Universidade Estadual de Campinas

Instituto de Matemática, Estatística e Computação Científica

Departamento de Matemática

Dissertação de Mestrado

EQUAÇÕES DIOFANTINAS CLÁSSICAS E APLICAÇÕES

por

Filardes de Jesus Freitas da Silva

Mestrado Profissional em Matemática - Campinas - SP

Orientador: Prof. Dr. Emerson Alexandre de Oliveira Lima

EQUAÇÕES DIOFANTINAS CLÁSSICAS E APLICAÇÕES

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Filardes de Jesus Freitas da Silva** e aprovada pela Comissão Julgadora.

Campinas, 31 de Julho de 2009.

Prof. Dr. Emerson A. de O. Lima
Orientador

Banca Examinadora:

1 Prof. Dr. Emerson Alexandre de Oliveira Lima

2 Prof. Dr. José Plinio de Oliveira Santos

3 Profa. Dra. Tatiana Bertoldi Carlos

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para a obtenção do título de **Mestre em Matemática**.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Fabiana Bezerra Müller – CRB8 / 6162

Silva, Filardes de Jesus Freitas da
Si38e Equações diofantinas clássicas e aplicações/Filardes de Jesus Freitas da Silva -- Campinas, [S.P. : s.n.], 2009.

Orientador : Emerson Alexandre de Oliveira Lima
Dissertação (mestrado profissional) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1.Equações diofantinas. 2.Congruências e restos. 3.Fermat, Teorema de. 4.Teoria dos números. I. Lima, Emerson Alexandre de Oliveira. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Classical diopantine equations and applications

Palavras-chave em inglês (Keywords): 1. Diophantine equations. 2. Congruences and residues. 3. Fermat's theorem. 4. Number theory.

Área de concentração: Teoria dos Números

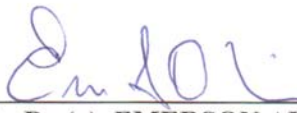
Titulação: Mestrado Profissional

Banca examinadora: Emerson Alexandre de Oliveira Lima – (UFRPE)
José Plínio de Oliveira Santos (IMECC-UNICAMP)
Tatiana Bertoldi Carlos (UFMGS)

Data da defesa: 31/07/2009

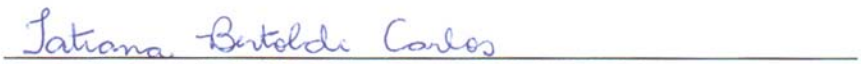
Programa de Pós-Graduação: Mestrado profissional em Matemática

Dissertação de Mestrado Profissional defendida em 31 de julho de 2009 e Aprovada pela Banca Examinadora composta pelos Profs. Drs.



Prof. (a). Dr (a). EMERSON ALEXANDRE DE OLIVEIRA LIMA

Prof. (a). Dr (a). JOSÉ PLÍNIO DE OLIVEIRA SANTOS



Prof. (a). Dr (a). TATIANA BERTOLDI CARLOS

Ao Senhor Deus e à minha familia.

"Toda a educação científica que não se inicia com a Matemática é, naturalmente, imperfeita na sua base ".
(Augusto Conte)

Agradecimentos

À Deus, em primeiro lugar;

Aos meus pais, Leonidas Domingos da Silva e Nair Freitas da Silva, por acreditarem em mim e aos meus amigos pelo apoio. Sem esse conjunto de pessoas nada disto poderia ter acontecido;

À minha noiva, Sâmia Josefina Brandão Silva pela compreensão e carinho;

Ao Prof°. Emerson Alexandre, que como orientador e amigo soube cobrar, mas também não mediu esforços em oferecer todas as condições necessárias à realização do presente trabalho;

Ao prof. Simão Stelmastchuk pela ajuda e generosidade em partilhar seus conhecimentos;

Às Universidades Estaduais de Campinas e do Maranhão e em especial ao CEFET-MA, conjuntamente com a Capes por propiciarem a realização do Mestrado Profissional em Matemática.

A todos os professores do Curso de Mestrado Profissional em Matemática, que de uma forma direta ou indireta contribuíram para a realização desse trabalho;

À minha sogra, Célia Dutra Brandão e aos amigos Robert Batista Pinheiro e Edvilson Silva, por suas palavras proféticas e interface entre mim e Sâmia;

Aos "frangotes" Marco, Emerson, Gladiston, Ronivaldo, Tubarão, Domingos, Nilson e Jotaquerles, amigos de todas as horas.

Ao Cristiano, Felix, Danilo e aos demais colegas do laboratório, que me ajudaram bastante e me "aturararem" por todos estes dias.

Resumo

FREITAS, Filardes J. S. *Equações Diofantinas Clássicas e Aplicações. Campinas - SP: Universidade Estadual de Campinas, 2009. Dissertação apresentada como requisito parcial para obtenção do Título de Mestre em Matemática.*

Neste trabalho focalizamos os principais conceitos da teoria elementar dos números objetivando uma melhor compreensão das Equações Diofantinas Clássicas e suas aplicações e para isto explicitamos os conceitos de Números primos, Algoritmo de Euclides, Máximo divisor comum e Mínimo múltiplo comum, assim como a teoria das Congruências, uma abordagem sobre a Criptografia RSA e Soma de Inteiros.

Palavras-Chave: Congruências Lineares, Soma de Inteiros, Equação de Fermat, Soma de Quadrados.

Abstract

FREITAS, Filardes J. S. *Classical diophantine equations and applications. Campinas - SP: Universidade Estadual de Campinas, 2009. Dissertation submitted as partial requirement for his Master's Degree in Mathematics.*

In this work we focus the main concepts of the elementary theory of numbers seeking a better understanding of Classical diophantine equations and their applications for this and explained the concepts of prime numbers, algorithms of Euclid, maximum common divisor and least common multiple and the theory of congruence , an approach on the RSA encryption and Sum of Integers.

Keywords: Linear congruence, Sum of Integers, equation of Fermat, Sum of Squares.

Sumário

Introdução

O objetivo desta dissertação, dentro dos propósitos deste programa, é o estudo e detalhamento de temas de interesse que tenham conexão com as disciplinas da área de matemática do ensino médio e superior, neste trabalho focalizaremos as equações diofantinas clássicas e suas aplicações e para isto, iniciaremos por uma revisão dos principais tópicos elementares da teoria dos números.

No primeiro capítulo, são introduzidos conceitos e definições da teoria elementar dos números, tais como, algoritmo de Euclides, máximo divisor comum, mínimo múltiplo comum, divisibilidade, congruências e criptografia RSA. No segundo capítulo faremos uma abordagem daS equações diofantinas representadas por soma de inteiros, um tópico de grande importância na análise combinatória com problemas que envolvem contagem.

Nos terceiro e quarto capítulos, abordamos as equações de Fermat numa perspectiva básica e avançada, sendo esta última com a contribuição dos Inteiros de Gauss e os Inteiros de Eisenstein dentro dos conceitos de Grupos, Anéis, Ideais e Soma de Quadrados.

Por fim, o quinto capítulo, mostraremos as aplicações das mais variadas equações diofantinas no campo da criptografia RSA e das funções geradoras, dentre outras, de modo que possamos ao final deste trabalho ter um material que de alguma forma possa contribuir para uma melhor compreensão das Equações Diofantinas.

Capítulo 1

UMA REVISÃO DA TEORIA ELEMENTAR DOS NÚMEROS

Neste capítulo enfatizaremos alguns conceitos da teoria dos números como o algoritmo de Euclides, máximo divisor comum e mínimo múltiplo comum de dois inteiros positivos além dos tópicos das congruências e resíduos que irão fortalecer e dinamizar as nossas aplicações.

1.1 Fatoração Única em $\mathbb{Z}$ e Algoritmo da Divisão

Para entendermos a fatoração única, precisamos em um primeiro momento definirmos dois números inteiros p e q, sendo que p divide q, se existir um inteiro k tal que $q = p.k$, com o uso da notação $p|q$. Se p não divide q escrevemos $p \nmid q$.

Todo número inteiro positivo $n \geq 2$ pode ser escrito de modo único, na forma,

$$n = p_1^{\theta_1}.p_2^{\theta_2}.\ldots.p_k^{\theta_k}$$

onde $1 < p_1 < p_2 < p_3 < \ldots < p_k$ são números primos e $\theta_1, \theta_2, \theta_3 \ldots \theta_k$ são inteiros positivos.

Os expoentes $\theta_1, \theta_2, \theta_3 \ldots \theta_k$ são chamados de multiplicidades. Em outras palavras a multiplicidade de p_1 é o maior expoente θ_1, tal que $p_1^{\theta_1}$ divide n. A representação por exemplo, do número 280 em fatoração única será $280 = 2^2.3^2.5$.

Dada a importância do algoritmo de Euclides para o nosso trabalho achamos oportuno iniciar com a seguinte proposição:

Proposição 1.1 *Sejam $a, b \in \mathbb{Z}$ com $b > 0$. Então existem únicos números inteiros q e r tais que*

$$a = qb + r \quad e \quad 0 \leq r < b$$

onde q chama-se quociente e r o resto da divisão de a por b.

Demonstração: Mostraremos em primeiro lugar a existência de q e r.
Dados $a, b \in \mathbb{Z}$ com $b > 0$, sendo o conjunto $S = \{a - bx | x \in \mathbb{Z},\ a - bx \geq 0\}$. Temos obviamente $S \subseteq \mathbb{N}^*$. Para $x = -|a|$ obtemos $a - bx = a - b(-|a|) = a + b|a| \geq a + |a| \geq 0$, pois $b \geq 1$. Isto mostra que $S \neq \emptyset$. Pelo princípio da indução temos que existe um $r \in S$ mínimo, isto é $r \leq y \ \ \forall y \in S$. Como $r \in S$ existe um $x = q \in \mathbb{Z}$ com $r = a - bq$. Segue então que $a = bq + r$. Precisamos provar que $0 \leq r < b$. Como $r \in S$ certamente $r \geq 0$ donde que $a - bq - b = r - b \geq 0$, ou seja, $r > a - (q + 1)\, b \in S$, contradizendo a minimalidade do $r \in S$. Isto mostra que $r \geq b$ é impossível. Logo temos que $r < b$.
Provaremos agora a unicidade de q e r.
Suponhamos que q, r, q' e r' são inteiros tais que

$$a = bq + r = bq' + r' \text{ e } 0 \leq r, r' < b$$

então $r' - r = bq - bq' = b(q - q')$ e segue $|r - r'| = |b(q - q')| = b|q - q'|$. Adicionando-se as desigualdades

$$\begin{cases} 0 \leq r\prime < b \\ -b < -r \leq 0 \end{cases}$$

Segue $-b < r' - r < b$, ou seja, $|r' - r| < b$. Daí temos a contradição

$$b > |r' - r| = b|q' - q| \geq b \ \ no\ caso\ de\ q \neq q'$$

Concluímos assim que $q = q'$ então $r = r'$. ■

Teorema 1.1 *(Algoritmo Geral da Divisão) Para quaisquer $a, b \in \mathbb{Z}$ com $b \neq 0$ existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = bq + r \text{ e } 0 \leq r < |b|$$

Demonstração: Como $|b| > 0$ pela Proposição 1.1 existem únicos $q', r \in \mathbb{Z}$ com $a = |b|\, q' + r$ tal que $0 \leq r < |b|$.
Se $b > 0$ então $|b| = b$ e podemos considerar $q = q'$ junto com r.
Se $b < 0$ então $|b| = -b$ e podemos considerar $q = -q'$ junto com r, obtendo

$$a = |b|\, q' + r = (-b)\, q' + r = b\,(-q') + r = bq + r$$

■

1.2 M.D.C. e M.M.C.

Definição 1.1 *Sejam a e b inteiros, com pelos menos um deles diferente de zero. O máximo divisor comum d de dois inteiros a e b (a ou b diferente de zero, denotado por (a, b) ou $mdc\,(a, b)$ é o maior inteiro que divide a e b.*

Teorema 1.2 *(Máximo divisor comum)*

1. *$d|a$ e $d|b$ (i. e. d é divisor comum de a e b.).*
2. *Se algum $c \in \mathbb{N}$ dividir ambos a e b então temos também $c|d$.*

Demonstração: Seja $d = mdc\,(a, b)$. Então, obviamente d verifica (1), e como $d \in D\,(a, b)$ a condição (2) afirma que, se $d' \in D\,(a, b)$, (D é o conjunto formados por divisores comuns de a e b), então, $d'|d$; logo $d' \leq d$, donde segue que d é o maior dos inteiros divisores comuns. Portanto, $d = mdc\,(a, b)$.

Proposição 1.2 *Se $a, b, c, x_1, y_1 \in \mathbb{Z}$, $c|a$ e $c|b$ então $c|\,(ax_1 + by_1)$*

Demonstração: Se $c|a$ e $c|b$ então $a = k_1 c$ e $b = k_2 c$, com $k_1, k_2 \in \mathbb{Z}$. Multiplicando estas duas equações respectivamente por x_1 e y_1, teremos $x_1 a = x_1 k_1 c$ e $y_1 b = y_1 k_2 c$. Somando membro a membro obtemos $ax_1 + by_1 = (x_1 k_1 + y_1 k_2)\, c$, o que nos diz que $c|ax_1 + by_1$. ■

Teorema 1.3 *Se a e b são inteiros e $a = qb + r$, onde q e r são inteiros , então* $(a, b) = (b, r)$.

