UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
PROGRAMA DE MESTRADO PROFISSIONAL EM
MATEMÁTICA EM REDE NACIONAL - PROFMAT

SIDMAR BEZERRA DOS PRAZERES

O Teorema Chinês dos Restos e a Partilha de Senhas

RECIFE-PE
JUNHO de 2014

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

O Teorema Chinês dos Restos e a Partilha de Senhas

Dissertação apresentada como exigência para o obtenção do título de Mestre em Matemática apresentado à Universidade Federal Rural de Pernambuco.

Autor: Sidmar Bezerra dos Prazeres
Orientador: Prof° Rodrigo José Gondim Neves

RECIFE-PE
16 de Junho de 2014

Agradecimentos

A DEUS, por estar presente em todos os momentos da minha vida.

Ao Professor Dr. Rodrigo José Gondim Neves, pelo trabalho de orientação, desenvolvido com muita dedicação, paciência e acima tudo a amizade.

À minha esposa e filhos, que me deram forças em todos os momentos desta longa jornada sempre me apoiando e acima tudo tendo paciência nos momentos mais difíceis.

A meus pais que sempre caminharam juntos comigo em todos os passos da minha vida.

Aos amigos do Mestrado pela amizade e companheirismo.

Ao corpo docente do programa do ProfMat, pelos conhecimentos e experiência repassados a mim.

DEDICATÓRIA

Dedico este trabalho aos meus filhos
na esperança que um dia leiam este trabalho.

Epígrafe

A grande glória da vida não é não cair nunca,
mas sim levantar todas as vezes em que caímos.
Nelson Mandela

RESUMO

Este trabalho tem como objetivo mostrar ao leitor a importância de alguns tópicos da Teoria dos Números. Trabalharemos aqui, além de pré-requisitos (Algoritmo de Euclides, Divisibilidade, Máximo Divisor Comum), conteúdos como Equações Diofantinas Lineares, Congruências e o principal tema, que é o poderoso Teorema Chinês dos Restos, apresentando suas teorias, importâncias, aplicabilidade no dia a dia e sua a utilidade na Teoria dos Números. A principal aplicabilidade do Teorema Chinês apresentada neste trabalho é a Partilha de Senhas. Esta partilha de senhas é um mecanismo de segurança, onde uma certa quantidade de pessoas tomam posse de uma chave de acesso sem a possibilidade de obter a senha principal com a sua própria chave.

Palavras-Chave: Algoritmo de Euclides, Teorema Chinês dos Restos, Equações Diofantinas, Partilha de Senhas.

ABSTRACT

This paper aims to show the reader the importance of some topics of Number Theory. Work here, and prerequisites (Euclid Algorithms, Divisibility, Maxim Common Divisor), content with Linear Diophantine equations, congruences, and the main theme, which is the mighty Chinese Remainder Theorem of presenting their theories, importance, applicability on the day and its usefulness in the Theory of Numbers. The main applicability of Chinese Remainder Theorem of this work is Sharing Passwords. Sharing of passwords is a security mechanism, where a certain amount of people take possession of a key to access the secret without the possibility of obtaining the secret with his own key.

Keyword: Euclidean Algorithm, Chinese Remainder Theorem, Diophantine equations, Sharing Passwords.

Sumário

Capítulo 1

INTRODUÇÃO

Apresentaremos alguns tópicos da Teoria dos Números, tais como Máximo Divisor Comum, Algoritmo de Euclides, Congruências, Teorema Chinês dos Restos e uma grande aplicação deste último, que é a partilha de senhas. Grandes matemáticos contribuiram nestes tópicos. Dentre eles, podemos destacar Euclides, Diofanto de Alexandria, Sun Zi.

Sobre Euclides, é dasapontador mas pouco se sabe sobre a vida e a personalidade de Euclides, salvo que foi ele, segundo parece, o criador da famosa e duradoura escola de matemática de Alexandria da qual, sem dúvida, foi professor. Desconhecem-se também a data e o local de seu nascimento, mas é provável que sua formação matemática tenha se dado na escola platônica de Atenas. Sua fama repousa principalmente sobre o seus *Elementos*. Esta obra era composta por treze livros, dos quais os seis primeiros versam sobre a Geometria Plana elementar, os três seguintes sobre a Teoria dos Números, o livro X sobre incomensuráveis e os três últimos sobre Geometria Espacial. Não há introdução ou preâmbulo, e o primeiro livro começa com uma lista de vinte e três definições. Tão logo, este trabalho apareceu, ganhou o mais alto respeito dos sucessores de Euclides até os tempos modernos. A mera citação do número de um livro e o de uma proposição de sua obra-prima é suficiente para identificar um teorema ou construção particular. Nenhum trabalho, exceto a Bíblia, foi tão largamente usado ou estudado e, provavelmente nenhum exerceu influência maior no pensamento científico.

Diofanto de Alexandria já usava e trabalhava as equações diofantinas em pleno século 3 d.C., tendo uma importância enorme para o desenvolvimento da álgebra e uma grande influência sobre os europeus que posteriormente se dedicaram à Teoria dos Números. Nada se sabe com certeza acerca da nacionalidade de Diofanto e nem tampouco da época em que viveu. A maioria dos historiadores, tendem a situá-lo no século 3 de nossa era. Além do fato de que sua carreira floresceu em Alexandria, nada mais de certo se sabe sobre ele. Ele escreveu três trabalhos: *Aritmética*, o mais importante, do qual remanesceram seis dos treze livros; *Sobre*

Números Poligonais do qual restou apenas um fragmento; e *Porismas*, que se perdeu.

> A *Aritmética* é uma abordagem analítica da teoria algébrica dos números que eleva o autor à condição de gênio em seu campo. A parte remanescente do trabalho se dedica à resolução de 130 problemas, numa variedade considerável, que levam a equações de primeiro e de segundo graus. Apenas uma cúbica muito particular é resolvida. O primeiro livro se ocupa de equações determinadas em uma incógnita e os demais de equações indeterminadas de segundo grau, e às vezes de grau maior. É notável a falta de métodos gerais e a aplicação repetida de artifícios engenhosos ideados para as necessidades de cada problema específico. Diofanto só admitia respostas entre números racionais positivos e, na maioria dos casos, se satisfazia com uma resposta apenas do problema. Sobre a vida pessoal de Diofanto, tudo que se sabe está contido no seguinte sumário de um epitáfio que aparece na *Antologia Grega:* **Diofanto passou** $1/6$ **de sua vida como criança,** $1/12$ **como adolescente e mais** $1/7$ **na condição de solteiro. Cinco anos depois de se casar, nasceu-lhe um filho que morreu** 4 **anos antes de seu pai, com metade da idade (final) de seu pai. Com quantos anos Diofanto morreu?** [3]

Entre os anos de 287 d.C. e 473 d.C. o matemático Sun Zi escreveu o Manual Aritmético SUNZI SUANJING, composto por três livros, onde definiu medidas para o comprimento, área e volume, para o peso de vários objetos; utilizou métodos iguais aos de hoje para somar duas frações (regra da cruz); descreveu um algoritmo para obter a raiz quadrada e construiu um calendário que levantou alguns problemas relacionados com a congruência de números, o que o levou à criação de um dos mais famosos teoremas na Teoria dos Números, o Teorema Chinês dos Restos, no qual está situado no terceiro capítulo. Este capítulo continha 36 problemas de aritmética com a 1° versão do Teorema Chinês do Resto, no qual foi desenvolvido para solucionar problemas de astronomia.

Eis alguns problemas da época que envolvem as equações diofantinas e o famoso Teorema Chinês dos Restos:

Exemplo 1: Distribuindo-se 100 buschels[1] de grãos entre 100 pessoas de modo que cada homem receba 3 buschels, cada mulher 2 e cada criança 1/2 buschels, quantos são os homens, quantas as mulheres e quantas as crianças?

[1]Na Inglaterra 1 buschel = 36,367 litros.

Exemplo 2: Qual é o número que deixa restos 2, 3 e 2 quando dividido, respectivamente por 3, 5 e 7? Problema proposto por Sun-Tsu no primeiro século de nossa era.

Exemplo 3: O Teorema Chinês tem numerosas aplicações. Na época, talvez uma delas tenha sido a maneira como os generais chineses a utilizaram para a contagem de seus soldados:
Alinhem-se em fileiras de 7!!!
Alinhem-se em fileiras de 11!!!
Alinhem-se em fileiras de 13!!!
Contando somente os soldados que ficavam nas filas incompletas, os generais inteligentes podiam saber o número exato de seus efetivos.

Alguns exercícios que envolvem o Teorema Chinês dos Restos são de fácil resolução e neste caso não se faz necessário a utilização do Teorema. Veja alguns exemplos:

Exercício 1.0.1 *Um fogueteiro produziu fogos de artifício e aos colocá-los em* 3 *caixas percebeu que sobrava um fogos de artifício e quando separou em* 5 *caixas também sobrava um. Quantos fogos de artifício sobrarão se colocá-los em* 15 *caixas?*

Solução: Este é um dos casos mais simples. Um número que é dividido por 3 e por 5, ele pode ser dividido por 15. No caso, como o resto é 1 na divisão por 3 e 5, então este número é um múltiplo de 3 somado com uma unidade, o mesmo acontecendo na divisão por 5, no caso um múltiplo de 5 somado com uma unidade. Podemos concluir que antecessor deste número quando dividido por 3 e por 5, deixará resto zero, isto é, é um múltiplo de 3 e 5. Logo, o antecessor será múltiplo de 15 e portanto o número que dividido por 3 ou por 5 deixa resto 1, também deixará resto 1 na divisão por 15.

Exercício 1.0.2 *Um número inteiro positivo quando dividido por* 5 *deixa resto* 4 *e quando dividido* 7 *por deixa resto* 6*. Ao dividir este número por* 35*, qual será o seu resto?*

Solução: Neste caso, sendo n um número natural, temos que n quando dividido por 5 deixa resto 4 e quando dividido por 7 deixa resto 6. Assim, podemos deduzir que o sucessor de n é múltiplo de 7 e de 5, ou seja, $n + 1$ será múltiplo de 35. Então os possiveis valores para n são $34, 79, 104, ...$ Então o resto da divisão destes números por 35 é igual 34.

Exercício 1.0.3 *Um camponês tem um certo número de ovos; quandos os divide por* 3*, sobra-lhe* 1*; quando os divide por* 4*, sobram* 2 *ovos; e quando os divide por* 5*, sobram* 3*. Qual a quantidade mínima de ovos que o camponês possui?*

Solução: Seja n a quantidade mínima de ovos deste camponês. De acordo com a situação do problema, teremos que n é um múltiplo de 3 adicionado de uma unidade, n é um múltiplo de 4 adicionado de 2 unidades e um múltiplo de 5 adicionado de 3 unidades. Observe que se adiocionarmos 2 unidades ao número n, este será múltiplo simultaneamente de 3, 4 e 5. Logo, $n + 2$ é múltiplo de $3.4.5 = 60$. Conclui-se então que o valor mínimo de $n + 2$ é 60. Portanto n será 58.

Nestes três exercícios, a resolução foi feita utilizando a técnica de somar um inteiro k ao inteiro n, tornado assim as divisões exatas. Todos os problemas que envolvem esta idéia apresentada nestes três exercícios, pode ser utilizada esta técnica. O problema é que em alguns exercícios, encontrar este valor inteiro k não é uma das tarefas mais fáceis. Por exemplo, acompanhe este exercício:

Exercício 1.0.4 *: Um número inteiro positivo n quando dividido por* 7 *deixa resto* 3 *e quando dividido por* 11 *deixa resto* 5*. Qual o resto da divisão deste número por* 77*?*

Aqui, temos n é da forma $n = 7k + 3$ e $n = 11k + 5$. Qual o valor de k devemos somar a n para que $n + k$ seja múltiplo de 7 e 11. Encontrar este k pode ser muito difícil e demorar muito tempo, assim como em outros problemas. Então, para resolver este tipo de problema, teremos que aplicar o Teorema Chinês dos Restos, que será visto nos capítulos seguintes.

Capítulo 2

ARITMÉTICA DE NÚMEROS INTEIROS

"Deus criou os inteiros. Tudo o mais é trabalho do Homem".
Leopold Kronecker,1823-1891

2.1 Divisibilidade

Dados dois números inteiros a e b, com $a \neq 0$, diremos que a divide b, escrevendo $a|b$, quando existir $c \in \mathbb{Z}$ tal que $b = ac$. Diremos, neste caso, que a é um divisor de b ou b é um múltiplo de a. Caso, não exista, escreveremos $a \nmid b$.

Proposição 2.1.1 *Sejam $a, b \in \mathbb{Z}$ e $c \in \mathbb{Z}^*$. Tem-se que:*
(i) $1|c, a|a$ e $a|0$;
(ii) Se $a|b$ e $b|c$, então $a|c$;
(iii) Se $a|b$ e $b|a$, então $|a| = |b|$;
(iv) Se $a|b$ e $a|c$, então $a|(b + c)$.

Demonstração:
(i) De fato, das igualdades $c.1 = c, a = a.1$ e $0 = a.0$, teremos que $1|c, a|a$ e $a|0$.
(ii) $a|b$ e $b|c$ implica na existência de $f, g \in \mathbb{Z}$ tal que $b = f.a$ e $c = g.b$. Substituindo o valor de b na segunda expressão teremos: $c = g.(f.a) = (f.g).a$, o que implica em que $c = k.a$. Logo, $a|c$.
(iii) Suponha que $a|b$ e $b|a$. Então existem $k_1, k_2 \in \mathbb{Z}$ tais que $b = a.k_1$ e $a = k_2.b$. Segue-se então que $b = k_2.b.k_1$. Assim, teremos que $k_1.k_2 = 1$. Portanto, teremos que $k_1 = k_2 = 1$ ou $k_1 = k_2 = -1$. Se $k_1 = k_2 = 1$, tem-se que $a = b$ e se $k_1 = k_2 = -1$, tem-se $a = -b$. Logo, conclui-se que $|a| = |b|$.
(iv) Suponha que $a|b$ e $a|c$. Então, existem $x, y \in \mathbb{Z}$, tais que $b = ax$ e $c = ay$. Como $a|a(x + y)$, então teremos que $a|(b + c)$.

Proposição 2.1.2 *Se $a, b, c, d \in \mathbb{Z}$, com $a \neq 0$ e $c \neq 0$, então $a|b$ e $c|d$ implica em $ac|bd$.*

Demonstração: Sejam $a, b, c, d \in \mathbb{Z}$ tais que $a|b$ e $c|d$. Logo, existem $m, n \in \mathbb{Z}$, tais que $b = ma$ e $d = nc$. Sendo a, c não nulos, multiplicando a igualdade $(b = ma)$ por d, teremos $bd = ma.d$. Mas $d = nc$. Substituindo, teremos $bd = ma.nc \Rightarrow bd = (mn).ac$. Logo, bd é um múltiplo de ac. Assim, ac divide bd.

Proposição 2.1.3 *Sendo $a, b, c \in \mathbb{Z}$, se $ac|bc$ então $a|b$, $\forall c \in \mathbb{Z}$ não nulo.*

Demonstração: Pela Lei do corte, temos que supondo $c > 0$ $(c < 0)$, teremos três possibilidades:
(i) Se $a < b$, então $ac < bc$ $(ac > bc)$;
(ii) Se $a > b$, então $ac > bc$ $(ac < bc)$;
(iii) Se $a = b$, então $ac = bc$.
Então, como $ac|bc$, segue-se que existe $y \in \mathbb{Z}$, tal que $bc = ac.y$, ou seja, pela Lei do corte, temos que $b = ay$, isto é, $a|b$.

Proposição 2.1.4 *Sejam $a, b, c \in \mathbb{Z}$ com $a \neq 0$, tais que $a|(b+c)$. Então $a|b$ se e somente se, $a|c$.*

Demonstração: $\Rightarrow$ Suponha que $a|b$. Logo, existe $n \in \mathbb{Z}$ tal que $b = na$. Como $a|(b + c)$, existe $m \in \mathbb{Z}$, tal que $b + c = ma$. Então, segue-se que $na + c = ma$. Daí, teremos que $c = am - an = a(m - n)$. Como $m - n \in \mathbb{Z}$, temos que c é um múltiplo de a. Logo, $a|c$.
$\Leftarrow$ Suponha que $a|c$ e que $a|(b + c)$. então, existem $m, n \in \mathbb{Z}$, tais que $c = ma$ e $b + c = na$. Segue-se que $b + ma = na$ e que $b = (n - m)a$. Logo, $a|b$.

Definição 2.1.1 (Princípio da Boa Ordenação (PBO)) *Todo subconjunto $X \subset \mathbb{N}$ possui um menor elemento. Isto significa que existe um elemento $m_0 \in X$ que é menor que todos os demais elementos do conjunto X.*

2.2 Algoritmo da Divisão

No livro VII de Euclides, encontra-se enunciada a divisão com resto de um número natural por outro, chamada de divisão euclidiana ou algoritmo da Divisão. Neste algoritmo, estamos interessados em encontrar dois números inteiros, denominados, quociente (q) e resto (r), na divisão de dados dois números inteiros quaisquer. Por se tratar de um algoritmo, a entrada são dois números inteiros (dividendo e divisor), a qual vamos chamar de a e b e a saída serão dois outros números inteiros, que denominaremos de q e r.

Teorema 2.2.1 *(Divisão Euclidiana) Sejam a e b números inteiros com $a > b > 0$. Existem únicos números inteiros q e r tais que $a = b.q + r$, com $0 \leq r < b$.*

Demonstração: Provemos a existência. Suponhamos que $b > 0$ e q o maior inteiro tal que $bq \leq a$. Então, teremos que $bq \leq a < b(q+1)$. Segue-se então que $0 \leq a - bq < b$. Definimos $r = a - bq$. Provemos agora, a unicidade. Sejam q, q', r, r' inteiros tais que $a = bq + r$, $a = bq' + r'$ e $0 \leq r, r' < |b|$. Então, teremos que

$$|r - r'| < |b| \qquad e \qquad b(q - q') = r' - r.$$

Suponha que $q \neq q'$. Então, teremos que $1 \leq |q - q'|$. Multiplicando esta desigualdade por $|b|$, teremos

$$|b| \leq |b||q - q'| = |r' - r| < |b|,$$

isto é, $|b| < |b|$, uma contradição. Logo, $q = q'$ e daí, tem-se $r = r'$.

2.3 Algoritmo de Euclides e o Máximo Divisor Comum (MDC)

O Algoritmo de Euclides é um processo no qual utilizamos para calcular o máximo divisor comum entre dois ou mais números inteiros. Ele possui este nome porque se encontra no início do Livro VII dos Elementos de Euclides, embora o processo em si, fosse conhecido muito tempo antes. Enunciado em forma de regra, o algoritmo de Euclides é o seguinte: *Divida o maior dos dois números inteiros positivos pelo menor e então divida o divisor pelo resto. Continue este processo de dividir o último divisor pelo último resto, até que a divisão seja exata. O divisor final é o m.d.c. procurado.*

Exemplo 2.3.1 *Calcular o mdc entre* 2187 *e* 30 *usando o método de Euclides citado acima.*

Quocientes $\rightarrow$		72	1	9
Divisores $\rightarrow$	2187	30	27	3
Restos $\rightarrow$	27	3	0	

Logo, 3 *é o máximo divisor comum entre* 2187 *e* 30*.*

Definição 2.3.1 *Sejam a e b dois números inteiros, não simultaneamente nulos. Sendo $d \in \mathbb{Z}$, dizemos que d é um divisor comum de a e b, quando $d|a$ e $d|b$.*

Por exemplo, 3,4,6 são divisores de 24 e 3,4,6 também são divisores de 72. Logo, 3,4,6 são divisores comuns de 24 e 72. O máximo divisor comum entre dois números inteiros é um número inteiro positivo que possui as seguintes propriedades:
(i) $d|a$ e $d|b$;
(ii) Se $c|a$ e $c|b$, então $c|d$.
Além disso, d é único, pois sendo d' o outro mdc entre a e b, teríamos que $d'|d$ e $d|d'$. Logo, $d = d'$. O mdc entre os números a e b será denotado por (a, b).

Casos Particulares:
(i) $(0, a) = a$;
(ii) $(1, a) = 1$;
(iii) $(a, a) = |a|$;
(iv) Se $a|b$, então $(a, b) = |a|$.

Lema 2.3.1 *(Euclides) Sejam $a, b, n \in \mathbb{Z}$. com $a, b > 0$. Se existe $(a, b - n.a)$, então (a, b) existe e $(a, b) = (a, b - n.a)$.*

Demonstração: Suponha que $(a, b-n.a)$ exista e seja $d = (a, b-n.a)$. Logo, $d|a$ e $d|(b - n.a)$. Como $d|a$, então teremos que $d|b$. Logo, d é um divisor comum de a e b. Seja c um divisor comum entre a e b. Logo, $c|a$ e $c|b$ e $c|(b - n.a)$. Como $d = (a, b-n.a)$, então $c|d$. Logo, $d = (a, b)$. Este Lema de Euclides é bastante útil para calcularmos o mdc entre dois números inteiros.

Algoritmo de Euclides: Sejam $a, b \in \mathbb{N}$. Podemos supor, sem perda de generalidade, que $a < b$. Se $a = 1$ ou $a|b$, então $(a, b) = a$. Suponhamos que $1 < a < b$ e que $a \nmid b$. Logo, pela divisão euclidiana, teremos:
$b = aq_1 + r_1$, com $0 < r_1 < a$. Teremos, então duas possibilidades:
(i) $r_1|a$, e nesse caso, $(a, b) = (a, b - q_1a) = (a, r_1) = (a, r_1) = r_1$ e termina o algoritmo, ou
(ii) $r_1 \nmid a$ e nesse caso efetuamos a divisão de a por r_1, obtendo $a = r_1q_2 + r_2$, com $0 < r_2 < r_1$. Neste caso, teremos novamente duas possibilidades:
(i') $r_2|r_1$ e em tal caso $(a, b) = (r_1, a) = (r_1, a - r_1q_2) = (r_1, r_2) = r_2$, ou,
(ii') $r_2 \nmid r_1$ e nesse caso recomeça o algoritmo.
Este procedimento não continua indefinidamente, pois teremos que $a > r_1 > r_2 > ... > r_n \geq 0$, que não possui menor elemento contrariando o Princípio da Boa Ordem.

Exemplo 2.3.2 *Calculemos o mdc entre* 330 *e* 240.

Solução:
$330 = 240.1 + 90$

$240 = 90.2 + 60$
$90 = 60.1 + 30$
$60 = 30.2 + 0$
Logo, $(330, 240) = 30$, isto é, $(330, 240) = (240, 90) = (90, 60) = (60, 30) = 30$.

Exemplo 2.3.3 *Dados $a, m \in \mathbb{N}$, com $a > 1$, provar que* $\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (a - 1, m)$.

Solução:
Seja $d = \left(\frac{a^m - 1}{a - 1}, a - 1\right)$. Temos que:

$$\frac{a^m - 1}{a - 1} = a^{m-1} + a^{m-2} + ... + a + 1 = (a^{m-1} - 1) + (a^{m-2} - 1) + ... + (a - 1) + (1 - 1) + m$$

Logo, como $(a - 1)|(a^m - 1)$, teremos $(a - 1)\left|\left[\frac{a^m - 1}{a - 1} - m\right]\right. \Rightarrow \frac{a^m - 1}{a - 1} - m = (a - 1).q \Rightarrow m = \frac{a^m - 1}{a - 1} - (a - 1)q$. Pelo Lema de Euclides, segue-se que $\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (m, a - 1)$.

Quando $(a, b) = d$ e queremos escrever d em função dos inteiros a *e* b, utilizamos o Algoritmo de Euclides Estendido.

