteiros a e b, $b \neq 0$. Na divisão de a por b, existem dois únicos números inteiros q e r, tais que $a = b \cdot q + r$, com $0 \leq r < |b|$. Neste caso, temos:
$\boldsymbol{a}$ – Dividendo;
$\boldsymbol{b}$ – Divisor;
$\boldsymbol{q}$ – Quociente;
$\boldsymbol{r}$ – Resto.

Observação 2.1 *: Quando $r = 0$, dizemos que a é divisível por b.*

Para demonstrar esse algoritmo, utilizaremos o *Princípio da boa ordenação*:*Todo conjunto não vazio A de inteiros não nagativos possui um menor elemento.*

Demonstração:

Existência: Vamos supor que $a > b$. Considere também, o conjunto $S = \{a, a - b, ..., a - n \cdot b, ...\}$, com n inteiro e $a - nb \geq 0$.

Pelo *Princípio da boa ordenação*, tal conjunto tem um menor elemento r tal que $r \geq 0$ e $r = a - bq$ ou $a = bq + r$, com $q \in \mathbb{Z}$. Além disso, temos que $r < b$, pois caso contrário,

$r \geq b$, teríamos: $r - b \geq 0 \Rightarrow a - bq - q \geq 0 \Rightarrow a - b\,(q+1) < r$, ou seja r não seria o menor elemento de S.

Unicidade: Suponhamos que existam q_1 e r_1 , tais que $a = bq_1 + r_1$ com $0 \leq r_1 < b$. Comparando $a = bq + r$, com $a = bq_1 + r_1$, temos:
$bq + r = a = bq_1 + r_1 \Rightarrow bq - bq_1 = r_1 – r \Rightarrow b\,(q - q_1) = r_1 - r$, logo, b divide $r_1 – r$. Como $r_1 < b$ e $r < b$, temos $|r_1 - r| < b$ e, portanto, como b divide $r_1 – r$, deve-se ter $r_1 – r = 0$, ou seja, $r_1 = r$.

Desta forma, $bq = bq_1$, como, por hipótese $b \neq 0$, temos $q = q_1$.

Exemplo 2.1 *: Determine o quociente q e o resto r nas divisões de :*

a) 48 por 5.

Solução: Observe, como proceder neste caso: $48 = 1 \cdot 5 + 43$;
$48 = 2 \cdot 5 + 38$;
$48 = 3 \cdot 5 + 33$;
$48 = 4 \cdot 5 + 28$;
$48 = 5 \cdot 5 + 23$;
$48 = 6 \cdot 5 + 18$;
$48 = 7 \cdot 5 + 13$;
$48 = 8 \cdot 5 + 8$;
$48 = 9 \cdot 5 + 3$.
Portanto, temos, na divisão de 48 por 5, quociente $q = 9$ e resto $r = 3$. Observe que os restos 43, 38, 33, 28, 23, 18, 13 e 8 eram todos maiores que 5.

b) 69 por 7.

Solução: De maneira mais prática, $69 = 9 \cdot 7 + 6$. Como $6 < 7$, temos que o quociente dessa divisão é $q = 9$ e o resto é $r = 6$.

c) 63 por -13.

Solução: Efetuando as divisões dos valores absolutos de 63 e -13, temos:
$63 = 13 \cdot 4 + 11 \Rightarrow 63 = -13 \cdot -4 + 11$, e $0 \leq 11 < |-13|$. Assim, obtemos quociente $q = -4$ e resto $r = 11$.

d) -78 por 11.

Solução: Efetuando as divisões dos valores absolutos de -78 e 11, temos:
$78 = 11 \cdot 7 + 1 \Rightarrow -78 = 11 \cdot -7 – 1$. Observe, neste caso, que o resto $r = -1$ não satisfaz a condição $0 \leq r < 11$. Vamos agora, utilizar o artifício de somar e subtrair 11 ao segundo membro da igualdade , assim, $-78 = 11 \cdot -7 - 11 – 1 + 11 \Rightarrow -78 = 11\,(-7 - 1) + 10 \Rightarrow -78 = 11 \cdot -8 + 10$. Como $0 \leqslant 10 < 11$, obtemos quociente $q = -8$ e resto $r = 10$.

e) 3 por -8.

Solução: $3 = -8 \cdot 0 + 3$, logo $q = 0$, $r = 3$ e $0 \leqslant 3 < |-8|$.

f) -4 por -11.

Solução: $-4 = -11 \cdot 1 + 7$, logo $q = 1$, $r = 7$ e $0 \leqslant 7 < |-11|$.

Observação 2.2 *Pelo algoritmo visto, na divisão de um número natural por 2, temos apenas dois possíveis restos, 0 ou 1. Portanto, sendo n um número natural, temos:* $n = 2q$, *sendo chamado par,ou* $n = 2q + 1$, *sendo chamado ímpar. Verificar a paridade de um número natural, é verificar se o mesmo é par ou ímpar.*

Exemplo 2.2 *: Verifique a paridade da soma de dois números naturais pares.*

Solução: Sejam $n_1 = 2q_1$ e $n_2 = 2q_2$, dois números pares. Assim:
$n_1 + n_2 = 2q_1 + 2q_2 = 2(q_1 + q_2)$. Fazendo $q_1 + q_2 = q$, temos, $n_1 + n_2 = 2q$. Portanto, a soma de dois números naturais pares é par.

Observação 2.3 *: Fixando um número natural* $m \leq 2$, *pode-se sempre escrever um número natural qualquer n, de modo único, na forma* $n = mk + r$, *onde k e r são naturais e* $r < m$.

Exemplo 2.3 *: Todo número natural n pode ser escrito em uma, e somente uma, das seguintes formas:* $6k, 6k + 1, 6k + 2, 6k + 3, 6k + 4$ *ou* $6k + 5$.

Exemplo 2.4 *Mostrar que todo natural ímpar é da forma 4k + 1 ou 4k + 3.*

Solução: Dividindo um número inteiro n por 4, temos os possíveis restos: 0, 1, 2, 3. Sendo assim: $n = 4k$, $n = 4k + 1$, $n = 4k + 2$ ou $n = 4k + 3$, com $k \in \mathbb{Z}$.
$n = 4k \Rightarrow n = 2 \cdot 2k \Rightarrow 2 \cdot k_1$, $k_1 \in \mathbb{Z}$, portanto n é par.
$n = 4k + 1 \Rightarrow n = 2 \cdot 2k + 1 \Rightarrow n = 2 \cdot k_1 + 1$, $k_1 \in \mathbb{Z}$, portanto n é ímpar.
$n = 4k + 2 \Rightarrow n = 2 \cdot (2k + 1) \Rightarrow n = 2 \cdot k_2 + 1$, $k_2 \in \mathbb{Z}$ e $k_2 = 2 \cdot k_1 + 1$, portanto n é par.
$n = 4k+3 \Rightarrow n = 4k+2+1 \Rightarrow n = 2\cdot(2k + 1)+1 \Rightarrow n = 2\cdot k_2+1$, $k_2 \in \mathbb{Z}$ e $k_2 = 2\cdot k_1+1$, portanto n é ímpar.

Capítulo 3

O Mínimo Múltiplo Comum e O Máximo Divisor Comum entre dois números inteiros

.

Agora que já conhecemos a ideia de múltiplos e divisores no conjunto dos números inteiros, veremos dois importantes conceitos: O Mínimo Múltiplo Comum (m.m.c) e O Máximo Divisor Comum (m.d.c), bem como as suas propriedades e aplicações na resolução de problemas.

3.1 Mínimo Múltiplo Comum (m.m.c)

Consideremos o número inteiro $a \neq 0$. Se multiplicarmos esse número pelos números inteiros, $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$, obteremos o conjunto M(a), denominado conjunto dos múltiplos de a.

Exemplo 3.1 *:*

a) $M(4) = \{..., -12, -8, -4, 0, 4, 8, 12, ...\} = \{0, \pm 4, \pm 8, \pm 12, \pm 16, \ldots\}$

b) $M(7) = \{..., -21, -14, -7, 0, 7, 14, 21, ...\} = \{0, \pm 7, \pm 14, \pm 21, \pm 28, \ldots\}$

c) $M(6) = \{.., -18, -12, -6, 0, 6, 12, 18, ...\} = \{0, \pm 6, \pm 12, \pm 18, \pm 24, \ldots\}$

d) $M(-7) = \{0, \pm 7, \pm 14, \pm 21, \ldots\}$

Observação 3.1 *: Verificamos imediatamente que, o inteiro zero é múltiplo de todo número inteiro e verificamos também que M(a) = M(-a).*

Observando os conjuntos M(4) e M(6), verificamos que os mesmos apresentam números comuns. Se considerarmos o conjunto M(4,6), como sendo o conjunto dos múltiplos comuns de 4 e de 6, temos: M(4,6) $=\{\pm 12, \pm 24, \pm 36, ...\}$.

Exemplo 3.2 *:*

a) M(2,5) $= \{0, \pm 10, \pm 20, \pm 30, \pm 40, ...\}$.

b) M(4,8) $= \{0, \pm 8, \pm 16, \pm 24, ...\}$.

Definição 1 *: Sejam a e b dois inteiros diferentes de zero. Chama-se mínimo múltiplo comum, de a e b, representado por m.m.c(a,b), o menor inteiro positivo m,* $m > 0$*, que é múltiplo comum de a e b.*

Exemplo 3.3 *:*

a) Sejam M(2) $= \{0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10, \pm 12, \ldots\}$ e M(5) $=\{0, \pm 5, \pm 10, \pm 15, \pm 20, \ldots\}$. Desta maneira, M(2,5) $= \{0, \pm 10, \pm 20, \pm 30, \pm 40, \ldots\}$, e m.m.c(2,5) = 10.

b) Sejam M(4) $=\{0, \pm 4, \pm 8, \pm 12, \pm 16, \pm 20, \ldots\}$ e M(8)$=\{0, \pm 8, \pm 16, \pm 24, \pm 32, \ldots\}$. Desta maneira M(4,8) $= \{0, \pm 8, \pm 16, \pm 24, \ldots\}$, e m.m.c(4,8) =8.

c) No conjunto M(10,6) $=\{0, \pm 30, \pm 60, \pm 90, \ldots\}$, tem-se m.m.c(10,6) = 30.

d) No conjunto M(-12, 30) $= \{0, \pm 60, \pm 120, \pm 180, \ldots\}$, tem-se m.m.c(-12, 30)= 60.