Demonstração: Da relação $a = qb+r$ podemos concluir que todo divisor de b e r é um divisor de a pela Proposição 1.2. Esta última relação pode ser escrita como, $r = a - qb$ e nos diz que todo divisor de a e b é um divisor de r. Logo o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r, o que nos garante o resultado $(a, b) = (b, r)$. ■

Teorema 1.4 *Sejam $a, b \in \mathbb{Z}$ não ambos zero e seja $d = (a, b)$. Então existem $x_1, y_1 \in \mathbb{Z}$ tais que*

$$ax_1 + by_1 = d.$$

Demonstração: Consideremos o conjunto $B = \{ax + by : x, y \in \mathbb{Z}\}$ de todas as combinações lineares. Este conjunto contém, claramente, números negativos, positivos e também o zero. Tomando x_1 e y_1 tais que $c = x_1a + y_1b$ seja o menor inteiro positivo pertencente ao conjunto B, vamos provar que $c|a$ e $c|b$. Como as demonstrações são similares, mostraremos apenas que $c|a$. A prova é por cotradição. Suponhamos que $c \nmid a$, neste caso, pelo Teorema 1.1 existe q e r tais que $a = cq + r$ com $0 < r < c$. Portanto $r = a - qc = a - q(x_1a + y_1b) = (1 - qx_1)a + (-qy_1)b$. Isto mostra que $r \in B$, pois $(1 - qx_1)$ e $(-qy_1)$ são inteiros, o que é uma contradição, uma vez que $0 < r < c$ e c é o menor elemento positivo de B. Logo $c|b$.
Como d é um divisor de a e b, existem inteiros k_1 e k_2 tais que $a = k_1d$ e $b = k_2d$ e portanto $c = x_1a + y_1b = x_1k_1d + y_1k_2d = d(x_1k_1 + y_1k_2)$ o que implica que $d|c$, então que $|d| \leq |c|$, onde ambos são positivos e como $d < c$ é impossível, uma vez que d é o máximo divisor comum, podemos concluir que $d = ax_1 + by_1$. ■

Exemplo 1.1 *Sendo o $mdc\,(413280, 211243) = d$, com o auxílio do Algoritmo Euclidiano Estendido, determine uma solução $x_1, y_1 \in \mathbb{Z}$. De modo que* $413280x_1 + 211243y_1 = d$.

Resolução: Precisamos encontrar o valor de d e para isto, faremos uso do Algoritmo Euclidiano.

$a = qb + r \Rightarrow r = a - qb$

$413280 = 211243.1 + 202037 \Rightarrow 202037 = 413280 - 211243.1 \quad (1)$

$211243 = 202037.1 + 9206 \Rightarrow 9206 = 211243 - 202037.1 \quad (2)$

$202037 = 9206.21 + 8711 \Rightarrow 8711 = 202037 - 21.9206 \quad (3)$

$9206 = 8711.1 + 495 \Rightarrow 495 = 9206 - 8711.1 \quad (4)$

$8711 = 495.17 + 296 \Rightarrow 296 = 8711 - 495.17 \quad (5)$

$495 = 296.1 + 199 \Rightarrow 199 = 495 - 296.1 \quad (6)$

$296 = 199.1 + 97 \Rightarrow 97 = 296 - 199.1 \quad (7)$

$199 = 97.2 + 5 \Rightarrow 5 = 199 - 97.2 \quad (8)$

$97 = 5.19 + 2 \Rightarrow 2 = 97 - 5.19 \quad (9)$

$5 = 2.2 + 1 \Rightarrow 1 = 5 - 2.2 \quad (10)$

Logo, $d = 1$.

O próximo passo é escrever a expressão $ax_1 + by_1 = d$. e realizar as devidas substituições, assim:

$1 = 5 - 2.2$, substituindo a equação (9) em (10) e fazendo o mesmo procedimento com o resto das equações seguintes,temos:

$1 = 5 - 2.(97 - 5.19)$

$1 = 39.5 - 2.97$

$1 = 39.(199 - 97.2) - 2.97$

$1 = 39.199 - 80.97$

$1 = 39.199 - 80.(296 - 199.1)$

$1 = 119.199 - 80.296$

$1 = 119.(495 - 296.1) - 80.296$

$1 = 119.495 - 199.296$

$1 = 119.495 - 199.(8711 - 495.17)$

$1 = 3502.495 - 199.8711$

$1 = 3502.(9206 - 8711.1) - 199.8711$

$1 = 3502.9206 - 3701.8711$

$1 = 3502.9206 - 3701.(202037 - 21.9206)$

$1 = 81223.9206 - 3701.202037$

$1 = 81223.(211243 - 202037.1) - 3701.202037$

$1 = 81223.211243 - 84924.202037$

$1 = 81223.211243 - 84924.(413280 - 211243.1)$

$1 = 211243.166147 + 413280.(-84924)$

$d = 413280x_1 + 211243y_1$

$1 = 413280.(-84924) + 211243.166147$, ou seja, $x_1 = -84924$ e $y_1 = 166147$ uma solução inteira.

Teorema 1.5 *Se $a|bc$ e $(a, b) = 1$, então $a|c$.*

Demonstração: Como $(a, b) = 1$, pelo Teorema 1.3 existem x_1 e y_1 tais que $ax_1 + by_1 = 1$. Multiplicando os dois lados dessa igualdade por c, temos: $(ac)\,x_1 + (bc)\,y_1 = c$. Como $a|ac$ e, por hipótese, $a|bc$, então, pela Proposição 1.2, $a|c$. ■

Definição 1.2 *Chama-se mínimo múltiplo comum de dois inteiros positivos a e b o menor inteiro positivo que é divisível por a e b, denotado por $[a, b]$ ou $mmc\,(a, b)$.*

Proposição 1.3 *Sejam a e b inteiros não-nulos, então:*

(i) $[a, b] \geq max\,\{|a|, |b|\}$;
(ii) é único o $[a, b]$;
(iii) $[a, b] = [b, a]$;
(iv) $[a, b] = [|a|, |b|]$.

Teorema 1.6 *sejam a e b inteiros, com $a \neq 0$,$d = (a, b)$ e $m = [a, b]$. então vale a relação:*

$$md = |ab|$$

.

Demonstração: Coloquemos $m' = \dfrac{|ab|}{d}$. Existem $r, t \in \mathbb{Z}$ tais que $dr = a$ e $dt = b$. Temos $m' = \dfrac{|a|}{d}|b| = \pm rb$ e também $m' = |a|\dfrac{b}{d} = \pm at$. Isto mostra que m' é múltiplo comum de a e b. Se $c \in \mathbb{N}$, tal que $a|c$ e $b|c$ e Existem $k_1, k_2 \in \mathbb{Z}$ tais que $ak_1 = c = bk_2$. Pelo Teorema 1.2 existem $x_1, y_1 \in \mathbb{Z}$ com $ax_1 + by_1 = d$, então segue

$$\frac{c}{m'} = \frac{cd}{|ab|} = \frac{c}{|ab|}(ax_1 + by_1) = \frac{c}{|b|}\frac{ax_1}{|a|} + \frac{c}{|a|}\frac{by_1}{|b|} = \pm\frac{c}{b}x_1 \pm \frac{c}{a}y_1 = \pm k_2x_1 \pm k_1y_1 \in \mathbb{Z}$$

e mostramos que $\dfrac{c}{m'} \in \mathbb{Z}$ o que significa que $m'|c$. Assim $m' = m$. ■

1.3 Congruências

A teoria de congruências está relacionada ao nome do grande matemático alemão Carl Friedrich Gauss (1777 - 1855). A introdução das congruências torna natural a criação de um novo "sistema numérico" no qual são definidas as operações de adição e multiplacação: Os conjuntos $\mathbb{Z}_m$.

Definição 1.3 *Se a e b são inteiros dizemos que a é congruente a b módulo m, com $m > 0$, se $m|(a-b)$. Denotamos isto por $a \equiv b\,(mod\,m)$. Se $m \nmid (a-b)$ dizemos que a é incongruente a b módulo m e denotaremos por $a \not\equiv b\,(mod\,m)$.*

Proposição 1.4 *Se a e b são inteiros $m > 0$, temos $a \equiv b\,(mod\,m)$ se, e somente se, existir um inteiro k_1 tal que $a = b + k_1 m$.*

Demonstração: Se $a \equiv b\,(mod\,m)$, então $m|(a-b)$, o que implica que existe um inteiro k_1 tal que $a - b = k_1 m$, isto é, $a = b + k_1 m$. A recíproca é provada tomando um inteiro k_1 satisfazendo $a = b + k_1 m$, ou seja, $k_1 m = a - b$ e portanto $m|(a-b)$, resultando que $a \equiv b\,(mod\,m)$. ■

Proposição 1.5 *Sejam a, b, m e d inteiros com $m > 0$, então as seguintes sentenças são verdadeiras:*

(i) sempre $a \equiv a\,(mod\,m)$ $(Reflexividade)$;
(ii) se $a \equiv b\,(mod\,m)$ então $b \equiv a\,(mod\,m)$ $(Simetria)$;
(iii) se $a \equiv b\,(mod\,m)$ e $b \equiv d\,(mod\,m)$ então $a \equiv d\,(mod\,m)$ $(Transitividade)$;

Demonstração: (i) como $m|0$, então $m|(a-a)$, o que implica $a \equiv a\,(mod\,m)$. (ii) Se $a \equiv b\,(mod\,m)$, então $a = b + k_1 m$ para $k_1 \in \mathbb{Z}$, logo $b = a - k_1 m$, o que implica pela Proposição 1.4 que $b \equiv a\,(mod\,m)$. (iii) Se $a \equiv b\,(mod\,m)$ e $b \equiv d\,(mod\,m)$, então existem $k_1, k_2 \in \mathbb{Z}$, tais que $a - b = k_1 m$ e $b - d = k_2 m$. Somando-se membro a membro as duas equações, temos $a - d = (k_1 + k_2)\,m$. Fazendo $k_1 + k_2 = k_3$, obtemos $a - d = k_3 m$ o que implica $a \equiv d\,(mod\,m)$. ■

Esta proposição nos diz que a relação definida no conjunto dos inteiros é uma relação de equivalência pois ela é reflexiva, simétrica e transitiva.

Teorema 1.7 *Se* $(k, m) = d$, *então* $ak \equiv bk\,(mod m) \Rightarrow a \equiv b\left(mod\frac{m}{d}\right)$

Demonstração: Se $ak \equiv bk\,(mod m)$ implica que $m|\,(ka - kb)$, ou seja, que $m|k\,(a - b)$. Dividindo os dois membros por d, temos, $\frac{m}{d}|\frac{k}{d}\,(a - b)$, mas por hipótese $(k, m) = d$ e pelo Teorema 1.3, $\left(\frac{k}{d}, \frac{m}{d}\right) = 1$ o que implica que $\frac{m}{d}\,(a - b)$, e fazendo $k_1 = \frac{k}{d} \in \mathbb{Z}$ temos que $a \equiv b\left(mod\frac{m}{d}\right)$. ■

Teorema 1.8 *Se* $(k, m) = 1$, *então* $ak \equiv bk\,(mod m) \Rightarrow a \equiv b\,(mod m)$.

Demonstração: Se $ak \equiv bk\,(mod m)$ então $m|\,(ka - kb)$, ou seja, $m|k\,(a - b)$, mas, pelo Teorema 1.3, se $m|k\,(a - b)$ e $(k, m) = 1$ então $m|a - b$, o que implica $a \equiv b\,(mod m)$. ■

Teorema 1.9 *Sejam a, b, c e m inteiros tais que* $a \equiv b\,(mod m)$, *então:*

(i) $a + c \equiv b + c\,(mod m)$;
(ii) $a - c \equiv b - c\,(mod m)$;
(iii) $ac \equiv bc\,(mod m)$.

Demonstração: (i) como $a \equiv b\,(mod m)$, temos que $a - b = km$ e como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c\,(mod m)$. (ii) como $(a - c) - (b - c) = a - b$ e por hipótese $a - b = km$, então temos que $a - c \equiv b - c\,(mod m)$. (iii) como $a - b = km$, multiplicando os dois membros por c, temos $ac - bc = ckm$ o que implica $m|\,(ac - bc)$ e, portanto, $ac \equiv bc\,(mod m)$. ■

Teorema 1.10 *Se a, b, c, d e m são inteiros tais que* $a \equiv b\,(mod m)$ *e* $c \equiv d\,(mod m)$, *então:*

(i) $a + c \equiv b + d\,(mod m)$;
(ii) $a - c \equiv b - d\,(mod m)$;
(iii) $ac \equiv bd\,(mod m)$.

Demonstração: (i) como $a \equiv b\,(mod m)$ e $c \equiv d\,(mod m)$, temos que $a - b = k_1 m$ e $c - d = k_2 m$, portanto, fazendo a soma membro a membro, obtemos $(a + c) - (b + d) = (k_1 + k_2)\,m$ com $k_1, k_2 \in \mathbb{Z}$, isso implica que $a + c \equiv b + d\,(mod m)$. (ii) como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = km$, então $a - c \equiv b - c\,(mod m)$. (iii) Sabemos que $a - b = k_1 m$, multiplicando os dois membros por c e $c - d = k_2 m$ por b, temos $ac - bc = ck_1 m$ e $bc - bd = bk_1 m$. Somando membro a membro, temos $ac - bc + bc - bd = (ck_1 + bk_2)\,m$ o que implica $m|\,(ac - bd)$ e portanto, $ac \equiv bd\,(mod m)$. ■

1.4 Resíduos e Conjunto completo de resíduos módulo m

Definição 1.4 *Se a e r são inteiros com $a \equiv r\,(mod m)$, dizemos que r é um resíduo de a módulo m.*

Definição 1.5 *Chamamos de conjunto completo de resíduos módulo m ao conjunto de m números cada um dos quais é congruente a $0, 1, 2, \cdots, m - 1\,(mod m)$, isto é, um conjunto que contém um representante para cada uma das m classes nas quais os inteiros módulo m se dividem.*

Definição 1.6 *O conjunto dos inteiros $\{r_1, r_2, r_3, \cdots, r_s\}$ é um sistema completo de resíduos módulo m se:*
(i) $r_i \not\equiv r_j\,(mod m)$ para $i \neq j$;
(ii) para todo inteiro n existe um r_i tal que $n \equiv r_i\,(mod m)$.

Teorema 1.11 *Dois números inteiros x e y são congruentes $(mod m)$ se, e apenas se, a divisão de cada um deles por m tem o mesmo resíduo.*

Demonstração: Pela Proposição 1.1 podemos escrever $x = k_1 m + r$ e $y = k_2 m + s$ com $0 < r, s < m$. Se $m|\,(x - y)$ então $m|\,(r - s)$ e como $|r - s| < m$ teremos que ter $r - s = 0$ o que implica que $r = s$. ■

Teorema 1.12 *Qualquer número inteiro é congruente* $(mod\, m)$ *com um e só um dos elementos de* $\{0, 1, 2, \cdots, m-1\}$.