Teorema 2.3.1 *(Algoritmo de Euclides Estendido) Dados $a, b \in \mathbb{Z}$ e seja $d = (a, b)$. Então existem $x_0, y_0 \in \mathbb{Z}$, tais que $ax_0 + by_0 = d$.*

Demonstração: Considere o conjunto com todas as combinações lineares $ax + by$ com $x, y \in \mathbb{Z}$. Este conjunto contêm números negativos, positivos e também o zero. Vamos escolher uma combinação linear tais que $c = ax_0 + by_0$ seja o menor inteiro positivo pertencente a este conjunto. Primeiro, vamos provar que $c|a$ e $c|b$. Suponha que $c \nmid a$. Então, pela Divisão Euclidiana, existem q e r, tal que $a = cq + r$, isto é, $r = a - cq$, com $0 < r < c$. Assim, teremos que:

$$r = a - cq = a - (ax_0 + by_0)q = a(1 - qx_0) + b(qy_0).$$

Isto mostra que r também é uma combinação linear entre a e b. Mas isto é uma contradição, pois como $0 < r < c$ e tomamos c como o menor elemento positivo do conjunto. Logo, $c|a$. De maneira análoga, provamos que $c|b$. Como d é o máximo divisor comum entre a e b, então $c|d$ e existem $k_1, k_2 \in \mathbb{Z}$, tais que $a = dk_1$ e $b = dk_2$. Segue-se que, $c = ax_0 + by_0 = dk_1x_0 + dk_2y_0 = d(k_1x_0 + k_2y_0)$, o que implica que $d|c$. Mas isso, no dá que $d \leq c$. Como $c, d > 0$ e $d < c$ não é

possivel, pois tomamos c como o menor elemento positivo, conclui-se $c = d$. Logo, $d = ax_0 + by_0$.

Dados os inteiros a e b, diremos que eles são *coprimos* quando o máximo divisor comum entre eles é igual a 1.

Proposição 2.3.1 *Dados $a, b \in \mathbb{Z}^*$, então* $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

Demonstração: Se $(a, b) = 1$, então a afirmação segue diretamente. Suponha que a e b não sejam coprimos, isto é, $(a, b) = k$, com $1 \neq k \in \mathbb{Z}^*$. Então, pelo algoritmo estendido de Euclides, existem x_0, y_0, tais que $ax_0 + by_0 = k$. Suponha que $\left(\frac{a}{k}, \frac{b}{k}\right) = d$. Então, segue-se que $k = (a, b) = \left(k.\frac{a}{k}, k.\frac{b}{k}\right) = k.d$. Logo, teremos que $d = 1$.

Proposição 2.3.2 *Suponha $a, b, c \in \mathbb{Z}$, com $c \neq 0$. Se $(a, b) = 1$ e $a|bc$, então $a|c$.*

Demonstração: Como $(a, b) = 1$, pelo Algoritmo de Euclides Estendido, existem $x, y \in \mathbb{Z}$, tais que $ax + by = 1$. Multiplicando a equação por $c \neq 0$, tem-se que $acx + bcy = c$. Temos que $a|ac$ e por hipótese $a|bc$. Logo, $a|(acx + bcy)$. Segue-se então que $a|c$, isto é, quando $(a, b) = 1$, temos que $a \nmid b$ e se $a|bc$, então $a|c$.

Proposição 2.3.3 *Sejam $x, y, a \in \mathbb{Z}$. Se $(x, y) = 1$, então $(x, ay) = (x, a)$.*

Demonstração: Seja $d = (x, ay)$. Então $d|x$ e $d|ay$, o que implica em $x = d.k$ e $ay = dt$, para $k, t \in \mathbb{Z}$. Como $(x, y) = 1$, pelo algoritmo estendido de Euclides, existem x_0, y_0, tais que $xx_0 + yy_0 = 1$. Multiplicando por a, teremos $a.xx_0 + a.yy_0 = a$. Segue-se que $a.dk.x_0 + a.dt.y_0 = a \Rightarrow d.(ak.x_0 + aty_0) = a$, ou seja $d|a$. Conclui-se, então que como $d|x$ e $d|a$, então $d = (a, x)$, como queríamos provar.

Lema 2.3.2 *Sejam $a, b, c \in \mathbb{Z}$ não nulos. Então, se $(b, c) = 1$, então $(a, bc) = (a, c).(a, b)$.*

Demonstração: Seja $d = (a, b)$. Então, teremos que existem inteiros x, y tais que $dx = a$ e $dy = b$, com $(x, y) = 1$. Daí, segue-se:
$(a, bc) = (dx, dyc) = d(x, yc) = d(x, c) = (a, b).(x, c)$. Mas $d|b$ e $(b, c) = 1$ implica em $(d, c) = 1$. Assim, segue-se que $(a, c) = (dx, c) = (x, c)$. Logo, $(a, bc) = (a, c).(a, b)$.

Proposição 2.3.4 *Sejam $a, m, n \in \mathbb{Z}$, tais que $(m, n) = 1$. Então:*

$$(a, mn) = 1 \Longleftrightarrow (a, m) = 1 = (a, n)$$

Demonstração: Sendo $(m, n) = 1$, segue pelo Lema anterior, que $(a, mn) = (a, m).(a, n)$. Logo, $(a, m).(a, n) = 1$. Como (a, n) e (a, m) são inteiros positivos, então teremos que $(a, n) = (a, m) = 1$. Reciprocamente, se $(a, m) = 1 = (a, n)$ e pelo Lema anterior temos $(a, mn) = (a, m).(a, n)$, o resultado segue.

2.4 Mínimo Múltiplo Comum (MMC)

Dados $a, m \in \mathbb{Z}^*$, diremos que m é um múltiplo de a, quando $a|m$, isto é, existe $y \in \mathbb{Z}$, tal que $m = y.a$. Diremos também, que dados $a, b, m \in \mathbb{Z}^*$, m é múltiplo comum de a e b, quando $a|m$ e $b|m$. Em qualquer caso, ab e 0(zero) são múltiplos de a e b.

Definição 2.4.1 *Diremos que um número inteiro m é o mínimo múltiplo comum entre inteiros a e b, quando m possuir as seguintes propriedades:*
(i) $a|m$ e $b|m$;
(ii) Se $c \in \mathbb{Z}$ é um múltiplo comum entre a e b, teremos que $m|c$, isto é, $m \leq c$.

De fato, se c e m são os mínimos múltiplos comuns entre a e b, então por (ii), teremos que $c|m$ e $m|c$, logo, teremos que $m \leq c$ e $c \leq m$. Logo, $m = c$. Vamos denotar o mínimo múltiplo comum entre a e b por $[a, b]$.

Teorema 2.4.1 *Dados $m, a, b \in \mathbb{Z}^*$, temos que $[a, b]$ existe e $[a, b].(a, b) = ab$.*

Demonstração: Vamos definir $m = \dfrac{ab}{(a, b)}$. Queremos provar que $m = [a, b]$. Podemos escrever m da seguinte forma: $m = a.\dfrac{b}{(a, b)}$ ou $m = b.\dfrac{a}{(a, b)}$. Daí, temos que $a|m$ e $b|m$. Seja $c \in \mathbb{Z}$, um múltiplo comum entre a e b. Logo, $a|c$ e $b|c$ e existe $n_1, n_2 \in \mathbb{Z}$, tal que $c = an_1$ e $c = bn_2$. Segue-se então que:
$n_1.\dfrac{a}{(a, b)} = n_2.\dfrac{b}{(a, b)}$ que pela **Proposição 2.3.1**, sabemos que $\left(\dfrac{a}{(a, b)}, \dfrac{b}{(a, b)}\right) = 1$. Logo, $\dfrac{a}{(a, b)}$ divide n_2, isto é, $\dfrac{a}{(a, b)}.b$ divide $n_2.b$. Logo, $m = b.\dfrac{a}{(a, b)}$ divide $n_2.b$ e portanto m divide c. Assim, m é o menor dos múltiplos entre a e b. Logo, m é igual ao mínimo múltiplo comum entre a e b, ou seja, $m = [a, b]$.

Proposição 2.4.1 *Sejam $a, b \in \mathbb{Z}$. Então* $\left(\dfrac{[a, b]}{a}, \dfrac{[a, b]}{b}\right) = 1$

Demonstração: Pela **Proposição 2.3.1**, sabemos que $\left(\dfrac{a}{(a, b)}, \dfrac{b}{(a, b)}\right) = 1$. Então, como $[a, b].(a, b) = ab$, teremos:
$1 = \left(\dfrac{a}{(a, b)}, \dfrac{b}{(a, b)}\right) = \left(\dfrac{a}{\frac{ab}{[a,b]}}, \dfrac{b}{\frac{ab}{[a,b]}}\right) = \left(\dfrac{[a, b]}{b}, \dfrac{[a, b]}{a}\right)$, como queríamos provar.

Proposição 2.4.2 *Sejam $k, s, a, b \in \mathbb{Z}^*$. Então* $\dfrac{ka}{(k, s)} = \dfrac{sb}{(k, s)} = [a, b]$.

Demonstração: Suponha que $\frac{ka}{(k,s)} = \frac{sb}{(k,s)} = T$. Queremos provar que $T = [a,b]$. Pela proposição anterior, sabemos que $\left(\frac{[a,b]}{a}, \frac{[a,b]}{b}\right) = 1$. Multiplicando por (k,s), vamos obter:
$\left(\frac{[a,b].(k,s)}{a}, \frac{[a,b].(k,s)}{b}\right) = (k,s) \Rightarrow \left(\frac{[a,b]}{a}.\frac{ka}{T}, \frac{[a,b]}{b}.\frac{sb}{T}\right) = (k,s) \Rightarrow$
$\left(\frac{[a,b]}{T}.k, \frac{[a,b]}{T}.s\right) = (k,s) \Rightarrow \frac{[a,b]}{T}.(k,s) = (k,s) \Rightarrow [a,b] = T.$

Proposição 2.4.3 *Se $(a,b) = 1$, $a|(m-n)$ e $b|(m-n)$, então $[a,b]|(m-n)$.*

Sabemos que $[a,b].(a,b) = ab$. Como $(a,b) = 1$, então segue-se que $[a,b] = ab$. Por hipótese, temos que $a|(m-n)$ e $b|(m-n)$. Então, existe $k, s \in \mathbb{Z}$, tal que $(m-n) = ka$ e $(m-n) = sb$, o que concluimos que $ka = sb$. Mas, pela proposição anterior, sabemos que $\frac{ka}{(k,s)} = \frac{sb}{(k,s)} = [a,b]$. Logo, teremos que $ka = sb = m - n = [a,b].(k,s)$, isto é, $[a,b]|(m-n)$.

2.5 Equações Diofantinas Lineares

Denomina-se de equações diofantinas às equações polinomiais com coeficientes inteiros, no qual o principal objetivo são as soluções inteiras.
Exemplos:
(i) $3x + 4y = 7$;
(ii) $2x - 5y = 2$;
(iii) $x^2 - 5y^2 = 1$ (Equação de Pell-Fermat)
(iv) $3x + 5y - 7z = 1$.

Então, dada uma equação diofantina, é natural formular as seguintes perguntas:
(a) A equação sempre admite solução?
(b) Caso haja solução, quantas são e como encontrá-las?

Exemplo 2.5.1 *Verifique se a equação $2x + 6y = 13$ possui solução inteira.*

Solução: Observe que os fatores $2x$ e $6y$ resultam em números pares. Logo, a soma deles também terá que ser um número par e não ímpar como no exemplo dado. Portanto, a equação não admite solução inteira.

Para responder a pergunta (a), vamos enunciar o seguinte teorema:

Teorema 2.5.1 *Seja $a, b, c \in \mathbb{Z}$, com $a, b \neq 0$. A equação $ax + by = c$, admite solução, se e somente se $(a,b)|c$.*

Demonstração: $\Rightarrow$ Suponha que a equação $ax+by=c$ admita a solução (x_0, y_0). Segue-se então que $ax_0 + by_0 = c$. Sabemos que $(a,b)|a$ e $(a,b)|b$. Logo, $(a,b)|ax_0$ e $(a,b)|by_0$. Segue-se que $(a,b)|(ax_0 + by_0)$. Logo, $(a,b)|c$.
$\Leftarrow$ Suponha que $(a,b)|c$. Então existe $t \in \mathbb{Z}$, tal que $(a,b).t = c$. Pelo Algoritmo de Euclides Estendido, existem inteiros $r, s \in \mathbb{Z}$, tal que $ar + bs = (a,b)$. Segue-se então que $(ar + bs)t = c$, isto é, $art + bst = c$. Sendo $rt = x_0$ e $st = y_0$, temos $ax_0 + by_0 = c$, isto é, a equação $ax + by = c$ admite solução.

Com este Teorema, podemos decidir se a equação diofantina possui ou não solução. Por exemplo,
(a) As equações $3x + 4y = 5$ e $2x + 5y + 6z = 15$ admitem solução inteira, pois $(3,4)|5$ e $(2,5,6)|15$ respectivamente;
(b) Já as equações $2x + 4y = 7$ e $5x - 15y = 7$ não admitem solução inteira, pois $(2,4) \nmid 5$ e $(5,15) \nmid 7$.
Agora, se a equação $ax + by = c$ admite solução, como encontrá-las? Observemos o próximo Teorema:

Teorema 2.5.2 *Considere a equação diofantina $ax + by = c$ e seja (x_0, y_0) uma solução particular. Tem-se que x e y é uma solução da equação se, e somente se $x = x_0 + t.\dfrac{b}{(a,b)}$ e $y = y_0 - t.\dfrac{a}{(a,b)}$, para algum $t \in \mathbb{Z}$.*

Demonstração: Considere a equação $ax + by = c$ e (x_0, y_0) uma solução particular. Então teremos que $ax_0 + by_0 = c$. Teremos que $ax + by = ax_0 + by_0 = c$ Segue-se então que $ax - ax_0 = by_0 - by$, isto é, $a(x - x_0) = b(y_0 - y)$. Dividindo esta equação por (a,b), teremos que:
$\dfrac{a}{(a,b)}.(x-x_0) = \dfrac{b}{(a,b)}.(y_0-y)$. Pela **Proposição 2.3.1**, sabemos que $\left(\dfrac{a}{(a,b)}, \dfrac{b}{(a,b)}\right) = 1$. Logo, teremos que $\dfrac{a}{(a,b)} \nmid \dfrac{b}{(a,b)}$. Assim, $\dfrac{a}{(a,b)}|(y_0 - y)$. Logo, existe $t \in \mathbb{Z}$ tal que $y_0 - y = t.\dfrac{a}{(a,b)}$. Logo, $y = y_0 - t.\dfrac{a}{(a,b)}$. Analogamente, encontramos $x = x_0 + t.\dfrac{b}{(a,b)}$. E reciprocamente, é fácil ver que $y = y_0 - t.\dfrac{a}{(a,b)}$ e $x = x_0 + t.\dfrac{b}{(a,b)}$ são soluções da equação $ax + by = c$.
Note que, se a equação admite solução, então ela possui infinitas soluções.

Exemplo 2.5.2 *Encontrar o conjunto solução da equação $5x+6y = 7$, caso exista.*

Solução: Temos que $(5,6) = 1|7$. Logo, a equação admite infinitas soluções. Pelo teorema anterior $y = y_0 - t.\dfrac{a}{(a,b)}$ e $x = x_0 + t.\dfrac{b}{(a,b)}$ são soluções da equação. Tem-se que $(a,b) = (5,6) = 1$ e $x = x_0 + 6t$ e $y = y_0 - 5t$. Resta agora, encontrar

uma solução particular para esta equação. Observe a equação $5x + 6y = 1$. Vê-se facilmente que, $x = -1$ e $y = 1$ é uma solução particular, isto é, $5.(-1)+6.(1) = 1$. Multiplicando a equação por 7, teremos $5.(-7) + 6.(7) = 7$. Logo, $x = -7$ e $y = 7$ é uma solução particular da equação $5x + 6y = 7$. Então a solução geral desta equação é dada por $x = -7 + 6t$ e $y = 7 - 5t$.

Exemplo 2.5.3 *Retomemos o* ***Exercício 1.0.4*** *do 1° Capítulo.*

Solução: Temos que dado um inteiro n, ele é da forma $n = 7k + 3$ e $n = 11t + 5$. Portanto, teremos que $11t + 5 = 7k + 3 \Rightarrow 7k - 11t = 2$, que é uma equação diofantina, que possui solução, pois $(7, 11) = 1|2$. Vamos determinar uma solução particular para equação $7k - 11t = 1$. Verifica-se facilmente que $t = 5$ e $k = 8$ é uma solução para esta equação, isto é, $7.(8) - 11(5) = 1 \Rightarrow 7.(16) - 11(10) = 2$. Então $t = 10$ e $k = 16$ é uma solução particular para a equação $7k - 11t = 2$. A solução geral é dada por:

$$\begin{matrix} t = 10 + 7a \\ k = 16 + 11a \end{matrix} , a \in \mathbb{Z}.$$

Assim, o valor de n será dado por: $n = 7k + 3 \Rightarrow n = 7(16 + 11a) + 3 \Rightarrow n = 115 + 77a = 38 + 77m$. Logo, o menor natural que dividido por 7 deixa resto 3 e quando dividido por 11 deixa resto 5 é 38.

Exemplo 2.5.4 *Determinar o menor número inteiro n que quando dividido por a_1 deixa resto b_1 e quando dividido por a_2 deixa resto b_2, de forma que $(a_1, a_2) = 1$.*

Solução: Temos que o inteiro n é da forma $n = b_1 + a_1q_1$ e $n = b_2 + a_2q_2$. Segue-se que $b_1 + a_1q_1 = b_2 + a_2q_2$, isto é, $a_1q_1 - a_2q_2 = b_2 - b_1$, que é uma equação diofantina, com variáveis q_1, q_2. Como $(a_1, a_2) = 1|(b_2 - b_1)$, temos que esta equação possui solução. Seja (k, s) uma solução particular da equação $a_1q_1 - a_2q_2 = b_2 - b_1$, isto é, $q_1 = k$ e $q_2 = s$. Então a solução geral desta equação é dada por $q_1 = k + a_2t$ e $q_2 = s + a_1t$. Então o menor inteiro que satisfaz estas condições é:
$n = b_1 + a_1q_1 = b_1 + a_1(k + a_2t) \Rightarrow n = b_1 + a_1k + a_1a_2t$.

Exemplo 2.5.5 *Um general decide dividir seu batalhão em colunas de 31 soldados e percebe que sobram 4; então tentou dividí-los em colunas de 50 soldados cada, desta vez sobrou um único soldado. Determine o número de soldados deste batalhão sabendo que tal número é menor que 1500.*

Solução:
Seja n o número de soldados. Equacionando o problema, teremos que $n = 31s + 4$ e $n = 50t + 1$. Portanto, teremos que $31s + 4 = 50t + 1$, isto é, $50t - 31s = 3$. Temos aqui, uma equação diofantina. Observe que $(50, 31) = 1|3$. Logo, esta equação possui solução. Considere a equação $50t - 31s = 1$. Usando o algoritmo

de Euclides, teremos:
$50 = 31.1 + 19 \Rightarrow 19 = 50 - 31.1$
$31 = 19.1 + 12 \Rightarrow 12 = 31 - 19.1$
$19 = 12.1 + 7 \Rightarrow 7 = 19 - 12.1$
$12 = 7.1 + 5 \Rightarrow 5 = 12 - 7.1$
$7 = 5.1 + 2 \Rightarrow 2 = 7 - 5.1$
$5 = 2.2+1 \Rightarrow 1 = 5-2.2$. Segue-se então que $1 = 5-2.(7-5.1) = (-2).7+3.5 = (-2).7 + 3.(12 - 7.1) = 3.12 - 5.7 = 3.12 - 5.(19 - 12.1) = (-5).19 + 8.12 = (-5).19+8.(31-19.1) = 8.31-13.19 = 8.31-13.(50-31.1) = 50.(-13)-31.(-21)$
Logo, teremos que $50(-13) - 31(-21) = 1$, $t = -39$ e $s = -63$ é uma solução particular da equação $50t - 31s = 3$ e portanto teremos que a solução geral desta equação é dada por:
$t = -39 + 31k$ e $s = -63 + 50k$. Segue-se então que o número de soldados é dado por $n = 50t+1 = 50(-39+31k)+1 = 50(-39+62+31k)+1 = 50(23+31k')+1 = 1151 + 31k'$. Então número de soldados é 1151.

2.6 Problemas Resolvidos

Problema 2.6.1 *O resto da divisão do inteiro N por 20 é 8. Qual o resto da divisão de N por 5?*

Solução: Como o resto da divisão de N por 20 é igual a 8, então N é um múltiplo de 20 adicionado de 8 unidades. Ao dividir N por 5, basta analisar o resto da divisão de 8 por 5, pois 20 já é divisível por 5. Segue-se que o resto da divisão de N por 5 será de 3.

Problema 2.6.2 *Determine uma solução inteira a, b, c tais que* $\dfrac{65}{273} = \dfrac{a}{3}+\dfrac{b}{7}+\dfrac{c}{13}$.

Solução: Temos que $\dfrac{65}{273} = \dfrac{a}{3}+\dfrac{b}{7}+\dfrac{c}{13}$ pode ser escrito da seguinte forma: $\dfrac{65}{273} = \dfrac{91a}{273} + \dfrac{39b}{273} + \dfrac{21c}{273}$, isto é, $91a + 39b + 21c = 65$. Basta agora, encontrar a solução inteira desta equação diofantina linear. Observe que $(91, 39, 21) = 1|65$. Logo, a equação possui solução. Temos que $91a+39b+21c = 65 \Rightarrow 91a+3(13b+7c) = 65$. Tomemos $13b+7c = k$, com $k \in \mathbb{Z}$. Segue-se então que $91a+3k = 65$. Resolvendo esta equação diofantina, teremos que a solução é dada por $a = 2+3t$ e $k = -39-91t$ com $t \in \mathbb{Z}$ e $a = 2, k = -39$ uma solução particular da equação $91a + 3k = 65$. Vamos determinar agora, valores para os inteiros b e c. Sabemos que $13b+7c = k$. tome $k = -39$. Então, teremos a equação diofantina $13b+7c = -39$. Uma solução particular para esta equação é dada por $b = 4$ e $c = -13$. A solução geral para a equação $13b + 7c = -39$ é dada por $b = 4 + 7s$ e $c = -13 - 13s$, com $s \in \mathbb{Z}$.

Conclui-se que um dos possíveis valores para a, b, c são respectivamente $2, 4, -13$, isto é, $\frac{65}{273} = \frac{2}{3} + \frac{4}{7} - \frac{13}{13}$, como queríamos mostrar.

Problema 2.6.3 *(OBM-1999) Quantos são os pares (x, y) de inteiros positivos que satisfazem a equação $2x + 3y = 101$?*
a) 13 *b)* 14 *c)* 15 *d)* 16 *e)* 17

Solução: Uma solução particular da equação é o par ordenado $(49, 1)$. Segue-se então que a solução geral desta equação é dada por $x = 49 + 3t$ e $y = 1 - 2t$, com $t \in \mathbb{Z}$. Estamos interessados nas soluções inteiras positivas, isto é, $x, y > 0$. Então, teremos que:

$$x > 0 \Rightarrow 49 + 3t > 0 \Rightarrow t > \frac{-49}{3} = -16,33$$

$$y > 0 \Rightarrow 1 - 2t > 0 \Rightarrow t < \frac{1}{2} = 0,5.$$

Segue-se que os possíveis valores para t são $0, -1, -2, -3, -4, \cdots, -16$, portanto são 17 possíveis valores para t. Conclui-se que a equação $2x + 3y = 101$ possui 17 soluções inteiras positivas, portanto altenativa (e).

Problema 2.6.4 *Ache o menor múltiplo de* 5 *que deixa resto* 2 *quando dividido* 3 *e por* 4.

Solução: Seja n o número procurado. Equacionando o problema, teremos: $\begin{cases} n = 3t + 2 \\ n = 4s + 2 \end{cases}$. Subtraindo 2 unidades de cada equação, teremos que $n - 2$ é múltiplo de 3 e 4. Logo, $n - 2$ também é um múltiplo de 12, ou seja $n - 2 = 12k$, $k \in \mathbb{Z}$. Então, segue-se que $n = 12k + 2$. Então, os possíveis valores de n são $2, 14, 26, 38, 50, 62, ...$ Assim, o menor múltiplo de 5 que quando dividido por 3 e por 4 deixa resto 2 é 50.