Observação 3.2 *: No exemplo anterior (a), verificamos que os números 2 e 5 são números primos, e que m.m.c(2,5) = 10* $= 2 \cdot 5$*. De forma geral, o m.m.c(a,b)* $= a \cdot b$*, todas as vezes que a e b são números primos.*

Observação 3.3 *: No exemplo anterior (b), verificamos que os números 4 e 8 são tais que, 8 é um múltiplo de 4, e que o m.m.c(4,8) = 8. De forma geral, sendo a e b dois números inteiros tais que b é um múltiplo de a, então o m.m.c(a,b) = b.*

Observação 3.4 *: Como M(-a) = M(a), então m.m.c(-a, b) = m.m.c(a, -b) = m.m.c(a, b).*

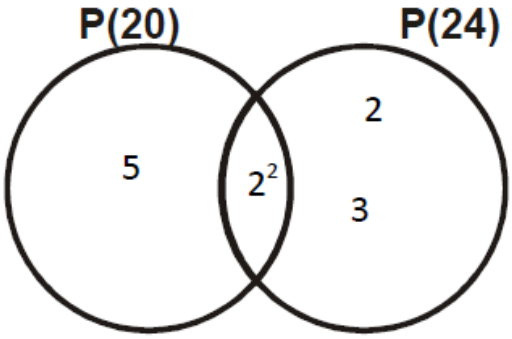
O conceito de m.m.c entre dois números inteiros pode ser estendido a mais de dois números.

Exemplo 3.4 *: Calcular o m.m.c(10, 12, 18).*

Solução: Como M(10,12,18) = $\{0, \pm 180, \pm 360, \pm 540, \ldots\}$, temos que m.m.c(10,12,18) = 180. Para calcular esse m.m.c, pode-se calcular m.m.c(10,12) e, dispondo desse resultado, calcular o m.m.c do mesmo com o inteiro 18.

Até agora, calcular o m.m.c entre números inteiros foi um trabalho relativamente fácil, pois estamos trabalhando com números inteiros pequenos. Mas, caso quiséssemos calcular o m.m.c(2400,3200), como faríamos?

Antes de responder a essa questão, considerando que o m.m.c(20,24)= 120, vamos calculá-lo de uma maneira diferente. Para tanto, vamos tomar os números 20 e 24 nas suas respectivas formas fatoradas, representando os seus fatores primos em dois conjuntos, P(20) e P(24), respectivamente:
Como $20 = 2^2 \cdot 5$ e $24 = 2^3 \cdot 3$, temos:



Observe que neste diagrama, na região comum aos conjuntos, aparece o fator 2^2, o que é fácil perceber pois $2^3 = 2^2 \cdot 2$. Se multiplicarmos todos os fatores que aparecem na união dos conjuntos P(20) e P(24) obteremos $2^2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5 = 120$ = m.m.c(20,24). Lembre-se que o m.m.c de dois números é o menor múltiplo comum entre eles, portanto nele devem aparecer fatores que são tanto do número 20 quanto do número 24, elevados aos seus maiores expoentes, pois caso contrário, ele poderá ser fator de um dos números, e não será do outro, basta verificar no exemplo, se tomássemos o fator 2^2. Desta maneira, podemos enunciar a seguinte propriedade:

Proposição 3.1 *: O m.m.c de dois números inteiros é dado pelo produto dos seus fatores primos positivos, comuns e não comuns, elevados aos seus maiores expoentes.*

Exemplo 3.5 *: Calcule:*

a) m.m.c(360, 150).

Solução: Escrevendo os números 360 e 150 na forma fatorada temos:
$360 = 2^3 \cdot 3^2 \cdot 5$ e $150 = 2 \cdot 3 \cdot 5^2$.
Assim, m.m.c(360,150) $= 2^3 \cdot 3^2 \cdot 5^2 = 1800$.

b) m.m.c(-2400, 3200).

Solução: Como m.m.c(-2400,3200) = m.m.c(2400,3200), temos:
$2400 = 2^5 \cdot 3 \cdot 5^2$
$3200 = 2^7 \cdot 5^2$
Assim, m.m.c(-2400, 3200) $= 2^7 \cdot 3 \cdot 5^2 = 9600$.

Exemplo 3.6 *: Os irmãos Pitágoras, Euclides e Tales, visitam o seu avô Arquimedes, respectivamente, a cada 6 dias, a cada 8 dias e a cada 4 dias. Se eles se encontraram na casa do avô no dia 5 de março desse mês, determinar em que dia eles se encontrarão novamente.*

Solução: Como precisamos descobrir em que dia eles voltarão a ser encontrar, devemos saber quantos dias se passarão até o próximo encontro. Para tanto, devemos determinar o m.m.c(6,8,4). Pois, este dia deverá ser um múltiplo comum de 4, 6 e 8.
Sabendo que $6 = 2 \cdot 3$; $8 = 2^3$ e $4 = 2^2$, temos que m.m.c(6,8,4) $= 2^3 \cdot 3 = 8 \cdot 3 = 24$.
Portanto, o próximo encontro dos irmãos na casa do vovô Arquimedes será no dia 29 de março.

3.2 Máximo Divisor Comum(m.d.c)

Nas seções anteriores, vimos a definição de divisibilidade no conjunto $\mathbb{Z}$. Observando o fato de que se um número inteiro a é divisível por um inteiro b, então $-a$ também divide b, podemos determinar o conjunto dos divisores inteiros de um número inteiro a, representado por D(a).

Exemplo 3.7 *:*

a) $D(9) = \{\pm 1, \pm 3, \pm 9\}$

b) $D(18) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$

c) $D(42) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}$

d) $D(56) = \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 8, \pm 14, \pm 28, \pm 56\}$.

Observando os conjuntos D(42) e D(56), verificamos que os mesmos apresentam números comuns. Se considerarmos o conjunto D(42,56), como sendo o conjunto dos divisores comuns de 42 e de 56, temos: $D(42,56) = \{\pm 1, \pm 2, \pm 7, \pm 14\}$.

Definição 2 *: Sejam a e b dois inteiros não conjuntamente nulos $a \neq 0$ ou $b \neq 0$. Chama-se máximo divisor comum de a e b, representado por mdc(a,b), o inteiro positivo d, $d > 0$, que é divisor comum de a e b.*

Exemplo 3.8 *:*

a) Os divisores comuns positivos dos inteiros 16 e 56 são tais que, D(16,56) =$\{1, 2, 4, 8\}$, logo mdc(16,56) = 8.

b) Os divisores comuns positivos de 24 e 48 são tais que, D(24,48) = $\{1, 2, 3, 6, 8, 12, 24\}$, logo mdc(24,48) = 24.

Observação 3.5 *:*

i) mdc(a,1) = 1.

ii) mdc(a,0) =|a|, com $a \neq 0$.

iii) Se a é divisor de b, então mdc(a,b) = a.

iv) Se mdc(a,b) = 1, então a e b são denominados primos entre si ou coprimos.

Exemplo 3.9 *:*

a) mdc(234,1) = 1

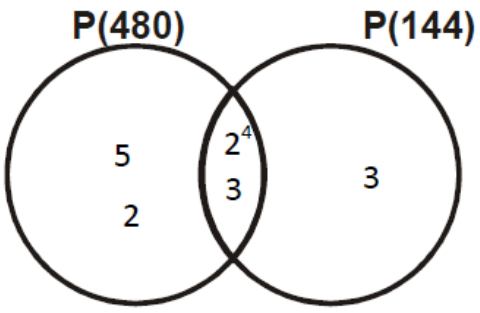
b) mdc(8,0) = 8

c) mdc(12,24) = 12, pois 12 é divisor de 24.

Observação 3.6 *: Sabendo que D(-a) = D(a), então mdc(-a, b) = mdc(a, -b) = mdc(a,b).*

Exemplo 3.10 *: mdc(-6, 8) = mdc(6,8) = 2.*

Vamos calcular o m.d.c(480,144) = 48, utilizando a noção de conjuntos. Para tanto, vamos considerar as formas fatoradas de 480 e 144, e P(480) e P(144), os respectivos conjuntos cujos elementos são os fatores primos de 480 e 144.
$480 = 2^5 \cdot 3 \cdot 5$ $144 = 2^4 \cdot 3^2$.



Observe que m.d.c (480,144) = $2^4 \cdot 3 = 48$, e que corresponde a região comum aos conjuntos P(480) e P(144), ou seja, a intersecção dos conjuntos. Lembre-se que o m.d.c(a,b) é o maior divisor comum desses números, portanto, se tomássemos um fator que não seja comum aos números, por exemplo, o fator 5, no cálculo do m.d.c(480,144), o mesmo não dividiria 144, visto que 5 não é fator de 144.

Desta forma, assim como fizemos para o mmc, podemos enunciar, sem o rigor matemático devido, a seguinte propriedade.

Proposição 3.2 *: O mdc de dois números inteiros é dado pelo produto dos seus fatores primos positivos e comuns, elevados aos seus menores expoentes.*

Exemplo 3.11 *: Calcule:*

a) m.d.c(54,36).

Solução: Escrevendo 54 e 36 nas suas formas fatoradas, temos: $54 = 2 \cdot 3^3$ e $36 = 2^2 \cdot 3^2$, logo, o mdc(54,36) $= 2 \cdot 3^2 = 2 \cdot 9 = 18$.

b) m.d.c(66,121).

Solução: Como $66 = 2 \cdot 3 \cdot 11$ e $121 = 11^2$, temos que mdc(66,121) = 11.

c) m.d.c(10,39)

Solução: Como $10 = 2 \cdot 5$ e $39 = 3 \cdot 13$, temos m.d.c(10,39) = 1, ou seja, 10 e 39 são *coprimos*.

Exemplo 3.12 *: Dois cabos de aço devem ser cortados em pedaços de tamanhos iguais, de forma que os pedaços fiquem com o maior comprimento possível. Se um cabo tem 60 m e o outro 48 m, que tamanho terá cada pedaço? Quantos pedaços serão obtidos?*

Solução: Devemos ter pedaços de tamanhos iguais e o maior possível, assim, devemos determinar o mdc(60,48). Como $60 = 2^2 \cdot 3 \cdot 5$ e $48 = 2^4 \cdot 3$, temos mdc(60,48) $= 2^2 \cdot 3 = 4 \cdot 3 = 12$. Logo, devemos cortar os cabos em pedaços de 12 m. Dividindo (60+48) por 12, temos 9 pedaços de cabo.

Proposição 3.3 *: Um número d é divisor comum de a e de b, não ambos nulos, se, e somente se, ele é um divisor comum de a e $b - a$.*

A justificativa dessa propriedade fundamenta-se na seção 1.1.