Demonstração: Dados $m \in \mathbb{N}$ e $x \in \mathbb{Z}$ pela Proposição 1.1 existem q e r únicos tais que $x = k_1 m + r$ com $0 \leq r < m$, portanto $x \equiv r\,(mod m)$ e $0 \leq r \leq m-1$. A unicidade resulta do Teorema 1.11. ■

Teorema 1.13 *Todos os sistemas completos de resíduos para um mesmo módulo têm o mesmo número de elementos.*

Demonstração: Consideremos um sistema completo de resíduos, digamos

$$R = \{r_1, r_2, r_3, \cdots, r_k\}$$

para um módulo $m > 1$ fixo; seja ainda $R_0 = \{1, 2, 3, \cdots, m-1\}$. De acordo com o Teorema 1.11, para cada $j = 1, 2, \cdots, k$ existe um e só um $r_o(j) \in R_0$ tal que $r_j \equiv r_o\,(j)\,(mod m)$, portanto R_0 tem pelo menos o mesmo número de resíduos de elementos de R; por outro lado R é também um sistema completo de resíduo e, por definição, para cada elemento de R_0 existe um e só um elemento de R com o qual aquele é congruente $(mod m)$, donde R tem pelo menos tantos elementos como R_0, ou seja R e R_0 têm de fato o mesmo número de elementos. ■

Exemplo 1.2 *Sendo* $\{0, 1, 2, 3, 4, 5, 6, 7\}$ *o conjunto dos menores restos não-negativos módulo 8, verifique se* $\{-28, -15, -6, 11, 15, 22, 101, 800\}$ *é um sistema completo de resíduos módulo 8.*

Resolução: Pela Definição 1.6, (i) $r_i \not\equiv r_j\,(mod m)$ para $i \neq j$, temos por exemplo $r_2 \not\equiv r_3\,(mod 8)$, implicando que $1 \not\equiv 2\,(mod 8) \Rightarrow 8 \nmid -1$ e (ii) para todo inteiro n existe um r_i tal que $n \equiv r_i\,(mod m)$, segue que

- Para $i = 1 \Rightarrow n = 800$, pois $800 \equiv 0\,(mod 8) \Rightarrow 8|800 \Rightarrow 100 = k_0 \in \mathbb{Z}$
- Para $i = 2 \Rightarrow n = -15$, pois $-15 \equiv 1\,(mod 8) \Rightarrow 8|-16 \Rightarrow -2 = k_1 \in \mathbb{Z}$
- Para $i = 3 \Rightarrow n = -6$, pois $-6 \equiv 2\,(mod 8) \Rightarrow 8|-8 \Rightarrow -1 = k_2 \in \mathbb{Z}$
- Para $i = 4 \Rightarrow n = 11$, pois $11 \equiv 3\,(mod 8) \Rightarrow 8|8 \Rightarrow 1 = k_3 \in \mathbb{Z}$

- Para $i = 5 \Rightarrow n = 4$, pois $-28 \equiv 4\,(mod 8) \Rightarrow 8|-32 \Rightarrow -4 = k_4 \in \mathbb{Z}$
- Para $i = 6 \Rightarrow n = 5$, pois $101 \equiv 5\,(mod 8) \Rightarrow 8|96 \Rightarrow 12 = k_5 \in \mathbb{Z}$
- Para $i = 7 \Rightarrow n = 6$, pois $22 \equiv 6\,(mod 8) \Rightarrow 8|16 \Rightarrow 2 = k_6 \in \mathbb{Z}$
- Para $i = 8 \Rightarrow n = 7$, pois $15 \equiv 7\,(mod 8) \Rightarrow 8|8 \Rightarrow 1 = k_7 \in \mathbb{Z}$

Observação 1.1 *Sendo $n \in \mathbb{N}$, $k_0, k_1, k_2, \cdots, k_{n-1} \in \mathbb{Z}$, então,*

$$\{n.k_0, n.k_1 + 1, n.k_2 + 2, \cdots, n.k_{n-1} + (n-1)\}$$

é um sistema completo de resíduos $(mod\, m)$. Além disso todo sistema completo de restos $(mod\, m)$ é obtido dessa forma.

No Exemplo 1.2, temos:

$$\{n.k_0, n.k_1 + 1, n.k_2 + 2, \cdots, n.k_{n-1} + (n-1)\} =$$

$$\{8.100, 8.(-2) + 1, 8.(-1) + 2, 8.1 + 3, 8.(-4) + 4, 8.12 + 5, 8.2 + 6, 8.1 + 7\} =$$

$$\{800, -15, -6, 11, -28, 101, 22, 15\}$$

1.5 Inverso Aritmético Módulo m e Congruências Lineares

Definição 1.7 *Um inverso aritmético de $a\,(mod\, m)$ é um número inteiro $\overline{a}$ tal que $\overline{a}.a \equiv a.\overline{a} \equiv 1\,(mod\, m)$.*

Teorema 1.14 *O número $a \in \mathbb{Z}\backslash\{0\}$ têm inverso aritmético $(mod\, m)$ se, e apenas se, $(a, m) = 1$*

Demonstração: Se $(a, m) = 1$, então existem $x, y \in \mathbb{Z}$, tais que $ax + my = 1$, por outro lado esta equação indica que $ax \equiv 1\,(mod\, m)$ e consequentemente, x é o inverso aritmético de $a\,(mod\, m)$, que existe se $(a, m) = 1$. Mas $a.\overline{a} \equiv 1\,(mod\, m)$, então deduz-se que $a.\overline{a} = km + 1$, para algum $k \in \mathbb{Z}$ pelo que $a.\overline{a} + (-k)\,m = 1$. Conclui-se assim,

que a e m são primos entre si. ■

Proposição 1.6 *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p se, e apenas se,* $a \equiv 1\,(mod p)$ *ou* $a \equiv -1\,(mod p)$.

Demonstração: Se a é o seu próprio inverso, então $a^2 \equiv 1\,(mod p)$ o que significa que $p|\,(a^2-1)$, mas se $p|\,(a-1)\,(a+1)$, sendo p um número primo, temos que $p|\,(a-1)$ ou $p|\,(a+1)$ o que nos leva a concluir que $a \equiv 1\,(mod p)$ ou $a \equiv -1\,(mod p)$. A recíproca também é imediata, pois se $a \equiv 1\,(mod p)$ ou $a \equiv -1\,(mod p)$ então $p|\,(a-1)$ ou $p|\,(a+1)$. Portanto $p|\,(a-1)\,(a+1)$ o que significa que $a^2 \equiv 1\,(mod p)$ ou ainda que $a.\overline{a} \equiv \overline{a}.a \equiv 1\,(mod p)$. ■

Exemplo 1.3 *Determine o inverso de* $211243\,(mod\ 413280)$.

Resolução: Neste caso, precisamos calcular o $mdc\,(413280, 211243)$ e aplicar o algoritmo euclidiano estendido, ver Exemplo 1.1, onde o $mdc\,(413280, 211243) = 1$ e $1 = 413280.(-84924) + 211243.(166147)$, ou seja, $x_1 = -84924$ e $y_1 = 166147$, logo o inverso de $211243\,(mod\ 413280)$ é $y_1 = 166147$, pois pela Definição 1.7, temos, $211243.(166171) \equiv 166171.(211243) \equiv 1\,(mod\ 413280)$.

Definição 1.8 *Chamamos de congruência linear em uma variável toda congruência da forma* $ax \equiv b\,(mod m)$, *onde x é uma incógnita.*

Teorema 1.15 *Se a têm inverso* $\overline{a}.\,(mod m)$, *então* $ax \equiv b\,(mod m)$ *se, e somente se,* $x \equiv \overline{a}b\,(mod m)$.

Demonstração: Supomos que $a.\overline{a} \equiv 1\,(mod m)$, logo se $ax \equiv b\,(mod m)$, então $\overline{a}.a.x \equiv \overline{a}b\,(mod m)$ ora $\overline{a}.a.x \equiv x\,(mod m)$, portanto $x \equiv \overline{a}b\,(mod m)$. Na volta teriamos que se $x \equiv \overline{a}b\,(mod m)$, analogamente, obtém-se $ax \equiv a.\overline{a}.b \equiv b\,(mod m)$ e daí $ax \equiv b\,(mod m)$. ■

Teorema 1.16 *Sejam a e b inteiros e $(a,b)=d$. Se $d \nmid c$ então a equação $ax+by=c$ não possui nenhuma solução inteira. Mas se $d|c$ essa equação possuirá infinitas soluções e se $x=x_0$ e $y=y_0$, teremos então uma solução particular e todas as demais soluções serão obtidas por $x=x_0+(b/d)\,k$ e $y=y_0-(a/d)\,k$, com k inteiro.*

Demonstração: Se $d \nmid c$, então a equação $ax+by=c$ não tem solução, como d é o máximo divisor comum de a e b, ele deveria dividir c, pois c é uma combinação linear de a e b. Suponhamos que $d|c$, pelo Teorema 1.2, existem x_1 e y_1, tais que $ax_1+by_1=c$. Entretanto se $d|c$, existe então um inteiro k de modo que $c=kd$, multiplicando ambos os membros da equação $ax_1+by_1=c$ por k, teremos $a(x_1k)+b(y_1k)=c$. Isso nos leva a concluir que o par ordenado (x_0,y_0), com $x_0=x_1k$ e $y_0=y_1k$ é uma solução da equação $ax+by=c$, uma vez que

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

Neste caso, (x_0,y_0) é uma solução particular e a partir dessa solução, podemos gerar infinitas soluções, para isso precisamos mostrar que toda equação do tipo $ax+by=c$, temos como soluções as expressãoes $x=x_0+(b/d)\,k$ e $y=y_0-(a/d)\,k$, entretanto iremos supor que o par ordenado (x,y), seja uma solução, logo poderemos escreve-la assim, $ax+by=c$, mas $ax_0+by_0=c$, logo $ax+by=ax_0+by_0$, o que implica em $a(x-x_0)=b(y_0-y)$, lembrando que $(a,b)=d$ recorrendo ao Teorema 1.6, $\left(\frac{a}{d},\frac{b}{d}\right)=1$, podemos, então dividir os dois termos da equação $a(x-x_0)=b(y_0-y)$ por d, temos $\frac{a}{d}(x-x_0)=\frac{b}{d}(y_0-y)$, pelo Teorema 1.3 $(b/d)\,|\,(x-x_0)$ e portanto existe um k, inteiro que satisfazendo $x-x_0=(b/d)\,k$ o que implica $x=x_0+(b/d)\,k$ e substituindo esse valor de na equação $\frac{a}{d}(x-x_0)=\frac{b}{d}(y_0-y)$, temos que $y=y_0-(a/d)\,k$. ■

Teorema 1.17 *Sejam a, b e m inteiros tais que $m>0$ e $(a,m)=d$. Se $d \nmid b$ a congruência $ax\equiv b(mod\,m)$ não possui nenhuma solução inteira e quando $d|b$, essa congruência possui exatamente d soluções incongruentes módulo m.*

Demonstração: Sabemos que x inteiro é solução da congruência $ax \equiv b\,(mod m)$ se, e somente se existir um inteiro y tal que pela Proposição 1.4 $ax = b + my$ que implica $ax - my = b$ e pelo Teorema 1.16, sabemos que esta equação não possui solução se $d \nmid b$, analisaremos agora quando $d|b$, para este caso a equação $ax - my = b$, possuirá infinitas soluções dadas por $x = x_0 - (m/d)\,k$ e $y = y_0 - (a/d)\,k$, onde (x_0, y_0) é uma solução particular da equação diofantina $ax - my = b$, objeto da nossa obordagem. Entretanto a congruência $ax \equiv b\,(mod m)$ possui infinitas soluções dadas por $x = x_0 - (m/d)\,k$. Para sabermos o número de soluções incongruentes, analisaremos sobre que condições as equações $x_1 = x_0 - (m/d)\,k_1$ e $x_2 = x_0 - (m/d)\,k_2$, são congruentes módulo m. Se x_1 e x_2 são congruentes então $x_0 - (m/d)\,k_1 \equiv x_0 - (m/d)\,k_2\,(mod m)$, implica dizer que $(m/d)\,k_1 \equiv (m/d)\,k_2\,(mod m)$ e como $(m/d)\,|m$, temos que $(m/d, m) = m/d$ e isso nos dá condição de aplicarmos o cancelamento de (m/d) na equação $(m/d)\,k_1 \equiv (m/d)\,k_2\,(mod m)$, consequência do Teorema 1.7, daí teremos $k_1 \equiv k_2\,(mod d)$, uma vez que podemos substituir m por d uma vez que $d = m/(m/d)$ e isso nos leva a identificar que as soluções incongruentes serão obtidas ao tomarmos $x = x_0 - (m/d)\,k$ uma vez que k é um inteiro que percorre todo o sitema completo de resíduos módulo d. ■

Teorema 1.18 *(Teorema de Wilson) Se p é primo, então $(p-1)! \equiv -1\,(mod p)$.*

Demonstração: Verificaremos para os primos 2 e 3 a veracidade do teorema de Wilson, então $(2-1)! \equiv -1\,(mod 2)$, implica que $2|2$ e $(3-1)! \equiv -1\,(mod 3)$, temos que $3|3$, logo o enunciado é verdadeiro para os primos 2 e 3. Suponhamos agora $p \geq 5$, pelo Teorema 1.16, a congruência $ax \equiv 1\,(mod p)$ onde a é qualquer dos $p-1$ inteiros positivos do conjunto $\{1, 2, 3, \ldots, p-1\}$ e como desses elementos apenas 1 e $p-1$ são seus próprios inversos módulo p, tais que $a \neq \overline{a}$, pelo Teorema 1.13, onde $a\overline{a} \equiv 1\,(mod p)$, com $1 \leq \overline{a} \leq p-1$, podemos então agrupar os numeros $2, 3, \ldots, (p-2)$ em $\dfrac{(p-3)}{2}$ pares, ao fazermos o produto dos elementos dessa sequência de modo que esse produto seja congruente a 1 módulo p, teremos pelo Teorema 1.9, a congruência $2.3.\cdots.(p-2) \equiv 1\,(mod p)$ e finalmente multiplicando ambos os membros desta congruência por $(p-1)$, temos $2.3.\cdots.(p-2)(p-1) \equiv (p-1)\,(mod p)$, logo $(p-1)! \equiv -1\,(mod p)$ uma vez que $(p-1) \equiv -1\,(mod p)$. ■

Teorema 1.19 *(Pequeno Teorema de Fermat) Seja p primo, se* $p \nmid a$, *então* $a^{p-1} \equiv 1\,(mod p)$.