Problema 2.6.5 *(OBM-1997) Uma das soluções inteiras e positivas da equação $19x + 97y = 1997$ é, evidentemente, $(x_0, y_0) = (100, 1)$. Além dessa, há apenas mais um par de números inteiros e positivos, (x_1, y_1), satisfazendo a equação. O valor de $x_1 + y_1$ é:*
a) 23 *b)* 52 *c)* 54 *d)* 101 *e)* 1997

Solução: Dada a equação $19x + 97y = 1997$ uma solução particular foi dada, no caso $(x_0, y_0) = (100, 1)$. Então, teremos que a solução geral desta equação é da forma: $x = 100 + 97t$ e $y = 1 - 19t$, com $t \in \mathbb{Z}$. Queremos encontar outra solução inteira positiva, isto é, $x_1 > 0, y_1 > 0$. Segue-se então que:

$$x_1 > 0 \Rightarrow 100 + 97t > 0 \Rightarrow t > \frac{-100}{97} = -1,030.$$

$y_1 > 0 \Rightarrow 1 - 19t > 0 \Rightarrow t < \dfrac{1}{19} = 0,052.$

Então os valores para t são 0 e -1. Para $t = 0$, teremos a solução dada. Para $t = -1$, teremos $x = 100 + 97.(-1) = 3$ e $y = 1 - 19.(-1) = 20$. Segue-se que a outra solução é o par ordenado $(20, 3)$, portanto alternativa (a).

Problema 2.6.6 *Para quais valores de c a equação $90x + 28y = c$ não possui solução inteira?*

Solução: Sabemos que uma equação diofantina $ax + by = c$ possui solução inteira se e somente se $(a, b)|c$. No caso, a equação $90x + 28y = c$ possui solução quando $(90, 28) = 2|c$. Assim, os valores de c para que a equação $90x + 28y = c$ tenha solução, é $c = 2n, \forall n \in \mathbb{Z}$.

Problema 2.6.7 *Numa criação de coelhos e galinhas, contaram-se 400 pés. Quantas são as galinhas e quantos são os coelhos, sabendo que a diferença entre esses dois números é a menor possível?*

Solução: Seja g e c o número de galinhas e coelhos respectivamente. Equacionando, teremos $2g + 4c = 400$, que simplificando temos a equação diofantina $g + 2c = 200$. Como $(1, 2) = 1|200$, esta equação diofantina possui solução inteira. Queremos obter valores de g e c tais que a diferença $|g - c|$ seja a menor possível. Uma solução particular da equação $g + 2c = 200$ é $g = 10$ e $c = 95$. Segue-se que a solução geral desta equação é dada por $g = 10 + 2t$ e $c = 95 - t$, com $t \in \mathbb{Z}$. Queremos que $|g - c|$ seja o menor possivel. Segue-se então que $|10 + 2t - (95 - t)| = |3t - 85| > 0 \Rightarrow t > 28,33$ ou $t < 28,33$. Na primeira solução, o menor valor de t é $t = 29$. Logo, o número de galinhas e o número de coelhos são $g = 10 + 2.29 = 68$ e $c = 95 - 29 = 66$, respectivamente. Observando a segunda solução, tomando agora $t = 28$, teremos $g = 10 + 2.28 = 66$ e $c = 95 - 28 = 67$.

Capítulo 3

CONGRUÊNCIAS

3.1 Introdução

Figura 3.1: Gauss foi o grande introdutor da congruência, ele começou a mostrar ao mundo a congruência a partir de um trabalho realizado Disquisitiones Arithmeticae (1801) quando ele tinha apenas 24 anos de idade. Várias ideias usadas na teoria dos números foram introduzidas nesse trabalho, até mesmo o símbolo usado na congruência atualmente foi o que Gauss usou naquela época.

Definição 3.1.1 *Sejam $a, b, m \in \mathbb{Z}$. Dizemos que a é congruente a b módulo m, quando a e b deixa o mesmo resto quando dividido por m. Denotamos por:*

$$a \equiv b \ (m).$$

Caso, a e b não deixem o mesmo resto na divisão por m, então escreveremos $a \not\equiv b \ (m)$.

Exemplos:
(i) $15 \equiv 3\ (2)$;
(ii) $7 \equiv 12\ (5)$;
(iii) $14 \equiv 30\ (4)$.

Proposição 3.1.1 *Suponha que $a, b, m \in \mathbb{Z}$. Tem-se que $a \equiv b\ (m)$ se, e somente se $m|(a-b)$.*

Demonstração: $\Rightarrow$ Suponha que $a \equiv b\ (m)$. Então, a e b deixam o mesmo resto quando divididos por m. Teremos então que:
$\begin{cases} a = mq_1 + r \\ b = mq_2 + r \end{cases} \Longrightarrow a - b = m(q_1 - q_2) + r - r = m(q_1 - q_2).$
Logo, $m|(a-b)$.
$\Leftarrow$ Suponha que $m|(a-b)$. Então existe um $t \in \mathbb{Z}$, tal que $(a-b) = t.m$. Segue-se que $a = tm + b$, isto é, $a \equiv b\ (m)$.

Decorre da definição, que congruências é uma relação de equivalência, pois:
(a) Reflexiva: $a \equiv a\ (m)$;
(b) Simétrica: Se $a \equiv b\ (m)$, então $b \equiv a\ (m)$;
(c) Transitiva: Se $a \equiv b\ (m)$ e $b \equiv c\ (m)$, então $a \equiv c\ (m)$.
De fato, os itens (a) e (b) seguem da definição. Já o item (c), sendo $a \equiv b\ (m)$ e $b \equiv c\ (m)$, teremos $m|(a-b)$ e $m|(b-c)$. Logo, $m|([(a-b)+(b-c)]$, isto é, $m|(a-c)$. Assim, teremos que $a \equiv c\ (m)$.

Note que todo número natural é congruente ao seu resto módulo m. Então, se $a \equiv b\ (m)$, com $b \leq m$, tem-se que b é o resto da divisão de a por m. Neste caso, os possíveis valores para b são os elementos do conjunto $A = \{0, 1, 2, 3, ..., m-1\}$. Este conjunto é denominado de *sistema completo de resíduos módulo m.*

Proposição 3.1.2 *Sejam $a, b, c, d, \in \mathbb{Z}$ e $m \in \mathbb{N}$, com $m > 1$.*
(i) Se $a \equiv b\ (m)$ e $c \equiv d\ (m)$, então $a + c \equiv b + d\ (m)$
(ii) Se $a \equiv b\ (m)$ e $c \equiv d\ (m)$, então $ac \equiv bd\ (m)$
(iii) Se $a \equiv b\ (mn)$, então $a \equiv b\ (m)$ e $a \equiv b\ (n)$.
(iv) Se $a \equiv b\ (m)$ e $a \equiv b\ (n)$, com $(m, n) = 1$, então $a \equiv b\ (mn)$;
(v) Se $ac \equiv bc\ (m)$ e $(c, m) = 1$, então $a \equiv b\ (m)$. [Lei do Corte]

Demonstração: (i) Suponha que $a \equiv b\ (m)$ e $c \equiv d\ (m)$. Então segue-se que $m|(a-b)$ e $m|(c-d)$. Logo, $m|(a-b)+(c-d)$. Daí, segue-se que $m|(a+c)-(b+d)$. Logo, $a + c \equiv b + d\ (m)$.
(ii) Suponha que $a \equiv b\ (m)$ e $c \equiv d\ (m)$. Então segue-se que $m|c.(a-b)$ e $m|b(c-d)$. Então $m|((ca - cb) + (bc - bd))$. Logo, $m|(ca - bd)$. Segue-se que $ac \equiv bd\ (m)$.
(iii) Suponha que $a \equiv b\ (mn)$. Então, pela **Proposição 2.4.3**, teremos que

$mn|(a-b)$. Segue-se que $m|(a-b)$ e $n|(a-b)$, pois $(m,n)=1$. Conclui-se que $a \equiv b\ (m)$ e $a \equiv b\ (n)$.
(iv) Seja $(m,n)=1$ e $a \equiv b\ (m)$ e $a \equiv b\ (n)$. Então, teremos que $[m,n]|(a-b)$, pela **Proposição 2.4.3**. Como $[m,n].(m,n) = mn$ pela **Proposição 2.3.1** e $(m,n)=1$, então teremos que $[m,n]=mn$ e então $mn|(a-b)$. Logo, $a \equiv b\ (mn)$.
(v) Seja $(c,m)=1$ e $ac \equiv bc\ (m)$. Então segue-se da definição que $m|(ac-bc)$. Logo, $m|c(a-b)$. Sendo c, m coprimos, tem-se que $m \nmid c$ e existem $x, y \in \mathbb{Z}$, tais que $cx+my=1$; Multiplicando a equação por $(a-b)$, teremos $c(a-b)x+m(a-b)y = (a-b)$ e usando a **Proposição 2.3.2**, o resultado segue.

Corolário 3.1.1 *Para todo $n \in \mathbb{N}$, tem-se que, se $a \equiv b\ (m)$, então $a^n \equiv b^n\ (m)$.*

Demonstração: Usemos o Princípio de Indução Matemática.
(i) Para $n=1$, teremos $a^1 \equiv b^1\ (m)$, o que é verdadeiro por hipótese.
(ii) Suponha que, se $a \equiv b\ (m)$, então $a^k \equiv b^k\ (m)$ seja verdadeiro para algum $k \in \mathbb{N}$. Então pelo princípio de indução matemática, teremos que $a^n \equiv b^n\ (m)$ é verdadeiro para $n = k+1$. De fato, pois pelo item (ii) da proposição anterior, como $a \equiv b\ (m)$ e $a^k \equiv b^k\ (m)$, então $a^{k+1} \equiv b^{k+1}\ (m)$. Logo, se $a \equiv b\ (m)$, então $a^n \equiv b^n\ (m)$, $\forall n \in \mathbb{N}$.

Exemplo 3.1.1 *Achar o resto da divisão de 7^{10} por 51.*

Solução: Sabemos que $7^2 \equiv -2\ (51)$. Segue-se então que:
$7^2 \equiv -2\ (51) \Rightarrow 7^4 \equiv (-2)^2\ (51) \Rightarrow 7^4 \equiv 4\ (51) \Rightarrow 7^4.7 \equiv 4.7\ (51) \Rightarrow 7^5 \equiv 28\ (51) \Rightarrow (7^5)^2 \equiv 28^2\ (51) \Rightarrow 7^{10} \equiv 19\ (51)$. Logo, o resto da divisão 7^{10} por 51 é 19.

3.2 Congruências Lineares

Nesta secção, vamos abordar as equações e os sistemas de congruências. Vamos verificar se as equações do tipo $ax \equiv b\ (m)$ existe ou não solução inteira, onde a, b, m são inteiros dados, com $a \neq 0$ e $m > 1$.

Definição 3.2.1 *Dizemos que um elemento a é invertível módulo m quando a congruência linear $ax \equiv 1\ (m)$ admite solução. Este inteiro x é denominado inverso de a módulo m.*

Exemplo 3.2.1 *Na equação $3x \equiv 1\ (7)$, se tomarmos $x=5$, teremos que $3.5 = 15 \equiv 1\ (7)$. Então, segue-se que 5 é o inverso de 3 módulo 7. Observe também, que $x = 12, 19, 26$ são outros inversos de 3 módulo 7.*

Assim, para verificar quando a admite inverso módulo m, teremos a seguinte proposição:

Proposição 3.2.1 *Um inteiro a é invertível módulo m se e só se $(a, m) = 1$. Neste caso, quaisquer dois inversos de a módulo m são congruentes módulo m.*

Demonstração: Seja a um inteiro invertível. Então por definição, teremos que $ax \equiv 1\ (m)$ admite solução. Logo, teremos que $m|(ax - 1)$. Segue-se que existe um inteiro y tal que $ax - 1 = my$, isto é, $ax - my = 1$. Temos uma equação diofantina linear, que apenas admite solução quando $(a, m) = 1$. Reciprocamente, se $(a, m) = 1$, pelo Algoritmo de Euclides Estendido, existem inteiros x, y tais que $ax - my = 1$. Logo, $m|(ax - 1)$ e segue-se que $ax \equiv 1\ (m)$. Por fim, sejam x e y inversos de a módulo m. Então teremos que $ax \equiv 1\ \equiv ay\ (m)$. Segue-se que $ax \equiv ay\ (m)$. Como $(a, m) = 1$, pelo item (v) da **Proposição 3.1.2**, teremos $x \equiv y\ (m)$. Assim, a possui um único inverso módulo m.

Corolário 3.2.1 *Sejam $a, m \in \mathbb{Z}$ com $m > 1$ e $(a, m) = d > 1$. Então a equação $ax \equiv 1\ (m)$ não admite solução.*

Demonstração É imediato da **Proposição 3.2.1**

Corolário 3.2.2 *Sejam $a, b, m \in \mathbb{Z}$ com $m > 1$. A congruência $ax \equiv b\ (m)$ admite solução se, e somente se, $(a, m)|b$.*

Demonstração: $\Rightarrow$ Suponha que $ax \equiv b\ (m)$ admita solução. Logo, teremos que $m|ax - b$. Assim, existe $y \in \mathbb{Z}$, tal que $ax - b = my$. Logo, $ax - my = b$. Temos então uma equação diofantina que possui solução quando $(a, m)|b$.
$\Leftarrow$ Sendo $(a, m)|b$, então existem $x, y \in \mathbb{Z}$, tais que $ax + my = b$. Logo, teremos que $b - ax = my$. Assim, $ax \equiv b\ (m)$.

Este corolário nos mostra como determinar se uma equação do tipo $ax \equiv b\ (m)$ admite solução. Mais ainda, podemos transformar a equação $ax \equiv b\ (m)$ em uma equação do tipo $x \equiv c\ (m)$, caso $(a, m) = 1$. Então, admitindo que a equação $ax \equiv b\ (m)$ haja solução, qual será o seu conjunto solução?

Definição 3.2.2 *Dado um inteiro a módulo m, os seus possíveis restos são elementos do conjunto $A = \{0, 1, 2, ..., m - 1\}$. Estes elementos formam um sistema completo de resíduos módulo m.*

Por exemplo, analisando um inteiro módulo 5, teremos que o sistema completo de resíduos é o conjunto $A = \{0, 1, 2, 3, 4\}$ e observe que quaisquer dois elementos deste conjunto são incongruentes módulo 5.

Proposição 3.2.2 *Sejam $a, b, m, d \in \mathbb{Z}$, com $m > 0$. Sendo $(a, m) = d$ e admitindo que $ax \equiv b\ (m)$ haja solução, então $\dfrac{ax}{(a,m)} \equiv \dfrac{b}{(a,m)}\ \left(\dfrac{m}{(a,m)}\right)$.*

Demonstração: Por hipótese, temos que $(a, m)|b$, pois $ax \equiv b\ (m)$ possui solução. Sabemos que $(a, m)|a$ e $(a, m)|m$. Então, existe $y \in \mathbb{Z}$ tal que: $ax \equiv b\ (m) \Leftrightarrow ax + my = b \Leftrightarrow \frac{ax}{(a,m)} + \frac{my}{(a,m)} = \frac{b}{(a,m)} \Leftrightarrow \frac{ax}{(a,m)} \equiv \frac{b}{(a,m)}\ \left(\frac{m}{(a,m)}\right)$, como queríamos mostrar.

Proposição 3.2.3 *Sejam $a, b, m \in \mathbb{Z}$ com $m > 1$ e $d = (a, m)$, tal que $(a, m)|b$. Se x_0 é uma solução da equação $ax \equiv b\ (m)$, então*

$$x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, x_0 + \frac{3m}{d}, ..., x_0 + \frac{(d-1).m}{d}$$

formam um sistema de soluções incongruentes módulo d.

Demonstração: Considere a congruência: $ax \equiv b\ (m)^{(*)}$. Como $(a, m)|b$, então a congruência (*) admite solução. Seja x_0 uma solução particular. Logo, existe y_0, tal que (x_0, y_0) é uma solução particular da equação diofantina $ax_0 - my_0 = b$. Segue-se que a solução geral será dada por:

$$x = x_0 + m\frac{t}{d} \text{ e } y = y_0 + a\frac{t}{d},\ \forall t \in \mathbb{Z}.$$

Portanto, toda solução da congruência (*) é do tipo $x = x_0 + t\frac{m}{d}$, $\forall t \in \mathbb{Z}$. Assim, tomando $t = 0, 1, 2, ..., (d-1)$, teremos as seguintes soluções módulo m: $x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, x_0 + 3\frac{m}{d}, ..., x_0 + (d-1)\frac{m}{d}$, como queríamos mostrar. Provemos agora, que $x_0 + i.\frac{m}{d}$ e $x_0 + j.\frac{m}{d}$ são incongruentes módulo m, para $i \neq j$, com $i, j \in \{0, 1, 2, ..., d-1\}$. Sejam $x_0 + i.\frac{m}{d}$ e $x_0 + j.\frac{m}{d}$ soluções da congruência $ax \equiv b\ (m)$. Segue-se então que:
$x_0 + i.\frac{m}{d} \equiv x_0 + j.\frac{m}{d} \Rightarrow i.\frac{m}{d} \equiv j.\frac{m}{d}\ (m)$. Como $\frac{m}{d}|m$, dividindo $i.\frac{m}{d} \equiv j.\frac{m}{d}\ (m)$ por $\frac{m}{d}$, proposição anterior, vamos obter $i \equiv j\ (m/\frac{m}{d}) \Rightarrow i \equiv j\ (d) \Rightarrow i = j$. Conclui-se então que $x_0 + i.\frac{m}{d}$ e $x_0 + j.\frac{m}{d}$ são incongruentes módulo d, para $i \neq j$, com $i, j \in \{0, 1, 2, ..., d-1\}$. É imediato desta proposição que o número de soluções incongruentes da congruência $ax \equiv b\ (m)$ é $(a, m) = d$.

3.3 Sistemas de Congruências Lineares

Quando temos um grupo de equações de congruências, no qual queremos obter uma solução que satisfaça estas equações, teremos um sistema de congruências. Vamos considerar inicialmente, o caso de um sistema de congruências com duas

equações $\begin{cases} x \equiv a\ (m) \\ x \equiv b\ (n) \end{cases}$, com $(m,n) = d$. Provaremos a seguir, que este sistema admite solução única módulo o mínimo múliplo comum entre m, n e é bastante útil na resolução do Teorema Chinês dos Restos, no caso em que $(m,n) = 1$. Para provar a proposição seguinte, vamos mostrar o seguinte lema:

Lema 3.3.1 *Sejam* $a, b, m, n, d \in \mathbb{Z}$, *tais que* $(*)$ $\begin{cases} x \equiv a\ (m) \\ x \equiv b\ (n) \end{cases}$ *e* $(m,n) = d$. *Este sistema admite solução, se e só se* $(m,n)|(b-a)$.

Demonstração: Observando o sistema (*), vamos verificar quando ele admite solução. A primeira equação admite solução se e só se $m|(x-a)$, isto é, $x = a+my$, com $y \in \mathbb{Z}$. Substituindo o valor x na segunda equação, teremos:
$a + my \equiv b\ (n) \Rightarrow my \equiv b - a\ (n)$. Esta congruência possui solução se e só se $(m,n)|(b-a)$.

Proposição 3.3.1 *Sejam* $a, b, m, n, d \in \mathbb{Z}$, *tais que o sistema* $(*)$ $\begin{cases} x \equiv a\ (m) \\ x \equiv b\ (n) \end{cases}$ *admita solução e* $(m,n) = d$. *Então, esta solução será única módulo* $mmc(m,n)$.

Demonstração: Como o sistema (*) possui solução, temos que $(m,n)|(b-a)$. Da primeira equação, teremos que existe $y \in \mathbb{Z}$, tal que $x = a + my$. Substituindo x na segunda equação, teremos $a + my \equiv b\ (n) \Rightarrow my \equiv b - a\ (n)$. Então teremos que $my \equiv b - a\ (n) \Rightarrow \left(\frac{my}{(m,n)}\right) \equiv \frac{b-a}{(m,n)}\ \left(\frac{n}{(m,n)}\right)$, pela **Proposição 3.2.3**. Sabemos que $\left(\frac{m}{(m,n)}, \frac{n}{(m,n)}\right) = 1$, pela **Proposição 2.3.1**. Logo, existe $k \in \mathbb{Z}$, tal que $k.\left(\frac{m}{(m,n)}\right) \equiv 1\ \left(\frac{n}{(m,n)}\right)$. Assim, teremos que $y \equiv \frac{k(b-a)}{(m,n)}\ \left(\frac{n}{(m,n)}\right) \Rightarrow y = \frac{k(b-a)}{(m,n)} + t.\left(\frac{n}{(m,n)}\right)$. Segue-se, então que:
$x = a+m.\left(\frac{k(b-a)}{(m,n)} + t.\left(\frac{n}{(m,n)}\right)\right) \Rightarrow x = a+\left(\frac{mk(b-a)}{(m,n)} + \left(\frac{mnt}{(m,n)}\right)\right)$. Pela **Proposição 2.3.1** $[m,n].(m,n) = mn$, onde $[m,n]$ é o mínimo múltiplo comum entre m e n. Conclui-se então que:
$x = a+\left(\frac{mk(b-a)}{(m,n)} + [m,n].t\right) \Rightarrow x \equiv a+\left(\frac{mk(b-a)}{(m,n)}\right)([m,n])$. Logo, o sistema (*) admite solução única módulo $[m,n]$.

Corolário 3.3.1 *Sejam* $a, b, m, n \in \mathbb{Z}$, *tais que* $\begin{cases} x \equiv a\ (m) \\ x \equiv b\ (n) \end{cases}$ *e* $(m,n) = 1$. *Então, este sistema de congruências admite solução e esta solução é única módulo* mn.

Demonstração: Tomando $d = 1$ na proposição anterior, o resultado segue.

Exemplo 3.3.1 *Um número inteiro deixa resto 3 quando dividido por 7 e deixa resto 5 quando dividido por 8. Determine o menor número inteiro positivo com estas condições.*

Solução 1: Observe que $(7, 8)|(5 - 3)$. Logo, o sistema admite solução. Seja x o número procurado. Então teremos o sistema:
$\begin{cases} x \equiv 3\ (7) \\ x \equiv 5\ (8) \end{cases}$ Resolvendo o sistema:
$x \equiv 3\ (7) \Rightarrow x = 3 + 7t$, com $t \in \mathbb{Z}$. Substituindo o valor de x na segunda congruência, vamos obter:
$x \equiv 5\ (8) \Rightarrow 3 + 7t \equiv 5\ (8) \Rightarrow 7t \equiv 2\ (8) \Rightarrow 49t \equiv 14\ (8) \Rightarrow t \equiv 6\ (8)$. Logo, teremos que $t = 6 + 8s$, com $s \in \mathbb{Z}$. Substituindo o valor de t em $x = 3 + 7t$, teremos $x = 3 + 7.(6 + 8s) = 45 + 56s$. Logo, o menor natural que deixa resto 3 quando dividido por 7 e deixa resto 5 quando dividido por 8 é 45.

Solução 2: Usando o **Corolário 3.3.1** cuja solução deste tipo de sistema é dada por $x \equiv a + my_1(b - a)\ (mn)$, tem-se que $a = 2,\ b = 6,\ m = 7,\ n = 8$ *e* y_1 é de tal forma que $y_1 m \equiv 1\ (n)$, isto é, $7y_1 \equiv 1\ (8)$, o que implica em $y_1 = 7$. Daí, segue-se que $x \equiv 3 + 7.7(5 - 3)\ (56) \Rightarrow x \equiv 101\ (56) \Rightarrow x \equiv 45\ (56)$.

O exemplo a seguir, ilustra um sistema de congruências quando $(m, n) = d \geq 1$.