Exemplo 3.13 *: 5 é um divisor comum de 25 e 75. Assim, 5 é divisor de (75 – 25).*

Se considerarmos na última propriedade, d como máximo divisor comum de a e b, temos:

$$m.d.c\,(a, b) = m.d.c\,(a, b - a)$$

Exemplo 3.14 *: Calcule:*

a) m.d.c(42,30).

Solução: mdc(42,30) = mdc(30, 42 – 30) =
mdc(30, 12) = mdc(12, 30 – 12) =
mdc(12,18) = mdc(12, 18 – 12) =
mdc(12, 6) = mdc(6, 12 – 6) =
mdc(6,6) = 6. Deta forma, mdc(42,30) = 6.

b) m.d.c(3 418, 1 424).

Solução:mdc(3 418, 1 424) = mdc(1 424, 3 418 – 1 424) =
mdc(1 424, 1 994) = mdc(1 424, 1 994 – 1 424) =
mdc(1 424, 570) = mdc (570, 1 424 – 570) =
mdc(570, 854) = mdc(570, 854 – 570) =
mdc(570, 284) = mdc(284, 570 – 284) =
mdc(284, 286) = mdc (284,286 – 284) =
mdc(284,2) = 2.

Observe que este processo é bastante trabalhoso, vejamos uma outra propriedade que nos auxiliará no cálculo do mdc de números inteiros.

Lema 3.1 *: Se a e b são inteiros e* $a = b \cdot q + r$*, onde q e r são inteiros, então mdc (a,b) = mdc (b, r), onde* $r = a–bq$ *é o resto da divisão de a por b(divisão euclidiana).*

Demonstração: Da igualdade $a = b \cdot q + r$ concluímos que todo divisor de b e r também é divisor de a (seção 1.1). Se escrevermos a igualdade anterior como $r = a–b \cdot q$ temos que, da mesma forma, todo divisor de a e b também é um divisor de r. Ou seja, os divisores comuns de a e b são os mesmo de b e r. Logo, mdc (a,b) = mdc (b, r).

Exemplo 3.15 *: Sejam a = 50 e b = 15. Dividindo a por b obtemos:* $50 = 3 \cdot 15 + 5$*. O mdc (50,15) = mdc (15,5) = 5.*

Exemplo 3.16 *: Calcule m.d.c (876, 597).*

Solução: 876 = 1 . 597 + 279 → Pelo Lema 3.1: mdc (876, 597) = mdc (597, 279)
597 = 2 . 279 + 39 → Idem: mdc (597, 279) = mdc (279, 39)
279 = 7 . 39 + 6 → Idem: mdc (279, 39) = mdc (39, 6)
39 = 6 . 6 + 3 → Idem: mdc (39, 6) = mdc (6, 3)
6 = 2 . 3 + 0 → Idem: mdc (6, 3) = mdc (3, 0) = 3.
Logo, temos: mdc (876, 597) = mdc (597, 279) = mdc (279, 39) = mdc (39, 6) = mdc (6, 3) = mdc (3, 0) = 3. Observe que, 3 é divisor de 6, assim, a última igualdade poderia ter sido dispensada.

Observe no exemplo anterior, que o Lema 3.1 foi aplicado inúmeras vezes até se obter resto zero nas divisões euclidianas. Sendo assim, vejamos o mesmo exemplo, através de um algoritmo, que utiliza tal propriedade, conhecido como *Algoritmo de Euclides* para o cálculo do mdc de inteiros.

	1	2	7	6	2
876	597	279	39	6	3
279	39	6	3	0	

Na primeira linha desse algoritmo, escrevemos os quocientes obtidos e na última linha, escrevemos os restos.

Exemplo 3.17 *: Utilizando o Algoritmo de Euclides, determine mdc(1 496,728).*

Solução:

	2	18	5
1496	728	40	8
40	8	0	

Observação 3.7 *: Pode-se calcular o mdc entre três ou mais números inteiros. Assim, se quisermos calcular o mdc(a,b,c), calculamos o mdc(a,b) = d, em seguida calculamos mdc(d,c).*

Exemplo 3.18 *: Calcular mdc(36,64,80).*

Solução: Calculemos inicialmente mdc(80,64).

	1	4
80	64	16
16	0	

Vamos calcular agora, mdc(36,16).

	2	4
36	16	4
4	0	

Logo, mdc(36,64,80) = 4.

3.2.1 Relação de Bézout

Dados inteiros a e b, quaisquer, mas não ambos nulos, existem dois inteiros n e m tais que $mdc(a, b) = a \cdot n + b \cdot m$. Em outras palavras, a relação diz que o mdc(a,b) pode ser escrito como combinação linear de a e b. De acordo com a relação de Bézout, podemos definir: Dois números inteiros a e b, com $a \neq 0$ ou $b \neq 0$ são coprimos, quando existem dois inteiros m e n, tais que $a \cdot n + b \cdot m = 1$.

Exemplo 3.19 *: O mdc(30,42) = 6. Observe que* $6 = 3 \cdot 30 + 42 \cdot (-2)$*, com* $n = 3$ *e* $m = -2$*.*

Você deve estar se perguntando, como descobrir esses inteiros n e m? A resposta está no algoritmo de Euclides.
Consideremos o algoritmo utilizado para determinar mdc(30,42).

	1	2	2
42	30	12	6
12	6	0	

Utilizando o algoritmo de Euclides de trás para a frente, temos:
$6 = 30–2 \cdot 12 = 30–2 \cdot (42–1 \cdot 30) = 30–2 \cdot 42 + 2 \cdot 30 = 3 \cdot 30–2 \cdot 42 = 30 \cdot 3 + 42 \cdot (-2)$.

3.3 Equações Diofantinas Lineares

Considere a seguinte situação problema: O valor da entrada de um cinema é 8,00 reais e da meia entrada 5,00 reais. Qual é o menor número de pessoas que pode assistir a uma sessão de maneira que a bilheteria seja de 500,00 reais?

Para resolver esse problema, vamos denominar o número de pessoas que pagam a entrada de 8,00 reias por X, e as pessoas que pagam meia entrada de Y. Assim, temos a equação $8X + 5Y = 500$. Equações como esta serão nosso objeto de estudo nessa seção, e são denominadas *Equações Diofantinas*, em homenagem a *Diofanto de Alexandria* (300 d.C).

Denomina-se Equação Diofantina Linear(EDL), toda equação da forma $ax + by = c$, onde a, b e c são números inteiros dados e x e y são incógnitas a serem determinadas em $\mathbb{Z}$.

Sendo assim, as equações $4x + 5y = 18$, $2x–3y = 20$, $4x + 8y = 23$, são Equações Diofantinas Lineares.

As soluções de uma EDL, consistem em pares de números x e y, caso existam. Desta forma, se uma EDL possui solução, teremos um número indeterminado das mesmas.

Exemplo 3.20 *: Na EDL* $3x + 6y = 18$*, temos:*

Para $x = 4$ e $y = 1$, temos $3 \cdot 4 + 6 \cdot 1 = 18$. Logo, $x = 4$ e $y = 1$ é uma solução da equação.
Para $x = -6$ e $y = 6$, temos $3 \cdot -6 + 6 \cdot 6 = 18$. Logo, $x = -6$ e $y = 6$ é uma solução da equação.
Para $x = 10$ e $y = -2$, temos $3 \cdot 10 + 6 \cdot -2 = 18$. Logo, $x = 10$ e $y = -2$ é uma solução da equação.
Para $x = 7$ e $y = -3$, temos $3 \cdot 7 + 6 \cdot -3 = 3 \neq 18$. Logo, $x = 7$ e $y = -3$ **não** é uma solução da equação.

Exemplo 3.21 *: Na EDL $4x+8y=57$, não há solução, pois $4x+8y=2\cdot(2x+4y)$ que é um número par, nunca podendo ser igual a 57.*

Como acabamos de ver, existem EDLs que possuem várias soluções e outras que não possuem solução. Como saber se uma EDL possui solução e como determina-las? Para responder a essa pergunta, vejamos o teorema abaixo, e para maiores detelhes ver [1]. Por hora, é interessante mostrar ao aluno, com exemplos, porque o mesmo funciona.

Teorema 2 *: A equação diofantina $ax+by=c$ admite infinitas soluções se, e somente se, mdc(a,b) divide c.*

Exemplo 3.22 *Considere a EDL $6x+9y=12$.*

Observe que mdc(6,9)= 3, e que 3 é divisor de 12. Logo, pelo teorema anterior, a mesma admite soluções. Vejamos:
Dividindo toda a equação por 3, temos a equação equivalente $2x+3y=4$.
Isolando a variável x, tem-se $x=\dfrac{4-3y}{2} \Rightarrow x=2-\dfrac{3y}{2}$.
Tomando $y=2k$, com $k\in\mathbb{Z}$, pois devemos encontrar soluções inteiras, obtemos infinitas soluções para tal equação, na forma $(2-3k,2k)$, com $k\in\mathbb{Z}$.

Exemplo 3.23 *Considere a equação $8x+12y=14$.*

Observe que mdc(8,12) = 4, e que 4 não é divisor de 14. Portanto, tal equação **não** admite soluções inteiras. Vejamos:
Isolando a variável y, temos:$y=\dfrac{14-8x}{12} \Rightarrow y=\dfrac{14}{12}-\dfrac{8x}{12} \Rightarrow y=\dfrac{7}{6}-\dfrac{2x}{3}$. Por mais que tomemos $x=3k$, com $k\in\mathbb{Z}$, jamais teríamos soluções inteiras, visto que $\dfrac{7}{6}\notin\mathbb{Z}$.

Exemplo 3.24 *: Verifique se as EDLs admitem solução:*

a) $8x+12y=44$

Solução: Como o mdc(8,12) = 4, e 4 divide 44, temos que a equação admite solução.

b) $6x+7y=1$.

Solução: Como o mdc(6,7) = 1, e 1 é divisor de 1, temos que a equação admite solução.

c) $10x+14y=5$.

Solução: Como o mdc(10,14) = 2, e 2 **não divide 5**, temos que a equação **não** admite solução.

Observação 3.8 *: Dada a equação diofantina linear $ax+by=c$, se mdc(a,b) = 1, então a equação sempre admite solução, pois 1 é divisor de qualquer número inteiro.*

Exemplo 3.25 *: Resolver a equação Diofantina linear* $3x + 5y = 7$.