Demonstração: Consideremos o conjunto formado pelos p números $0, 1, 2, \ldots, p-1$ que constitui um sistema completo de resíduos módulo p, onde qualquer conjunto que contenha no máximo p elementos incongruentes módulo p, pode ser correspondido biunivocamente a um subconjunto de $\{0, 1, 2, 3, \ldots, p-1\}$. Dados a sequência $a, 2a, 3a, \ldots, (p-1)\,a$ e tomados dois elementos dela incongruentes entre si, módulo p, se tivermos a congruência $ax \equiv ay\,(mod p)$, com $1 \leq x, y \leq p-1$, como $(a, p) = 1$, aplicando o cancelamento na congruência teremos $x \equiv y\,(mod p)$ o que não acontece pois os elementos do subconjunto $\{0, 1, 2, 3, \ldots, p-1\}$, não são congruentes entre si módulo p. Além disso não existe a congruência a zero módulo p, uma vez que se $p|ax$, com $1 \leq x \leq p-1$, então $p|x$ ou $p|a$, o que não acontece, segue então que o conjunto $\{a, 2a, \ldots, (p-1)\,a\}$ são congruentes aos elementos do conjunto $\{1, 2, \ldots, p-1\}$ numa ordem conviniente, onde teremos $p-1$ congruência da forma

$$\begin{aligned}
a &\equiv x_1\,(mod p)\\
2a &\equiv x_2\,(mod p)\\
3a &\equiv x_3\,(mod p)\\
&\vdots\\
(p-1)\,a &\equiv x_{p-1}\,(mod p)
\end{aligned}$$

Onde $x_1, x_2, x_3, \cdots, x_{p-1}$, são os inteiros $1, 2, 3, \cdots, p-1$, eventualmente em outra ordem, ver Exemplo 1.1. Multiplicando ordenadamente essas congruências , temos $a.2a.3a.\cdots.(p-1)\,a \equiv 1.2.3.\cdots.(p-1)\,(mod p)$ que implica em $(p-1)!a^{p-1} \equiv (p-1)!\,(mod p)$ e como $((p-1)!, p) = 1$ podemos aplicar o cancelamento, logo concluímos que $a^{p-1} \equiv 1\,(mod p)$. ■

Definição 1.9 *Chamamos de Função* ϕ *de Euler a função aritmética definida para todo inteiro positivo n e denotada por* $\phi\,(n)$ *e que é igual ao número de elementos do conjunto* $\{k \in \mathbb{N} :\ 1 \leq k \leq n\ e\ \ (k, n) = 1\}$.

Exemplo 1.4 *Para* $n = 12$, *calcule* $\phi\,(12)$.

Resolução: O conjunto procurado é $\{1, 5, 7, 11\}$, pois $1 \leq k \leq 12$ e $(k, 12) = 1$, temos:

$(1,12)=1; (2,12)\neq 1; (3,12)\neq 1; (4,12)\neq 1;$
$(5,12)=1; (6,12)\neq 1; (7,12)=1; (8,12)\neq 1;$
$(9,12)\neq 1; (10,12)\neq 1; (11,12)=1; (12,12)\neq 1;$

Portanto $\phi(12)=4$

Teorema 1.20 *Se o inteiro $p>1$, então $\phi(p)=p-1$ se, e somente se, p é primo.*

Demonstração: Se $p>1$ é primo, então cada um dos inteiros positivos menores do que p é primo com p, e portanto $\phi(p)=p-1$. A recíproca , se $\phi(p)=p-1$, com $p>1$, então p, é primo, pois se p fosse um número composto, teria pelo menos um divisor k, tal que $1<k<p$, de modo que pelo menos dois dos inteiros $1,2,3,\ldots,p$, não seriam primos com p e k, isto é $\phi(p)=p-2$. logo p é primo. ■

1.6 Teorema Chinês do Resto e Criptografia

Teorema 1.21 *Considere o seguinte sistema de congruência,*

$$\begin{cases} x\equiv a_1\,(mod\, m_1) \\ x\equiv a_2\,(mod\, m_2) \\ x\equiv a_3\,(mod\, m_3) \\ \quad\vdots \\ x\equiv a_n\,(mod\, m_n) \end{cases}$$

onde $(m_i,m_j)=1$ se $i\neq j$, $\quad i,j=1,2,3,\ldots,n$. Queremos determinar sobre quais condições haverá solução desse sistema.

Demonstração: O sistema acima conhecido como Sistema Chinês do Resto nas condições mencionadas sempre possui soluções e mais ainda, duas soluções diferem por um múltiplo de $m=m_1,m_2,m_3,\ldots,m_n$, consideremos,

$$N_j=\prod_{\substack{i=j\\ i\neq j}}^{n} m_i$$

Sabemos que o $(m_i,m_j)=1$, se $i\neq j$, sendo $i,j\in\{1,2,\ldots,n\}$, segue que $(m_i,N_j)=1$, donde existem $r_j,s_j\in\mathbb{Z}$, tais que $r_jm_j+s_jN_j=1$, defina então,

$x = \sum_{i=1}^{n} a_i s_i N_i$
note que,
$x \equiv \sum_{i=1}^{n} a_i s_i N_i \equiv a_j s_j N_j \equiv a_j \, (mod m_j)$
pois,
$N_i \equiv 0 \, (mod m_j), \quad i \neq j$ e $s_j N_j \equiv 1 \, (mod m_j)$

Assim, $x \equiv \sum_{i=1}^{n} a_i s_i N_i$ é solução do sistema. Tomando duas soluções x_1 e x_2 inteiras, desse sistema, teremos,
$x_1 \equiv a_2 \equiv x_2 \, (mod m_2)$
$x_1 \equiv a_n \equiv x_2 \, (mod m_n)$
Donde $x_1 - x_2 \equiv 0 \, (mod m_i)$, $i = 1, 2, \ldots, n$,
logo $m_i | \, (x_1 - x_2)$ e como o $(m_i, m_j) = 1$, com $i, j = 1, 2, 3, \ldots, n$
segue que $m_1, m_2, m_3, \ldots, m_n | \, (x_1 - x_2)$, indicando que as duas soluções diferem por um múltiplo de $m_1, m_2, m_3, \ldots, m_n$

Exemplo 1.5 *Um certo número de laranjas (menor do que* 20*) foi arrumado em caixas de três laranjas cada, sobrando duas, se a arrumação fosse em caixas de cinco laranjas cada, sobraria uma laranja, qual a quantidade de laranjas?*

Resolução: Neste caso, precisamos aplicar o teorema chinês do resto, chamando de x a quantidade de laranjas, teremos,

$$\begin{cases} x \equiv a_1 \, (mod m_1) \\ x \equiv a_2 \, (mod m_2) \end{cases} \Rightarrow \begin{cases} x \equiv 2 \, (mod 3) \\ x \equiv 1 \, (mod 5) \end{cases}$$

comparando as variáveis correspondentes, temos,

$$\begin{cases} a_1 = 2 \\ a_2 = 1 \\ m_1 = 3 \\ m_2 = 5 \\ (m_1, m_2) = 1 \end{cases}$$

Daí, podemos escrever que $1 = r.3 + s.5$ e usando o algoritmo de Euclides, concluimos que $\begin{cases} r = 2 \\ s = -1 \end{cases}$

O número de laranjas que é o objeto do problema sera definido por,

$\alpha = r.m_1.a_2 + s.m_2.a_1$

$\alpha = 2.3.1 + (-1).5.2$

$\alpha = 6 - 10$

$\alpha = -4$

O conjunto solução é uma P.A. de termo inicial -4 e razão $m_1.m_2 = 15$, ou seja,

$x \in \{-4, -4 + 15, -4 + 30, -4 + 45, \ldots\}$

$x \in \{-4, 11, 26, 41, \ldots\}$

como $0 \leq x < 20$, então temos como solução do problema $x = 11$.

Criptografia

O impulso para descobrir segredos está profundamente enraizado na natureza humana. Durante milhares de anos, reis e rainhas dependiam de algum tipo de comunicação, mesmo que não eficiente, para governar seus países. Ao mesmo tempo, todos estavam cientes dos riscos das mensagens serem interceptadas pelo inimigo. Foi essa ameaça que gerou o desenvolvimento de métodos para mascarar as mensagens, denominados códigos e cifras. Segundo alguns historiadores e analistas militares, a Terceira Guerra Mundial será a guerra dos matemáticos, uma vez que estes terão o controle sobre a próxima grande arma de guerra: a transmissão segura da informação.

Os principais códigos usados atualmente para a proteção das informações militares foram elaborados por matemáticos ou por pesquisadores com conhecimento profundo em tal aréa. Embora a Criptografia seja de importância fundamental em termos militares, os sistemas criptográficos são amplamente utilizados no meio civil, em transações bancárias, em negociações e em simples trocas de mensagens que são efetuadas via internet. A proliferação dos computadores e sistemas de comunicação em 1960 criou uma grande demanda do setor privado buscando, na Criptografia, meios para proteger a informação na forma digital e fornecer serviços de segurança. Esta fase começou com o trabalho de H. Feistel na IBM em 1973, culminando em 1977, com a adoção de um

Processamento Padrão de Informação Federal (USA) para criptografar informação não classificada; a DES (Data Encryption Standard) é o mecanismo criptográfico melhor conhecido na história.

A segurança desse sistema criptográfico está baseada em um antigo problema matemático: obter os fatores primos de um número dado. O RSA explora essa situação ao utilizar um número, que atualmente varia de 512 a 1024 bits, e que é o produto de dois números primos muito grandes. Diversos métodos de fatoração foram desenvolvidos. Vários matemáticos estudaram caminhos alternativos para solucionar este problema tais como Carl Gauss, Leonard Euler e Pierre de Fermat. Mas essa área era considerada inútil para fins práticos. No entanto, com o advento da cifra assimétrica, a mesma se tornou interessante a todos os profissionais relacionados à tecnologia da informação, inclusive aos matemáticos. A engenhosidade de todos esses profissionais produziram resultados importantes no problema da fatoração. Porém, nenhum método desenvolvido é considerado satisfatório a fim de ser executado em tempo polinomial, e portanto, o tamanho da chave é suficiente para garantir a segurança da informação no método RSA, em tempo real.

O algoritmo RSA foi patentiado pelo M.I.T. em 1983 nos Estados Unidos, mas expirou em 21 de setembro de 2000. O RSA é, atualmente, o mais usado em aplicações comerciais. Este é o método utilizado, por exemplo, no Netscape, o mais popular dos softwares de navegação na Internet.

Representação de Knuth

Em criptografia um dos principais problemas computacional consiste em manipular inteiros grandes sem aproximações em um computador com memória limitada (tipicamente, as principais linguagens de programação conseguem apenas manipular inteiros de ordem 10^{10}, algoritmos simples de criptografia geralmente exigem manipular inteiros da ordem de 10^{100} ou maiores).

As operações necessárias ao RSA, são

(i) Soma de inteiros;

(ii) Produto de inteiros;
(iii) Potências naturais de números inteiros.

Donal Knuth na década de 70 imaginou uma fórmula de representar números de qualquer ordem, provando as três operações acima sem modificação de característica de hardware tal como o tamanho dos inteiros em máquinas com velocidade próxima da velocidade das operações de tipos nativos em hardware esquematicamente,

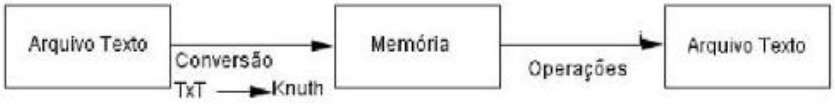


Figura 1.1: Representação de Knuth

As conversões $TxT \rightarrow Knuth$ e $Knuth \rightarrow TxT$, são lentas mas, só precisam ser realizadas no início e no fim dos cálculos, as operações intermediárias são realizadas na representação de Knuth e são de velocidades comparável às operações nativas.

Seja n inteiro positivo qualquer e dados $p_1, p_2, p_3, p_4, \ldots, p_k$ números primos igualmente na ordem 10^{10} cada, ou seja, representáveis na arquitetura padrão dos computadores, e tal que $n < p_1, p_2, p_3, p_4, \ldots, p_k$, podemos calcular os resíduos de n módulo cada primo, (conversão $TxT \rightarrow Knuth$). É possivel que realize tal representação por inteiros negativos. Ao leitor interessado recomendamos [11]. Obtendo de forma unica-

mente determinada $a_1, a_2, a_3, a_4, \ldots, a_k$, inteiros tais que,
(i) $x \equiv a_i mod(p_i)$ com $i = 1, 2, 3, \ldots, k$
(ii) $0 \leq a_i < p_i$.

Denotaremos $[[n]]_P = [a_1, a_2, a_3, a_4, \ldots, a_k]$, a representação de Knuth do número na base "fixa", $P = \{p_1, p_2, p_3, p_4, \ldots, p_k\}$, note também que dado o vetor $(a_1, a_2, a_3, a_4, \ldots, a_k)$ representando um inteiro na base P, pelo teorema chinês do resto, pode recuperar n como única solução do sistema,

$$\begin{cases} n \equiv a_1 \, (mod p_1) \\ n \equiv a_2 \, (mod p_2) \\ n \equiv a_3 \, (mod p_3) \quad \text{com } 0 \leq n < p_1, p_2, p_3, p_4, \ldots, p_k. \\ \quad \vdots \\ n \equiv a_k \, (mod p_k) \end{cases}$$

Dado uma base $P = \{p_1, p_2, p_3, p_4, \ldots, p_k\}$ e $n_1, n_2 \in \mathbb{Z}$, tendo as representações,
$[[n_1]] = (a_1, a_2, a_3, a_4, \ldots, a_k)$
$[[n_2]] = (b_1, b_2, b_3, b_4, \ldots, b_k)$
sendo,
$n_1 \equiv a_i mod(p_i)$
$n_2 \equiv b_i mod(p_i)$
resulta em,
(i) $n_1 + n_2 \equiv (a_i + b_i) \, mod(p_i)$;
(ii) $n_1.n_2 \equiv (a_i.b_i) \, mod(p_i)$;
(iii) $n_i^e \equiv (a_i^e) \, mod(p_i)$; com $i = 1, 2, 3, \ldots, k$.

Pelas propriedades de congruência, não existirá nenhum caso em que através das operações, resulte em números superiores a $p_1, p_2, p_3, p_4, \ldots, p_k$, daí segue,
(i) $[[n_1 + n_2]] = [(a_1 + b_1) \,\%p_1, (a_2 + b_2) \,\%p_2, \ldots, (a_k + b_k) \,\%p_{k1},]$
(ii) $[[n_1.n_2]] = [(a_1.b_1) \,\%p_1, (a_2.b_2) \,\%p_2, \ldots, (a_k.b_k) \,\%p_k,]$
(iii) $[[n_1^e]] = [(a_1^e) \,\%p_1, (a_2^e) \,\%p_2, \ldots, (a_k^e) \,\%p_k,]$
onde $\alpha\%p$ denota o único resíduo de α módulo p entre 0 e $p - 1$.