Exemplo 3.3.2 *Um número natural quando dividido por 6 deixa resto 4 e quando dividido por 10 deixa resto 8. Determine o menor número natural com estas condições.*

Solução: Equacionando o problema, sendo x o número procurado, teremos o seguinte sistema de congruências: $\begin{cases} x \equiv 4\ (6) \\ x \equiv 8\ (10) \end{cases}$. Observe que o $(6, 10) = 2 \geq 1$.
Da primeira equação, teremos que $x = 4 + 6t$, com $t \in \mathbb{Z}$. Substituindo na segunda equação, teremos que: $4 + 6t \equiv 8\ (10) \Rightarrow 6t \equiv 4\ (10) \Rightarrow 3t \equiv 2\ (5) \Rightarrow t \equiv 4\ (5) \Rightarrow t = 4 + 5k$, com $k \in \mathbb{Z}$. Logo, teremos que $x = 4 + 6(4 + 5k) = 28 + 30k$. Assim, o menor número que quando dividido por 6 deixa resto 4 e quando dividido por 10 deixa resto 8 é 28. Observe que a solução é única módulo o $mmc(6, 10) = 30$.

Exemplo 3.3.3 *Determine o menor inteiro positivo que satisfaça o sistema de congruências a seguir:*
$\begin{cases} x \equiv 1\ (5) \\ x \equiv 2\ (7) \\ x \equiv 3\ (9) \\ x \equiv 4\ (11) \end{cases}$

Solução: Multiplicando cada equação do sistema por 2, vamos obter:

$$\begin{cases} 2x \equiv 2\ (5) \\ 2x \equiv 4\ (7) \\ 2x \equiv 6\ (9) \\ 2x \equiv 8\ (11) \end{cases} \Rightarrow \begin{cases} 2x = 2 + 5t \\ 2x = 4 + 7t \\ 2x = 6 + 9t \\ 2x = 8 + 11t \end{cases}$$

Somando-se três unidades a cada equação, teremos:

$$\begin{cases} 2x + 3 = 2 + 3 + 5t \\ 2x + 3 = 4 + 3 + 7t \\ 2x + 3 = 6 + 3 + 9t \\ 2x + 3 = 8 + 3 + 11t \end{cases} \Rightarrow \begin{cases} 2x + 3 = 5t' \\ 2x + 3 = 7t' \\ 2x + 3 = 9t' \\ 2x + 3 = 11t' \end{cases} \Rightarrow 2x + 3 = 3465k,\ k, t, t' \in \mathbb{Z}$$

Logo, o menor inteiro que satisfaz o sistema é $2x + 3 = 3465 \Rightarrow x = 1731$.

3.4 Teorema Chinês dos Restos

Na seção anterior, vimos como resolver um sistema do congruências lineares com duas equações. O que se pode dizer de um sistema que possui k equações? Será que tal sistema sempre admitirá solução? Caso afirmativo, a solução também será única? O Teorema Chinês dos Restos é uma generalização para estes sistemas de congruências. Ele examina a existência de soluções e mostra também que a solução é única, módulo o produto dos modulandos, desde que esses sejam dois a dois coprimos. O Teorema a seguir, mostra uma solução geral de um sistema de congruências lineares. Para o melhor entendimento, considere este exemplo:

Exemplo 3.4.1 *Qual o menor natural que dividido por 7 deixa resto 3 e quando dividido por 6 deixa resto 5?*

Solução: Equacionando o problema, teremos o seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv 3\ (7) \\ x \equiv 5\ (6) \end{cases}$$

.

Sejam x_1, x_2 inteiros tais que $x = x_1 + x_2$, onde $\begin{cases} x_1 \equiv 3\ (7) \\ x_1 \equiv 0\ (6) \end{cases}$ e $\begin{cases} x_2 \equiv 0\ (7) \\ x_2 \equiv 5\ (6) \end{cases}$.

Observe que $x_1 = 6t_1$ e $x_2 = 7t_2$. Logo, a solução é dada por $x = x_1 + x_2 = 6t_1 + 7t_2$. Resta agora encontrar os valores de t_1 e t_2. Como $x_1 \equiv 3\ (7)$, então segue-se que $6t_1 \equiv 3\ (7) \Rightarrow 36t_1 \equiv 18\ (7) \Rightarrow t_1 \equiv 4\ (7)$. Logo, $t_1 = 4 + 7k_1$. Analogamente, como $x_2 \equiv 5\ (6)$, então segue-se que $7t_2 \equiv 5\ (6) \Rightarrow t_2 \equiv 5\ (6)$. Logo, $t_2 = 5 + 6k_2$. Achados $t_1 = 4 + 7k_1$ e $t_2 = 5 + 6k_2$, substituindo na equação $x = 6t_1 + 7t_2$, teremos:

$x = 6(4 + 7k_1) + 7(5 + 6k_2) = 59 + 42(k_1 + k_2) = 17 + 42k$. Logo, a solução deste sistema será $x = 17 + 42k$. Então o menor inteiro que dividido por 6 deixa resto 5 e quando dividido por 7 deixa resto 3 é 17.

Observe que na resolução deste problema, particionamos a solução x em duas partes ($x = x_1 + x_2$). Este procedimento é perfeitamente correto, pois pela **Proposição 3.1.2**, temos que se $a \equiv b\ (m)$ e $c \equiv d\ (m)$, temos que $a + c \equiv b + d\ (m)$. Portanto, no caso de um sistema da forma $\begin{cases} x \equiv b_1\ (a_1) \\ x \equiv b_2\ (a_2) \end{cases}$, podemos particionar x como sendo $x = x_1 + x_2$, de tal forma que:

$$\begin{cases} x_1 \equiv b_1\ (a_1) \\ x_1 \equiv 0\ (a_2) \end{cases} \text{e} \begin{cases} x_2 \equiv 0\ (a_1) \\ x_2 \equiv b_2\ (a_2) \end{cases} \Rightarrow \begin{cases} x_1 + x_2 \equiv b_1 + 0\ (a_1) \\ x_1 + x_2 \equiv 0 + b_2\ (a_2) \end{cases} \Rightarrow \begin{cases} x \equiv b_1\ (a_1) \\ x \equiv b_2\ (a_2) \end{cases}.$$

Proposição 3.4.1 *Considere um sistema* $\begin{cases} x \equiv b_1\ (a_1) \\ x \equiv b_2\ (a_2) \end{cases}$, *com* $(a_1, a_2) = 1$. *Ele admite solução única módulo* $a_1.a_2$ *e é dada por* $x = a_2.y_1.b_1 + a_1.y_2.b_2$, *onde* y_1, y_2 *é solução da equação* $y_i a_j \equiv 1\ (a_i)$, *para* $i, j = 1, 2$, *com* $i \neq j$.

Demonstração: Sejam x_1, x_2 inteiros tais que $x = x_1 + x_2$, onde $\begin{cases} x_1 \equiv b_1\ (a_1) \\ x_1 \equiv 0\ (a_2) \end{cases}$ e $\begin{cases} x_2 \equiv 0\ (a_1) \\ x_2 \equiv b_2\ (a_2) \end{cases}$. Observe que $x_1 = a_2.t_1$ e $x_2 = a_1.t_2$. Logo, a solução é dada por $x = x_1 + x_2 = a_2.t_1 + a_1.t_2$. Resta agora encontrar os valores de t_1 e t_2. Como $x_1 \equiv b_1\ (a_1)$, então segue-se que $a_2 t_1 \equiv b_1(a_1)$. Como $(a_1, a_2) = 1$, pela **Proposição 3.2.1** temos que existe $y_1 \in \mathbb{Z}$ que é o inverso de a_2 módulo a_1, isto é, $y_1.a_2 \equiv 1\ (a_1)$. Segue-se então que $y_1.a_2 t_1 \equiv y_1.b_1\ (a_1) \Rightarrow t_1 \equiv y_1 b_1\ (a_1)$. Analogamente, sendo $x_2 \equiv b_2\ (a_2)$, então segue-se que $a_1 t_2 \equiv b_2\ (a_2)$. Como $(a_1, a_2) = 1$, temos que existe $y_2 \in \mathbb{Z}$ que é o inverso de a_1 módulo a_2, isto é, $y_2.a_1 \equiv 1\ (a_2)$. Segue-se então que $y_2.a_1 t_2 \equiv y_2.b_2\ (a_2) \Rightarrow t_2 \equiv y_2 b_2\ (a_2)$. Logo, teremos que $t_1 = y_1 b_1 + a_1 k_1$ e $t_2 = y_2 b_2 + a_2 k_2$. Substituindo em $x_1 = a_2.t_1$ e $x_2 = a_1.t_2$, teremos:
$x_1 = a_2.(y_1 b_1 + a_1 k_1)$ e $x_2 = a_1.(y_2 b_2 + a_2 k_2)$ e segue-se que $x_1 = a_2.y_1 b_1 + a_1 a_2 k_1$ e $x_2 = a_1.y_2 b_2 + a_1 a_2 k_2$. Como $x = x_1 + x_2$, teremos que $x = (a_2.y_1 b_1 + a_1 a_2 k_1) + (a_1.y_2 b_2 + a_1 a_2 k_2) \Rightarrow x = a_2.y_1 b_1 + a_1.y_2 b_2 + a_1 a_2 k$. Logo, a solução da congruência linear é $x = a_2.y_1 b_1 + a_1.y_2 b_2$ módulo $a_1 a_2$ como queríamos mostrar.
Unicidade. Suponha que x_a e x_b sejam soluções do sistema. Então teremos que:

$$\begin{matrix} x_a \equiv a_2.y_1 b_1 + a_1.y_2 b_2\ (a_1 a_2) \\ x_b \equiv a_2.y_1 b_1 + a_1.y_2 b_2\ (a_1 a_2) \end{matrix} \Rightarrow x_a \equiv x_b\ (a_1 a_2).$$

Segue-se então que $x_a = x_b$.
Nesta proposição, resolvemos um sistema de duas equações. E se o sistema houvesse k equações? O próximo Teorema (O Teorema Chinês dos Restos) mostra como encontrar a solução de um sistema com várias equações. Para demonstrar, na **proposição anterior**, particionamos x em duas partes, porque tínhamos duas

equações. Neste caso, vamos particionar x em k partes pois teremos exatamente k equações.

Teorema 3.4.1 (Teorema Chinês dos Restos) *Sejam $a_1, a_2, ..., a_k$ números inteiros positivos, de tal forma que $(a_i, a_j) = 1$, $\forall i, j = 0, 1, 2, ..., k$ e $i \neq j$. Dados inteiros quaisquer $b_1, b_2, ..., b_k$, o sistema de congruências lineares:*

$$\begin{cases} x \equiv b_1 \ (a_1) \\ x \equiv b_2 \ (a_2) \\ \quad \vdots \\ x \equiv b_k \ (a_k) \end{cases} \tag{3.1}$$

admite solução única, módulo $a_1a_2...a_k$ dada por $x = N_1y_1b_1 + N_2y_2b_2 + ... + N_ky_kb_k$, onde $N = a_1a_2...a_k$, $N_i = \dfrac{N}{a_i}$, com $1 \leq i \leq k$ e y_i é solução da equação $y_iN_i \equiv 1 \ (a_i)$.

Demonstração: Considere o sistema **(3.1)** A solução deste sistema é dada por $x = x_1 + x_2 + ... + x_k$, onde:

$$(1)\begin{cases} x_1 \equiv b_1 \ (a_1) \\ x_1 \equiv 0 \ (a_2) \\ x_1 \equiv 0 \ (a_3) \\ \quad \vdots \\ x_1 \equiv 0 \ (a_{k-1}) \\ x_1 \equiv 0 \ (a_k) \end{cases} \quad (2)\begin{cases} x_2 \equiv 0 \ (a_1) \\ x_2 \equiv b_2 \ (a_2) \\ x_2 \equiv 0 \ (a_3) \\ \quad \vdots \\ x_2 \equiv 0 \ (a_{k-1}) \\ x_2 \equiv 0 \ (a_k) \end{cases} \quad \cdots \quad (k)\begin{cases} x_k \equiv 0 \ (a_1) \\ x_k \equiv 0 \ (a_2) \\ x_k \equiv 0 \ (a_3) \\ \quad \vdots \\ x_k \equiv 0 \ (a_{k-1}) \\ x_k \equiv b_k \ (a_k) \end{cases}$$

Defina $N = a_1a_2...a_k$. Observemos o sistema (1).
Nele temos que $x_1 \equiv 0 \ (a_2), x_1 \equiv 0 \ (a_3), ..., x_1 \equiv 0 \ (a_k)$. Logo, por hipótese de $a_2, a_3, ..., a_k$ serem dois a dois coprimos, teremos que $x_1 \equiv 0 \ (a_2a_3...a_k)$, ou seja, $x_1 = (a_2a_3...a_k)t_1$. Analogamente, teremos que no sistema (2), $x_1 \equiv 0 \ (a_2), x_1 \equiv 0 \ (a_3), ..., x_1 \equiv 0 \ (a_k)$. Logo, teremos que $x_2 \equiv 0 \ (a_1a_3...a_k)$, ou seja, $x_2 = (a_1a_3...a_k)t_2$ e portanto tem-se que $x_k = (a_1a_2...a_{k-1})t_k$. Então, teremos que $x = x_1 + x_2 + ... + x_k = (a_2a_3...a_k)t_1 + (a_1a_3...a_k)t_2 + ... + (a_1a_2...a_{k-1})t_k$. Nos resta agora, encontrar os valores de $t_1, t_2, ..., t_k$. Do sistema (1), sabemos que:
$x_1 \equiv b_1 \ (a_1)$ e que $x_1 = (a_2a_3...a_k)t_1$. Então, teremos que $(a_2a_3...a_k)t_1 \equiv b_1 \ (a_1)$. Como $(a_i, a_j) = 1$ para $i \neq j$, então $(a_2a_3...a_k, a_1) = 1$. Logo, existe $y_1 \in \mathbb{Z}$ tal que $y_1a_2a_3...a_k \equiv 1 \ (a_1)$. Logo, teremos que $t_1 \equiv y_1b_1 \ (a_1)$. Analogamente, resolvendo os outros sistemas, teremos $t_m \equiv y_mb_m \ (a_m)$, para todo $m \in \{1, 2, 3, ..., k\}$. Segue-se então que $t_m = y_mb_m + a_mt$, com $t \in \mathbb{Z}$ e portanto a solução será dada por:

$$x = x_1 + x_2 + ... + x_k = (a_2a_3...a_k)t_1 + (a_1a_3...a_k)t_2 + ... + (a_1a_2...a_{k-1})t_k \Rightarrow$$

$$x = (a_2a_3...a_k)(y_1b_1 + a_1t) + (a_1a_3...a_k)(y_2b_2 + a_2t) + ... + (a_1a_2...a_{k-1})(y_kb_k + a_kt)$$

$$\Rightarrow x = a_2a_3...a_ky_1b_1 + Nt + a_1a_3...a_ky_2b_2 + Nt + ... + a_1a_2...a_{k-1}y_kb_k + Nt$$

$$\Rightarrow x = \frac{a_1a_2a_3...a_ky_1b_1}{a_1} + \frac{a_1a_2a_3...a_ky_1b_1}{a_2} + ... + \frac{a_1a_2a_3...a_ky_1b_1}{a_k} + Nt.k$$

$$\Rightarrow x = N_1y_1b_1 + N_2y_2b_2 + ... + N_ky_kb_k + Ntk.$$

Logo, a solução do sistema **(3.1)** é dada por $N_1y_1b_1 + N_2y_2b_2 + ... + N_ky_kb_k$ módulo $N = a_1a_2...a_k$. Como queríamos mostrar. Para provar a unicidade, usamos o método análogo à demonstração da Proposição 3.4.1. Vamos provar agora, que $x = N_1y_1b_1 + N_2y_2b_2 + ... + N_ky_kb_k$ realmente é solução do sistema **(3.1)**. De fato, temos que $a_i|N_j$, para $i \neq j$. Como $N_iy_i \equiv 1\ (a_i)$, segue-se que:
$x = N_1y_1b_1 + N_2y_2b_2 + ... + N_ky_kb_k \equiv N_iy_ib_i \equiv b_i\ (a_i)$. Logo, $x = N_1y_1b_1 + N_2y_2b_2 + ... + N_ky_kb_k$ é solução do sistema **(3.1)**.

Exemplo 3.4.2 *Três garimpeiros trabalhavam em um rio a procura de ouro. Certo dia, os três encontraram x pedras de ouro. Ao dividir as pedras em grupos, perceberam o seguinte: Se as pedras fossem separadas em grupos de* 7 *unidades, sobrariam* 5 *pedras de ouro; se separassem em grupos de* 11 *unidades,* 8 *pedras de ouro sobrariam e se separassem em grupos de* 13 *unidades,* 4 *pedras de ouro ficariam sobrando. Supondo que eles encontraram entre* 1000 *e* 2000 *pedras de ouro, quantas pedras de ouro foram encontradas?*

Solução: Equacionando o problema, teremos no seguinte sistema de congruências:

$$x \equiv 5\ (7) \tag{3.2}$$

$$x \equiv 8\ (11) \tag{3.3}$$

$$x \equiv 4\ (13) \tag{3.4}$$

Aplicando o Teorema Chinês dos Restos, temos que a solução é única módulo 7.11.13=1001. Então a solução é dada por: $x = \frac{1001.y_1.5}{7} + \frac{1001.y_2.8}{11} + \frac{1001.y_3.4}{13}$. Resta-nos agora, encontrar os valores de y_1, y_2, e y_3. Temos que y_1 é dado por $y_1a_2a_3 \equiv 1\ (a_1)$, isto é, $y_1.143 \equiv 1\ (7)$. Resolvendo, teremos $3y_1 \equiv 1\ (7) \Rightarrow y_1 \equiv 5\ (7)$. Tome $y_1 = 5$. Calculemos y_2, que é dado por $y_2a_1a_3 \equiv 1\ (11) \Rightarrow y_2.91 \equiv 1\ (11) \Rightarrow 3y_2 \equiv 1\ (11) \Rightarrow y_2 \equiv 4\ (11)$. Tome $y_2 = 4$. Calculemos y_3, que é dado por $y_3a_1a_2 \equiv 1\ (13) \Rightarrow y_3.77 \equiv 1\ (13) \Rightarrow 12y_3 \equiv 1\ (13) \Rightarrow y_3 \equiv 12\ (13)$. Tome $y_3 = 12$. Então a solução do problema será dada por:
$x = \frac{1001.y_1.5}{7} + \frac{1001.y_2.8}{11} + \frac{1001.y_3.4}{13} \Rightarrow x = \frac{1001.5.5}{7} + \frac{1001.4.8}{11} + \frac{1001.12.4}{13} \Rightarrow$
$x = 3575 + 2912 + 3696 = 10183$. Sabemos que $10183 \equiv 173\ (1001)$. Logo, a quantidade de ouro é um número da forma $x = 173 + 1001k$, $k \in \mathbb{N}$. No caso, x é um número entre 1000 e 2000, os garimpeiros acharam 1174 pedras de ouro.

Exemplo 3.4.3 *Determinar as soluções da congruência* $501x \equiv 345\ (504)$.

Solução: Observe que $504 = 7.8.9$ e que $(504, 501) = 3$. Logo, teremos três soluções incongruentes módulo 504. Como $501x \equiv 345\ (504)$, então podemos simplificar nosso problema ao sistema

$$\begin{cases} 501x \equiv 345\ (7) \\ 501x \equiv 345\ (8) \\ 501x \equiv 345\ (9) \end{cases} \qquad (*)$$

e aplicar o Teorema Chinês do Resto. Então, considerando o sistema (*), segue-se que:

$$\begin{cases} 501x \equiv 345\ (7) \\ 501x \equiv 345\ (8) \\ 501x \equiv 345\ (9) \end{cases} \Rightarrow \begin{cases} 4x \equiv 2\ (7) \\ 5x \equiv 1\ (8) \\ 6x \equiv 3\ (9) \end{cases} \Rightarrow \begin{cases} 2x \equiv 1\ (7) \\ 5x \equiv 1\ (8) \\ 2x \equiv 1\ (3) \end{cases} \Rightarrow \begin{cases} x \equiv 4\ (7) \\ x \equiv 5\ (8) \\ x \equiv 2\ (3) \end{cases}.$$

Resolvendo o último sistema de congruências, temos que:
$N = 7.8.3, N_1 = 8.3, N_2 = 7.3, N_3 = 7.8, b_1 = 4, b_2 = 5, b_3 = 2$. Encontrando os valores de y_1, y_2, y_3, teremos:
$y_1.N_1 \equiv 1\ (7) \Rightarrow 8.3y_1 \equiv 1\ (7) \Rightarrow 3y_1 \equiv 1\ (7) \Rightarrow y_1 \equiv 5\ (7) \Rightarrow y_1 = 5$;
$y_2.N_2 \equiv 1\ (8) \Rightarrow 7.3y_2 \equiv 1\ (8) \Rightarrow 5y_2 \equiv 1\ (8) \Rightarrow y_2 \equiv 5\ (8) \Rightarrow y_2 = 5$;
$y_3.N_3 \equiv 1\ (3) \Rightarrow 7.8y_3 \equiv 1\ (3) \Rightarrow 2y_3 \equiv 1\ (3) \Rightarrow y_3 \equiv 2\ (3) \Rightarrow y_3 = 2$;
Segue-se que a solução será dada por $x = N_1.y_1.b_1 + N_2.y_2.b_2 + N_3.y_3.b_3$ módulo $7.8.3 = 168$. Com isso, teremos que $x = 8.3.5.4 + 7.3.5.5 + 7.8.2.2 = 1229$, que módulo 168 nos resulta em $x = 53$. Daí, conclui-se que a solução do sistema (*) é dada por $x = 53 + 168t$, $t \in \mathbb{Z}$. As soluções incongruentes são $53, 221$ e 389, para $t = 0, t = 1$ e $t = 2$, respectivamente.

Exemplo 3.4.4 *Resolver o sistema de congruência,* $\begin{cases} n \equiv 6\ (12) \\ n \equiv 2\ (15) \end{cases}$ *, caso haja solução.*

Solução: Observe que o mdc dos modulandos é diferente de 1, pois $(12, 15) = 3$. Não podemos, então, aplicar o Teorema Chinês dos Restos diretamente. Mas, podemos adequá-lo, de forma que o Teorema possa ser utilizado. Vejamos:
Observe que se $n \equiv 6\ (12)$, teremos que $n \equiv 6\ (3)$ e $n \equiv 6\ (4)$ e que se $n \equiv 2\ (15)$, teremos que $n \equiv 2\ (3)$ e $n \equiv 2\ (5)$. Temos o seguinte sistema de congruências:

$$\begin{cases} n \equiv 0\ (3) \\ n \equiv 2\ (4) \\ n \equiv 2\ (3) \\ n \equiv 2\ (5) \end{cases}$$

Neste caso, o sistema não possui solução, pois observando a primeira e a terceira equação, temos que $0 \equiv 2\ (3)$, o que é um absurdo. Poderíamos, usar também o **Lema 3.3.1**, concluindo que $(12, 15) \nmid (2 - 6)$.

Exemplo 3.4.5 *Resolver o sistema de congruência,* $\begin{cases} n \equiv 8\ (12) \\ n \equiv 2\ (15) \end{cases}$ *, caso haja solução.*

Solução: Como $(12, 15) = 3$, então não podemos aplicar diretamente o Teorema Chinês dos Restos. Para tanto, podemos fazer uma modificação de forma que o Teorema possa ser utilizado. Observando a congruência $n \equiv 8\ (12)$, podemos obter duas congruências: $n \equiv 8\ (3)$ e $n \equiv 8\ (4)$, o que equivale a $n \equiv 2\ (3)$ e $n \equiv 0\ (4)$. Analogamente, da congruência $n \equiv 2\ (15)$, podemos obter $n \equiv 2\ (3)$ e $n \equiv 2\ (5)$. Assim, teremos o seguinte sistema de congruências:

$$\begin{cases} n \equiv 2\ (3) \\ n \equiv 0\ (4) \\ n \equiv 2\ (3) \\ n \equiv 2\ (5) \end{cases} \Longrightarrow \begin{cases} n \equiv 2\ (3) \\ n \equiv 0\ (4) \\ n \equiv 2\ (5) \end{cases}.$$

Resolvendo este sistema aplicando o Teorema Chinês dos Restos, teremos:
$N = 3.4.5 = 60, N_1 = 4.5 = 20, N_2 = 3.5 = 15, N_3 = 3.4 = 12, b_1 = 2, b_2 = 0$ e $b_3 = 2$. Encontrando os valores de y_1, y_2, y_3, teremos:
$y_1.N_1 \equiv 1\ (3) \Rightarrow 4.5y_1 \equiv 1\ (3) \Rightarrow 2y_1 \equiv 1\ (3) \Rightarrow y_1 \equiv 2\ (3) \Rightarrow y_1 = 2$;
$y_2.N_2 \equiv 1\ (4) \Rightarrow 3.5y_2 \equiv 1\ (4) \Rightarrow 3y_2 \equiv 1\ (4) \Rightarrow y_2 \equiv 3\ (4) \Rightarrow y_2 = 3$;
$y_3.N_3 \equiv 1\ (5) \Rightarrow 4.3y_3 \equiv 1\ (5) \Rightarrow 2y_3 \equiv 1\ (5) \Rightarrow y_3 \equiv 3\ (5) \Rightarrow y_3 = 3$;
Segue-se que a solução do sistema é dada por:
$n = N_1y_1b_1 + N_2y_2b_2 + N_3y_3b_3$ módulo $4.3.5 = 60$. Assim, teremos que $n = 20.2.2 + 15.3.0 + 12.2.3 = 152$ que módulo 60 nos dá $n = 32$.