Solução: Observe que mdc(3,5) = 1, portanto a equação possui solução. Vamos determinar soluções particulares para a equação, e a partir daí, determinar soluções gerais. Note que:
$3 \cdot 2 + 5 \cdot -1 = 1$. Multiplicando toda a equação por 7, temos: $3 \cdot 14 + 5 \cdot -7 = 7$. Percebemos então que $x_0 = 14$ e $y_0 = -7$ é uma solução particular de tal equação.
Consideremos agora, as equações $3x + 5y = 7$ e $3x_0 + 5y_0 = 7$. Subtraindo uma equação da outra, temos $3(x - x_0) + 5(y - y_0) = 0$. Fazendo $(x - x_0) = a$ e$(y - y_0) = b$, tem-se $3a + 5b = 0$. Para que esta última igualdade seja verdadeira, devemos ter b divisível por 3, e a divisível por 5. Supondo $a = 5k$, temos, $15k + 5b = 0 \Rightarrow b = -3k$. Fazendo $(x - x_0) = 5k \Rightarrow x = x_0 + 5k \Rightarrow x = 14 + 5k$ e $(y - y_0) = -3k \Rightarrow y = y_0 - 3k \Rightarrow y = -7 - 3k$, que são as soluções da equação, para todo inteiro k.

Acontece que nem sempre é fácil encontrar soluções particulares para tais equações, utilizando o processo de tentativas e erros. O próximo resultado irá facilitar a resolução das mesmas.

Observação 3.9 *: Se* $x = x_0$ *e* $y = y_0$ *são soluções particulares de uma equação diofantina* $ax + by = c$*, então todas as soluções são dadas por* $x = x_0 + \frac{b}{d} \cdot k$ *e* $y = y_0 - \frac{a}{d} \cdot k$*, com* k *um inteiro qualquer.Para maiores detalhes, consultar [8].*

Exemplo 3.26 *: Resolver a equação 40X – 65Y = 135.*

Solução: Inicialmente temos que mdc(40,65) = 5, e 5 divide 135. Podemos desta maneira, dividir toda a equação por 5, obtendo $8X–13Y = 27$. Como mdc(8,13) = 1, podemos, através do algoritmo de Euclides, escrever $1 = 8n + 13m$. Observe:
$13 = 8 \cdot 1 + 5$
$8 = 5 \cdot 1 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 1 \cdot 2 + 1$
Assim, com um procedimento análogo ao do exemplo 5, verificamos que $1 = 8 \cdot 5–3 \cdot 13$. Multiplicando esta igualdade por 27, obtemos $8 \cdot 135–13 \cdot 81 = 27$. Portanto, obtemos a solução particular $x_0 = 135$ e $y_0 = 81$. Concluímos então que as soluções de tal equação são da forma: $x = 135 - 13k$ e $y = 81 - 8k$, para todo k inteiro.

Capítulo 4

Fazendo contas com restos

Considere o seguinte problema:

João mora em Salvador e seus pais em Recife. Para matar a saudade, ele telefona para seus pais a cada três dias. O primeiro telefonema foi feito num domingo, o segundo telefonema foi feito na quarta-feira seguinte, o terceiro telefonema foi feito no sábado, e assim por diante. Em qual dia da semana João telefonou para os seus pais pela centésima vez?(*banco de questões da obmep 2010*).

Você pode resolver esse problema, construindo uma tabela, constando o dia da semana e a posição da ligação de João para os seus pais.

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
1^a	6^a	4^a	2^a	7^a	5^a	3^a
8^a	13^a	11^a	9^a	14^a	12^a	10^a

É claro que se você continuasse a completar essa tabela, descobriria em qual dia da semana foi realizada a centésima ligação. Porém, vamos analisá-la sobre outro ponto de vista.

Verificando a primeira linha da tabela, notamos que aparecem os 7 primeiros telefonemas, um para cada dia da semana. A partir do sétimo telefonema, os dias começam a se repetir. Observe que os elementos da segunda linha da tabela foram obtidos a partir da soma do elemento que se encontra na mesma coluna na linha anterior, com 7. Por exemplo, os elementos da coluna referente a quarta-feira, seriam: 2, 9, 16, 23, 30,..., ou seja, só aparecem números que quando divididos por 7, deixam resto 2. Desta forma, podemos relacionar o dia da semana, com o resto da divisão do número correspondente da ligação por 7.

Domingo $\rightarrow$ resto 1

Segunda $\rightarrow$ resto 6

Terça $\rightarrow$ resto 4

Quarta $\rightarrow$ resto 2

Quinta $\rightarrow$ resto 0

Sexta → resto 5
Sábado → resto 3
Assim, dividindo 100 por 7, tem-se $100 = 7 \cdot 14 + 2$, e a centésima ligação foi realizada numa quarta-feira.

Pudemos verificar que para resolver esse problema, levamos em consideração a repetição ou periodicidade com que ele acontecia, analisando os restos da divisão de um inteiro por 7, ou seja, periodicidade 7, portanto período 7 [1].

Este comportamento não é um fato raro, ele é comum em várias situações do cotidiano.

Exemplo 4.1 *:*

a) Nos relógios, onde as horas se repetem de 12 em 12 horas, ou, de 24 em 24 horas.

b) Nos calendários, em que os dias da semana se repetem de 7 em 7 dias.

c) Fenômenos naturais como as fases da Lua.

Vejamos outra situação: Vamos construir uma tabela, em que nela aparecem a sequência dos números inteiros não negativos, e os seus respectivos restos na divisão por 3.

Inteiro	0	1	2	3	4	5	6	7	8
Resto	0	1	2	0	1	2	0	1	2

Observamos assim, que os restos na divisão de inteiros por 3, são periódicos de período 3. De maneira geral, os restos dos inteiros sucessivos na divisão por um inteiro positivo qualquer n repetem-se com período n. A justifivicativa dessa afirmação, encontra-se na seção referente a divisão euclidiana.

Vejamos agora, outras características interessantes no cálculo com restos.

4.1 O resto da soma é a soma dos restos?

Vejamos as seguintes situações:

1) Qual é o resto da divisão de (9 457 + 2 734) por 4?

Solução: Vejamos a solução desse problema de duas formas distintas.
1ª) Forma:

Sabendo que 9 457 + 2 734 = 12 191. Dividimos 12 191 por 4, obtendo quociente 3047 e resto 3.

[1] Entende-se por período, o intervalo com que as ligações se repetiam com regularidade.

2ª) Forma:

Façamos o seguinte: Vamos dividir 9 457 e 2 734 por 4, tomar os restos dessas divisões e somá-los. Assim, $9457 = 2364 \cdot 4 + 1$ e $2734 = 683 \cdot 4 + 2$. Observe que os restos obtidos foram 1 e 2, que quando somados dão igual ao resto da divisão da soma (9 457 + 2 734). Considerando $9457 = 2364 \cdot 4 + 1$ e $2734 = 683 \cdot 4 + 2$, temos:

$$9457 + 2734 = 2364 \cdot 4 + 1 + 683 \cdot 4 + 2$$

$$= 2364 \cdot 4 + 683 \cdot 4 + 1 + 2$$

$$= 4 \cdot (2364 + 683) + (1 + 2)$$

2) Qual é o resto da divisão de (12 369 + 24 734) por 6?

Solução: Temos que $12369 = 2061 \cdot 6 + 3$ e $24734 = 4122 \cdot 6 + 2$. Como $12369 + 24734 = 37103 = 6183 \cdot 6 + 5$. Observe que, o resto da soma dos valores em parênteses por 6, é igual a soma dos restos da divisão de cada uma das parcelas por 6.

Mas será que isso sempre ocorre? A resposta é **não!** Observe o próximo exemplo:

3) Qual é o resto da divisão de (16 + 20) por 3?

Solução: Observe que $16 + 20 = 36 = 12 \cdot 3$. Temos, também, que $16 = 5 \cdot 3 + 1$ e $20 = 6 \cdot 3 + 2$.

Assim, verificamos que a soma (16 + 20) = 36, que é um múltiplo de 3. Porém, a soma dos restos das parcelas 16 e 20 por 3, é igual a 3, que quando dividido por 3, tem resto igual ao de 36 por 3.

Desta forma, verificamos: *O resto da divisão por $m \neq 0$ da soma de dois números naturais quaisquer é igual ao resto da divisão por $m \neq 0$ da soma de seus respectivos restos.*

De maneira mais geral:

Consideremos dois números naturais N_1 e N_2, tais que a soma $N_1 + N_2$, quando divida por $m \neq 0$, deixa resto s, $0 \leq s < m$, ou seja, $N_1 + N_2 = mk + s$, e que quando divididos pelo natural $m \neq 0$, deixam restos r_1 e r_2, com $0 \leq r_1 < m$, $0 \leq r_2 < m$. Sendo assim, existem naturais k_1 e k_2, tais que: $N_1 = m \cdot k_1 + r_1$ e $N_2 = m \cdot k_2 + r_2$. Desta forma, temos:

$N_1 + N_2 = m \cdot k_1 + r_1 + m \cdot k_2 + r_2 = m \cdot k_1 + m \cdot k_2 + r_1 + r_2 = m \cdot (k_1 + k_2) + (r_1 + r_2)$.

Consideremos, agora, $r_1 + r_2 = mk' + r'$, e $k_1 + k_2 = k$" com $0 \leq r' < m$. Assim:$N_1 + N_2 = m \cdot (k_1 + k_2) + (r_1 + r_2) = mk" + mk' + r' = m \cdot (k" + k') + r'$, com $0 \leq r' < m$. Logo pela unicide do resto $s = r'$.

4.2 O resto do produto é o produto dos restos?

Assim como vimos na *seção 4.1*, vamos verificar se o resto do produto de dois números naturais é igual ao produto dos restos na divisão de naturais. Vejamos as seguintes situações:

1) Qual é o resto da divisão de (2 367 · 5 986) por 5?

Solução: Efetuando o produto $2367 \cdot 5986$, temos como resposta 14 168 862, que dividido por 5 é igual a $14168862 = 2833772 \cdot 5 + 2$. Observe que $2367 = 473 \cdot 5 + 2$ e $5986 = 1197 \cdot 5 + 1$. Desta forma, os restos das divisões de 2 367 e 5 986 por 5 são, respectivamente, 2 e 1, que quando multiplicados dão o mesmo resultado da divisão do produto (2 367 x 5 986) por 5.

2) Qual é o resto da divisão de $(25 \cdot 44)$ por 7?

Solução: Observe que $25 = 7 \cdot 3 + 4$ e $44 = 7 \cdot 6 + 2$. Como $(25 \cdot 44) = 1100 = 157 \cdot 7 + 1$. Multiplicando os restos das divisões de 25 e 44 por 7, temos $2 \cdot 4 = 8 = 1 \cdot 7 + 1$, este produto tem o mesmo resto da divisão de $(25 \cdot 44)$ por 7.

Desta forma, assim como na soma, verificamos: *O resto da divisão por $m \neq 0$ do produto de dois números naturais quaisquer é igual ao resto da divisão por $m \neq 0$ do produto dos seus respectivos restos.*

A demonstração segue um princípio análogo da demonstração realizada na *seção 4.1*, e é facilmente verificada.