Devemos observar que uma operação típica na representação de Knuth utilizando k primos é a aproximadamente k vezes mais lenta que a operação nativa, a máquina não

chega a ser proibitivo, pois tomando-se, digamos 100 primos de ordem 10^{10}, podem representar números inteiros da ordem de $(10^{10})^{10} = 10^{1000}$, sem erro de arredondamento de operações e de custo de apenas 100 vezes mais limitado que as operações normais.

Criptografia RSA

Devido às diversas aplicações em criptografia com o auxílio dos mais variados tópicos da Teoria dos Números, daremos destaque à criptografia RSA, para mostrarmos a importância das equações diofantinas como ferramenta para o desenvolvimento dos mais sofisticados sistema de computação e no *quinto capítulo apresentaremos uma aplicação*. Ao leitor interessado recomendamos [9]

Este processo de criptografia dividiremos em duas etapas a pré-codificação e a codificação-decodificação. Ao leitor interessado sugerimos [12]

Na primeira etapa, devemos converter a mensagem a ser criptografada em uma mensagem numérica, há várias maneiras de fazer isso, o procedimento mais comum é com o uso da tabela ASCII, assim cada letra, acentos ou espaços em branco entre palavras corresponde a uma numeração, desta tabela.

Denominaremos de chave pública, um número n inteiro positivo, tal que $n = p.q$, onde p e q são primos, após converter a mensagem em uma sequência numérica, devemos "quebrar" essa sequência em blocos numéricos, de tal modo que a numeração correspondente a cada um deles, devem ser menor do que o valor de n. A maneira de escolher esses blocos não é única, mas devemos evitar que o bloco inicie com o número zero e que não correspondam a nenhuma unidade linguística, para evitar futuros problemas na decodificação.

A codificação e decodificação será feita com o auxílio do número n e de um inteiro positivo α que seja inversível módulo $\phi(n)$, ver Teorema 1.20. Em outras palavras, $mdc(\alpha, (p-1)(q-1)) = 1$, ou seja, α e $\phi(n)$ são coprimos. Os blocos oriundos da sequência numérica representaremos por b. O par (n, α) denominaremos de chave de codificação do sistema RSA. Este processo será feito por bloco de mensagem separadamente e a mensagem codificada será a sequência de blocos codificados. A codificação do bloco b será feita por uma função $C(b)$ "codificação do bloco" e não podemos omitir que $b < n$. Assim,

$$C(b) \equiv b^{\alpha} mod n, \text{ onde } 0 \leq C(b) < n$$

.

Após este procedimento de codificação de todos os blocos, obtemos assim, a mensagem cifrada.

Para realizar a decodificação de um bloco de mensagem cifrada é necessário a informação contida no par (n, d), onde d é o inverso de α módulo $\phi(n)$, que chamaremos de chave de decodificação. Seja c um bloco da mensagem decodificado, então $D(c)$ é o resultado do processo de decodificação. Assim,

$$D(c) \equiv c^{d} mod n, \text{ onde } 0 \leq D(c) < n$$

.

Para o cálculo de d, precisaremos dos valores conhecidos anteriormente, α e $\phi(n)$ e com o auxílio do Algoritmo Euclidiano Estendido, ver Teorema 1.4, encontraremos o valor de d, sem o conhecimento de p e q é praticamente impossível encontrar o valor de d.

Capítulo 2

SOMA DE INTEIROS

Neste capítulo resolveremos diversos problemas de equações diofantinas lineares com o auxílio da teoria elementar da contagem, através dos princípios da contagem, do binômio de Newton e das funções geradoras, analisando a solução geral de problemas de soma de inteiros e suas aplicações.

2.1 Teoria Elementar da Contagem

Consideremos o seguinte problema: De quantas maneiras podemos escolher seis crianças dentre dez para formar uma equipe?

Conforme visto nos cursos elementares de combinatória, a resposta a esta indagação será obtida pelo coeficiente binomial C_{10}^{6}, uma vez que a ordem da escolha das crianças é irrelevante, ou seja $C_{10}^{6} = \dfrac{10!}{6!4!} = 210$, onde C_{n}^{m} lê-se combinação de m dentre n e é suposto tacitamente que $n \geq m$.

O seguinte teorema cuja demonstração é imediata, resume os principais fatos acerca destes coeficientes.

Teorema 2.1 *Sejam $m, n \in \mathbb{Z}^{+}$ com $m \leq n$ e definida $C_{n}^{m} = \binom{n}{m} = \dfrac{n!}{m!\,(n-m)!}$.*

i) $\binom{n}{0} = \binom{n}{n} = 1$;

ii) $\binom{n}{1} = \binom{n}{n-1} = n$;

(iii) $\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}$ (Relação de Stiefel);

(iv) $\binom{n}{m} = \binom{n}{n-m}$. (Coeficientes complementares).

Outro resultado elementar de combinatória que utilizaremos no decorrer deste capítulo é o teorema binomial de Newton.

Teorema 2.2 *Seja $a, b \in \mathbb{R}$ e $n \in \mathbb{Z}^+$, então* $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.

O teorema binomial de Newton é frequentemente apresentado na forma do triângulo de Pascal cuja construção baseia-se nas propriedades do Teorema 2.1.
Definimos como polinômio formal $\mathbb{R} = [[x_1, x_2, \cdots x_n,]]$ um polinômio nas variáveis $x_1, x_2, \cdots x_n$ com coeficientes reais para o qual não são atribuídos valores às variáveis, ainda que valerá o resultado $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$, que pode ser demonstrado por argumentos simples de combinatória.

Corolário 2.1 *Substituindo valores convenientes para a e b no Teorema 2.2 é fácil mostrar as propriedades clássicas do triângulo de Pascal.*

(i) $\sum_{i=0}^{n} \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n} = 2^n$;

(ii) $\sum_{i=0}^{n} \binom{n}{i} (-1)^i = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^n \binom{n}{n} = 0$;

Retomando às equações diofantinas, consideremos o seguinte problema: "Tem-se cinco doces iguais para serem distribuídos entre três crianças diferentes, de quantas maneira isto pode ser feito, se cada criança receber, ao menos um doce"?

Podemos enumerar as possibilidades conforme a tabela:

Quantidade de doces por criança		
Criança 01	*Criança 02*	*Criança 03*
1	2	2
2	1	2
2	2	1
3	1	1
1	3	1
1	1	3

O processo acima, claramente é impossÍvel para valores grandes. Denotaremos por x_i a quantidade de doces da i-ésima criança, o que essencialmente queremos calcular é a quantidade de soluções da equação $x_1 + x_2 + x_3 = 5 \quad \text{com} \quad x_1 \geq 1$, $x_2 \geq 1$ e $x_3 \geq 1$.

Chamamos de equações diofantinas lineares as equações do tipo

$$\begin{gathered} a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_mx_m = n \\ \alpha_1 \leq x_1 \leq \beta_1 \\ \alpha_2 \leq x_2 \leq \beta_2 \\ \alpha_3 \leq x_3 \leq \beta_3 \qquad (1) \\ \vdots \\ \alpha_m \leq x_m \leq \beta_m \end{gathered}$$

onde $a_1, a_2, a_3, \cdots, a_m$, $\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_m$, $\beta_1, \beta_2, \beta_3, \cdots, \beta_m$, $n \in \mathbb{Z}$, mais do que enumerar todas as soluções, nosso interesse aqui é determinar a existência de alguma solução. Observamos que em nossas considerações, temos distintas soluções que definam o valor e/ou na ordem com relação às variáveis, $x_1, x_2, x_3, \cdots, x_m$ (como no exemplo anterior $(1, 2, 2)$ e $(2, 1, 2)$ são consideradas distintas pois diferem na ordem dos valores atribuidos ao vetor (x_1, x_2, x_3)). [Santos].

Inicialmente, consideremos um caso mais simples

$$x_1 + x_2 + x_3 + \cdots + x_m = n \qquad (2)$$

$$x_i \geq 1 \text{ e } i = 1, 2, 3, \cdots, m$$

Se $n < m$ é fácil verificar que não haverá nenhuma solução, portanto,assumiremos que $n \geq m$. Podemos associar a cada solução de (2) um sorteio de $m-1$ dentre as posições de forma análoga ao exemplo que iniciamos neste capítulo.

Exemplo 2.1 *Quantas são as soluções da equação diofantina* $x_1 + x_2 + x_3 = 5$ *com* $x_1, x_2, x_3 \geq 1$

Resolução: Já sabemos por enumeração que o resultado são seis soluções, vejamos um processo mais sistemático, distribuições de $1's$, assim
$1 - 1 - 1 - 1 - 1$
Onde observamos a existencia de quatro posições (espaços) e dois sinais de mais (+), entre as posições, podemos então enumerar todas as soluções do seguinte modo:

Enumeração por distribuição de $1's$		
(x_1, x_2, x_3)	*modo 01*	*modo 02*
(1,2,2)	1-1+1-1+1	1/+1+1/+1+1
(2,1,2)	1+1-1-1+1	1+1/+1/+1+1
(2,2,1)	1+1-1+1-1	1+1/+1+1/+1
(3,1,1)	1+1+1-1-1	1+1+1/+1/+1
(1,3,1)	1-1+1+1-1	1/+1+1+1/+1
(1,1,3)	1-1-1+1+1	1/+1/+1+1+1

Dado que a ordem de escolha das posições nas quais os sinais de mais (+), serão colocados é irrelevante, segue que temos um sorteio simples de dois (+) dentre quatro posições (-) o que pode ser feito assim,

$$\binom{4}{2} = \frac{4!}{2!2!} = 6.$$

Concordando com o resultado que já haviamos obtido, pelo processo de enumeração tradicional e com a teoria elementar da combinatória. Então, de modo análogo ao exemplo anterior, que o número de soluções de $x_1 + x_2 + x_3 + \cdots + x_m = n$ com $x_i \geq 1$ será $\binom{n-1}{m-1}$, em particular se $n \geq m$, sempre haverá alguma solução. Observamos neste ponto que, uma vez estabelecida uma correspondência entre as soluções de uma equação diofantina e um procedimento combinatório, a geração das soluções em si é

um processo computacional simples. Ao leitor interessado recomendamos [10].

Aumentando a complexidade do problema, consideremos agora

$$x_1 + x_2 + x_3 + \cdots + x_m = n \qquad (3)$$

$$x_i \geq \alpha_i,\ \alpha_i \in \mathbb{Z} \text{ e } i = 1, 2, 3, \cdots, m$$

Tal problema pode ser reduzido ao problema do Exemplo 2.1 por uma simples mudança de variáveis $y_i = x_i - \alpha_i + 1$ o que fará uma correspondência entre as soluções de (3) e as soluções de

$$y_1 + y_2 + y_3 + \cdots + y_m = n + \sum_{i=0}^{m} (1 - \alpha_i), \text{ com } y_i \geq 1, \quad i = 1, 2, 3, \cdots, m.$$

O que pode ser verificado por uma substituição direta.

Exemplo 2.2 *No problema anterior quantas serão as soluções da equação diofantina* $x_1 + x_2 + x_3 = 5$, *se a última criança necessariamente ganhar dois ou mais doces e as demais crianças receberem uma quantidade qualquer (inclusive nenhuma) de doce?*

Resolução:

$x_1 + x_2 + x_3 = 5$

$x_1 \geq 0$

$x_2 \geq 0$

$x_3 \geq 2$

O procedimento para mudança de variáveis é o seguinte, consideremos,

$$\begin{cases} y_1 = x_1 + 1 \\ y_2 = x_2 + 1 \\ y_3 = x_1 - 1 \end{cases}$$

Substituindo esses valores na equação diofantina do problema acima,

$y_1 - 1 + y_2 - 1 + y_3 + 1 = 5$

$y_1 + y_2 + y_3 = 6$

$y_i \geq 1$

E o número de soluções inteiras dessa equação é definido pelo coeficiente binomial $\binom{6-1}{3-1}$ ou seja, 10.

Assim, o problema $x_1 + x_2 + x_3 + \cdots + x_m = n$ com $\alpha_i \leq x_i \leq \beta_i$, sempre poderá ser reduzido por mudança de variáveis ao problema

$$x_1 + x_2 + x_3 + \cdots + x_m = n \qquad (4)$$

$$1 \leq x_i \leq \beta_i,\ i = 1, 2, 3, \cdots, m$$

Trataremos a seguir da solução de (4) e para isto é necessario recorremos ao importante resultado de combinatória chamado Princípio da Inclusão e Exclusão e a sua demonstração pode ser encontrada em [6].

2.2 Princípio da Inclusão e Exclusão

Teorema 2.3 *Sejam $A_1, A_2, A_3, \cdots, A_n$ conjuntos finitos não necessariamente distintos, então a quantidade de elementos na união destes é dado pela fórmula,*

$$\left|A_1 \bigcup A_2 \bigcup \cdots \bigcup A_n\right| = \sum_{k=1}^{n} \sum_{i_1 \leq i_2 \leq \cdots \leq i_k} (-1)^{k+1} \left|A_{i_1} \bigcap A_{i_2} \bigcap \cdots \bigcap A_{i_k}\right|.$$

Na fórmula $|.|$ significa cardinalidade do conjunto e o segundo somatório é tomado sobre todos os multi-indices $(i_1, i_2, i_3, \cdots, i_k) \in \{1, 2, 3, \cdots, n\}^k$, vejamos alguns casos,

(i) $|A_1 \bigcup A_2| = |A_1| + |A_2| - |A_1 \bigcap A_2|$;
(ii) $|A_1 \bigcup A_2 \bigcup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \bigcap A_2| - |A_1 \bigcap A_3| - |A_2 \bigcap A_3| + |A_1 \bigcap A_2 \bigcap A_3|$;
(iii) $|A_1 \bigcup A_2 \bigcup A_3 \bigcup A_4| = |A_1| + |A_2| + |A_3| + |A_4| - |A_1 \bigcap A_2| - |A_1 \bigcap A_3| - |A_1 \bigcap A_4| - |A_2 \bigcap A_3| - |A_2 \bigcap A_4| - |A_3 \bigcap A_4| + |A_1 \bigcap A_2 \bigcap A_3| + |A_1 \bigcap A_2 \bigcap A_4| + |A_2 \bigcap A_3 \bigcap A_4| - |A_1 \bigcap A_2 \bigcap A_3 \bigcap A_4|$;

Retornando ao problema (4), $x_1 + x_2 + x_3 + \cdots + x_m = n$, $1 \leq x_i \leq \beta_i$, $i = 1, 2, 3, \cdots, m$, temos

A_1: É solução de $x_1 + x_2 + x_3 + \cdots + x_m = n$, com $x_i \geq 1$, $i = 1, 2, 3, \cdots, m$, para os quais $x_1 \geq \beta_1 + 1$.