3.5 Classes de Congruências

Definição 3.5.1 *Seja* a, m *inteiros com* $m > 1$. *Define-se classe residual de* a *módulo* m, *como sendo o conjunto* $[a] = \{x \in \mathbb{Z}; x \equiv a(m)\}$.

Exemplo 3.5.1 *Dado um inteiro qualquer* b, *tal que* $[b] = [a]$, *então dizemos que* b *é um representante da classe residual de* $[a]$. *Assim, os números* $6, 11, 16, 21, 26, ...$ *são representantes da classe residual* $[1]$ *módulo* 5.

Exemplo 3.5.2 *1. Considere* $m = 3$. *Então, segue-se que as classes de congruências módulo* 3 *são:*
(i) $[0] = \{x \in \mathbb{Z}; x \equiv 0\ (3)\}$, *números inteiros da forma* $3x, x \in \mathbb{Z}$;
(ii) $[1] = \{x \in \mathbb{Z}; x \equiv 1\ (3)\}$, *números inteiros da forma* $3x + 1, x \in \mathbb{Z}$;
(iii) $[2] = \{x \in \mathbb{Z}; x \equiv 2\ (3)\}$, *números inteiros da forma* $3x + 2, x \in \mathbb{Z}$.

2. Considere $m = 7$. *Então, segue-se que as classes de congruências módulo* 7 *são:*

(i) $[0] = \{x \in \mathbb{Z}; x \equiv 0\ (7)\}$, *números inteiros da forma* $7x, x \in \mathbb{Z}$;
(ii) $[1] = \{x \in \mathbb{Z}; x \equiv 1\ (7)\}$, *números inteiros da forma* $7x + 1, x \in \mathbb{Z}$;
(iii) $[2] = \{x \in \mathbb{Z}; x \equiv 2\ (7)\}$, *números inteiros da forma* $7x + 2, x \in \mathbb{Z}$;
(iv) $[3] = \{x \in \mathbb{Z}; x \equiv 3\ (7)\}$, *números inteiros da forma* $7x + 3, x \in \mathbb{Z}$;
(v) $[4] = \{x \in \mathbb{Z}; x \equiv 4\ (7)\}$, *números inteiros da forma* $7x + 4, x \in \mathbb{Z}$;
(vi) $[5] = \{x \in \mathbb{Z}; x \equiv 5\ (7)\}$, *números inteiros da forma* $7x + 5, x \in \mathbb{Z}$;
(vii) $[6] = \{x \in \mathbb{Z}; x \equiv 6\ (7)\}$, *números inteiros da forma* $7x + 6, x \in \mathbb{Z}$.

Propriedades 3.5.1 *As classes residuais possuem as seguintes propriedades:*

(i) $[a] = [b] \Leftrightarrow a \equiv b\ (m)$;

(ii) Se $[a] \cap [b] \neq \emptyset$, *então* $[a] = [b]$;

(iii) Sendo $a \in \mathbb{Z}$, $\bigcup [a] = \mathbb{Z}$.

Demonstração:
(i) Suponha que $[a] = [b]$. Por definição das classes residuais, temos que $[a] = \{x \in \mathbb{Z}, x \equiv a\ (m)\}$ e $[b] = \{x \in \mathbb{Z}, x \equiv b\ (m)\}$. Segue-se que $x \equiv a\ (m)$ e $x \equiv b\ (m)$. Logo, pela transitividade, tem-se que $a \equiv b\ (m)$. Por outro lado, se $a \equiv b\ (m)$, então $x \equiv a$ se e somente se $x \equiv b\ (m)$ e o resultado segue.
(ii) Suponha que $[a] \cap [b] \neq \emptyset$. Então, teremos que existe um elemento $c \in [a]$ e $c \in [b]$. Logo, teremos que $a \equiv c\ (m)$ e $b \equiv c\ (m)$. Novamente pela transitividade, tem-se que $a \equiv b\ (m)$, isto é, $[a] = [b]$.
(iii) Temos que $[a] = \{x \in \mathbb{Z}; x \equiv a\ (m)\}$. Como $a \in \{0, 1, 2, 3, \cdots, m-1\}$, isto é, a pertence ao sistema completo de resíduos módulo m. Daí, segue-se que a é da forma $mk, mk + 1, mk + 2, \cdots, mk + (m-1)$. A união destas classes resulta em $\mathbb{Z}$.

Proposição 3.5.1 *Existem exatamente* m *classes residuais módulo* m *distintos, a saber* $[0], [1], [2], [3], [4], ..., [m-1]$.

Demonstração: Considere o conjunto das classes residuais, isto é, $[a] = \{x \in \mathbb{Z}; x \equiv a\ (m)\}$. Na congruência $x \equiv a\ (m)$, temos que o resto da divisão x por m deixa resto a. Então, os possíveis restos desta divisão são elementos do conjunto $\{0, 1, 2, 3, 4, ..., m-1\}$, conjunto este que possui exatamente m elementos. Logo, existem m classes residuais módulo m.

Exemplo 3.5.3 *Mostrar que os elementos do conjunto* $A = \{1^2, 2^2, 3^2, 4^2, ..., m^2\}$, $m > 2$, *não formam um sistema completo de resíduos módulo* m.

Solução: Sabemos que o sistema completo de resíduos módulo m é dado por $\{[0], [1], [2], [3], ..., [m-1]\}$. Queremos mostrar que o conjunto A acima não é um

sistema completo de resíduos módulo m. Sejam n e k inteiros tal que $n > k$ e $n + k = m$. Assim, teremos que $n^2 - k^2 \neq 0$ e:
$n^2 - k^2 = (n + k)(n - k) = m.(n - k) \equiv 0\ (m) \Rightarrow n^2 \equiv k^2\ (m)$. Com isso, temos dois elementos distintos em A que não são incongruentes entre si módulo m. Logo, o conjunto A não forma um sistema completo de resíduos módulo m.

3.6 O Conjunto Quociente $\mathbb{Z}_m$ e $\mathbb{Z}_m^*$

O conjunto $\mathbb{Z}_m = \{[0], [1], [2], [3], ..., [m-1]\}$ é chamado de sistema completo de resíduos módulo m, se para todo $a \in \mathbb{Z}$, existir um $i \in \{0, 1, 2, ..., m-1\}$, tal que $a \equiv a_i\ (m)$.

Exemplo 3.6.1 $\mathbb{Z}_3 = \{[0], [1], [2]\}$; $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$; $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$. *Ao tomarmos um inteiro qualquer, digamos* 57*, ele está presente em todos estes conjuntos acima. No caso do conjunto* $\mathbb{Z}_3$*, ele é representado pela classe residual* $[0]$*, pois* $57 \equiv 0\ (3)$*, e analogamente* 57 *é representado pelas classes residuais* $[2]$ *e* $[1]$ *nos conjuntos* $\mathbb{Z}_5$ *e* $\mathbb{Z}_8$*, respectivamente.*

As operações em $\mathbb{Z}_m$ estão definidas da seguintes forma:
(I) ***Adição***: $[a] + [b] = [a + b]$;
(II) ***Multiplicação***: $[a].[b] = [a.b]$;

Propriedades 3.6.1 $\forall [a], [b], [c] \in \mathbb{Z}_m$*, teremos:*
(I) *Quanto à Adição:*
$(A1)$ *Associativo:* $[a] + ([b] + [c]) = ([a] + [b]) + [c]$;
$(A2)$ *Comutativo:* $[a] + [b] = [b] + [a]$;
$(A3)$ *Elemento Neutro:* $[a] + [0] = [a]$;
$(A4)$ *Elemento Inverso Simétrico:* $[a] + [-a] = [0]$;
(II) *Quanto à Multiplicação:*
$(M1)$ *Associativo:* $[a].([b].[c]) = ([a].[b]).[c]$;
$(M2)$ *Comutativo:* $[a].[b] = [b].[a]$;
$(M3)$ *Elemento Neutro:* $[a].[1] = [a]$;
$(M4)$ *Distributividade:*$[a].([b] + [c]) = [a].[b] + [a].[c]$;

Definição 3.6.1 *Denomina-se* ***domínio de integridade*** *o conjunto que não possui divisores de zero, isto é, dados,* $[a], [b]$ *classes residuais não nulas, teremos que* $[a].[b] \neq 0$*, ou de forma equivalente, se* $[a].[b] = 0$*, então* $[a] = 0$ *ou* $[b] = 0$.

Definição 3.6.2 *Denomina-se* ***corpo*** *o conjunto munido das operações* ***soma*** *e* ***multiplicação*** *com a propriedades vistas acima adicionada da propriedade de que:*

M(5) *Elemento Inverso Multiplicativo: Dada a classe residual* $[a]$ *não nula, existe uma classe* $[b]$ *tal que* $[a].[b] = 1$.

Exemplo 3.6.2 *Considere o conjunto* $\mathbb{Z}_5$. *Construir as tabelas da adição e multiplicação.*

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[6]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\times$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

É interessante notar que $\mathbb{Z}_4$ (por exemplo) não é domínio de integridade, pois $[2] \neq [0]$, e temos que $[2].[2] = [4] = [0]$, isto é $\mathbb{Z}_4$ possui divisores de zero. Verifica-se também, que $\mathbb{Z}_4$ também não é corpo, pois não existe em $\mathbb{Z}_4$ o inverso multiplicativo de $[2]$. Já os conjuntos $\mathbb{Z}_3$, $\mathbb{Z}_5$ e $\mathbb{Z}_7$ são considerados corpos, pois para todo $[a]$ não nulo pertencente $\mathbb{Z}_3$, $\mathbb{Z}_5$ ou $\mathbb{Z}_7$, existe uma classe $[b]$ pertencente a $\mathbb{Z}_3$, $\mathbb{Z}_5$ ou $\mathbb{Z}_7$, tal que $[a].[b] = 1$. Neste caso, $[b]$ é o inverso de $[a]$. Então, dado um conjunto $\mathbb{Z}_m$, para que valores de m, os elementos $\mathbb{Z}_m$ são invertíveis?

Teorema 3.6.1 *Um elemento* $[a] \in \mathbb{Z}_m$ *é invertível, se e somente se,* $(a, m) = 1$.

Demonstração: $\Rightarrow$ Sabemos que um elemento em $\mathbb{Z}_m$ é invertível, quando existe um elemento $[b] \in \mathbb{Z}_m$, tal que $[a].[b] = 1$, isto é, $ab \equiv 1\ (m)$. Suponha que $[a]$ seja um elemento invertível em $\mathbb{Z}_m$. Logo, teremos que existe $[b]$ e $ab \equiv 1\ (m)$.Logo, $(a, m) = 1$, pela **Proposição 3.2.1**.
$\Leftarrow$ Suponha que $(a, m) = 1$. Então existem inteiros x, y, tal que $ax - my = 1$. Segue-se que $ax \equiv 1\ (m)$. Logo, $[x]$ é o inverso de $[a]$ módulo m.

Proposição 3.6.1 $\mathbb{Z}_m$ *é corpo, se e somente se,* m *é primo.*

Demonstração: $\Rightarrow$ Suponha por absurdo que $\mathbb{Z}_m$ é corpo e m não é primo. Então existem inteiros m_1, m_2 com $1 < m_1 < m_2 < m$ tais que $m = m_1.m_2$. Segue-se que $[m_1].[m_2] = [m_1.m_2] = [m] = [0]$. Absurdo, pois um corpo não admite divisores de zero, por se tratar de um domínio de integridade. Logo, m é primo.
$\Leftarrow$ Suponha m primo. Então para todo $[a]$ pertecente a $\mathbb{Z}_m$, temos que $(a, m) = 1$. Logo, pelo Teorema anterior, teremos que os elementos não nulos de $\mathbb{Z}_m$ são invertíveis. Logo, $\mathbb{Z}_m$ é um corpo.

Definição 3.6.3 *O conjunto* $\mathbb{Z}_m^*$ *é o conjunto formado pelos elementos invertíveis de* $\mathbb{Z}_m$. *É denominado de sistema reduzido de resíduos módulo* m.

Exemplo 3.6.3 *No conjunto $\mathbb{Z}_8$ o sistema completo de resíduos módulo 8 é formado pelo conjunto $\mathbb{Z}_8 = \{[0],[1],[2],[3],[4],[5],[6],[7]\}$. Neste conjunto, os elementos invertíveis são os coprimos com 8, no caso, $[1],[3],[5]$ e $[7]$. Logo, $\mathbb{Z}_m^* = \{[1],[3],[5],[7]\}$, no qual denominaremos de* sistema reduzido de resíduos módulo 8.

3.7 O Teorema Chinês Revisitado

Considere agora o produto cartesiano $\mathbb{Z}_m \times \mathbb{Z}_n$. Pelas proposições vistas no apêndice, teremos que este produto cartesiano é um anel. Suponha que $(m,n) = 1$ e considere a função:

$$\psi : \begin{array}{c} \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \\ [a_{mn}] \mapsto ([a_m],[a_n]) \end{array}$$

Já provamos que ψ é um homomorfismo **Proposição 6.3.4 (Apêndice)**. Queremos mostrar que a função acima é um isomorfismo de anéis. Para melhor entendimento, acompanhe o exemplo a seguir:

Exemplo 3.7.1 *Mostrar que $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ é um isomorfismo de anéis.*

Solução:
Sabemos que $\mathbb{Z}_6 = \{[0],[1],[2],[3],[4],[5]\}$ e que $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{([0],[0]),([0],[1]),([0],[2]),([1],[0]),([1],[1]),([1],[2])$. Pensemos assim: Um número inteiro $n \in \mathbb{Z}_6$ possui classes residuais $\{[0],[1],[2],[3],[4],[5]\}$. Analisando cada classe residual módulo 2 e 3, na ordem, teremos os seguintes pares ordenados:

$\mathbb{Z}_6$	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_2 \times \mathbb{Z}_3$
0	0	0	$(0,0)$
1	1	1	$(1,1)$
2	0	2	$(0,2)$
3	1	0	$(1,0)$
4	0	1	$(0,1)$
5	1	2	$(1,2)$

.

Observe que na 4° coluna, estão presentes todos os pares ordenados do conjunto $\mathbb{Z}_2 \times \mathbb{Z}_3$. É facil ver que os conjuntos $\mathbb{Z}_2 \times \mathbb{Z}_3$ e $\mathbb{Z}_6$ possuem mesma cardinalidade e que pela tabela a função é injetiva. Logo, temos um homomorfismo bijetivo, portanto um isomorfismo de anéis **(Proposição 6.3.1 item (iii) (Apêndice))**, como queríamos mostrar.

Neste isomorfismo, tem-se uma aplicação direta do Teorema Chinês dos Restos. No caso, dado um número inteiro k, sabendo o resto da divisão por mn, podemos

encontrar os restos da divisão por m e n e vice-versa. Por exemplo, sabendo que $n \equiv 5\ (6)$, temos que $n \equiv 1\ (2)$ e $n \equiv 2\ (3)$ e mais, tendo um sistema de congruências módulo 2 e módulo 3, podemos analisar a congruência módulo 6, tudo isso devido a este isomorfismo. Mas será que esta função é sempre um isomorfismo para todo m, n? Não, pois considere a função: $\phi : \mathbb{Z}_8 \to \mathbb{Z}_2 \times \mathbb{Z}_4$. Será ϕ também um isomorfismo? Vejamos:
Sabemos que $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$ e que $\mathbb{Z}_2 \times \mathbb{Z}_4 = \{([0], [0]), ([0], [1]), ([0], [2]), ([0], [3]), ([1], [0]), ([1], [1]), ([1], [2], ([1], [3]))$. Analisando cada classe residual módulo 2 e 4, na ordem, teremos os seguintes pares ordenados:

$\mathbb{Z}_8$	$\mathbb{Z}_2$	$\mathbb{Z}_4$	$\mathbb{Z}_2 \times \mathbb{Z}_4$
0	0	0	$(0, 0)$
1	1	1	$(1, 1)$
2	0	2	$(0, 2)$
3	1	3	$(1, 3)$
4	0	0	$(0, 0)$
5	1	1	$(1, 1)$
6	0	2	$(0, 2)$
7	1	3	$(1, 3)$

.
Observe que a função não é injetiva e nem sobrejetiva, pois os números da forma $8k$ e $8k+4$ deixam os mesmos restos quando divididos por 2 e por 4 e não exite uma classe $[a]$ em $\mathbb{Z}_8$, tal que $\phi([a]) = ([m], [n])$, onde $([m], [n]) \in \{([0], [1]), ([0], [3]), ([1], [0]), ([1], [2])\}$. Logo, $\phi : \mathbb{Z}_8 \to \mathbb{Z}_4 \times \mathbb{Z}_2$ não é um isomorfismo de anéis.
Então, para que valores de m, n, temos que ψ será um isomorfismo? O próximo Teorema, nos diz para que valores de m e n a função $\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ é um isomorfismo.

Teorema 3.7.1 *A função* $\psi : \begin{array}{c} \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \\ [a_{mn}] \mapsto ([a_m], [a_n]) \end{array}$ *é um isomorfismo de anéis se e somente se* $(m, n) = 1$.

Primeira Demonstração (Injetividade): Seja $(k_1, k_2) \in \mathbb{Z}_m \times \mathbb{Z}_n$ e $[a]$ e $[b]$ classes residuais de $\mathbb{Z}_{mn}$. Suponha que $\psi([a]) = \psi([b])$. Para provar que a função ψ é um isomorfismo, basta provar que as classes $[a]$ e $[b]$ são congruentes módulo mn, isto é, $[a] = [b]$. Então, teremos que:

$$\begin{cases} a \equiv k_1\ (m) \\ a \equiv k_2\ (n) \end{cases} \quad e \quad \begin{cases} b \equiv r_1\ (m) \\ b \equiv r_2\ (n) \end{cases} .$$

Então $\psi([a]) = ([k_1], [k_2])$ e $\psi([b]) = ([r_1], [r_2])$. Como $\psi([a]) = \psi([b])$, teremos que:
$k_1 \equiv r_1\ (m) \Rightarrow a \equiv b\ (m)$

$k_2 \equiv r_2\ (n) \Rightarrow a \equiv b\ (n)$
Logo, $a - b$ é múltiplo de m e n. Como $(m, n) = 1$ por hipótese, então $a - b$ é múltiplo de mn, isto é, $a \equiv b\ (mn)$ como queríamos mostrar.

Segunda Demonstração (Sobrejetividade): Para provar que a função é um isomorfismo, devemos provar que a função é um homomorfismo bijetivo. Sabemos que $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \times \mathbb{Z}_n$ possuem mesma cardinalidade, a saber mn elementos. Então basta provar que a função é injetiva. Seja $[a] \in \mathbb{Z}_{mn}$. Então, teremos que $a \equiv k\ (mn)$, onde $k \in \{0, 1, 2, ..., m, m+1, ..., n, n+1, ..., mn-1\}$. Seja $(k_1, k_2) \in \mathbb{Z}_m \times \mathbb{Z}_n$, onde $k_1 \in \mathbb{Z}_m$ e $k_2 \in \mathbb{Z}_n$. Como $a \equiv k\ (mn)$, teremos que $k \equiv k_1\ (m)$ e $k \equiv k_2\ (n)$. Temos então uma aplicação direta do Teorema Chinês dos Restos. Como $(m, n) = 1$, então o sistema

$$\begin{cases} k \equiv k_1\ (m) \\ k \equiv k_2\ (n) \end{cases}$$

admite solução única módulo mn. Logo, para cada par ordenado $(k_1, k_2) \in \mathbb{Z}_m \times \mathbb{Z}_n$, existe um único $k \in \mathbb{Z}_{mn}$. Assim, teremos que a função é sobrejetiva e injetiva. Logo, teremos um homomorfismo bijetivo, concluindo então que $\mathbb{Z}_m \times \mathbb{Z}_n$ é um isomorfismo de anéis.

Definição 3.7.1 (Função ϕ de Euler) *Seja $m \in \mathbb{Z}$. A função ϕ de Euler é uma função que denota a quantidade de números inteiros coprimos e menores com m, ou seja, o único divisor comum entre eles é 1. Denotamos por $\phi(m)$ e escrevemos $\phi : \mathbb{N} \to \mathbb{N}$, onde*

$$\#\mathbb{Z}_n^* = \phi(n) = \#\{k \in \{1, ..., n\}; (k, n) = 1\}.$$

Exemplo 3.7.2 *Considerando $m = 20$, sabemos que os números coprimos com 20 são os elementos do conjunto $A = \{1, 3, 7, 9, 11, 13, 17, 19\}$, portanto 8 elementos. Logo, $\phi(20) = 8$.*

Exemplo 3.7.3 *Considere a função* $\psi : \begin{array}{c} \mathbb{Z}_{15}^* \simeq \mathbb{Z}_5^* \times \mathbb{Z}_3^* \\ [a] \mapsto ([a], [a]) \end{array}$.
(a) Será ψ um isomorfismo?
(b) Caso afirmativo, este é um isomorfismo de anéis?
(c) Será $\#\mathbb{Z}_{15}^* \simeq \#\mathbb{Z}_5^* \times \#\mathbb{Z}_3^*$, isto é, $\phi(15) = \phi(5).\phi(3)$?

Solução: (a), (b) Para que ψ seja um isomorfismo, teremos que obter um homomorfismo bijetivo. Sabemos que $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$, $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ e $\mathbb{Z}_3^* = \{1, 2, 3\}$. Montando uma tabela, vamos obter:

$\mathbb{Z}_{15}^*$	$\mathbb{Z}_5^* \times \mathbb{Z}_3^*$
1	$(1,1)$
2	$(2,2)$
4	$(4,1)$
7	$(2,1)$
8	$(3,2)$
11	$(1,2)$
13	$(3,1)$
14	$(4,2)$

Observe que ψ apresenta uma bijeção. Vamos verificar agora se ψ é um homomorfismo de anéis.
(i) Temos que $f(1) = (1,1)$;
(ii) Observe que $f(a+b) \neq f(a)+f(b)$. De fato, pois sendo $a = 1$ e $b = 2$, teremos que $a + b = 3 \notin \mathbb{Z}_{15}^*$;
(iii) Temos que $f(a.b) = f(a).f(b)$, $\forall a, b \in \mathbb{Z}_{15}^*$. Neste caso temos um isomorfismo de grupos com respeito à multiplicação, **observação da definição 6.3.1, apêndice**.
(c) Observe que $\#\mathbb{Z}_{15}^* = 8$ e que $\#\mathbb{Z}_5^* = 4$ e $\#\mathbb{Z}_3^* = 2$. Logo, $\phi(15) = \phi(5).\phi(3)$.

Com este exemplo, mostramos através de um contra-exemplo, que $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$, sendo $(m,n) = 1$, nunca será isomorfismo de anéis. A proposição a seguir, mostra que $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ será um isomorfismo de grupos multiplicativos e que $\phi(mn) = \phi(m).\phi(n)$.