Exemplo 4.2 *: Qual é o resto da divisão de* $(25 \cdot 73 + 45 \cdot 34 + 97 \cdot 76)$ *por 11?*

Solução: Fazendo as divisão de 25, 73, 45, 34, 97 e 76 por 11, obtemos os respectivos restos, 3, 7, 1, 1, 9 e 10. Desta maneira, substituindo esses valores na expressão, temos:$(3 \cdot 7 + 1 \cdot 1 + 9 \cdot 10) = 112$, que quando dividido por 11, deixa resto 2.

Exemplo 4.3 *: Qual é o resto da divisão de* 13^{200} *por 12?*

Solução: Sabe-se que 13^{200} apresenta 200 fatores iguais a 13, basta calcular o resto da divisão de 13 por 12 e elevá-lo a 200. Como o resto da divisão de 13 por 12 é 1, temos que o resto de 13^{200} por 12 é igual a $1^{200} = 1$.

Exemplo 4.4 *: Prove que* $n^5 + 4n$ *é divisível por 5 qualquer que seja o natural* n*.*

Solução: Na divisão de um número natural n por 5, temos os possíveis restos: 0, 1, 2, 3, 4, sendo assim, vejamos a tabela, com os possíveis restos para $n^5 + 4n$ na divisão por 5.

Resto de n por 5	Resto de n^5 por 5	Resto de 4n por 5	Resto de $n^5 + 4n$ por 5.
0	0	0	0
1	1	4	5
2	2	3	5
3	3	2	5
4	4	1	5

Analisando a última coluna, verificamos que os possíveis valores para o resto de n^5+4n por 5 são 0, logo o mesmo será divisível por 5, ou 5 que é divisível por 5.

Exemplo 4.5 *: Determine o último algarismo do número* 2^{50}*.*

Solução: Observe a sequência abaixo das primeiras potências de base 2:
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$.

Vemos que os últimos algarismos das primeiras potências de base 2, são: 2, 4, 8, 6, 2, 4, ..., ou seja, elas se repetem ciclicamente. Desta forma, para determinar o último algarismo de 2^{50}, basta determinar 2^r, onde r é o resto da divisão de 50 por 4. Assim, $50 = 4 \cdot 12 + 2 \Rightarrow 2^{12} = 4$. Portanto, o último algarismo do número 2^{50} é 4.

Capítulo 5

Congruência Modular

Na *seção 2*, vimos uma importante definição no conjunto dos números inteiros que foi a divisão euclidiana. Nela, verificamos que na divisão de dois números inteiros, quando um não é múltiplo do outro, a existência de restos. Na *seção 4*, vimos o comportamento do resto na resolução de problemas.

Vários matemáticos, a exemplo *Euler*, *Fermat* e *Gauss*, se dedicaram a estudar a aritmética com restos na divisão euclidiana por um número fixado, dando início a um importante ramo da matemática na teoria dos números, a congruência modular.

Introduzida por Gauss no seu livro *Disquisitiones Arithmeticae*, a congruência modular tornou-se uma importante ferramenta nas resoluções de problemas que estão associados a fatos periódicos. Deve-se a Gauss também, a simbologia utilizada nesta teoria.

Definição 5.1 *: Sejam* $\boldsymbol{a}$ *e* $\boldsymbol{b}$ *inteiros quaisquer e seja* $\boldsymbol{m} > 1$ *um inteiro positivo fixo. Diz-se que* $\boldsymbol{a}$ *é congruente a* $\boldsymbol{b}$ *módulo* $\boldsymbol{m}$*, representado por* $a \equiv b(mod\ m)$*, se, e somente se,* $\boldsymbol{m}$ *divide a diferença* $\boldsymbol{a} - \boldsymbol{b}$*. Em outros termos* $\boldsymbol{a}$ *é congruente a* $\boldsymbol{b}$ *módulo* $\boldsymbol{m}$ *se, e somente se, existe um inteiro* $\boldsymbol{k}$ *tal que* $a–b = km$*.*

Exemplo 5.1 *:*

a) $38 \equiv 18$ *(mod 5), pois 38 – 18 = 20 e 5 é divisor de 20.*

b) $2 \equiv 8$ *(mod 6), pois 2 – 8 = -6 e 6 é divisor de -6.*

c) $23 \equiv 7$ *(mod 8), pois 23 – 7 = 16 e 8 divide 16.*

d) $10 \equiv -4$ *(mod 7), pois 10 – (-4) = 10 + 4 = 14 e 7 divide 14.*

Observação 5.1 *: Quando* $\boldsymbol{a}$ *não é congruente a* $\boldsymbol{b}$ *módulo* $\boldsymbol{m}$*, representamos* $a \not\equiv b$ *(mod m).*

Assim, $24 \not\equiv 18$ (mod 5), pois 24 - 18 = 6, e 5 não é divisor de 6.

Observação 5.2 *: $a \equiv 0$ (mod m) se, e somente se, m é divisor de a.*

Observação 5.3 *: Da definição de congruência, podemos concluir que, dois inteiros* $\boldsymbol{a}$ *e* $\boldsymbol{b}$ *são congruentes módulo* $\boldsymbol{m}$ *se, e somente se,* $\boldsymbol{a}$ *e* $\boldsymbol{b}$ *deixam o mesmo resto quando divididos por* $\boldsymbol{m}$*. Verifiquemos:*

($\Rightarrow$) Da definição de congruência, $a \equiv b$(mod m)$\Leftrightarrow$ a–$b = km$, com k inteiro.
Seja r o resto da divisão de b por m, de tal maneira que $b = qm + r$, com $0 \leq r < m$, e $q \in \mathbb{Z}$. Sendo assim, temos: $a = km + b \Rightarrow a = km + qm + r \Rightarrow a = m\,(k + q) + r$, portanto a quando dividido por m, também tem resto r.
($\Leftarrow$) Supondo que a e b quando divididos por m têm o mesmo resto, temos:
$a = qm + r$ e $b = tm + r \Rightarrow a$–$b = qm + r$– $(tm + r) \Rightarrow a$–$b = qm + r$–tm–$r \Rightarrow a$–$b = m\,(q$–$t) \Rightarrow m$ divide a–b , portanto $a \equiv b$(mod m).

Exemplo 5.2 *:*

a) $25 \equiv 19$ *(mod 6), pois* $25 = 6 \cdot 4 + 1$ *e* $19 = 3 \cdot 6 + 1$.

b) $-78 \equiv 21$ *(mod 11), pois* $-78 = 11 \cdot (-8) + 10$ *e* $21 = 11 \cdot 1 + 10$.

c) $37 \equiv 17$ *(mod 5), pois* $37 = 5 \cdot 7 + 2$ *e* $17 = 5 \cdot 3 + 2$.

Observação 5.4 *: Ao dividir um número inteiro positivo a por m, obtemos* $k \in \mathbb{Z}$ *e* $0 \leq r < m$*, tais que* $a = mk + r \Rightarrow a$–$r = mk \Rightarrow a \equiv r$*(mod m).Desta maneira, todo inteiro positivo é congruente módulo m ao resto de sua divisão por m.*

Exemplo 5.3 *:*

a) $20 \equiv 6$ (mod 7), pois $20 = 2 \cdot 7 + 6$.

b) $53 \cdot 5$ (mod 8), pois $53 = 6 \cdot 8 + 5$.

Uma consequência imediata das observações 5.3 e 5.4 , é que todo número inteiro a é congruente módulo m a exatamente um dos números 0, 1, 2, ..., m – 1 e estes últimos são incongruentes entre si módulo m.

Definição 5.2 *: Seja* $m > 0$*. Chama-se sistema completo de resíduos (restos) módulo m, um conjunto de m números* $\{r_1, r_2, r_3, ..., r_m\}$*, tal que cada a inteiro é congruente a exatamente um dos números* r_1*,* r_2*,* r_3*,...,* r_m*, ou ainda, podemos dizer que os* r_1*,* r_2*,* r_3*,...,* r_m *são congruentes, em alguma ordem, módulo m aos números 0, 1, 2, 3, ..., m.*

Exemplo 5.4 *: Seja* $m = 4$*, temos que o conjunto 0, 1, 2, 3 é um sistema completo de resíduos módulo 4. Observe que o conjunto -12, 19, 22, 41 também é um sistema completo de resíduos módulo 4, pois* $-12 \equiv 0$ *(mod 4),* $19 \equiv 3$ *(mod 4),* $22 \equiv 2$ *(mod 4) e* $41 \equiv 1$ *(mod 4).*

5.1 Propriedades da congruência modular.

Seja m um inteiro positivo fixo ($m > 1$) e sejam a, b e c inteiros quaisquer. Valem as propriedades:

i) $a \equiv a$ (mod m). (reflexiva)

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

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

Demonstrações:

i) Como m divide 0, então m divide (a – a), ou seja, $a \equiv a$ (mod m).

ii) $a \equiv b$ (mod m)$\Rightarrow$ a–$b = km$, para $k \in \mathbb{Z}$. Desta forma, $b = a$–$km \Rightarrow b$–$a = (-k)\, m \Rightarrow b \equiv a$ (mod m).

iii) se $a \equiv b$ (mod m) e $b \equiv c$ (mod m), então existem inteiros k e q, tais que: a–$b = km$ e b–$c = qm$. Somando membro a membro as equações anteriores, temos: a–$b + b$–$c = km + qm \Rightarrow a$–$c = m\,(k + q)$, ou seja, $a \equiv c$ (mod m).

5.2 Propriedades operatórias da congruência modular.

Veremos nesta seção, propriedades operatórias das congruências modulares. Faremos a demonstração de algumas delas. Para verificação das demais, consultar [5].

P_1) Sejam a, b, c e d números inteiros tais que $a \equiv b$(mod m) e $c \equiv d$(mod m). Tem-se que:$a \pm c \equiv b \pm d$(mod m).

Prova: se $a \equiv b$ (mod m) e $c \equiv d$ (mod m), então existem inteiros k e q, tais que: $a = km + b$ e $c = qm + d$. Somando membro a membro as equações anteriores, temos: $a \pm c = m\,(k \pm q) + (b \pm d) \Rightarrow a \pm c \equiv b \pm d$ (mod m).

P_2) Sejam a, b, c e d números inteiros tais que $a \equiv b$(mod m) e $c \equiv d$(mod m). Tem-se que:$ac \equiv bd$(mod m).

P_3) Se $a \equiv b$ (mod m), então $a \pm c \equiv b \pm c$ (mod m), para algum $c \in \mathbb{Z}$.