A_2: É solução de $x_1 + x_2 + x_3 + \cdots + x_m = n$, com $x_i \geq 1$, $i = 1, 2, 3, \cdots, m$, para os quais $x_2 \geq \beta_2 + 1$.

A_3: É solução de $x_1 + x_2 + x_3 + \cdots + x_m = n$, com $x_i \geq 1$, $i = 1, 2, 3, \cdots, m$, para os quais $x_3 \geq \beta_3 + 1$ e assim por diante.

Denotando A_0 como o conjunto das soluções de $x_1 + x_2 + x_3 + \cdots + x_m = n$, $1 \leq x_i \leq \beta_i$, $i = 1, 2, 3, \cdots, m$, a quantidade de soluções de (4) será obtida calculando o valor da expressão $|A_0| - |A_1 \bigcup A_2 \bigcup \cdots \bigcup A_n|$.

Sabemos que $|A_0| = \binom{n-1}{m-1}$ para $n > m$ e $|A_1 \bigcup A_2 \bigcup \cdots \bigcup A_n|$ pode ser calculado pelo princípio da inclusão e exclusão se soubermos calcular $|A_{i_1} \bigcap A_{i_2} \bigcap \cdots \bigcap A_{i_k}|$, o que é simples pois as soluções em $A_{i_1} \bigcap A_{i_2} \bigcap \cdots \bigcap A_{i_k}$, são soluções de

$$\begin{aligned} x_1 + x_2 + x_3 + \cdots + x_m &= n \\ x_{i_1} &\geq \beta_{i_1} + 1 \\ x_{i_2} &\geq \beta_{i_2} + 1 \\ x_{i_3} &\geq \beta_{i_3} + 1 \\ &\vdots \\ x_{i_k} &\geq \beta_{i_k} + 1 \end{aligned} \qquad (5)$$

Sendo $x_i \geq 1$, $i \notin \{i_1, i_2, i_3, \cdots, i_k\}$ e $1 \leq i \leq m$, que é um problema do tipo (3) que sabemos resolver por uma mudança de variável.

Exemplo 2.3 *Retomando ao problema anterior quantas serão as soluções da equação diofantina* $x_1 + x_2 + x_3 = 5$, *sabendo que* $-2 \leq x_1 \leq 4$, $0 \leq x_2 \leq 2$ *e* $-4 \leq x_3 \leq 1$.

Resolução:

Realizando a mudança de variáveis, temos

$y_1 - 5 + y_2 - 3 + y_3 - 1 = 5$

$y_1 + y_2 + y_3 = 14$

$1 \leq y_1 \leq 7$

$1 \leq y_2 \leq 3$

$1 \leq y_3 \leq 6$

Aplicando o princípio da inclusão e exclusão, temos:

$$|A_0| = \binom{n-1}{m-1} = \binom{14-1}{3-1} = \binom{13}{2}$$

A_1:

$y_1 - 5 + y_2 - 3 + y_3 - 1 = 5$

$y_1 + y_2 + y_3 = 14$

$y_1 \geq 8$

$y_2, y_3 \geq 1$

Aplicando a mudança de variável pela segunda vez, tem-se

$$\begin{cases} z_1 = y_1 - 7 \\ z_2 = y_2 \\ z_3 = y_3 \end{cases}$$

A equação diofantina equivalente é $z_1 + z_2 + z_3 = 7$, com $z_i \geq 1$.

$$|A_1| = \binom{n-1}{m-1} = \binom{7-1}{3-1} = \binom{6}{2}$$

A_2:

$y_1 + y_2 + y_3 = 14$

$y_2 \geq 4$

$y_1, y_3 \geq 1$

Aplicando a mudança de variável pela segunda vez, tem-se

$$\begin{cases} z_1 = y_1 \\ z_2 = y_2 - 3 \\ z_3 = y_3 \end{cases}$$

A equação diofantina equivalente é $z_1 + z_2 + z_3 = 11$, com $z_i \geq 1$.

$$|A_2| = \binom{n-1}{m-1} = \binom{11-1}{3-1} = \binom{10}{2}$$

A_3:

$y_1 + y_2 + y_3 = 14$

$y_3 \geq 7$

$y_1, y_2 \geq 1$

Aplicando a mudança de variável pela segunda vez, tem-se

$$\begin{cases} z_1 = y_1 \\ z_2 = y_2 \\ z_3 = y_3 - 6 \end{cases}$$

A equação diofantina equivalente é $z_1 + z_2 + z_3 = 8$, com $z_i \geq 1$.

$$|A_3| = \binom{n-1}{m-1} = \binom{8-1}{3-1} = \binom{7}{2}$$

$A_1 \bigcap A_2$:

$y_1 + y_2 + y_3 = 14$

$y_1 \geq 8$

$y_2 \geq 4$

$y_3 \geq 1$

Aplicando a mudança de variável pela segunda vez, tem-se

$$\begin{cases} z_1 = y_1 - 7 \\ z_2 = y_2 - 3 \\ z_3 = y_3 \end{cases}$$

A equação diofantina equivalente é $z_1 + z_2 + z_3 = 4$, com $z_i \geq 1$.

$$|A_1 \bigcap A_2| = \binom{n-1}{m-1} = \binom{4-1}{3-1} = \binom{3}{2}$$

$A_1 \bigcap A_3$:

$y_1 + y_2 + y_3 = 14$

$y_1 \geq 8$

$y_2 \geq 4$

$y_3 \geq 1$

Aplicando a mudança de variável pela segunda vez, tem-se

$$\begin{cases} z_1 = y_1 - 7 \\ z_2 = y_2 \\ z_3 = y_3 \end{cases}$$

A equação diofantina equivalente é $z_1 + z_2 + z_3 = 7$, com $z_i \geq 1$.

$$|A_1 \bigcap A_3| = \binom{n-1}{m-1} = \binom{7-1}{3-1} = \binom{6}{2}$$

$A_2 \bigcap A_3$:

$y_1 + y_2 + y_3 = 14$

$y_1 \geq 8$

$y_2 \geq 4$

$y_3 \geq 1$

Aplicando a mudança de variável pela segunda vez, tem-se

$$\begin{cases} z_1 = y_1 \\ z_2 = y_2 - 3 \\ z_3 = y_3 \end{cases}$$

A equação diofantina equivalente é $z_1 + z_2 + z_3 = 11$, com $z_i \geq 1$.

$$|A_2 \bigcap A_3| = \binom{n-1}{m-1} = \binom{11-1}{3-1} = \binom{10}{2}$$

$A_1 \bigcap A_2 \bigcap A_3$:

$y_1 + y_2 + y_3 = 14$

$y_1 \geq 8$

$y_2 \geq 4$

$y_3 \geq 1$

Aplicando a mudança de variável pela segunda vez, tem-se

$$\begin{cases} z_1 = y_1 - 7 \\ z_2 = y_2 - 3 \\ z_3 = y_3 \end{cases}$$

A equação diofantina equivalente é $z_1 + z_2 + z_3 = 4$, com $z_i \geq 1$.

$$|A_1 \bigcap A_2 \bigcap A_3| = \binom{n-1}{m-1} = \binom{4-1}{3-1} = \binom{3}{2}$$

Logo a quantidade de soluções de (4) será obtida calculando o valor da expressão, $|A_0| - |A_1 \bigcup A_2 \bigcup A_3|$, uma vez que sabemos que,
$|A_1 \bigcup A_2 \bigcup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \bigcap A_2| - |A_1 \bigcap A_3| - |A_2 \bigcap A_3| + |A_1 \bigcap A_2 \bigcap A_3|$, fica fácil, precisamos apenas substituir os valores ja conhecidos.

$$|A_0| - |A_1 \bigcup A_2 \bigcup A_3|$$

$$|A_0| - (|A_1| + |A_2| + |A_3| - |A_1 \bigcap A_2| - |A_1 \bigcap A_3| - |A_2 \bigcap A_3| + |A_1 \bigcap A_2 \bigcap A_3|)$$

$$|A_0| - |A_1 \bigcup A_2 \bigcup A_3| = |A_0| - \left[\binom{6}{2} + \binom{10}{2} + \binom{7}{2} - \binom{3}{2} - \binom{6}{2} - \binom{10}{2} + \binom{3}{2}\right]$$

$$|A_0| - |A_1 \bigcup A_2 \bigcup A_3| = \binom{13}{2} - \binom{7}{2}$$

$$|A_0| - |A_1 \bigcup A_2 \bigcup A_3| = 57.$$

Para tratarmos casos mais gerais de equações diofantinas lineares $a_1x_1+a_2x_2+a_3x_3+\cdots+a_mx_m = n$, necessitamos do conceito binomial generalizado e de funções geradoras.

2.3 Binomial Generalizado e Funções Geradoras

Teorema 2.4 *Seja x uma variável formal e $\alpha \in \mathbb{Q}$, então $(1+x)^\alpha = \sum_{i=0}^{\infty} \binom{\alpha}{i} x^i$, onde ambos os lados desta equação são tratados como Polinômios (Bolinômios) e séries formais e definimos,*

$$\binom{\alpha}{i} = \frac{\alpha.(\alpha-1).\ldots.(\alpha-i+1)}{i!}$$

Chamado coeficiente binomial generalizado (para $i \geq 0$, inteiro e $\alpha \in \mathbb{R}$ qualquer).

Exemplo 2.4 *Calcule os primeiros cinco termos do desenvolvimento formal de $\sqrt{1+x}$.*

Resolução:

$\sqrt{1+x} = (1+x)^{\frac{1}{2}} = \sum_{i=0}^{\infty} \binom{\frac{1}{2}}{i} x^i$.

Aplicando a definição das propriedades elementares, temos,

$$\binom{\frac{1}{2}}{0}x^0 = 1$$

$$\binom{\frac{1}{2}}{1}x^1 = \frac{1}{2}x$$

$$\binom{\frac{1}{2}}{2}x^2 = \frac{\frac{1}{2}.\left(\frac{1}{2}-1\right)}{2!}x^2 = -\frac{1}{8}x^2$$

$$\binom{\frac{1}{2}}{3}x^3 = \frac{\frac{1}{2}.\left(\frac{1}{2}-1\right).\left(\frac{1}{2}-2\right)}{3!}x^3 = \frac{1}{16}x^3$$

$$\binom{\frac{1}{2}}{4}x^4 = \frac{\frac{1}{2}.\left(\frac{1}{2}-1\right).\left(\frac{1}{2}-2\right).\left(\frac{1}{2}-3\right)}{4!}x^4 = -\frac{5}{128}x^4$$

Logo podemos escrever que $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \frac{5}{128}x^4$.

O conceito de funções geradoras será introduzido mediante um exemplo e de uma aplicação contextualizada no quinto capítulo.

Exemplo 2.5 *Quantas são as soluções da equação* $2x_1 + 3x_2 + x_3 = 9$.

Resolução:
Consideremos formalmente os seguintes polinômios
$p_1(x) = x^2 + x^4 + x^6 + x^8 + \cdots$
$p_2(x) = x^3 + x^6 + x^9 + x^{12} + \cdots$
$p_3(x) = x + x^2 + x^3 + x^4 + \cdots$

A cada solução de $2x_1 + 3x_2 + x_3 = 9$, com $x_i \geq 1$, corresponde a contribuição de uma unidade no coeficiente de x^9 no produto.

$$q(x) = p_1(x).p_2(x).p_3(x)$$

Portanto se soubermos calcular os coeficientes de x^k no desenvolvimento de produtos de séries formais, o problema de calcular as soluções de (4) estará essencialmente resolvido de fato,

$$x_1 + x_2 + x_3 + \cdots + x_m = n \qquad (4)$$

$$1 \leq x_i \leq \beta_i,\ i = 1, 2, 3, \cdots, m$$

possui tantas soluções quanto for o valor do coeficiente de x^n no produto formal,
$p(x) = p_1(x).p_2(x).p_3(x).....p_m(x)$.

O cálculo do coeficiente de x^n naquele produto, pode ser realizado com o auxílio de diversas ferramentas de computação algébrica (por exemplo MAPLE ou MAXIMA) que permite de forma rápida e eficiente para identificar esses coeficientes por exemplo no caso anterior, dado que queremos o coeficiente de x^9 em,
$p_1(x).p_2(x).p_3(x)$ com,

$p_1(x) = x^2 + x^4 + x^6 + x^8 + \cdots$

$p_2(x) = x^3 + x^6 + x^9 + x^{12} + \cdots$

$p_3(x) = x + x^2 + x^3 + x^4 + \cdots$

O que é facil ver que tal coeficiente é o mesmo no produto,

$p(x) = (x^2 + x^4 + x^6 + x^8)(x^3 + x^6 + x^9)(x + x^2 + x^3 + \cdots + x^8 + x^9)$

$p(x) = x^{26} + x^{25} + 2x^{24} + 3x^{23} + 4x^{22} + 5x^{21} + 7x^{20} + 8x^{19} + 9x^{18} + 9x^{18} +$

$+9x^{17} + 10x^{16} + 9x^{15} + 9x^{14} + 8x^{13} + 7x^{12} + 5x^{11} + 4x^{10} + 3x^9 + 2x^8 + x^7 + x^6.$

Teorema 2.5 *O coeficiente de x^p na expansão de $(1 + x + x^2 + x^3 + \cdots)^n$ é igual a C^p_{n+p-1}.*

Demonstração: Pelo Teorema 2.4, uma vez que $(1 + x + x^2 + x^3 + \cdots)^n = \left(\frac{1}{1-x}\right)^n = (1-x)^{-n}$ procedendo a troca de x por $-x$ e a de α por $-n$, temos $(1-x)^{-n} = \sum_{i=0}^{\infty} \binom{-n}{i} (-x)^i = \sum_{i=0}^{\infty} \binom{-n}{i} (-1)^i x^i$, utilizando a definição do coeficiente binomial generalizado, temos que o coeficiente de x^p é dado por,

$$\binom{-n}{p}(-1)^p = \frac{(-n)(-n-1)(-n-2)\cdots(-n-p+1)(-1)^p}{p!}$$

$$\binom{-n}{p}(-1)^p = \frac{(-1)^p(n)(n+1)(n+2)\cdots(n+p-1)(-1)^p}{p!}$$

$$\binom{-n}{p}(-1)^p = \frac{(n)(n+1)(n+2)\cdots(n+p-1)}{p!}$$

$$\binom{-n}{p}(-1)^p = \frac{(n+p-1)(n+p-2)\cdots(n+1)n(n-1)!}{p!(n-1)!}$$

$$\binom{-n}{p}(-1)^p = \frac{(n+p-1)!}{p!(n-1)!}$$

$$\binom{-n}{p}(-1)^p = \binom{n+p-1}{p}$$

■

Polinômios formais cujos coeficientes são relacionados às soluções de algum problema de contagem são chamados de funções geradoras (polinomiais). Para o leitor interessado recomendamos [6]. Para terminar este capítulo apresentaremos um exem-

plo prático nos quais os cálculos dos coeficientes de x^n podem ser feitos com o uso do teorema binomial generalizado, ou seja, sem recorrer ao auxílio computacional.