Proposição 3.7.1 *Sejam $m, n \in \mathbb{Z}, (m,n) = 1$ e $\#\mathbb{Z}_{mn}^*$ a quantidade de elementos invertíveis do conjunto $\mathbb{Z}_{mn}$. Então $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$, isto é, $\phi(mn) = \phi(m).\phi(n)$.*

Demonstração: Provamos anteriormente que $\psi : \begin{array}{c} \mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n \\ [a] \mapsto ([a],[a]) \end{array}$ é um isomorfismo de anéis quando $(m,n) = 1$. Queremos provar que $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ também é um isomorfismo, no caso um isomorfismo de grupos, pois pelo exemplo anterior, $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ não é um homomorfismo aditivo. Vamos mostrar que $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ é um homomorfismo multiplicativo, concluindo que $\#\mathbb{Z}_{mn}^* = \#\mathbb{Z}_m^* \times \#\mathbb{Z}_n^*$. Para provar que $\mathbb{Z}_{mn}^*$ e $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ são isomorfos, basta mostrar que dada uma classe $[a]$ em $\mathbb{Z}_{mn}$ tal que $(a, mn) = 1$, implica em $(a,m) = 1 = (a,n)$, no qual foi provado na **Proposição 2.3.4**. Conclui-se então que $\#\mathbb{Z}_{mn}^* = \#\mathbb{Z}_m^* \times \#\mathbb{Z}_n^*$ isto é, $\phi(mn) = \phi(m).\phi(n)$.

Proposição 3.7.2 *Sejam $p \in \mathbb{Z}$, $e \in \mathbb{N}$ e p primo. Então, $\phi(p^e) = p^e - p^{e-1}$.*

Demonstração: Considere o inteiro p^e. Então o sistema completo de resíduos módulo p^e é formado pelos elementos do conjunto $A = \{0, 1, 2, 3, ..., p, p+1, ..., 2p, ..., 2p-1, ..., 3p, ..., p^{e-1}.p\}$. Observe que os elementos do conjunto que são da forma $k.p$, com $k \in \mathbb{Z}$, são divisores de p^e, isto é $(n, p^e) \neq 1$ para todo $n \neq kp$. Como o conjunto A possui exatamente p^e elementos e os divisores de p^e do conjunto A são p^{e-1}, então existem $p^e - p^{e-1}$ elementos menores que p^e que são coprimos com p^e. Assim, teremos que $\phi(p^e) = p^e - p^{e-1}$.

Teorema 3.7.2 *Seja* $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. *Então* $\phi(n) = n.\left(1 - \frac{1}{p_1}\right).\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$.

Demonstração: Pelas proposições anteriores, temos que $\phi(p^e) = p^e - p^{e-1}$ e que $\phi(mn) = \phi(m).\phi(n)$. Então, sendo $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, teremos que $\phi(n)$ será dado por:
$\phi(n) = \phi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \phi(p^{e_1}).\phi(p^{e_2}) \cdots \phi(p^{e_k}) =$
$(p^{e_1} - p^{e_1-1}).(p^{e_2} - p^{e_2-1}) \cdots (p^{e_k} - p^{e_k-1}) = p_1^e \left(1 - \frac{1}{p_1}\right).p_2^e \left(1 - \frac{1}{p_2}\right) \cdots p_k^e \left(1 - \frac{1}{p_k}\right)$
$= n.\left(1 - \frac{1}{p_1}\right).\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$

Exemplo 3.7.4 *:*
$\phi(100) = \phi(2^2.5^2) = 100.\left(1 - \frac{1}{2}\right).\left(1 - \frac{1}{5}\right) = 40$*;*
$\phi(725) = \phi(5^2.29) = 725.\left(1 - \frac{1}{29}\right).\left(1 - \frac{1}{5}\right) = 560$*;*
$\phi(7^3) = 7^3 - 7^2 = 294.$

3.8 Interpretação Gráfica do Teorema Chinês dos Restos

No capítulo 3, seção 3.4, enunciamos e demonstramos o Teorema Chinês dos Restos. Vamos interpretá-lo agora de forma gráfica usando uma tabela. Considere o caso que o sistema de congruências possua duas equações lineares, isto é, um sistema do tipo:

$$\begin{cases} x \equiv a\ (m) \\ x \equiv b\ (n) \end{cases}, \text{ com } (m, n) = 1$$

Para facilitar o entendimento, considere $m = 5$ e $n = 4$. Como $(5, 4) = 1$, temos que $\mathbb{Z}_{20} \simeq \mathbb{Z}_5 \times \mathbb{Z}_4$ é um isomorfismo de anéis, como foi provado. Pois bem,

vamos construir uma tabela $\mathbb{Z}_5 \times \mathbb{Z}_4$, colocando os elementos de $\mathbb{Z}_5$ na coluna à esquerda da tabela e os elementos de $\mathbb{Z}_4$ na linha do alto da tabela. Pelo isomorfismo, sabemos que um elemento de $\mathbb{Z}_{20}$ admite um único par ordenado em relação ao conjunto $\mathbb{Z}_5 \times \mathbb{Z}_4$, isto é, se $x \in \mathbb{Z}_{20}$, teremos que $x \equiv a\ (5)$ e $x \equiv b\ (4)$, onde $([a],[b]) \in \mathbb{Z}_5 \times \mathbb{Z}_4$. Assim, duas casas da tabela, serão ocupadas por números inteiros distintos com as seguintes condições:
(i) $0 \leq x \leq 19$, lembre-se $\mathbb{Z}_{20} = \{0, 1, 2, ..., 19\}$;
(ii) $x \equiv a\ (5)$ e $x \equiv b\ (4)$. Diremos que o par $([a],[b])$ são as coordenadas de $x \in \mathbb{Z}_{20}$ na tabela.

	0	1	2	3
0	0	5	10	15
1	16	1	6	11
2	12	17	2	7
3	8	13	18	3
4	4	9	14	19

Para preencher a tabela, basta usar o item (ii). Por exemplo, tome a classe $[18] \in \mathbb{Z}_{20}$. Segue-se $18 \equiv 3\ (5)$ e $18 \equiv 2\ (4)$. Logo, as coordenadas de $[18]$ é $([3],[2])$, isto é, $[18]$ ficará linha 3 e na coluna 2. Usando este procedimento, preenchemos toda a tabela. Mas isso, significaria resolver (neste exemplo) 20 sistemas de congruências. E se fôssemos montar uma tabela $\mathbb{Z}_{50} \times \mathbb{Z}_{40}$? Teríamos que resolver 2000 sistemas de congruências!!! A seguir mais uma tabela referente a $\mathbb{Z}_{28} \simeq \mathbb{Z}_4 \times \mathbb{Z}_7$.

	0	1	2	3	4	5	6
0	0	8	16	24	4	12	20
1	21	1	9	17	25	5	13
2	14	22	2	10	18	26	6
3	7	15	23	3	11	19	27

Vamos apresentar um método fácil de completar a tabela sem resolver todos esses sistemas de congruências. Para facilitar, acompanhe a tabela abaixo, referente a $\mathbb{Z}_{20} \simeq \mathbb{Z}_5 \times \mathbb{Z}_4$, onde colocamos apenas os elementos de $0, 1, 2, 3, 4, 5$ nesta ordem:

	0	1	2	3
0	0	5		
1		1		
2			2	
3				3
4	4			

Observe que a medida que colocamos os números $0, 1, 2, 3$, fomos "pulando" uma coluna e passando para a próxima linha. Para colocar o elemento 4, seguindo esta

ideia, ele ficaria fora da tabela, isto é, para colocá-lo, vamos passar da linha 3 para a linha 4 e teríamos que passar da coluna 3 para a coluna 4 (que não existe). Então, como $4 \equiv 0\ (4)$, então a 4°coluna corresponde a coluna 0. Para colocar o elemento 5, passamos da coluna 0 para a coluna 1, teríamos que passar da linha 4 para a linha 5 (que não existe). Mas temos que $5 \equiv 0\ (5)$. Logo, a linha 5 corresponde a linha 0. Seguindo este procedimento, preencheremos toda a tabela sem resolver nenhum sistema de congruências.
Agora, para preencher a tabela, o que acontece quando $(m, n) = d \neq 1$? Vamos montar uma tabela correspondente a $\mathbb{Z}_{24} \simeq \mathbb{Z}_4 \times \mathbb{Z}_6$:

	0	1	2	3	4	5
0	0; 12		8; 20		4; 16	
1		1; 13		9; 21		5; 17
2	6; 18		2; 14		10; 22	
3		7; 19		3; 15		11; 23

Observe que cada casa da tabela possui exatamente dois elementos (o que corresponde ao $(6, 4)$) e ainda contamos com casas vazias. Estes dois elementos são dois a dois incongruentes módulo o 24, mas são congruentes módulo o m.m.c entre 4 e 6 que é 12. Com relação às casas vazias, significam que o sistema não admite solução módulo $[6, 4]$ com as coordenandas da casa em questão. Por exemplo, tomando a casa que está na coluna 2 e na linha 3, teríamos o seguinte sistema de congruências:
$\begin{matrix} x \equiv 2\ (6) \\ x \equiv 3\ (4) \end{matrix}$, que não admite solução, pois $2 = (6, 4) \nmid (3 - 2) = 1$. Logo, teremos que $\mathbb{Z}_{24} \simeq \mathbb{Z}_4 \times \mathbb{Z}_6$ não é um isomorfismo de anéis, pois não teremos um homomorfismo injetivo e nem sobrejetivo.

Para montar uma tabela referente a expressão $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, procedemos da mesma forma que fizemos anteriormente. Supondo que $(m, n) = 1$, e dispondo os elementos de $\mathbb{Z}_m$ na primeira coluna à esquerda e os elementos de $\mathbb{Z}_n$ na linha superior da tabela, teremos que cada casa será ocupada por um número inteiro distinto com as seguintes características:
(i) $0 \leq x \leq mn - 1$;
(ii) $x \equiv a\ (m)$ e $x \equiv b\ (m)$.
Dizemos que o par $([a], [b])$ serão as coordenadas do inteiro na tabela. Pelo fato de $(m, n) = 1$, temos um isomorfismo de anéis. Logo, todas as casas da tabela serão preenchidas. Caso o $(m, n) = d \neq 1$, então nem todas as casas serão preenchidas, pelo fato de $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ não ser um isomorfismo. Este critério de construção da tabela funciona, pois sabemos que: $\begin{matrix} x \equiv a\ (m) \\ x \equiv b\ (n) \end{matrix} \Rightarrow \begin{matrix} x + 1 \equiv a + 1\ (m) \\ x + 1 \equiv b + 1\ (n) \end{matrix}$. É claro que a utilização da tabela é muito útil para valores pequenos. Caso, tenhamos que analisar o isomorfismo $\mathbb{Z}_{37250} \simeq \mathbb{Z}_{250} \times \mathbb{Z}_{149}$, por exemplo, fica praticamente

inviável desenhar a tabela e ainda sim encontrar a solução. Neste caso, a maneira mais prática seria utilizar o Teorema Chinês dos Restos.

3.9 Problemas Resolvidos

Problema 3.9.1 *Mostre que a função*

$$f: \begin{array}{l} \mathbb{Z} \to \mathbb{Z}_{12} \\ x \mapsto [9x] \end{array}$$

é tal que, para todos $a, b \in \mathbb{Z}$, $f(a+b) = f(a)+f(b)$, $f(a.b) = f(a).f(b)$ *e* $f(1) \neq 1$.

Solução: Sejam $a, b \in \mathbb{Z}$, então teremos que:
(i) $f(1) = 9.[1] = 9 \neq 1$;
(ii) $f(a) = [9a] = 9.[a]$; $f(b) = [9b] = 9.[b]$ e $f(a+b) = [9a+9b] = 9[a]+9[b] = f(a)+f(b)$;
(iii) $f(a.b) = [9a.9b] = 9[a].9[b] = f(a).f(b)$.
Observe que esta função não é um homomorfismo, pois $f(1) \neq 1$, como constatou-se no item (i).

Problema 3.9.2 *Usando a tabela gráfica, resolver o seguinte problema: Um ancião possui uma certa quantidade milho em sua residência. Quando ele separa em recipientes que comportam* 7 *kg,* 5 *kg de milho ficam sobrando. Quando separa em recipientes de* 11 *kg,* 8 *kg ficam sobrando. Sendo assim, quantos kg de milho, no mínimo, esse ancião possui em sua residência?*

Solução: Vamos construir uma tabela do tipo $\mathbb{Z}_7 \times \mathbb{Z}_{11}$. Queremos descobrir o elemento que está na linha 5 e na coluna 8. Preenchendo a tabela, teremos:

	0	1	2	3	4	5	6	7	8	9	10
0	0	56	35	14	70	49	28	7	63	42	21
1	22	1	57	36	15	71	50	29	8	64	43
2	44	23	2	58	37	16	72	51	30	9	65
3	66	45	24	3	59	38	17	73	52	31	10
4	11	67	46	25	4	60	39	18	74	53	32
5	33	12	68	47	26	5	61	40	19	75	54
6	55	34	13	69	48	27	6	62	41	20	76

Pela tabela, o número inteiro que está na linha 5 e na coluna 8 é 19. portanto, o ancião possui em sua casa um número do tipo $19 + 77k, k \in \mathbb{Z}$. A quantidade mínima de milho é 19 kg.

Problema 3.9.3 *Determine o menor inteiro positivo que deixa resto* 2 *na divisão por* 5*, resto* 4 *na divisão por* 7 *e resto* 5 *na divisão por* 11*.*

Solução: Equacionando o problema, teremos o seguinte sistema de congruências: $\begin{cases} x \equiv 2\ (5) \\ x \equiv 4\ (7) \\ x \equiv 5\ (11) \end{cases}$. Como $(a_1, a_2, a_3) = (5, 7, 11) = 1$, este sistema admite solução única módulo $5.7.11 = 385$. Vamos aplicar o Teorema Chinês dos Restos, cuja solução é dada por $x = N_1y_1b_1 + N_2y_2b_2 + N_3y_3b_3$, onde $b_1 = 2$, $b_2 = 4$, $b_3 = 5$, $N_1 = 7.11 = 77$, $N_2 = 5.11 = 55$, $N_3 = 5.7 = 35$, y_1, y_2, y_3 são soluções da equação $y_iN_i \equiv 1\ (a_i)$, para $i = 1, 2, 3$. Calculemos y_1, y_2, y_3:
$y_1.77 \equiv 1\ (5) \Rightarrow 2y_1 \equiv 1\ (5) \Rightarrow y_1 = 3.$
$y_2.55 \equiv 1\ (7) \Rightarrow 6y_2 \equiv 1\ (7) \Rightarrow y_2 = 6.$
$y_3.35 \equiv 1\ (11) \Rightarrow 2y_3 \equiv 1\ (11) \Rightarrow y_3 = 6.$
Segue que a solução é dada por:
$x = 77.3.2 + 55.6.4 + 35.6.5 = 2832$ que módulo 385 nos dá 137. Logo, o menor inteiro positivo que deixa resto 2 na divisão por 5, resto 4 na divisão por 7 e resto 5 na divisão por 11 é 137.

Problema 3.9.4 *Três satélites passarão sobre o Recife-PE à noite. O primeiro a* 1 *hora da madrugada, o segundo às* 4 *horas e o terceiro às* 8 *horas da manhã. Cada satélite tem um período diferente. O primeiro leva* 13 *horas para completar uma volta em torno da Terra; o segundo,* 15 *horas e, o terceiro,* 19 *horas. Determine quantas horas decorrerão, a partir da meia-noite, até que os três satélites passem ao mesmo tempo sobre à cidade do Recife.*

Solução: Lá na resolução, montamos um sistema de equações que transformando em um sistema de equação de congruências, obteremos: $\begin{cases} x \equiv 1\ (13) \\ x \equiv 4\ (15) \\ x \equiv 8\ (19) \end{cases}$. Apliquemos, aqui o Teorema Chinês dos Restos. Nele, temos que a solução é dada por $x = N_1y_1b_1 + N_2y_2b_2 + N_3y_3b_3$, onde $b_1 = 1, b_2 = 4, b_3 = 8, N_1 = 15.19, N_2 = 13.19, N_3 = 13.15$ e y_1, y_2, y_3 são soluções da equação $N_iy_i \equiv 1(a_i)$. Encontrando estes inversos multiplicativos, teremos:
$y_1N_1 \equiv 1\ (a_1) \Rightarrow 15.19y_1 \equiv 1\ (13) \Rightarrow 12y_1 \equiv 1\ (13) \Rightarrow y_1 \equiv 12\ (13) \Rightarrow y_1 = 12;$
$y_2N_2 \equiv 1\ (a_2) \Rightarrow 13.19y_2 \equiv 1\ (15) \Rightarrow 7y_2 \equiv 1\ (15) \Rightarrow y_2 \equiv 13\ (15) \Rightarrow y_2 = 13;$
$y_3N_3 \equiv 1\ (a_3) \Rightarrow 13.15y_3 \equiv 1\ (19) \Rightarrow 5y_3 \equiv 1\ (19) \Rightarrow y_3 \equiv 4\ (19) \Rightarrow y_3 = 4.$
Segue-se que a solução será dada por $x = 15.19.12.1 + 13.19.13.4 + 13.15.8.4 = 22504$, que módulo $13.15.19 = 3705$, resulta em $x = 274$. Então, teremos que o satélite, a partir da meia-noite de hoje, passarão juntos daqui a 274 horas.

Problema 3.9.5 *Um velho problema chinês: Três fazendeiros cultivavam juntos todo o seu arroz e o dividiam igualmente entre si no tempo da colheita. Um certo*

ano, cada um deles foi a um mercado diferente vender o seu arroz. Cada um destes mercados só comprava arroz em múltiplos de um peso padrão, que deferia em cada um dos mercados. O primeiro fazendeiro vendeu seu arroz em um mercado onde o peso padrão era de 87 *kg. ele vendeu tudo que podia e voltou para casa com* 18 *kg de arroz. O segundo fazendeiro vendeu todo o arroz que podia em um mercado cujo o peso padrão era de* 170 *kg e voltou para casa com* 58 *kg de arroz. O terceiro fazendeiro vendeu todo o arroz que podia em um mercado cujo peso padrão era de* 143 *kg e voltou (ao mesmo tempo que os outros dois) com* 40 *kg. Qual a quantidade mínima de arroz que eles podiam ter cultivado, no tocal?*

Solução: Após a colheita, o montante produzido de arroz é distribuido de forma igualitária entre os três fazendeiros. Então, seja x a quantidade de arroz de cada um dos fazendeiros. Equacionando o problema, teremos que:
Primeiro Fazendeiro: $x \equiv 18\ (87)$;
Segundo Fazendeiro: $x \equiv 58\ (170)$;
Terceiro Fazendeiro: $x \equiv 40\ (143)$.
De acordo com estas equações e como $87 = 3.29, 170 = 2.5.17, 143 = 11.13$, teremos o seguinte sistema de congruências:

$$\begin{cases} x \equiv 18\ (3) \Rightarrow x \equiv 0\ (3) \\ x \equiv 18\ (29) \Rightarrow x \equiv 18\ (29) \\ x \equiv 58\ (2) \Rightarrow x \equiv 0\ (2) \\ x \equiv 58\ (5) \Rightarrow x \equiv 3\ (5) \\ x \equiv 58\ (17) \Rightarrow x \equiv 7\ (17) \\ x \equiv 40\ (11) \Rightarrow x \equiv 7\ (11) \\ x \equiv 40\ (13) \Rightarrow x \equiv 1\ (13) \end{cases} \Rightarrow \begin{cases} x \equiv 0\ (6) \\ x \equiv 3\ (5) \\ x \equiv 1\ (13) \\ x \equiv 7\ (11) \\ x \equiv 7\ (17) \\ x \equiv 18\ (29) \end{cases}$$

Apliquemos agora, o Teorema Chinês dos Restos. Aqui, temos que: $b_1 = 0, b_2 = 3, b_3 = 1, b_4 = 7, b_5 = 7, b_6 = 18, N_1 = 5.13.11.17.29, N_2 = 6.13.11.17.29, N_3 = 6.5.11.17.29, N_4 = 6.5.13.17.29, N_5 = 6.5.13.11.29, N_6. = 6.5.13.11.17, a_1 = 6, a_2 = 5, a_3 = 13, a_4 = 11, a_5 = 17$ e $a_6 = 29$. Basta agora, encontrar os valores de $y_1, y_2, y_3, y_4, y_5, y_6$ que são dados por:
$y_1N_1 \equiv 1\ (a_1) \Rightarrow y_1.5.13.11.17.29 \equiv 1\ (6) \Rightarrow y_1.5.5.1.5.5 \equiv 1\ (6) \Rightarrow y_1 \equiv 1\ (6)$;
$y_2N_2 \equiv 1\ (a_2) \Rightarrow y_2.6.13.11.17.29 \equiv 1\ (5) \Rightarrow y_2.1.3.1.2.4 \equiv 1\ (5) \Rightarrow y_2.4 \equiv 1\ (5) \Rightarrow y_2 \equiv 4\ (5)$;
$y_3N_3 \equiv 1\ (a_3) \Rightarrow y_3.6.5.11.17.29 \equiv 1\ (13) \Rightarrow y_3.30.11.4.3 \equiv 1\ (13) \Rightarrow y_3.4.11.4.3 \equiv 1\ (13) \Rightarrow y_3.3.11.3 \equiv 1\ (13) \Rightarrow y_3.8 \equiv 1\ (13) \Rightarrow y_3 \equiv 5\ (13)$;
$y_4N_4 \equiv 1\ (a_4) \Rightarrow y_4.6.5.13.17.29 \equiv 1\ (11) \Rightarrow y_2.8.2.6.7 \equiv 1\ (11) \Rightarrow y_4 \equiv 1\ (11) \Rightarrow y_4 \equiv 1\ (11)$;
$y_5N_5 \equiv 1\ (a_5) \Rightarrow y_5.6.5.13.11.29 \equiv 1\ (17) \Rightarrow y_5.13.13.11.12 \equiv 1\ (17) \Rightarrow y_5.16.11.12 \equiv 1\ (17) \Rightarrow y_5.(-11).12 \equiv 1\ (17) \Rightarrow y_5.72 \equiv 1\ (17); \Rightarrow 4y_5 \equiv 1\ (17) \Rightarrow y_5 \equiv 13\ (17)$
$y_6N_6 \equiv 1\ (a_6) \Rightarrow y_6.6.5.13.11.17 \equiv 1\ (29) \Rightarrow y_6.13.11.17 \equiv 1\ (29) \Rightarrow y_6.27.17 \equiv 1\ (29) \Rightarrow y_6.(-2).17 \equiv 1\ (29) \Rightarrow y_6.(-34) \equiv 1\ (29); \Rightarrow 24y_6 \equiv 1\ (29) \Rightarrow y_6 \equiv$

23 (29).
Assim, segue-se que a solução será dada por:
$x = N_1.y_1.b_1 + N_2.y_2.b_2 + N_3.y_3.b_3 + N_4.y_4.b_4 + N_5.y_5.b_5 + N_6.y_6.b_6$ módulo o produto dos modulandos.
$x = 5.13.11.17.29.1.0 + 6.13.11.17.29.4.3 + 6.5.11.17.29.5.1 + 6.5.13.17.29.1.17 + 6.5.13.11.29.13.7 + 6.5.13.11.17.23.18 = 48.749.598$ que módulo $6.5.13.11.17.29 = 2.114.970$ nos dá 105.288 kg de arroz.

Problema 3.9.6 *Resolver o sistema de congruências* $\begin{cases} 2x + 7y \equiv 2\ (5) \\ 3x - y \equiv 1\ (5) \end{cases}$.