P_4) Se $a \equiv b$ (mod m), então $ac \equiv bc$ (mod m), para algum $c \in \mathbb{Z}$.

P_5) Sejam $a \equiv b$ (mod m) e $n \in \mathbb{N}$, temos que $a^n \equiv b^n$(mod m).

P_6) Se $a \equiv b$ (mod m), e se n é um divisor de m, com $n > 0$, então $a \equiv b$ (mod n).

P_7) Se $a \equiv b$ (mod m) e se a, b, m são todos divisíveis pelo inteiro $d > 1$, então $\frac{a}{d} \equiv \frac{b}{d}(\text{mod } \frac{m}{d})$.

Prova: Se $a \equiv b(\text{mod m})$, então: $a - b = km$, $k \in \mathbb{Z} \Rightarrow \frac{a}{d} - \frac{b}{d} = k \cdot \frac{m}{d} \Rightarrow \frac{a}{d} \equiv \frac{b}{d}(\text{mod } \frac{m}{d})$.

P_8) Se $ac \equiv bc$ (mod m) e se o $mdc(c, m) = d$, então $a \equiv b$ (mod d/m) .

P_9) Se $ac \equiv bc$ (mod m) e se o $mdc(c, m) = 1$, então $a \equiv b$ (mod m).

Esta propriedade mostra que é permitido cancelar fatores de ambos os membros de uma congruência que são *coprimos* com o módulo.

P_{10}) Se $ac \equiv bc(\text{mod p})$, onde p é um número primo, e se p divide c então $a \equiv b($ mod p).

Prova: Temos que p não divide c e p é primo, desta forma, mdc(p,c)=1, garantindo o cancelamento pela P_9.

Fazendo uso da definição e das propriedades da congruência modular, vejamos algumas situações problemas:

Exemplo 5.5 *: Calcule o resto da divisão de* 3006^{3006} *por 5.*

Solução: Como $3006 = 6000 \cdot 5 + 1$, temos: $3006 \equiv 1$ (mod 5)$\Rightarrow 3006^{3006} \equiv 1^{3006}$ (mod 5)$\Rightarrow 3006^{3006} \equiv 1$ (mod 5). Portanto o resto procurado é 1.

Exemplo 5.6 *: Sabendo que 01/01/2013 foi uma terça-feira, determine em que dia da semana cairá 06/07/2013, sem fazer consulta a qualquer tipo de calendário.*

Solução: Se 01/01/2013, foi numa terça, temos:
02/01→ quarta-feira, 03/01→ quinta-feira; 04/01→ sexta-feira; 05/01→ sábado; 06/01→ Domingo; 07/01→ segunda –feira; 08/01→ terça-feira; 09/01→ quarta-feira, e assim por diante. Observe que a partir daí, para saber o dia em que caiu determinada data, basta determinar o número de dias que se passarão até ela, na congruência módulo 7, pois são 7 dias na semana, e que toda data congruente a 1 módulo 7, será uma terça; congruente a 2 módulo 7 será uma quinta, e assim por diante. Desta forma:
Janeiro = 31 dias; Fevereiro = 28 dias; Março = 31 dia; Abril = 30 dias; Maio = 31 dias; Junho = 30 dias; Julho = 6 dias. Desta forma, terão se passado 187 dias até 06/07. Como $187 \equiv 5$ (mod 7), temos que tal data será num sábado, pois 05/01 foi num sábado.

Exemplo 5.7 *: Sabendo que agora são 11 horas da manhã, que horas serão daqui a 230 horas?*

Solução: Sabendo que as horas se repetem num período de 24 horas, e sabendo que $230 \equiv 14 \pmod{24}$, temos $11 + 14 = 25 \equiv 1 \pmod{24}$, portanto, será 1 hora da manhã.

Exemplo 5.8 *: Verifique se* $30^{99} + 61^{100}$ *é divisível por 31.*

Solução: Da definição de congruência modular, temos: $30 \equiv -1$ (mod 31) e $61 \equiv -1$ (mod 31).
Assim: $30^{99} + 61^{100} \equiv (-1)\,99 + (-1)\,100 = -1 + 1 = 0$, equivalente a $30^{99} + 61^{100} \equiv 0$ (mod 31). Portanto, $30^{99} + 61^{100}$ é divisível por 31.

Exemplo 5.9 *: Determine o resto da divisão de* $5^{1311} + 7^{1311} + 11^{1311} + 25^{131}$ *por 8.*

Solução: $5^{1311} + 7^{1311} + 11^{1311} + 25^{1311} \equiv (-3)^{1311} + (-1)^{1311} + 3^{1311} + 1^{1311} = 0$ (mod 8).

Exemplo 5.10 *: Prove que* $11^{n+2} + 12^{2n+1}$ *é divisível por 133 qualquer que seja o número natural* n*.*

Solução: $11^{n+2} + 12^{2n+1} = 11^2 \cdot 11^n + 12 \cdot 12^{2n} = 121 \cdot 11^n + 12 \cdot 12^{2n}$. Escrevendo $121 \cdot 11^n$ na forma $133 \cdot 11^n - 12 \cdot 11^n$,temos:
$133 \cdot 11^n - 12 \cdot 11^n + 12 \cdot 12^{2n}$
$\equiv 12\,(12^{2n} - 11^n) =$
$(144^n - 11^n)$, como $144 \equiv 11 \pmod{133}$, pela propriedade P_5, temos $(144^n - 11^n) \equiv 0 \pmod{133}$.

5.3 Congruências Lineares.

Denomina-se congruência linear, toda congruência da forma $ax \equiv b$ (mod m), com a, b, $m > 0$ e x inteiros,onde x são as soluções procuradas.

Exemplo 5.11 *: São congruências lineares:* $4x \equiv 7$ *(mod 5),* $3x \equiv 9$ *(mod 6),* $5x \equiv 8$ *(mod 4).*

Mas será que toda congruência linear tem solução? A resposta é não! Vejamos agora sob quais condições essas congruências admitiram solução, e caso admitam, quantas são.

i) Uma congruência linear $ax \equiv b$ (mod m) admite solução se, e somente se,d = mdc(a,m) divide b.

ii) Se d = mdc(a,m) divide b, então $ax \equiv b$ (mod m) possui exatamente d soluções *incongruentes* entre si módulo m. Se $X_0 \in \mathbb{Z}$ é uma solução particular, então as soluções incongruentes são da forma X_0 ; $X_0 + \dfrac{m}{d}$; $X_0 + 2 \cdot \dfrac{m}{d}$; $X_0 + 3 \cdot \dfrac{m}{d}$; ...; $X_0 + (m-1) \cdot \dfrac{m}{d}$.

Demonstração:

i) Observe que a congruência $ax \equiv b$ (mod m) é equivalente, para algum $y \in \mathbb{Z}$, a uma equação Diofantina linear $ax + my = b$, admitindo solução quando o mdc(a,m) divide b.

ii) Se d divide b e sendo $X_0 \in \mathbb{Z}$ uma solução particular, com $ax_0 \equiv b$(mod m), ou seja, $ax_0 + my_0 = b$, para algum Y_0 inteiro. Por se tratar de uma EDL, toda solução da congruência $ax \equiv b$ (mod m) são da forma $x = x_0 + \frac{m}{d} \cdot t$,com $t \in \mathbb{Z}$. Escrevendo-se $t = qd + k$, com q, k inteiros e $0 \leq k \leq d - 1$, temos:

$x = x_0 + \frac{m}{d} \cdot t \Rightarrow x = x_0 + \frac{m}{d} \cdot (qd + k) \Rightarrow x = x_0 + mq + \frac{m}{d} \cdot k \equiv x_0 + k \cdot \frac{m}{d}$(mod m).

Além disso, consideremos as soluções: $x = x_0 + e \cdot \frac{m}{d}$, $x = x_0 + f \cdot \frac{m}{d}$, de tal maneira que $x_0 + e \cdot \frac{m}{d} \equiv x_0 + f \cdot \frac{m}{d}$(mod m), com $0 \leq e, f \leq d - 1$, temos:
$e \cdot \frac{m}{d} \equiv f \cdot \frac{m}{d}$ (mod m), desta forma podemos escrever $e \cdot \frac{m}{d} = f \cdot \frac{m}{d} + wm$, com $w \in \mathbb{Z}$. Como $\frac{m}{d} \neq 0$, tem-se: $e = f + wd \equiv f$ (mod m).

De $0 \leq |e - f| \leq d - 1$, conclui-se que $w = 0$ ou $e = f$. Portanto as soluções indicadas são incongruentes módulo m.

Exemplo 5.12 *: Resolver a congruência linear* $9x \equiv 3$*(mod 12).*

Solução: Inicialmente verificamos que d = mdc(9,12) = 3, como d =3 divide b=3, a congruência possui 3 soluções. Pela propriedade P_8, podemos escrever a congruência da seguinte forma: $3x \equiv 1$(mod 4).
Verificamos, por tentativas e erros, a solução particular $X_0 = 3$. As demais soluções incongruentes são: $X_1 = 3 + \frac{12}{3} \Rightarrow X_1 = 7$ e $X_2 = 3 + 2 \cdot \frac{12}{3} \Rightarrow X_2 = 11$.

Exemplo 5.13 *: Resolver a congruência* $2x \equiv 5$*(mod 6).*

Solução: Observe que mdc(2,6) = 2, e 2 não divide 5. Portanto, a congruência não possui solução.

Exemplo 5.14 *: Resolva a equação* $3x \equiv 5$ *(mod 7).*

Solução: O mdc(3,7) =1 e 1 divide 5. A congruência possui solução única. Por tentativas e erros, chega-se a $X_0 = 4$.

Exemplo 5.15 *: Pode o triplo de um número natural deixar resto 14, quando dividido por 18?*

Solução: Sendo x o número procurado, devemos verificar se existe solução para a congruência $3x \equiv 14 \pmod{18}$. Como mdc(3,18) = 3, e 3 não divide 14, concluímos que não há nenhum número natural com tal característica.

Capítulo 6

Aplicações das congruências modulares.

Dentre as várias aplicações da congruência modular, iremos destacar, nesta seção, o famoso *Teorema Chinês dos Restos* e, numa sequência lógica, veremos uma importante aplicação de tal teorema, que é a *Partilha de Senhas*.

O matemático Chinês Sun Tzu Suan Ching, no seu livro "Manual Aritmético do Mestre Sol", escrito provavelmente entre 280 d.C e 483 d.C, enunciou o seguinte problema:
"Temos coisas, mas não sabemos quantas; se as contarmos de três em três, o resto é 2; se as contarmos de cinco em cinco, o resto é 3; se as contarmos de sete em sete, o resto é 2. Quantas coisas temos?"