Exemplo 2.6 *De quantas maneiras diferentes podemos escolher* 10 *alunos para formar uma equipe para representar a escola em uma exposição, se nessa sala de aula existem alunos de quatro bairros diferentes da cidade?*

Resolução: Como não há nenhuma restrição quanto ao número de alunos de um determinado bairro, podemos definir a função geradora que "controla"o número de alunos de um determinado bairro, assim, $1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}$, entretanto são 4 bairros, logo a resposta a esse problema será encontrado pelo coeficiente de x^{10} na expansão,
$(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10})^4 = \left(\frac{1-x^{11}}{1-x}\right)^4$, de modo que,
$(1+x+x^2+x^3+x^4+x^5+x^6+\cdots+x^{10})^4 = (1-x^{11})^4(1-x)^{-4}$, fica fácil observar que o coeficiente de x^{10} não está no desenvolvimento de $(1-x^{11})^4$, uma vez que $(1-x^{11})^4 = 1-4x^{11}+6x^{22}-4x^{33}+x^{44}$, então precisaremos aplicar o Teorema 2.3 no desenvolvimento de $(1-x)^{-4}$, assim, $(1-x)^{-4} = \sum_{i=0}^{\infty}\binom{-4}{i}(-x)^i$, o coeficiente de x^{10} é definido por,
$\binom{-4}{10}(-1)^{10} = \frac{4.5.6.7.8.9.10.11.12.13}{10!} = \binom{13}{10} = 286$

Capítulo 3

A EQUAÇÃO DE FERMAT

Neste capítulo abordaremos as equações diofantinas conhecidas como equação de Fermat, em um primeiro momento iremos desenvolvê-las por um processo mais acessível para alunos e professores do ensino básico, em seguida iremos mostrar essas equações em tópicos mais avançados que são os domínios $\mathbb{Z}[i]$ e $\mathbb{Z}[w]$, onde usaremos $\mathbb{Z}[i]$ para exibir todas as soluções de $x^2 + y^2 = z^2$, com $x, y, z \in \mathbb{Z}$ e $\mathbb{Z}[w]$ para mostrar que $x^3 + y^3 = z^3$, com $x, y, z \in \mathbb{Z}$, não possui solução. O caso de $x^4 + y^4 = z^4$, também não possui solução ou seja,com $x, y, z \in \mathbb{Z}$, o que provaremos por descendência.

Finalizaremos demonstrando que se $n = 2p + 1$, com p primo, n também primo, então $x^n + y^n = z^n$, não possui solução inteira (teorema de Sophie Germain's) e para isto, precisaremos fazer uma breve abordagem na teoria de Grupos.

3.1 Grupos, Anéis e Ideais

Definição 3.1 *Um conjunto $\mathbb{G}$, munido de uma operação $*$ é um grupo se, para quaisquer $a, b, c \in \mathbb{G}$ são válidas as propriedades:*

(a) *Associatividade*: $a * (b * c) = (a * b) * c$, $\forall a, b, c \in \mathbb{G}$

(b) *Elemento neutro*: Existe $e \in \mathbb{G}$ tal que $a * e = e * a = a$.

(c) *Elemento inverso*: Dado $a \in \mathbb{G}$, existe um elemento $a^{-1} \in \mathbb{G}$ tal que $a * a^{-1} = a^{-1} * a = e$.

Se para quaisquer $a, b \in \mathbb{G}$, é satisfeita a propriedade $a * b = b * a$, dizemos que $\mathbb{G}$ é um grupo abeliano.

Definição 3.2 *A ordem de um grupo é o seu número de elementos.*

Definição 3.3 *Seja $\mathbb{G}$ um grupo e $n \in \mathbb{G}$. Se existe $m \in \mathbb{Z}$ tal que $n^m = U(n)$ é chamado de ordem de n. Entretanto, se $m = 0$ diremos que a ordem de n é zero. Usaremos a notação $U(n)$ para a ordem de n. Uma melhor abordagem sobre a função $U(n)$, pode ser encontrada na Definição1.9.*

Definição 3.4 *Seja $\mathbb{A}$ um conjunto não vazio e duas operações definidas nele (que chamaremos de adição, " + ", e multiplicação, " . "). O conjunto $\mathbb{A}$ é um anel se são válidas as propriedades:*

(a) *Associatividade aditiva*: $(a + b) + c = a + (b + c)$, $\forall a, b, c \in \mathbb{A}$
(b) *Comutatividade aditiva*: $a + b = b + a$, $\forall a, b \in \mathbb{A}$
(c) *Elemento neutro aditivo*: Existe $0 \in \mathbb{A}$ tal que $a + 0 = 0 + a = a$
(d) *Elemento inverso aditivo*: Para $a \in \mathbb{A}$ existe um único $-a$ tal que $a + (-a) = (-a) + a = 0$
(e) *Associatividade da multiplicação*: $a\,(bc) = (ab)\,c$, $\forall a, b, c \in \mathbb{A}$
(f) *Comutatividade da multiplicação*: $a.b = b.a$, $\forall a, b \in \mathbb{A}$
(g) *Elemento neutro multiplicativo*: Existe $1 \in \mathbb{A}$ tal que $a.1 = 1.a = a$, $\forall a \in \mathbb{A}$
(h) *Leis Distribuitivas*: $a.\,(b + c) = a.b + a.c$ e $(a + b)\,.c = a.c + b.c$, $\forall a, b, c \in \mathbb{A}$.

Chamaremos $(\mathbb{A}, +, .)$ de anel e na definição formal as propriedades (f) e (g), não são estritamente necessárias, sendo que um anel com tais propriedades é denominado anel comutativo com unidade. Além dessas propriedades, temos:
(1) $\mathbb{A}$ é um anel sem divisores de zero se, para quaisquer $a, b \in \mathbb{A}$, $ab = 0$ então ou $a = 0$ ou $b = 0$.
(2) $\mathbb{A}$ é um anel de integridade se $\mathbb{A}$ é um anel comutativo, com unidade e sem divisores de zero.
(3) $\mathbb{A}$ é um **corpo** se é um anel de integridade, onde todo elemento não-nulo possui inverso multiplicativo, ou seja,
$\forall a \neq 0$, $a \in \mathbb{A}$, existe a^{-1} tal que $a.a^{-1} = a^{-1}.a = 1$.

3.2 Equações de Fermat numa perspectiva básica

Teorema 3.1 *As soluções (x, y, z) da equação $x^2 + y^2 = z^2$, com $x, y, z \in \mathbb{Z}$ não nulos são dadas por $(x, y, z) = (2uvd, (u^2 - v^2)\, d, (u^2 + v^2)\, d)$, onde d, u, v são inteiros não nulos com $u \neq v$, $mdc\,(u, v) = 1$ e u e v com paridade distintas (d representa a multiplicidade da solução racional da equação diofantina pitagórica).*

Demonstração: Sejam x, y, z inteiros positivos quaisquer satisfazendo a equação $x^2 + y^2 = z^2$ e os demais casos análogos, d é o $mdc\,(x, y)$, então d^2 divide z^2 e daí temos que d divide z. Existem portanto inteiros não nulos, a, b, c, $mdc\,(a, b) = 1$, tais que $(x, y, z) = (da, db, dc)$ de modo que $x^2 + y^2 = z^2$ se, e somente se $a^2 + b^2 = c^2$, neste caso é suficiente determinarmos as soluções (a, b, c) da equação, sujeita à condição $mdc\,(a, b) = 1$ que por sua vez implica $mdc\,(a, c) = 1$ e $mdc\,(b, c) = 1$.
Dado um inteiro ρ qualquer, temos que ρ^2 deixa resto 0 ou 1 na divisão por 4, e daí $c^2 = a^2 + b^2$ deixaria resto 2 quando dividido por 4, o que é um absurdo. Como a e b são primos entre si não podem ser ambos pares, há então duas possibilidades a é ímpar e b é par e a outra a é par e b é ímpar, analisando a primeira possibilidade.
Se a for ímpar e b par, então c também é ímpar. De $a^2 + b^2 = c^2$, obtemos $b^2 = c^2 - a^2$ implica que $b^2 = (c - a)(c + a)$, conclui-se que $mdc\,(c - a, c + a) = 2$, podemos então escrever $\left(\frac{b}{2}\right)^2 = \left(\frac{c-a}{2}\right)^2 + \left(\frac{c+a}{2}\right)^2$. Note que $\left(\frac{c-a}{2}\right)$ e $\left(\frac{c+a}{2}\right)$, são primos entre si. Mas se o produto de dois naturais primos entre si $\left(\frac{c-a}{2}\ e\ \frac{c+a}{2}\right)$ é um quadrado perfeito, então cada um deles deve ser um quadrado perfeito. Existem então inteiros positivos primos entre si u e v, tais que $c - a = 2v^2$, $c + a = 2u^2$ é daí $(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2)$. Como $u^2 + v^2 = c$ é impar, u e v devem ter paridades distintas. ■

Algumas equações diofantinas podem não ter soluções, além das triviais, uma ferramenta poderosa para provar a existência ou inexistência de soluções dessas equações é o método *Descendência Infinita*, cuja criação é atribuída ao matemático francês Pierre de Fermat $(1601 - 1665)$. Esse método consiste em assumirmos uma existência de solução inteira e positiva e a partir dela, mostrarmos que podemos obter outra solução de valor inteiro positivo menor que a anterior, prosseguindo assim, construímos uma

seqüência infinita decrescente de valores positivos, mas pelo principio da boa ordem (que que todo conjunto não-vazio de números naturais possui um menor elemento) e ai chegaremos a uma contradição, concluindo assim que o problema não tem solução.

Proposição 3.1 *A equação $x^2 + y^2 = 3z^2$ não tem soluções inteiras não nulas.*

Demonstração: Suponhamos que a equação dada tenha soluções (x, y, z) em inteiros positivos não nulos, assim, seja (a, b, c) a solução que tenha a coordenada $z = c$ mínima. Sabemos que se um inteiro n não for múltiplo de 3, então o seu quadrado n^2 deixa resto 1 quando dividido por 3. Daí a e b tem que ser ambos múltiplos de 3, ou seja, existem inteiros r e s, tais que $a = 3r$ e $b = 3s$, assim $9r^2 + 9s^2 = 3c^2$ o que implica em $3(r^2 + s^2) = c^2$, portanto c é múltiplo de 3, logo existe um inteiro ρ de modo que $c = 3\rho$, por fim, temos $3(r^2 + s^2) = 9\rho^2$ e daí, $r^2 + s^2 = 3\rho^2$, ora dizer que o terno (r, s, ρ) é solução da equação dada, com $\rho = \dfrac{c}{3} < c$ que contraria o fato da coordenada c ser mínima. ■

Proposição 3.2 *A equação diofantina $x^n + y^n = z^n$ não tem soluções inteiras não nulas, se n for um inteiro positivo múltiplo de 4.*

Demonstração: Suponhamos que $n = 4\rho$, onde ρ é um inteiro positivo. Se $x^n + y^n = z^n$, então temos que $(x^\rho)^4 + (y^\rho)^4 = (z^{2\rho})^2$, ou seja, $(x^\rho, y^\rho, z^{2\rho})$ será uma solução da equação $a^4 + b^4 = c^2$, assim, o problema fica reduzido a se mostrar que esta última equação não tem soluções além das triviais. Suponhamos por absurdo que a, b e c sejam inteiros positivos que satisfaçam a equação $a^4 + b^4 = c^2$, além disso, para aplicarmos o método da Descendência Infinita de Fermat, vamos incluir a hipótese adicional de que c seja mínima, isto é, que não exista uma outra solução (a_1, b_1, c_1), em inteiros positivos, com $c_1 < c$. Então, a e b são primos entre si, pela Proposição 3.1, existem inteiros positivos primos entre si u e v, tais que $a^2 = u^2 - v^2$, $b^2 = 2uv$ e $c = u^2 + v^2$. Como $a^2 + v^2 = u^2$, ainda pela Proposição 3.1, temos que existem inteiros positivos primos entre si, p e q, tais que $a = p^2 - q^2$, $v = 2pq$ e $u = p^2 + q^2$, daí, segue que $b^2 = 2uv = 4pq(p^2 + q^2)$, como p e q são relativamente primos, ambos relativamente primos com $p^2 + q^2$, agora, sendo $4pq(p^2 + q^2)$ um quadrado perfeito, devemos ter p, q e $p^2 + q^2$ também quadrados perfeitos, portanto, existem positivos α, β, γ de modo que $p = \alpha^2$, $q = \beta^2$ e $p^2 + q^2 = \gamma^2$ daí segue que $\alpha^4 + \beta^4 = \gamma^2$, sendo $c = u^2 + v^2 > u = p^2 + q^2 = \gamma^2 > \gamma$ e isso contradiz a minimalidade de c. ■

3.3 Equações de Fermat numa perspectiva avançada

Exemplo 3.1 (Inteiros de Gauss) *Seja* $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}, i^2 = -1\}$, *calcule* $z_1 + z_2$, $z_1.z_2$ *e prove que* $(\mathbb{Z}[i], +, .)$ *é domínio de integridade.*

Resolução: Dados $z_1 = a + bi$ e $z_2 = c + di$, com a, b, c e d inteiros, teremos então, $z_1 + z_2 = (a + bi) + (c + di)$ implica que $Z_1 + Z_2 = (a + c) + (b + d)\, i$, logo $z_1 + z_2 \in \mathbb{Z}[i]$. No caso da multiplicação, temos $Z_1.Z_2 = (a + bi).(c + di)$ implica que $Z_1.Z_2 = (ac - bd) + (ad + bc)\, i$, pois $i^2 = -1$ logo $Z_1.Z_2 \in \mathbb{Z}[i]$. Para provar que $(\mathbb{Z}[i], +, .)$ é domínio de integridade, precisamos verificar a propriedade de integridade desse anel, ou seja, precisamos analisar a sua comutatividade com unidade e a nulidade.