Solução: Observando a segunda equação do sistema de congruências e a multiplicando por 7, teremos $21x - 7y \equiv 7\ (5)$. Temos agora o seguinte sistema congruências:
$\begin{cases} 2x + 7y \equiv 2\ (5) \\ 21x - 7y \equiv 7\ (5) \end{cases}$. Aplicando a **Proposição 3.1.2 item (i)**, vamos obter:
$23x \equiv 9\ (5) \Rightarrow 3x \equiv 4\ (5)$. Como em $\mathbb{Z}_5$ o inverso multiplicativo de 3 é 2, então segue-se que multiplicando a congruência $3x \equiv 4\ (5)$ por 2, teremos $2.3x \equiv 4.2\ (5) \Rightarrow x \equiv 3\ (5)$. Logo, $x = 3 + 5t$, $t \in \mathbb{Z}$. Para encontrar os valores y, usemos a equação $2x + 7y \equiv 2$ $2x + 7y \equiv 2\ (5) \Rightarrow 2(3 + 5t) + 7y \equiv 2\ (5) \Rightarrow 6 + 10t + 7y \equiv 2\ (5) \Rightarrow 2y + 1 \equiv 2\ (5) \Rightarrow 2y \equiv 1\ (5)$. Como em $\mathbb{Z}_5$ o inverso multiplicaivo de 2 é 3, então segue-se que multiplicando a congruência $2y \equiv 1\ (5)$ por 3, tem-se $y \equiv 3(5)$. Logo, $y = 3 + 5s$, $s \in \mathbb{Z}$. Conclui-se que a solução do sistema é $x = 3 + 5t$ e $y = 3 + 5s$.

Capítulo 4

Aplicação do Teorema Chinês dos Restos

4.1 Partilha de Senhas

"Três pessoas só conseguem guardar um segredo,
se duas delas já estiverem mortas"
Benjamim Franklim.

4.1.1 Introdução

A partilha de senhas é uma maneira muito eficiente de se distribuir uma chave entre várias pessoas. Principalmente em grandes corporações, a ideia é bastante utilizada na proteção de dados e processos que necessitam de um nível maior de segurança. A proposta central é dividir uma senha entre várias pessoas de forma que nenhuma delas tenha posse da senha inteira e que não sejam necessárias todas as "partes"para se ter a chave reconstruída. Trazendo o problema para o campo prático, imagine alguns exemplos:

Exemplo 4.1.1 *Um banco onde empréstimos de grandes somas só possam ser liberados se forem aprovados por, no mínimo, três gerentes de um grupo de cinco.*

Exemplo 4.1.2 *A recuperação de dados criptografados de funcionários de empresas onde são necessárias as aprovações de pelo menos dois gestores de segurança em um grupo de três.*

Exemplo 4.1.3 *Suponha que um banco possua cinco gerentes e um grande cofre no qual possui uma imensa fortuna no seu interior. É sabido que para abrir tal cofre se faz necessário o uso de uma senha específica. Por medida de segurança, o*

banco entrega a cada um dos cinco gerentes uma chave de acesso, no qual um ou dois gerentes não consigam desvendar este segredo, apenas três ou mais gerentes.

Generalizando, a solução permite que a responsabilidade seja compartilhada entre várias pessoas, garantindo que a transação só seja efetuada com um número seguro de autorizações e ainda proteja o sistema em caso de morte, demissão, etc.. Assim, sendo este segredo criptografado com uma chave de segurança, estamos preocupados com a possibilidade da chave se perder e não mais conseguir a informação. O modelo da partilha de senhas que analisaremos é incrivelmente simples e eficaz.

4.1.2 O Algoritmo da Partilha de Senhas

Um esquema de divisão de senhas é caracterizado por um par $\{k, n\}$, onde k representa a quantidade de pessoas necessárias para recuperar o segredo ou senhas e n a quantidade de pessoas que estão envolvidas no caso. Por exemplo, o par $\{7, 12\}$ significa que 12 pessoas receberão uma chave (uma parte da senha) e que bastam 7 pessoas (escolhidas aleatoriamente) para recuperá-los, se juntarem suas respectivas partes. Pelo fato de haver um compartilhamento de senhas, vamos exigir que $n > 2$ e $2 < k < n$.

O conteúdo para se realizar esta partilha de senhas é o Teorema Chinês dos Restos. A grande vantagem deste método da partilha, é que todas as pessoas recebem chaves distintas uma das outras, de forma que uma pessoa sozinha não consiga decifrar a senha, e consequentemente desvendar o segredo. Outra vantagem é que não é necessária a presença de todas as pessoas com suas respectivas chaves, bastam que k ou mais pessoas se façam presentes no momento.

Considere $\mathbb{S}$ o conjunto formado pelas chaves que cada pessoa vai receber, k a quantidade de pessoas que são necessárias para desvendar a senha, no qual vamos denominar de s; e n a quantidade de pessoas que irão receber as chaves. Então, teremos que $\mathbb{S}$ contém exatamente n chaves, onde para cada $k \leq n$ previamente escolhido, tem-se que:
(i) *Qualquer subconjunto de* $\mathbb{S}$ *com* k *elementos permite determinar* s *facilmente;*
(ii) *É muito difícil determinar* s *com menos de* k *elementos de* $\mathbb{S}$.

O primeiro passo é construir um conjunto $\mathbb{F}$ formado por números inteiros positivos e distintos quaisquer, dois a dois coprimos, de forma que sua cardinalidade seja igual à quantidade de pessoas que receberão a chave, isto é, o conjunto deve possuir exatamente n elementos. Vamos definir dois números M e N com as seguintes características:
(i) N é o produto dos k menores números do conjunto $\mathbb{F}$;
(ii) M é o produto dos $k-1$ maiores números do conjunto $\mathbb{F}$.
Achados M, N devemos escolher a senha s, que deve estar contida no intervalo

$]M, N[$ ou $]N, M[$. Veremos adiante, escolhendo o conjunto $\mathbb{F}$ de tal forma que $N < M$, o algoritmo não funciona. Então, vamos considerar a escolha do conjunto $\mathbb{F}$, de tal forma que $M < s < N$. Até aqui, temos as seguintes informações:
(i) $\mathbb{F} = \{p_1, p_2, p_3, ..., p_n\}$ com $(p_i, p_j) = 1,\ \forall i \neq j$, com $i, j \in \{1, 2, ..., n\}$, supondo que os elementos de $\mathbb{F}$ estejam em ordem crescente;
(ii) k o número de pessoas que se deseja estarem presentes para a decifragem da senha;
(iii) $N = p_1.p_2...p_k$, produto dos k números menores do conjunto $\mathbb{F}$;
(iv) $M = p_x.p_{x+1}...p_n$, produto dos $k-1$ números maiores do conjunto $\mathbb{F}$;
(v) s é a senha aleatória que não tem relação alguma com $\mathbb{F}$, no qual deve ser escolhida no intervalo $M < s < N$;

Diante desses dados, vamos agora construir o conjunto $\mathbb{S}$, cujo elementos são as chaves que serão entregues a cada uma das n pessoas. Esses elementos são pares de números da forma (p_i, s_p), onde $p_i \in \mathbb{F}$ e s_p é a forma reduzida de s módulo p_i, isto é, s_p é solução da congruência $s \equiv s_p(p_i)$. Então supondo que sejam conhecidas $t \geq k$ pares de elementos de $\mathbb{S}$, isto é, existam t pessoas presentes na decifragem, o conjunto $\mathbb{S}$ será formado pelos pares:

$$\mathbb{S} = \{(p_1, s_1), (p_2, s_2), ..., (p_t, s_t)\}$$

Assim, para se chegar a senha s (finalmente), se faz necessário resolver o sistema de congruências:

$$\begin{cases} x \equiv s_1\ (p_1) \\ x \equiv s_2\ (p_2) \\ \quad\ \vdots \\ x \equiv s_t\ (p_t) \end{cases}$$

Aplicamos o poderoso Teorema Chinês dos Restos, no qual provamos que a solução deste sistema é única. Vamos resolver um problema numérico e ver como funciona este algoritmo da partilha das senhas:

Exemplo 4.1.4 *Em um banco há cinco funcionários responsáveis pela manutenção da senha de um cofre, e pelo menos duas pessoas têm que estar presentes para a abertura da mesma.*
a) Construir a senha s e as chaves a serem entregues cada à funcionário;
b) Desvendar a senha.

a) **Primeiro Passo:** Construção dos Conjuntos $\mathbb{F}$ e $\mathbb{S}$.
(i) Temos que $n = 5$, o qual corresponde ao número de pessoas que receberão uma chave; tem-se também que $k = 2$, que é o número de pessoas que deverão estar presentes na abertura da senha;
(ii) Vamos contruir agora, o conjunto $\mathbb{F}$ que deve possuir $n = 5$ números inteiros

positivos dois a dois coprimos. Tome $\mathbb{F} = \{11, 13, 15, 17, 19\}$, por exemplo;
(iii) Calculemos os valores de M e N:
Como $k = 2$, então os dois menores números inteiros do conjunto $\mathbb{F}$ são 11 e 13. Logo, $N = 11.13 = 143$. Segue-se também, que como $k = 2$ e $k - 1 = 1$, então o maior número inteiro do conjunto $\mathbb{F}$ é 19. Logo, $M = 19$;
(iv) Então, para escolher a senha s, tome s no intervalo $19 < s < 143$. Seja $s = 50$;

Segundo Passo: (v) Vamos construir o conjunto $\mathbb{S}$. Como $s = 50$ e sabendo que $50 \equiv 6\ (11)$, $50 \equiv 11\ (13)$, $50 \equiv 5\ (15)$, $50 \equiv 16\ (17)$, e $50 \equiv\ 12\ (19)$, segue-se que o conjunto $\mathbb{S}$ é formado pelos pares $\{(11, 6), (13, 11), (15, 5), (17, 16), (19, 12)\}$. Estas são as chaves que cada um dos funcionários terão em mãos.

b) **Terceiro Passo:** Desvendando a senha.
Pelo problema, ao escolhermos duas chaves quaisquer deste conjunto podemos desvendar a senha, pois $k = 2$. Digamos $(15, 5)$ e $(19, 12)$. Para isso, vamos resolver o sistema de congruências: $\begin{cases} x \equiv 5\ (15) \\ x \equiv 12\ (19) \end{cases}$.
Pelo Teorema Chinês dos Restos, sabemos que este sistema admite solução, pois $(15, 19) = 1 | (12 - 5)$ e é única módulo $15.19 = 285$. Temos aqui, que $b_1 = 5, b_2 = 12, N_1 = 19, N_2 = 15$. A solução deste sistema é dada por $x = N_1 y_1 b_1 + N_2 y_2 b_2$ módulo 285. Encontrando os valores de y_1, y_2, teremos:
$y_1 N_1 \equiv 1\ (a_1) \Rightarrow 19y_1 \equiv 1\ (15) \Rightarrow 4y_1 \equiv 1\ (15) \Rightarrow y_1 \equiv 4\ (15)$;
$y_2 N_2 \equiv 1\ (a_2) \Rightarrow 15y_2 \equiv 1\ (19) \Rightarrow y_2 \equiv 14\ (19)$.
Segue-se que a solução será $x = 19.5.4 + 15.12.14 = 380 + 2520 = 2900$ que módulo 285 nos dá $x = 50$, isto é, a senha é $s = 50$, como havíamos previsto no início do problema.

4.2 Porque o Método Funciona?

Suponha que existam n pessoas nos quais k delas receberão, cada uma delas, uma chave (uma parte da senha). Vamos mostrar porque o método funciona. Para tanto, formado o conjunto $\mathbb{S}$, temos que provar que para todo $k \leq n$ previamente escolhido, terá que satisfazer as condições seguintes:
(i) *Qualquer subconjunto de* $\mathbb{S}$ *com* k *elementos permite determinar a senha* s *facilmente;*
(ii) *É muito difícil determinar a senha* s *com menos de* k *elementos do conjunto* $\mathbb{S}$.

Quando definimos o conjunto $\mathbb{F}$ e calculamos os valores de M, N, podemos obter $N > M$ *ou* $N < M$. Vamos mostrar através de um contra-exemplo que o caso em que $N < M$ o algoritmo não funciona perfeitamente.

Exemplo 4.2.1 *Tomemos o* ***Exemplo 5.1.4*** *que nos diz: Em um banco há cinco funcionários responsáveis pela manutenção da senha de um cofre, e pelo menos duas pessoas têm que estar presentes para a abertura da mesma.*
a) Construir a senha s e as chaves a serem entregues cada à funcionário;
b) Desvendar a senha.

Solução: Vamos escolher o conjunto $\mathbb{F} = \{2, 3, 5, 7, 11\}$. Então, definindo os valores de M e N teremos $N = 2.3 = 6$ e $M = 11$. Tome uma senha s no intervalo $6 < s < 11$. Seja $s = 8$, por exemplo. Produzindo o conjunto $\mathbb{S}$, formado pelas chaves de acesso (p_i, s_i) entregues a cada funcionário, teremos:

$$s_i \equiv s\ (p_i) \Rightarrow \begin{cases} 8 \equiv 0\ (2) \Rightarrow (2, 0) \\ 8 \equiv 2\ (3) \Rightarrow (3, 2) \\ 8 \equiv 3\ (5) \Rightarrow (5, 3) \\ 8 \equiv 1\ (7) \Rightarrow (7, 1) \\ 8 \equiv 8\ (11) \Rightarrow (11, 8) \end{cases}$$

Vamos escolher agora, duas chaves aleatórias deste conjunto. Tomemos $(2, 0)$ e $(3, 2)$. Então, resolvendo o sistema:

$$\begin{cases} x \equiv 0\ (2) \\ x \equiv 2\ (3) \end{cases}$$

vamos obter $x = 2$, isto é a senha será 2, absurdo, pois a senha escolhida foi 8. É claro que fazendo uma busca, podemos encontrar a senha, pois ela é da forma $s = 2 + 6k$.

Então, para provar que o método funciona, vamos assegurar que $M < N$ e para tanto, vamos seguir a ideia do **Exemplo 5.1.4**. O Primeiro passo, está na construção dos conjuntos $\mathbb{F}$ e $\mathbb{S}$. Temos um conjunto com n pessoas, onde k delas receberão uma chave. Este k é denominado de limiar. Segue-se então que o conjunto $\mathbb{F}$ terá exatamente n números inteiros positivos dois a dois coprimos. Digamos $\mathbb{F} = \{p_1, p_2, ..., p_n\}$, onde $(p_i, p_j) = 1$, $\forall i \neq j$. Calculemos agora os valores de M e N. Observando conjunto $\mathbb{F}$ (supondo que seus elementos estejam em ordem crescente), temos que N é o produto dos k menores números inteiros positivos e M o produto dos $k - 1$ maiores números inteiros positivos, isto é,

$$\mathbb{F} = \{\ \overbrace{p_1, p_2, ..., p_k}^{k\ menores\ inteiros}\ , p_{k+1}, ..., p_{s-1},\ \underbrace{p_s, p_{s+1}, ..., p_n}_{k-1\ maiores\ inteiros}\ \} \Rightarrow$$

$N = p_1.p_2...p_k$ *e* $M = p_s.p_{s+1}...p_n$.

Vamos escolher a senha s de tal forma que $M < s < N$. Então, o conjunto $\mathbb{S}$, conjunto este formado pelas chaves que cada pessoa vai receber, é formado pelos pares (p_i, s_i), onde $p_i \in \mathbb{F}$ e s_i é a forma reduzida de s módulo p_i. Note que, quando $k > 1$, teremos que $p_i < s$, para qualquer $p_i \in \mathbb{F}$, pois, teremos que

$p_i < M < s < N$. Portanto, na congruência $s \equiv s_i\ (p_i)$ sempre teremos que $s_i < p_i < s$.

Suponha que são conhecidos t pares dentre os elementos do conjunto $\mathbb{S}$, tal que $t \geq k$. Então, teremos as seguintes chaves de acesso conhecidas: $(p_1, s_1), (p_2, s_2), ...,$ $(p_k, s_k), ..., (p_t, s_t)$, obtendo assim, o seguinte sistema de congruências:

$$\begin{aligned} x &\equiv s_1\ (p_1) \\ x &\equiv s_2\ (p_2) \\ &\vdots \\ x &\equiv s_k\ (p_k) \\ &\vdots \\ x &\equiv s_t\ (p_t) \end{aligned} \tag{4.1}$$

De acordo com Teorema Chinês dos Restos, sabemos que a solução deste sistema é única módulo o produto dos modulandos. Seja x_0 a solução deste sistema. Então, segue-se que $x = x_0 + m.(p_1.p_2...p_k...p_t)$, com $m \in \mathbb{Z}$. Será que $x_0 = s$? Como $t \geq k$, temos que $s < N = p_1.p_2...p_k \leq (p_1.p_2...p_k...p_t)$. Portanto, segue-se que $s < p_1.p_2...p_k...p_t$. Como o sistema **4.1** admite solução única menor que $p_1.p_2...p_k...p_t$ e que s também solução do sistema, então segue-se que $s = x_0 + m.(p_1.p_2...p_k...p_t)$, ou seja, $s \equiv x_0\ (p_1.p_2...p_k...p_t)$. Como $x_0 < p_1.p_2...p_k...p_t$ e $s < p_1.p_2...p_k...p_t$, então segue-se que $s = x_0$. Provamos aqui o item (i).

Provaremos agora o item (ii). E se $t < k$? Nada nos impede de resolver um sistema com menos de k equações. O problema é que o produto de menos de k módulos de $\mathbb{F}$ é sempre menor que s. Assim, a solução do sistema é um número congruente a s, mas não pode ser igual a s. É claro que é sempre possivel encontrar s fazendo uma busca. De fato, sabemos que $M < s < N$ e que s satisfaz o sistema **(4.1)**, só que agora com $t < k$. Seja x_0 uma solução do sistema. Como $x_0 < M < s$, pois teremos que $p_1.p_2...p_t \leq M < s < N$. Sendo x_0 a solução dos sistema **(4.1)**, então pelo Teorema Chinês dos Restos, tem-se que $x = x_0 + y(p_1.p_2...p_t)$ com $y \in \mathbb{Z}$, isto é, $x_0 < p_1.p_2...p_t \leq M < s$. Conclui-se então que $x_0 < s$ e não $x_0 = s$. Assim, não encontramos s. Mas, o sistema **(4.1)** também é satisfeito por s, logo, $s = x_0 + y.(p_1.p_2...p_t)$, onde y é um inteiro positivo. Como $x_0 < M < s < N$ e $y = \dfrac{s - x_0}{(p_1.p_2...p_t)}$, temos que:

$$\begin{gathered} x_0 < M < s < N \Rightarrow M - x_0 < s - x_0 < N - x_0 \Rightarrow \\ \frac{M - x_0}{(p_1.p_2...p_t)} \leq \frac{s - x_0}{(p_1.p_2...p_t)} = y \leq \frac{N - x_0}{(p_1.p_2...p_t)}. \end{gathered}$$

Isto significa que precisamos fazer uma busca para achar o valor correto de y entre,

pelo menos $d = \left[\frac{N-M}{p_1.p_2...p_t}\right]$ inteiros. Escolhendo os módulos de forma que d seja muito grande, fica praticamente impossivel encontrar s através de uma busca.

4.3 Problemas Resolvidos

Problema 4.3.1 *Uma marcroempresa possui um grande cofre, no qual por motivo de segurança, todos os seis gerentes desta macroempresa estão de posse de uma chave de acesso e sua abertura somente é permitida com a presença de no mínimo três chaves de acesso.*
a) Suponha que foi utilizada a partilha de senhas como segurança e que o conjunto $\mathbb{F}$ *escolhido foi* $\{11, 13, 15, 17, 19, 23\}$ *e a senha escolhida é* 1200*, construir as chaves a serem entregues a cada gerente.*
b) Escolhendo-se três chaves aleatórias, descubra a senha, confirmando que realmente $s = 1200$.

Solução:
a) Temos $n = 6$, $k = 3$ e o conjunto $\mathbb{F} = \{11, 13, 15, 17, 19, 23\}$, onde encontramos os valores $N = 11.13.15 = 2145$ e $M = 19.23 = 437$. Observe que $M = 437 < s = 1200 < N = 2145$. As chaves a serem entregues a cada gerente da macroempresa é do tipo (s_i, p_i), onde $p_i \in \mathbb{F}$ e s_i é solução da congruência $s \equiv s_i\ (p_i)$. Então, segue-se que:
$gerente\ 1:\ 1200 \equiv 1\ (11)$;
$gerente\ 2:\ 1200 \equiv 4\ (13)$;
$gerente\ 3:\ 1200 \equiv 0\ (15)$;
$gerente\ 4:\ 1200 \equiv 10\ (17)$;
$gerente\ 5:\ 1200 \equiv 3\ (19)$;
$gerente\ 6:\ 1200 \equiv 4\ (23)$;
Então as chaves que serão entregues a cada gerente são pares ordenados do conjunto $\mathbb{S} = \{(11, 1), (13, 4), (15, 0), (17, 10), (19, 3), (23, 4)\}$.
b) Suponha que as chaves escolhidas sejam $(13, 4), (15, 0), (17, 10)$, no qual teremos o seguinte sistema de congruências:

$$\begin{cases} x \equiv 4\ (13) \\ x \equiv 0\ (15) \\ x \equiv 10\ (17) \end{cases}$$

Aplicando o Teorema Chinês dos Restos, cuja solução é dada por $x = N_1y_1b_1 + N_2y_2b_2 + N_3y_3b_3$, onde $b_1 = 4, b_2 = 0, b_3 = 10, N_1 = 15.17, N_2 = 13.17$ e $N_3 = 13.15$. Basta encontrar agora, os valores de y_1, y_2, y_3, onde:
$y_1.N_1 \equiv 1\ (13) \Rightarrow 15.17y_1 \equiv 1\ (13) \Rightarrow 8y_1 \equiv 1(13) \Rightarrow y_1 = 5$;
$y_2.N_2 \equiv 1\ (15) \Rightarrow 13.17y_2 \equiv 1\ (15) \Rightarrow 11y_2 \equiv 1(15) \Rightarrow y_2 = 11$;
$y_3.N_3 \equiv 1\ (17) \Rightarrow 13.15y_3 \equiv 1\ (17) \Rightarrow 8y_3 \equiv 1(17) \Rightarrow y_3 = 15$;

Então, teremos que a solução é dada por $x = 15.17.5.4 + 13.17.11.0 + 13.15.15.10 = 5100 + 0 + 29250 = 34350$ que módulo $13.15.17 = 3315$ nos dá $x = 1200$.

Problema 4.3.2 *Considerando o problema anterior, suponha que houve uma troca da senha e no momento da abertura do cofre, dispõe-se das chaves* $(11, 1), (13, 0), (23, 21)$. *Qual é a nova senha?*

Solução: Equacionando, vamos obter o seguinte sistema de congruências:
$\begin{cases} x \equiv 1\ (11) \\ x \equiv 0\ (13) \\ x \equiv 21\ (23) \end{cases}$.
Aplicando o Teorema Chinês dos Restos, vamos obter a seguinte solução:
$b_1 = 1, b_2 = 0, b_3 = 21, N_1 = 13.23, N_2 = 11.23, N_3 = 11.13$. Encontrando os inversos y_1, y_2, y_3, teremos:
$y_1 N_1 \equiv 1\ (11) \Rightarrow 13.23y_1 \equiv 1\ (11) \Rightarrow 2y_1 \equiv 1(11) \Rightarrow y_1 = 6$;
$y_2 N_2 \equiv 1\ (13) \Rightarrow 11.23y_2 \equiv 1\ (13) \Rightarrow 6y_2 \equiv 1\ (13) \Rightarrow y_2 = 11$;
$y_3 N_3 \equiv 1\ (23) \Rightarrow 11.13y_3 \equiv 1\ (23) \Rightarrow 5y_3 \equiv 1\ (23) \Rightarrow y_3 = 14$;
Logo, a solução será $x = 13.23.6.1 + 11.23.11.0 + 11.13.14.21 = 1794 + 0 + 42042 = 43836$ que módulo $11.13.23 = 3289$ nos resulta em $x = 1079$. Logo, a nova senha do cofre é 1079.

Capítulo 5

Proposta Pedagógica

5.1 A Sequência Didática

Nesta seção, vamos apresentar uma sugestão de como trabalhar em sala de aula alguns conteúdos apresentados neste trabalho. São eles: Congruências, Equações Diofantinas e o Teorema Chinês dos Restos. Nosso intuito é encontrar uma maneira de lecionar estes conteúdos de tal forma que possa facilitar o seu entendimento, além do mais, de forma que eles fiquem mais dinâmicos e mais simples sua compreensão. Vamos separar em tópicos, descrevendo cada um deles.