De acordo com o que aprendemos no capítulo anterior, podemos escrever esse problema utilizando a notação de congruência. Seja x o número de coisas procuradas, tem-se:

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

Observe que a solução desse *sistema de congruências* nos dará o valor de x procurado.

Vejamos alguns exemplos de como resolver sistemas de congruências lineares.

Exemplo 6.1 *: Resolver o sistema* $\begin{cases} x & \equiv 1 \pmod{2} \\ x & \equiv 2 \pmod{3} \\ x & \equiv 4 \pmod{5} \end{cases}$

Solução: Observe que somando 1 a cada uma das congrências, temos que $x+1$ será múltiplo de 2, 3 e 5, pois teremos:
$x+1 \equiv 2 \pmod 2 \Rightarrow x+1 \equiv 0 \pmod 2$
$x+1 \equiv 3 \pmod 3 \Rightarrow x+1 \equiv 0 \pmod 3$
$x+1 \equiv 4 \pmod 5 \Rightarrow x+1 \equiv 0 \pmod 5$

Como 2, 3 e 5 são coprimos dois a dois, a menor solução deverá ser o menor múltiplo comum(mmc) desses números, ou seja, $x + 1 = 30 \Rightarrow x = 29$. As demais soluções desse sistema são da forma $29 + 30K$, com $k \in \mathbb{Z}$.

Exemplo 6.2 *: Resolver o sistema* $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \end{cases}$

Solução: Utilizando a definição de congruência e realizando algumas substituições, podemos encontrar a solução desse sistema. Observe, nesse caso, que não dá pra resolver o sistema utilizando o mesmo raciocínio do exemplo anterior. Assim, tem-se:
$x \equiv 1 \pmod 3 \Rightarrow x = 3k_1 + 1$ e $x \equiv 2 \pmod 5 \Rightarrow x = 5k_2 + 2$, com $k_1, K_2 \in \mathbb{Z}$.
Substituindo $x = 5k_2 + 2$ na congruência $x \equiv 1 \pmod 3$, temos: $5k_2 + 2 \equiv 1 \pmod 3 \Leftrightarrow 2k_2 + 2 \equiv 1 \pmod 3$, pois $5 \equiv 2 \pmod 3$.
Assim, $2k_2 + 2 \equiv 1 \pmod 3 \Leftrightarrow 2k_2 \equiv -1 \pmod 3 \Leftrightarrow 2k_2 \equiv 2 \pmod 3 \Leftrightarrow k_2 \equiv 1 \pmod 3 \Rightarrow k_2 = 3k_3 + 1$, para $k_3 \in \mathbb{Z}$. Observe que utilizamos o fato de $-1 \equiv 2 \pmod 3$, para facilitar a resolução.

Desta forma, $x = 5k_2 + 2 = 5(3k_3 + 1) + 2 \Rightarrow x = 15k_3 + 7$. Como:

i) $x = 15k_3 + 7 = 3 \cdot 5k_3 + 2 \cdot 3 + 1 = 3 \cdot (5k_3 + 2) + 1$, temos que x é congruente a 1 mod 3.

ii) $x = 15k_3 + 7 = 5 \cdot 3k_3 + 5 \cdot 1 + 2 = 5 \cdot (3k_3 + 1) + 2$, temos que x é congruente a 2 mod 5.

Logo, as soluções desse sistema são da forma $x = 15k_3 + 7$, com $k_3 \in \mathbb{Z}$.

Observação 6.1 *: Poderíamos resolver esse último sistema, transformando-o numa EDL. Partindo de* $x = 3k_1 + 1$ *e* $x = 5k_2 + 2$*, e igualando as sentenças, temos:*
$3k_1 + 1 = 5k_2 + 2 \Rightarrow 3k_1 - 5k_2 = 1$*(EDL). Utilizando as técnicas de resolução dessas equações, chega-se à mesma solução.*

6.1 Teorema Chinês dos Restos (TCR)

O sistema de congruências lineares:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Com mdc(m_i, m_j)[1] = 1, para $i \neq j$, possui uma *única* solução módulo $M = m_1 \cdot m_2 \cdot m_3 \cdot ... \cdot m_k$. Tal solução pode ser obtida como segue:

$$x = M_1 x_1 a_1 + M_2 x_2 a_2 + ... + M_k x_k a_k$$

,
onde $M_i = \dfrac{M}{m_i}$ e x_i é solução de $M_i X \equiv 1 (\text{mod } m_i)$, $i = 1, ..., k$.

Demonstração:
Existência:
Vamos provar que x é uma solução simultânea do sistema. De fato, como m_i divide M_j, se $i \neq j$, e $M_i x_i \equiv 1 \pmod{m_i}$, segue:
$x = M_1 x_1 a_1 + M_2 x_2 a_2 + ... + M_k x_k a_k \equiv M_i x_i a_i \equiv a_i (\text{ mod } m_i)$.
Unicidade:
Seja $x^{'}$ uma outra solução do sistema, então $x \equiv a_r \pmod{m_r} \equiv x^{'} (\text{mod } m_r)$, com r = 1, 2, 3, 4, ..., k. Sendo assim, m_r divide $\left(x–x^{'}\right)$, basta observar a definição de congruência. Mas mdc$(m_i, m_j) = 1 \Rightarrow (M = m_1 \cdot m_2 \cdot \ldots \cdot m_k)$ divide $\left(x–x^{'}\right)$, ou seja, M divide $\left(x–x^{'}\right)$ e $x \equiv x^{'} (\text{mod M})$.

Exemplo 6.3 *: Resolver os sistemas de congruências:*

a) $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{11} \end{cases}$

Solução: Observamos que o sistema tem solução, pois mdc(5,7) = mdc(5,11) = mdc(7,11) = 1. Sejam, m_1, m_2 e m_3, respectivamente 5, 7 e 11. Então, $m = 5 \cdot 7 \cdot 11 = 385$. Considere: $M_1 = 77$, $M_2 = 55$ e $M_3 = 35$.
Para determinar as soluções desse sistema, devemos encontrar as menores soluções positivas de :
$77x_1 \equiv 1$ (mod 5) , $55x_2 \equiv 1$ (mod 7) e $35x_3 \equiv 1$ (mod 11). Levando em consideração que $77 \equiv 2 \pmod 5$, $55 \equiv 6 \pmod 7$ e $35 \equiv 2 \pmod{11}$, devemos resolver as congruências:
$2x_1 \equiv 1$ (mod 5)$\Rightarrow x_1 = 3$
$6x_2 \equiv 1$(mod 7)$\Rightarrow x_2 = 6$
$2x_3 \equiv 1$(mod 11)$\Rightarrow x_3 = 6$
Logo, a solução do sistema será dada por:
$x \equiv 3 \cdot 77 \cdot 3 + 5 \cdot 55 \cdot 6 + 7 \cdot 35 \cdot 6$ (mod 385)$\Rightarrow x \equiv 3813 \pmod{385}$, como $3813 \equiv 348$

[1]Nesta seção, estaremos interessados na resolução de sistemas lineares em que m_i e m_j são coprimos, pois nem sempre há solução quando esta característica não ocorre.

(mod 385), temos que a menor solução positiva desse sistema é 348, e as demais soluções são da forma $348 + 385K$, com $K \in \mathbb{Z}$.

b) $\begin{cases} 3x & \equiv 1 \pmod 7 \\ 5x & \equiv 2 \pmod{11} \\ 4x & \equiv 3 \pmod{13} \end{cases}$

Solução: Inicialmente verificamos que mdc(7, 11) = mdc(7,13) = mdc(11,13) = 1. Desta maneira, o sistema tem solução. Levemos em consideração que:
$3x \equiv 1 \pmod 7 \Leftrightarrow x \equiv 5 \pmod 7$
$5x \equiv 2 \pmod{11} \Leftrightarrow x \equiv 7 \pmod{11}$
$4x \equiv 3 \pmod{13} \Leftrightarrow x \equiv 4 \pmod{13}$
Assim, o sistema inicial é equivalente ao sistema $\begin{cases} x & \equiv 5 \pmod 7 \\ x & \equiv 7 \pmod{11} \\ x & \equiv 4 \pmod{13} \end{cases}$. Pelo (TCR), temos:
$m = 7 \cdot 11 \cdot 13 = 1001$, com $M_1 = 143$, $M_2 = 91$ e $M_3 = 77$, e :
$143x_1 \equiv 1 \pmod 7 \Leftrightarrow 3x_1 \equiv 1 \pmod 7 \Rightarrow x_1 = 5$.
$91x_2 \equiv 1 \pmod{11} \Leftrightarrow 3x_2 \equiv 1 \pmod{11} \Rightarrow x_2 = 4$.
$77x_3 \equiv 1 \pmod{13} \Leftrightarrow 12x_3 \equiv 1 \pmod{13} \Rightarrow x_3 = 12$.

Logo, a solução do sistema será dada por: $x \equiv 5 \cdot 143 \cdot 5 + 7 \cdot 91 \cdot 4 + 4 \cdot 77 \cdot 12 \pmod{1001} \Rightarrow x \equiv 9819 \pmod{1001}$, como $9819 \equiv 810 \pmod{1001}$, temos que a menor solução positiva do sistema é 810, e as demais soluções são da forma $810 + 1001K$, com $K \in \mathbb{Z}$.

Exemplo 6.4 *: Um camponês tem um 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:

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

onde x representa o número de ovos do camponês.
Como mdc(3,4) = mdc(3,5) = mdc(4,5) =1, temos, pelo TCR:
$m = 3 \cdot 4 \cdot 5 = 60$ e $M_1 = 20$, $M_2 = 15$ e $M_3 = 12$. Devemos resolver as congruências:
$20x_1 \equiv 1 \pmod 3 \Leftrightarrow 2x_1 \equiv 1 \pmod 3 \Rightarrow x_1 = 2$.

$15x_2 \equiv 1 \pmod 4 \Leftrightarrow 3x_2 \equiv 1 \pmod 4 \Rightarrow x_2 = 3$.
$12x_3 \equiv 1 \pmod 5 \Leftrightarrow 2x_3 \equiv 1 \pmod 5 \Rightarrow x_3 = 3$.
Assim, $x \equiv 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 \pmod{60} \Rightarrow x \equiv 238 \pmod{60} \Rightarrow x \equiv 58 \pmod{60}$.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.

6.2 Partilha de senhas

Os cofres de bancos e empresas de valores utilizam, para maior segurança, senhas para a abertura dos mesmos. Acontece que estas senhas não são entregues a uma única pessoa, pois assim, ficaria um pouco mais fácil para um assaltante descobrir tal pessoa e consequentemente a senha. Elas são distribuídas entre um determinado número de funcionários, escolhidos dentre os funcionários da empresa, sendo que a abertura do cofre fica condicionada à presença de um determinado número desses, ou seja, cada um deles recebe parte da senha. Este método utilizado pelos bancos para a escolha de senhas é denominado *Partilha de senhas.*Trata-se de uma importante aplicação do TCR,com a finalidade de distribuir uma *senha* s, entre k ou mais pessoas escolhidas de um conjunto S, composto por n pares de números inteiros positivos, de forma que de cada inteiro positivo $k \leq n$ previamente escolhidos, tem-se que:

- Qualquer subconjunto de S com k elementos permite determinar facilmente s.
- É muito difícil determinar s conhecendo menos que k elementos de S.

6.2.1 Como funciona a Partilha de senhas?

Antes de verificar o funcionamento da partilha de senhas, vamos definir alguns importantes conceitos.

Definição 3 *:(Limiar de um conjunto)Sejam $\mathbb{L}$ um conjunto de n inteiros positivos, dois a dois coprimos, N o produto dos k menores elementos de $\mathbb{L}$ e M o produto dos $k-1$ maiores elementos de $\mathbb{L}$.Diz-se que o conjunto $\mathbb{L}$ tem limiar k se $M < s < N$, onde s é a senha que se quer partilhar entre n pessoas e que poderá ser escolhida como sendo qualquer inteiro no intervalo citado.*

Exemplo 6.5 *: Seja $\mathbb{L} = \{5, 11, 13, 17, 19\}$, verificar se este conjunto possui limiar 2.*

Solução: Seja $k = 2$, temos:
$N = 5 \cdot 11 = 55$, o produto dos $k = 2$ menores elementos de $\mathbb{L}$.

$M = 19$, o produto dos $k-1$ elementos de $\mathbb{L}$.
Como $M = 19 < N = 55$, temos que o conjunto possui limiar 2, e a senha s pode ser escolhida no intervalo $19 < s < 55$.

Exemplo 6.6 *: Seja* $\mathbb{L} = \{11, 13, 17, 19, 23, 31\}$*, verificar se este conjunto possui limiar 3.*

Solução: $N = 11 \cdot 13 \cdot 17 = 2431$, o produto dos $k = 3$ menores elementos de $\mathbb{L}$.
$M = 23 \cdot 31 = 713$, o produto dos $k - 1 = 2$ elementos de $\mathbb{L}$.
Como $M = 713 < N = 2431$, temos que o conjunto possui limiar 3, e a senha s pode ser escolhida no intervalo $713 < s < 2431$.

Observação 6.2 *: Observe que a escolha dos elementos do conjunto* $\mathbb{L}$ *é que torna possível a escolha do limiar* k *de acordo com as definições.*

Exemplo 6.7 *: Seja* $\mathbb{L} = \{3, 5, 11, 13, 17, 19, \}$*, verificar se este conjunto possui limiar 3.*

Solução: $N = 3 \cdot 5 \cdot 11 = 165$, o produto dos $k = 3$ menores elementos de $\mathbb{L}$.
$M = 17 \cdot 19 = 323$, o produto dos $k - 1 = 2$ elementos de $\mathbb{L}$.
Observe que $M = 323 > N = 165$, portanto o conjunto não possui limiar 3.

Definição 4 *(Conjunto gerador de senhas): Seja* $\mathbb{L}$ *um conjunto de n inteiros positivos, dois a dois coprimos, e com limiar* k*. Definimos o conjunto S, conjunto gerador de senhas, que será constituído pelos pares da forma* (p, s_p)*, onde* $p \in \mathbb{L}$ *e* s_p *é a forma reduzida de* $s (mod\ p)$*.*

Exemplo 6.8 *: No exemplo 6.3, escolhendo a senha 43, no intervalo* $19 < s < 55$*, temos:*

Solução: $S = \{(5, 3), (11, 10), (13, 4), (17, 9), (19, 5)\}$.Visto que:
$43 \equiv 3 (\text{mod } 5)$; $43 \equiv 10 (\text{mod } 11)$;$43 \equiv 4 (\text{mod } 13)$;$43 \equiv 9 (\text{mod } 17)$;$43 \equiv 5 (\text{mod } 19)$.

Observação 6.3 *: Um limite* $k \geq 2$ *implica em* $s > p$ *para qualquer* $p \in \mathbb{L}$*. Logo* $s_p < s$ *para qualquer* $p \in \mathbb{L}$*.*

Observação 6.4 *: Supondo que sejam conhecidos, em um dado momento,* $t \geq k$ *pares de elementos de S,ou seja, existem t pessoas presentes para decifrar uma senha s. Denota-se esses pares por* $(p_1, s_1), (p_2, s_2), ..., (p_t, s_t)$ *e* $S = \{(p_1, s_1), (p_2, s_2), ..., (p_t, s_t)\}$.

Sendo assim, para se chegar a senha s é necessário resolver o seguinte sistema de congruências:

$$\begin{cases} x & \equiv s_1 \pmod{p_1} \\ x & \equiv s_2 \pmod{p_2} \\ x & \equiv s_3 \pmod{p_3} \\ \vdots & \\ x & \equiv s_t \pmod{p_t} \end{cases}$$

Observe que pelo TCR, obtém-se x_0 como solução, tal que :
$x_0 \equiv s \pmod{p_1,p_2,...,p_t}$.

Observação 6.5 *: Como $t \geq k$, temos $(p_1 \cdot p_2 \cdot ... \cdot p_t) \geq N > k$, e o sistema acima tem uma única solução menor que $(p_1 \cdot p_2 \cdot ... \cdot p_t)$.*

Exemplo 6.9 *: No banco "PROFMAT BANK" há 5 funcionários responsáveis pela manutenção da senha de um cofre, e pelo menos 2 pessoas ($k = 2$) têm que estar presentes para a abertura do mesmo.Vamos determinar uma senha s, e verificar como dois funcionários fariam para abrir o cofre deste banco.*

Solução: Vamos definir um conjunto $\mathbb{L}$ composto de elementos que são números primos relativamente pequenos, assim, $\mathbb{L} = \{7, 11, 13, 17, 19\}$.
De acordo com a definição, vamos determinar os valores de N e M.
$N = 7 \cdot 11 = 77$ e $M = 19$. Portanto, a senha s deverá ser escolhida no intervalo $19 < s < 77$. Vamos escolher a senha de valor 60.
Desta forma, temos o conjunto $S = \{(7, 4), (11, 5), (13, 8), (17, 9), (19, 3)\}$.
Escolhendo os funcionários que possuem as senhas (7,4) e (13,8), basta resolver o sistema de congruências lineares: $\begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 8 \pmod{13} \end{cases}$

Pelo TCR:
$m = 7 \cdot 13$; $M_1 = 91 \div 7 = 13$;$M_2 = 91 \div 13 = 7$. Assim:
$13x_1 \equiv 1 (\text{mod } 7) \Leftrightarrow 6x_1 \equiv 1 (\text{mod } 7) \Rightarrow x_1 = 6$.
$7x_2 \equiv 1 (\text{mod } 13) \Rightarrow x_2 = 2$.
Sendo assim, $x \equiv 4 \cdot 6 \cdot 13 + 8 \cdot 7 \cdot 2 \pmod{91} \Rightarrow x \equiv 424 (\text{mod } 91) \Rightarrow x \equiv 60 (\text{mod } 91)$.
Assim, verifica-se que $x_0 = 60$ é o menor valor inteiro positivo congruente a x que é a senha correta.

Exemplo 6.10 *: Como duas pessoas só sabem guardar um segredo se uma delas já estiver morta, o "PROFMAT BANK" resolveu fazer uma mudança completa no esquema de segurança e a senha foi trocada, além disso ficou estabelecido que estejam presentes, no mínimo, 3 pessoas para que o cofre possa ser aberto. Três funcionários estão com as chaves (11,3), (17,11) e (21,6). Qual é a senha?*

Solução: Devemos resolver o sistema de congruências lineares: $\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 11 \pmod{17} \\ x \equiv 6 \pmod{21} \end{cases}$

Pelo TCR:
$m = 11 \cdot 17 \cdot 21 = 3927$; $M_1 = 3927 \div 11 = 357$; $M_2 = 3927 \div 17 = 231$;
$M_3 = 3927 \div 21 = 187$

Assim:
$357x_1 \equiv 1(\text{mod } 11) \Leftrightarrow 5x_1 \equiv 1(\text{mod } 11) \Rightarrow x_1 = 9.$
$231x_2 \equiv 1(\text{mod } 17) \Leftrightarrow 10x_2 \equiv 1(\text{mod } 17) \Rightarrow x_2 = 12.$
$187x_3 \equiv 1(\text{mod } 21) \Leftrightarrow 18x_3 \equiv 1(\text{mod } 21) \Rightarrow x_3 = 10.$
Sendo assim, $x \equiv 3 \cdot 357 \cdot 9 + 11 \cdot 231 \cdot 12 + 6 \cdot 187 \cdot 10 \ (\text{mod } 3927) \Rightarrow x \equiv 51351(\text{mod } 3927) \Rightarrow x \equiv 300(\text{mod } 3927)$.

Verificamos que $x_0 = 300$ é o menor valor inteiro positivo congruente a x. Portanto,a senha desse cofre é $s = 300$.

Referências Bibliográficas

[1] HEFEZ, Abramo. *Iniciação à Aritmética-Programa de Iniciação Científica OBMEP*, Ed. da SBM, Rio de Janeiro-RJ,2012.

[2] COUTINHO, S. C. *Criptografia-Programa de Iniciação Científica OBMEP*, Ed. da SBM, Rio de Janeiro-RJ, 2008.

[3] HEFEZ, Abramo. *Elementos de Aritmética-Coleção Textos Universitários*, Ed. da SBM, Rio de Janeiro-RJ, 2. ed. 2011.

[4] *Banco de Questões 2010*, SBM, IMPA.

[5] FONSECA,Rubens Vilhena. *Teoria dos Números*, UEPA, BELÉM- PA.

[6] COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Série de Computação e Matemática n. 2, IMPA, Rio de Janeiro-RJ, 2005.

[7] WIKIPÉDIA, A ENCICLOPÉDIA LIVRE.

[8] SANTOS, José Plynio de Oliveira. *Introdução à Teoria dos Números*, Ed. do IMPA, Rio de Janeiro-RJ, 3. ed., 2010.

[9] FOMIN, D.; GENKIN, S.; ITENBERG, I.*Círculos Matemáticos - A experiência Russa*, Ed. do IMPA, Rio de Janeiro - RJ, 2010.