5.1.1 Congruências Lineares

Esta sequência didática tem como objetivo orientar o ensino da congruência para alunos do ensino fundamental e médio. É esperado que os alunos tenham conhecimento dos números inteiros. Este aplicação será útil em conteúdos como Números Complexos (potências de i), Trigonometria (arcos côngruos) e Divisibilidade (questões da OBMEP e OBM). É claro que o rigor destes conteúdos não será repassado a estes discentes, visto que o conhecimento acadêmico e o conhecimento escolar se distinguem pelas diversidades presentes em cada contexto.

Algoritmo Divisão Euclidiana

Antes de mostrar a divisão euclidiana, é importante ressaltar o seu histórico, citando o Livro de Euclides, Os Elementos, e sua importância na Matemática. Depois de apresentar este histórico enunciar a divisão euclidiana explicando as definições de quociente e resto na divisão entre dois números inteiros e depois produzir diversos exemplos de uma divisão encontrando estes valores.

Exemplo: Encontrar o resto e quociente das divisões a seguir:
a) 30 por 7
b) 56 por 9
c) -54 por 12
Observação: Além do aluno poder utilizar a divisão euclidiana, ele pode construir a reta numerada e usar outra técnica, que é de subtrações sucessivas.

Alguns Problemas Contextualizados:
1. Deseja-se repartir 45 canetas em 7 caixas. Quantas canetas ficarão em cada caixa e quantas canetas sobrarão fora das caixas?

2. Uma padaria recebeu uma encomenda para fazer 10.000 salgados. Se esta padaria tem capacidade para fazer 157 salgados por dia, em quantos dias serão feitos todos os salgados?

3. Em 11.720 dias há quantos meses? Quantos dias sobram?

4. Hoje é terça-feira. Que dia da semana será daqui 358 dias?

Definição e Notação de Congruências

Seria interessante mostrar o conceito geral e mostrar diversos exemplos numéricos que explorem a definição e a notação de congruência. A partir da definição, resolvemos vários problemas numéricos. Observe alguns:

Exemplo 5.1.1 *Temos que* $47 \equiv 22\ (5)$*, pois ao dividirmos* 47 *por* 5 *e* 22 *por* 5*, teremos que* $47 = 9.5 + 2$ *e* $22 = 4.5 + 2$*, isto é, ambos têm resto 2 na divisão por 5;*
Temos que $13 \not\equiv 16\ (7)$*, pois ao dividirmos* 13 *por* 7 *e* 16 *por* 7*, teremos que* $13 = 1.7 + 6$ *e* $16 = 2.7 + 2$*, isto é, ambos não têm o mesmo resto na divisão por* 7*;*

Propriedades de Congruências

Vistos os conceitos, chega a hora de trabalhar com os alunos as propriedades de congruências. Para começar, expomos a primeira proposição que diz:

Proposição 5.1.1 *Suponha que* $a, b, m \in \mathbb{Z}$*. Tem-se que* $a \equiv b\ (m)$ *se, e somente se* $m|(a - b)$*.*

A nível médio, podemos trabalhar esta proposição com uma imensa quantidade de exemplos numéricos e partindo dessa proposição, mostrar as propriedades da congruência (relações de equivalência).

5.1.2 Equações Diofantinas Lineares

Esta sequência diática terá como objetivo a mostrar ao corpo discente a importância das equações diofantinas lineares, bem encontrar suas soluções inteiras. No primeiro momento, mostramos o conceito de uma equação diofantina e bem como alguns exemplos. Um exemplo interessante é mostrar que nem sempre uma equação diofantina possui solução inteira, como por exemplo:
Problema 1: Verifique se a equação $2x + 6y = 13$ possui solução inteira.

Em um segundo momento, mostra-se em quais condições uma equação diofantina possui solução inteira, isto é, mostrar que uma equação diofantina possui solução inteira se e somente se o máximo divisor comum entres os coeficientes das incógnitas divide o termo independente. Como exemplos, citar algumas equações e verificar se elas possuem solução ou não.
Verificar se as equações abaixo possui solução inteira:
a) $2x + 6y = 15$;
b) $5x - 6y + 7z = 15$;

Em um terceiro momento, deve-se mostrar como encontrar a solução de uma equação diofantina linear, fazendo ele observar uma equação com mais de uma variável possui infinitas soluções inteiras. Por exemplo, considerando a equação $2x + 6y = 15$, podemos sugerir soluções desta equação. Daí, segue-se que a partir de uma solução particular, podemos encontrar a solução geral em função de um parâmetro. Alguns problemas que podem ser utilizados para aplicação das equações diofantinas lineares.

Problema 1: (OBM-1999) Quantos são os pares (x, y) de inteiros positivos que satisfazem a equação $2x + 3y = 101$?
a) 13 *b*) 14 *c*) 15 *d*) 16 *e*) 17

Problema 2: (OBM-1997) Uma das soluções inteiras e positivas da equação $19x + 97y = 1997$ é, evidentemente, $(x_0, y_0) = (100, 1)$. Além dessa, há apenas mais um par de números inteiros e positivos, (x_1, y_1), satisfazendo a equação. O valor de $x_1 + y_1$ é:
a) 23 *b*) 52 *c*) 54 *d*) 101 *e*) 1997

5.1.3 Teorema Chinês dos Restos

No capítulo 3, provamos o grande Teorema Chinês dos Restos, com todas as suas formalidades matemáticas. Este Teorema dos nos diz:

Sejam $a_1, a_2, ..., a_n$ números inteiros, tais que $(a_i, a_j) = 1$, para todo $i \neq j$, com

$i, j \in \{0, 1, ..., n\}$. Sendo $b_1, b_2, ..., b_n \in \mathbb{Z}$, então o sistema de congruências

$$\begin{cases} x \equiv b_1 \ (a_1) \\ x \equiv b_2 \ (a_2) \\ \quad \cdots \\ x \equiv b_n \ (a_n) \end{cases}$$

Admite solução única módulo o produto dos modulandos.

Pois bem, para um melhor compreendimento deste Teorema, podemos começar a desenvolvê-lo com apenas duas equações. No caso, vamos resolver um sistema de congruências com duas equações. Observe na seção 3.8 apresentamos um método de interpretação gráfica do Teorema Chinês dos Restos. Este seria um dos métodos, no qual podemos iniciar a apresentação do conteúdo. Com isso, o discente irá concreticamente perceber que o sistema sempre possui solução quando o mdc entre os modulandos é igual a 1 e quando este mdc entre os modulandos for diferente de 1 nem sempre o sistema admitirá solução. Por exemplo, o sistema $\begin{cases} x \equiv 3 \ (7) \\ x \equiv 5 \ (6) \end{cases}$, equivale ao seguinte problema: Quais os números inteiros que quando divididos por 7 deixa resto 3 e quando divididos por 6 deixa resto 5?

Neste caso, podemos construir a tabela gráfica e o problema será resolvido facilmente. Alguns problemas que podem ser úteis na aplicação do Teorema Chinês dos Restos usando a Interpretação Gráfica:

Problema 1: Um fogueteiro produziu fogos de artifício e aos colocá-los em 3 caixas percebeu que sobrava um fogos de artifício e quando separou em 5 caixas também sobrava um. Quantos fogos de artifício sobrarão se colocá-los em 15 caixas?

Problema 2: Um número positivo quando dividido por 5 deixa resto 4 e quando dividido 7 por deixa resto 6. Ao dividir este número por 35, qual será o seu resto?

Problema 3: Um camponês tem um certo número de ovos; quandos os divide por 3, sobra-lhe 1; quando os divide por 4, sobram 2 ovos; e quando os divide por 5, sobram 3. Qual a quantidade mínima de ovos que o camponês possui?

Problema 4: Três garimpeiros trabalhavam em um rio a procura de ouro. Certo dia, os três encontraram x pedras de ouro. Ao dividir as pedras em grupos, perceberam o seguinte: Se as pedras fossem separadas em grupos de 7 unidades, sobrariam 5 pedras de ouro; se separassem em grupos de 11 unidades, 8 pedras de ouro sobrariam e se separassem em grupos de 13 unidades, 4 pedras de ouro ficariam sobrando. Supondo que eles encontraram entre 1000 e 2000 pedras de ouro, quantas pedras de ouro foram encontradas?

Capítulo 6

Apêndice

6.1 Anéis

A teoria dos Anéis é um dos principais assuntos do vasto campo da álgebra. Ela foi introduzida na segunda década do século XX.

6.2 Conceitos e Propriedades

Seja $\mathbb{A}$ um conjunto e $(+)$ e $(.)$ duas operações em $\mathbb{A}$, denominadas de Adição e Multiplicação. A terna $(\mathbb{A}, +, .)$ será chamada de ***Anel*** se possuir as seguintes propriedades, sendo $a, b, c \in \mathbb{A}$:

Propriedades 6.2.1 (i) *Quanto à Adição:*
$(A1)$ *Associatividade:* $a + (b + c) = (a + b) + c$*;*
$(A2)$ *Comutatividade:* $a + b = b + a$*;*
$(A3)$ *Elemento Neutro: Existe* $0 \in \mathbb{A}$*, tal que* $a + 0 = 0 + a$*;*
$(A4)$ *Elemento Inverso Aditivo:* $a + (-a) = 0$*;*
(ii) *Quanto à Multplicação:*
$(M1)$ *Associatividade:* $a.(b.c) = (a.b).c$*;*
$(M2)$ *Comutatividade:* $a.b = b.a$*;*
$(M3)$ *Elemento Neutro:* $a.1 = 1.a = a$*;*
$(M4)$ *Distributividade em relação à Adição:* $a.(b + c) = ab + ac$*;*

Exemplos: Os conjuntos $\mathbb{Z}$, $\mathbb{Z}_m$ (veremos adiante o porquê), $\mathbb{Q}$, $\mathbb{R}$, são anéis, pois satisfazem todas as propriedades acima. Já o conjunto $\mathbb{N}$, não é um anel, pois a propriedade (A4) não é satisfeita.

Um anel $\mathbb{A}$ será chamado de domínio de integridade, se gozar da seguinte propriedade: (M5) Dados $a, b \in \mathbb{A}$, se $a \neq 0$ e $b \neq 0$, então $a.b \neq 0$, ou de maneira equivalente, se $a.b = 0$, então $a = 0$ ou $b = 0$.

Um elemento $a \in \mathbb{A}$ será dito invertível, se existir um elemento $b \in \mathbb{A}$ (inverso multiplicativo), tal que $a.b = 1$. O elemento b será chamado de inverso de a. O inverso de um elemento a será denotado por a^{-1}. Se todos os elementos não nulos deste anel admitirem inverso multiplicativo, então este anel será um corpo, pela **Definição 3.6.2**.

6.3 Homomorfismos de Anéis

As funções naturais no âmbito dos anéis são aquelas que preservam as operações. Tais funções são chamadas de homomorfismos.

Definição 6.3.1 *Considere dois anéis $\mathbb{A}$ e $\mathbb{B}$ e uma função $f : \mathbb{A} \longrightarrow \mathbb{B}$. Temos que f é um homomorfismo se valerem, para todos $a, b \in \mathbb{A}$, as seguintes propriedades:*
(i) $f(1) = 1$;
(ii) $f(a + b) = f(a) + f(b)$;
(iii) $f(a.b) = f(a).f(b)$;

Observação: Caso, um homomorfismo satisfaça apenas as condições (i) e (ii) ou apenas as condições (i) e (iii), teremos um homomorfismo de grupos aditivos e um homomorfismo de grupos multiplicativos, respectivamente.

Observe que as **Propriedades 4.2.1**, são as mesmas das classes de congruências. Então, podemos dizer que o conjunto $\mathbb{Z}_m$ também é um Anel, no qual chamamos de *anel das classes residuais módulo m ou anel quociente*. Assim, a aplicação:

$$\phi : \begin{array}{c} \mathbb{Z} \to \mathbb{Z}_m \\ a \mapsto [a] \end{array}$$

é um homomorfismo de anéis. De fato, temos que $f(1) = 1, f(a + b) = [a + b] = [a] + [b] = f(a) + f(b)$ e $f(a.b) = [a.b] = [a].[b] = f(a).f(b)$.

Definição 6.3.2 (Isomorfismo de Anéis) *Seja a função $f : \mathbb{A} \longrightarrow \mathbb{B}$. Quando f é um homomorfismo bijetivo, dizemos f é um isomorfismo. Assim, dois anéis que admitem um isomorfismo, são ditos isomorfos, isto é, possuem a mesma forma. Escrevemos $\mathbb{A} \simeq \mathbb{B}$.*

Proposição 6.3.1 *Se $f : \mathbb{A} \longrightarrow \mathbb{B}$ é um homomorfismo de anéis, então:*
(i) $f(0) = 0$;
(ii) Quaisquer que sejam $a, b \in \mathbb{A}$, temos que $f(a-b) = f(a)-f(b)$. Em particular, $f(-a) = -f(a)$;
(iii) Se f é bijetiva, então $f^{-1} : \mathbb{B} \longrightarrow \mathbb{A}$ é um homomorfismo de anéis.

Demonstração: (i) Queremos mostrar que $f(0) = 0$. Sabemos que f é um homomorfismo. Logo, $f(a+b) = f(a) + f(b)$. Tomando $a = b = 0$, teremos que $f(0) = f(0) + f(0)$. Subtraindo $f(0)$ em ambos os membros da equação, teremos $f(0) - f(0) = f(0) + f(0) - f(0) \Rightarrow 0 = f(0)$, como queríamos provar.
(ii) Vamos provar que $f(-a) = -f(a)$. De fato, como f é um homomorfismo, temos $f(a+b) = f(a)+f(b)$. Tomando $b = -a$, teremos $f(a+(-a)) = f(a)+f(-a) \Rightarrow f(0) = f(a) + f(-a)$. Como $f(0) = 0$, item (i), teremos que $f(a) + f(-a) = 0$. Subtraindo $f(a)$ em ambos membros da equação, segue-se $f(a) - f(a) + f(-a) = -f(a) \Rightarrow f(-a) = -f(a)$. Segue-se que $f(a-b) = f(a+(-b)) = f(a)+f(-b) = f(a) - f(b)$.
(iii) Suponha f bijetiva. Então, teremos que f é injetiva e sobrejetiva. Logo, teremos que $f(\mathbb{A}) = \mathbb{B}$. Então dados $y_1, y_2 \in \mathbb{B}$, existem $x_1, x_2 \in \mathbb{A}$, tal que $f^{-1}(y_1) = x_1$ e $f^{-1}(y_2) = x_2$. Queremos provar que f^{-1} é um homomorfismo. De fato, pois:
$f^{-1}(y_1+y_2) = f^{-1}(f(x_1)+f(x_2)) = f^{-1}(f(x_1+x_2)) = x_1+x_2 = f^{-1}(y_1)+f^{-1}(y_2)$;
$f^{-1}(y_1.y_2) = f^{-1}(f(x_1).f(x_2)) = f^{-1}(f(x_1.x_2)) = x_1.x_2 = f^{-1}(y_1).f^{-1}(y_2)$. Logo, f^{-1} é um homomorfismo.

Exemplo 6.3.1 *Considere a função* $f : \begin{array}{c} Z_8 \longrightarrow \mathbb{Z}_4 \\ [a] \mapsto [a] \end{array}$ *, onde* $[a_8] \in \mathbb{Z}_8$ *e* $[a_4] \in \mathbb{Z}_4$. *f é um homomorfismo?*

Temos que $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$ e que $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. Queremos saber se a função f acima é um homomorfismo. Sejam $[a_8], [b_8]$ e $[a_4], [b_4]$ classes de $\mathbb{Z}_8$ e $\mathbb{Z}_4$, respectivamente. Observe que:
$f([0_8]) = [0_4]$; $f([1_8]) = [1_4]$; $f([2_8]) = [2_4]$;
$f([3_8]) = [3_4]$; $f([4_8]) = [4_4] = [0_4]$; $f([5_8]) = [5_4] = [1_4]$;
$f([6_8]) = [6_4] = [2_4]$; $f([7_8]) = [7_4] = [3_4]$.
Pelos exemplos, percebe-se que a função f é sobrejetiva, mas não é injetiva, pois $f([3_8]) = f([7_8])$. Para que f seja um homomorfismo, temos que verificar suas propriedades:
(i) $f(1) = 1$, de fato, pois $f([1_8]) = [1_4]$.
(ii) $f(a+b) = f(a) + f(b)$ e $f(a.b) = f(a).f(b)$. Sendo $[a_8], [b_8] \in \mathbb{Z}_8$ e tomando $f([a_8]) = [a_4]$ e $f([b_8]) = [b_4]$, teremos que $f([a_8] + [b_8]) = [a_4 + b_4] = [a_4] + [b_4] = f([a_8]) + f([b_8])$. Analogamente, provamos $f(a.b) = f(a).f(b)$. Logo, a função $f : \mathbb{Z}_8 \longrightarrow \mathbb{Z}_4$ é um homomorfismo sobrejetivo.

Definição 6.3.3 *Considere as classes* $[a] \in \mathbb{A}$ *e* $[b] \in \mathbb{B}$. *Define-se produto cartesiano* $\mathbb{A} \times \mathbb{B}$ *como sendo um conjunto tal que* $([a], [b]) \in \mathbb{A} \times \mathbb{B}$.

Sejam os anéis $\mathbb{A}$ e $\mathbb{B}$. É possivel dotar o produto cartesiano $\mathbb{A} \times \mathbb{B}$ como um estrutura de anel munida das operações *soma* $((a, b)+(a'+b') = (a+a', b+b'))$ e o

produto $((a,b).(a'+b') = (a.a', b.b'))$. Então, dados os anéis $\mathbb{A}$ e $\mathbb{B}$, podemos afirmar que o produto cartesiano $\mathbb{A} \times \mathbb{B}$ também será um anel? A próxima proposição, nos garante que $\mathbb{A} \times \mathbb{B}$ também é um anel.

Proposição 6.3.2 *Se* $\mathbb{A}$ *e* $\mathbb{B}$ *são anéis, então o conjunto* $\mathbb{A} \times \mathbb{B}$ *também é um anel.*

Demonstração: Para provar que $\mathbb{A} \times \mathbb{B}$ é um anel, temos que verificar que o produto cartesiano satisfaz todas as propriedades de um anel. De fato, sendo $a, a', c \in \mathbb{A}$, $b, b', d \in \mathbb{B}$ temos que:
(i) **Comutatividade Adição e Produto**:
$(a,b) + (a',b') = (a+a', b+b') = (a'+a, b'+b) = (a',b') + (a,b)$ e $(a,b).(a',b') = (a.a', b.b') = (a'.a, b'.b) = (a',b').(a,b)$;
(ii) **Associatividade Adição e Produto**:
$(c,d) + [(a,b) + (a',b')] = (c,d) + (a+a', b+b') = (c+a'+a, d+b'+b) = [(c,d) + (a',b')] + (a,b)$ e $(c,d)[(a,b).(a',b')] = (c,d).(a.a', b.b') = (c.a'.a, d.b'.b) = [(c,d).(a',b')].(a,b)$;
(iii) **Elemento Neutro da Adição e Multiplicação**:
$(a,b) + (0,0) = (a,b)$ e $(a,b).(1,1) = (a,b)$;
(iv) **Inverso Aditivo**:
$(a,b) + (-a,-b) = (0,0)$.
Logo, teremos que $\mathbb{A} \times \mathbb{B}$ também é um anel.

Proposição 6.3.3 *Um elemento* $(a,b) \in \mathbb{A} \times \mathbb{B}$ *é inversível se, e somente se,* a *e* b *são inversíveis nos anéis* $\mathbb{A}$ *e* $\mathbb{B}$*, respectivamente. Denotamos o inverso de* (a,b) *por* $(a^{-1}, b^{-1}) = (a,b)^{-1}$.

Demonstração: Sejam os anéis $\mathbb{A}$ e $\mathbb{B}$. Sabemos que um elemento $a \in \mathbb{A}$ é inversível quando existe um elemento $a' \in \mathbb{A}$, tal que $a.a' = 1$. Denotamos a' por a^{-1}. Pois bem, supondo que a e b sejam inversíveis, então existe a^{-1} e b^{-1}, tal que $a.a^{-1} = 1$ e $b.b^{-1} = 1$, onde $a \in \mathbb{A}$ e $b \in \mathbb{B}$. Então teremos que: $(1,1) = (a.a^{-1}, b.b^{-1}) = (a,b).(a^{-1}, b^{-1})$.
Reciprocamente, suponha que o par ordenado (a,b) admita inverso, isto é, existe (c,d), tal que $(a,b).(c,d) = (1,1)$. Então teremos que $ac = 1$ e $bd = 1$. Segue-se que c e d são inversos de a e b.

Exemplo 6.3.2 *Prove que* $\mathbb{A} \times \mathbb{B}$ *nunca é um domínio de integridade.*

Solução: Sabemos que anel $\mathbb{A} \times \mathbb{B}$ é domínio de integridade quando $(a,b).(c,d) = (0,0)$, se e somente se $(a,b) = (0,0)$ ou $(c,d) = (0,0)$, com $a \in \mathbb{A}$ e $b \in \mathbb{B}$. Suponha que $a \neq 0$, $b = 0$, $c = 0$ e $d \neq 0$. Temos que $(a,0).(0,d) = (0,0)$. Logo, $\mathbb{A} \times \mathbb{B}$ nunca é domínio de integridade.

Proposição 6.3.4 *Dados o anel quociente $\mathbb{Z}_{mn}$, o anel cartesiano $\mathbb{Z}_m \times \mathbb{Z}_n$ e a função* $\psi : \begin{array}{c} \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \\ [a_{mn}] \mapsto ([a_m], [a_n]) \end{array}$ *, então ψ é um homomorfismo de anéis.*

Demonstração: Para mostrar que ψ é um homomorfismo, temos que verificar as propriedades da **Definição 6.3.1**:
(i) $\psi([1]) = ([1], [1])$. De fato, pois $\psi([1_{mn}]) = ([1_m], [1_n])$;
(ii) $\psi([a+b]_{mn}) = \psi([a]_m) + \psi([b]_n)$. De fato, pois $\psi([a+b]_{mn}) = ([a_m + b_m], [a_n + b_n]) = ([a_m] + [b_m], [a_n] + [b_n]) = ([a_m], [a_n]) + ([b_m], [b_n]) = \psi([a_{mn}]) + \psi([b_{mn}])$;
(iii) $\psi([a.b]_{mn}) = \psi([a]_m).\psi([b]_n)$. De fato, pois $\psi([a.b]_{mn}) = ([a_m.b_m], [a_n.b_n]) = ([a_m].[b_m], [a_n].[b_n]) = ([a_m], [a_n]).([b_m], [b_n]) = \psi([a_{mn}]).\psi([b_{mn}])$;
Logo, a função ψ é um homomorfismo de anéis. Caso, ψ seja uma função bijetiva, então ψ^{-1} também é um homomorfismo de anéis **Proposição 6.3.1, item (iii)**, então ψ será um isomorfismo de anéis.

Referências Bibliográficas

[1] Carl Benjamim Boyer. *História da Matemática*. Editora da Universidade de São Paulo, São Paulo, primeira edition, 1974.

[2] S.C. Coutinho. *Números Inteiros e Criptografia RSA*. IMPA, Rio de Janeiro, segunda edition, 2009.

[3] Howard Eves. *Introdução à História da Matemática*. Editora Unicamp, 2008.

[4] Adilson Gonçalves. *Introdução à Álgebra*. SBM, Rio de Janeiro, primeira edition, 2012.

[5] Abramo Hefez. *Elementos de Aritmética*. SBM, Rio de Janeiro, segunda edition, 2011.

[6] Abramo Hefez. *Curso de Álgebra*, volume 1. IMPA, Rio de Janeiro, quinta edition, 2013.

[7] Antonio Caminha Muniz Neto. *Tópicos de Matemática Elementar*, volume 5. SBM, Rio de Janeiro, primeira edition, 2012.

[8] John Stillwell. *Mathematics and Its History*, volume Volume 5, Teoria dos Números. Springer, San Francisco, USA, third edition, 2010.