Neste caso precisamos mostrar que $z_1.z_2 = z_2.z_1$, que $z_1.e = z_1$ e por fim a nulidade, $z_1.z_2 = 0$ implica que $z_1 = 0$ ou $z_2 = 0$. De fato, $z_1.z_2 = (ac - bd) + (ad + bc)\, i$, daí, $z_1.z_2 = (ca - db) + (da + cb)\, i$, então, segue que $z_1.z_2 = (c + di).(a + bi)$, logo $z_1.z_2 = z_2.z_1$ o que mostra a comutatividade de $(\mathbb{Z}[i], +, .)$. Provar que esse anel é comutativo com unidade, será preciso tomar $e \in \mathbb{Z}[i]$, sendo $e = e_1 + e_2 i$ e $z_1 = a + bi$ com $a \neq 0$ ou $b \neq 0$, de modo que $z_1.e = z_1$, ou seja, $(a + bi).(e_1 + e_2 i) = a + bi$, daí segue que $(ae_1 - be_2) + (ae_2 + be_1)\, i = a + bi$, logo para encontramos os valores de e_1 e e_2 será preciso resolver o sistema,

$$\begin{cases} ae_1 - be_2 = a \\ ae_2 + be_1 = b \end{cases}$$

ou seja,

$$\begin{cases} ae_1 - be_2 = a \\ be_1 + ae_2 = b \end{cases}$$

Resolvendo o sistema, $(a^2 + b^2)\, e_1 = (a^2 + b^2)$, fazendo $(a^2 + b^2) \neq 0$, encontraremos, $e_1 = 1$ e $e_2 = 0$, portanto $(\mathbb{Z}[i], +, .)$ é um anel comutativo com unidade, onde $e = 1 + 0i$. Nesta última parte mostraremos a nulidade desse anel, ou seja, $z_1.z_2 = 0$ implica que $z_1 = 0$ ou $z_2 = 0$, então $z_1.z_2 = (a + bi).(c + di) = 0$ implica que $(ac - bd) + (ad + bc)\, i = 0 + 0i$, logo,

$$\begin{cases} ac - bd = 0 \\ ad + bc = 0 \end{cases}$$

Analisando o sistema, temos $a(c^2+d^2)=0$, tomando $z_2 \neq 0$ e sendo $\mathbb{Z}$ um anel de integridade, daí, resulta $a=0$ e $b=0$, o que prova que $\mathbb{Z}[i]$ é um um domínio de integridade.

Exemplo 3.2 (Inteiros de Eisenstein) *Considere a equação $x^3+1=0$ em $\mathbb{C}$, com as raízes $x=1$ e $x=\pm w$, com $w=\dfrac{-1+\sqrt{3i}}{2}$, defina $\mathbb{Z}[w]=\{a+bw, a,b\in\mathbb{Z}\}$, dados $w_1=a+bw$ e $w_2=c+dw$, calcule w_1+w_2, $w_1.w_2$ e prove que $(\mathbb{Z}[w],+,.)$ é domínio de integridade.*

Resolução: Dados $w_1=a+bw$ e $w_2=c+dw$, com a, b, c e d inteiros, teremos então, $w_1+w_2=(a+bw)+(c+dw)$ implica que $w_1+w_2=(a+c)+(b+d)w$ logo $w_1+w_2\in\mathbb{Z}[w]$. No caso da multiplicação, temos $w_1.w_2=(a+bw).(c+dw)$ implica que $w_1.w_2=ac+adw+bcw+bdw^2$, mas $w^2=-(1+w)$, implica $w_1.w_2=(ac-bd)+(ad+bc-bd)w$, logo $w_1.w_2\in\mathbb{Z}[w]$. Para provar que $(\mathbb{Z}[w],+,.)$ é domínio de integridade, precisamos verificar a propriedade de integridade desse anel, ou seja, precisamos analisar a sua comutatividade com unidade e a nulidade.

Neste caso precisamos mostrar que $w_1.w_2=w_2.w_1$, que $w_1.e=w_1$ e por fim a nulidade, $w_1.w_2=0$ implica que $w_1=0$ ou $w_2=0$. De fato a comutatividade $w_1.w_2=(ac-bd)+(ad+bc-bd)w$, daí, $w_1.w_2=(ca-db)+(da+cb-bd)w$, então, segue que $w_1.w_2=(c+dw).(a+bw)$, logo $w_1.w_2=w_2.w_1$ o que mostra a comutatividade de $(\mathbb{Z}[w],+,.)$. Provar que esse anel é comutativo com unidade, será preciso tomar $e\in\mathbb{Z}[w]$, sendo $e=e_1+e_2w$ e $w_1=a+bw$ com $a\neq 0$ ou $b\neq 0$, de modo que $w_1.e=w_1$, ou seja, $(a+bw).(e_1+e_2w)=a+bw$, daí segue que $(ae_1-be_2)+(ae_2+be_1-be_2)i=a+bw$, logo para encontramos os valores de e_1 e e_2 será preciso resolver o sistema,

$$\begin{cases} ae_1-be_2=a \\ ae_2+be_1-be_2=b \end{cases}$$

ou seja,

$$\begin{cases} ae_1-be_2=a \\ be_1+(a-b)e_2=b \end{cases}$$

Analisando as equações do sistema, $[(a^2-ab)+b^2]e_1=[(a^2-ab)+b^2]$, fazendo $[(a^2-ab)+b^2]\neq 0$, encontraremos, $e_1=1$ e $e_2=0$, portanto $(\mathbb{Z}[w],+,.)$ é um

anel comutativo com unidade, $e = 1 + 0i$. Nesta última parte mostraremos a nulidade desse anel, ou seja, $w_1.w_2 = 0$ implica que $w_1 = 0$ ou $w_2 = 0$, então $w_1.w_2 = (a + bw).(c + dw) = 0$ implica que $(ac - bd) + (ad + bc - bd)w = 0 + 0w$, logo,

$$\begin{cases} ac - bd = 0 \\ ad + bc - bd = 0 \end{cases}$$

Resolvendo o sistema, temos $a(c - d) = bc$, fazendo $w_2 = 0$ e sendo $\mathbb{Z}$ um anel de integridade, daí, resulta que $(c - d) \neq 0$, logo $a = bc$, substituindo este valor em uma das equações do sistema, teremos $a = 0$ e $b = 0$, o que prova que $(\mathbb{Z}[w]$ é um domínio de integridade.

Definição 3.5 *Seja* $(\mathbb{A}, +, .)$ *um anel e* $\mathbb{I} \subseteq \mathbb{A}$ *dizemos que* $\mathbb{I}$ *é um ideal de* $\mathbb{A}$ *se,*

(1) $0 \in \mathbb{I}$
(2) $\forall a, b \in \mathbb{I}, a + b \in \mathbb{I}$
(3) Para $a \in \mathbb{I}$ e $b \in \mathbb{A}$, temos:
(i) $a.b \in \mathbb{I}$, ideal à esquerda;
(ii) $b.a \in \mathbb{I}$, ideal à direita.

Exemplo 3.3 *Provar que o conjunto dos números pares é um ideal em* $\mathbb{Z}$.

Resolução: Dado o conjunto $\mathbb{I}$ representando os números inteiros pares, ou seja, $\mathbb{I} = \{n : n = 2k, k \in \mathbb{Z}\}$. Como $\mathbb{I} \subset \mathbb{Z}$, com $\mathbb{I} \neq \emptyset$ é um ideal em $\mathbb{Z}$ se, e somente se,
(i) para todo $n_1, n_2 \in \mathbb{I}$, implica que $n_1 - n_2 \in \mathbb{I}$ de fato, $n_1 - n_2 = 2k_1 - 2k_2 = 2(k_1 - k_2)$ que é par e pertence ao conjunto $\mathbb{I}$.
(ii) para todo $a \in \mathbb{Z}$ e $n \in \mathbb{I}$ implica que $an \in \mathbb{I}$, de fato, $an = a(2k) = 2(ak)$ com $k \in \mathbb{Z}$, logo an é par e pertence ao conjunto $\mathbb{I}$. Portanto o conjunto dos números pares é um ideal em $\mathbb{Z}$.

Definição 3.6 *O ideal* $\mathbb{I} = \mathbb{A}x$ *é dito ideal principal (à esquerda) gerado por* $x \in \mathbb{A}$.

Sejam $\mathbb{A}$ um anel e $\mathbb{I} = \mathbb{A}z$, com $z \in \mathbb{A}$, um ideal principal de $\mathbb{A}$. Para $a_1, a_2 \in \mathbb{A}$, define-se a relação,
$a_1 \equiv a_2 \, (mod(\mathbb{I})) \Leftrightarrow a_1 - a_2 \in \mathbb{I}$.

A relação " $\equiv$ " é uma relação de equivalência em A. O conjunto,
$\overline{a} = \{y \in \mathbb{A} : y \equiv a_1 \, (mod(\mathbb{I}))\}$ é uma classe de equivalência do elemento $y \in \mathbb{A}$, observe que $y \in \overline{a} \Leftrightarrow y - a_1 \in \mathbb{I}$.

$$\text{Notação: } \overline{a} = a_1 + \mathbb{I} = \{a_1 + a_3 : a_3 \in \mathbb{I}\}$$

Nem todo ideal em um anel arbitrário é principal. Se todos os ideais de um domínio de integridade são principais, diremos que o domínio é um domínio de ideais principais (DIP).

Proposição 3.3 *$\mathbb{Z}$ é um domínio de ideais principais ou ($\mathbb{Z}$ é DIP).*

Demonstração: Pelo princípio da boa ordem em $\mathbb{N}, \mathbb{I}_+$, possui menor elemento que denotaremos por d, vamos demonstrar que, pela divisão euclidiana $a = qd + r$, pois $d \neq 0$, onde $0 \leq r < d$.
Se $r \neq 0$, com $r = a - qd$ e $d \in \mathbb{I} \Rightarrow -qd \in \mathbb{I} \Rightarrow a - qd \in \mathbb{I}$, pois $a \in \mathbb{I}$, logo $r \in \mathbb{I}$. Mas $r > 0$, (pois $r \neq 0$ e $0 \leq r < d$)$\Rightarrow r \in \mathbb{I} \cap \mathbb{N}$ o que contradiz a escolha de d, como menor elemento de $\mathbb{I} \cap \mathbb{N}$, logo $r = 0$ e $a = qd$, isso mostra que $\forall a \in \mathbb{I}, \exists q \in \mathbb{Z}$ tal que $a = qd$, donde $\mathbb{I} \cap (d)$, ((d): conjunto dos múltiplos de d), segue que $(d) \subseteq \mathbb{I}$, logo $\mathbb{I} = (d)$. ■

Proposição 3.4 *Dados $a, b \in \mathbb{Z}$, então $(a, b) = (d)$, onde d é o máximo divisor comum de a e b.*

Demonstração: $(a, b) = \{ax + by : x, y \in \mathbb{Z}\}$ é ideal. Pela Proposição 3.3, segue que existe $d \in \mathbb{Z}$ tal que $(a, b) = (d)$. Queremos mostrar que d é o máximo divisor comum de a e b, com efeito,
(i) Se $d|a$ e $d|b$ pois $\begin{cases} a \in (a, b), \text{quando } x = 1 \text{ e } y = 0 \\ b \in (a, b), \text{quando } x = 0 \text{ e } y = 1 \end{cases} \Rightarrow \begin{cases} a \in (d) \\ b \in (d) \end{cases}$ de modo que,

$$\begin{cases} \exists q_1 \in \mathbb{Z}, \text{tal que } a = q_1 d \\ \exists q_2 \in \mathbb{Z}, \text{tal que } a = q_2 d \end{cases} \Rightarrow \begin{cases} d|a \\ d|b \end{cases}$$

(ii) Seja $c \in \mathbb{Z}$ tal que $c|a$ e $c|b$ então $c|d$, $c \geq 0$, (em particular, $c \leq d$.
De fato, $(d) = (a, b) \Rightarrow \exists x, y \in \mathbb{Z}$ tais que $d = ax + by$, como,

$$\begin{cases} c|a \Rightarrow \exists q_1 \in \mathbb{Z}, \text{tal que } a = q_1 c \\ c|b \Rightarrow \exists q_2 \in \mathbb{Z}, \text{tal que } b = q_2 c \end{cases}$$

donde,
$d = ax + by = x.(q_1 c) + y(q_2 c) = (xq_1)c + (yq_2)c = (xq_1 + yq_2)c \Rightarrow c|d.$ ■.

Proposição 3.5 *$\mathbb{Z}[i]$ é domínio de ideais principais.*

Demonstração: Definindo $\lambda : \mathbb{Z}[i] \to \mathbb{Z}$, $z \to z.\overline{z}$, onde $\overline{z}$ é o conjugado complexo de z, (ou seja, se $z = a + bi$, temos $\overline{z} = a - bi$ e $\lambda(z) = z.\overline{z} = a^2 + b^2$).
Sejam então z e w, com $w \neq 0$, existem $s, r \in \mathbb{Z}[i]$ de modo que $z = ws + r$ e $\lambda(r) < \lambda(w)$, tem-se $\frac{z}{w} = \frac{z\overline{w}}{\lambda(w)} = \frac{Re(z\overline{w})}{\lambda(w)} + \frac{Im(z\overline{w})}{\lambda(w)} = x + yi$ para alguns x e y racionais, sejam q_1 e q_2 inteiros, tal que $q_1 = \lfloor x \rfloor$ e $q_2 = \lfloor y \rfloor$, (onde $\lfloor \alpha \rfloor$ maior inteiro menor ou igual a α), então $\frac{z}{w} = (q_1 + q_2 i) + (\epsilon_1 + \epsilon_2 i)$, com $|\epsilon_1| \leq \frac{1}{2}$ e $|\epsilon_2| \leq \frac{1}{2}$, fazendo $q = q_1 + q_2 i$, $\epsilon = \epsilon_1 + \epsilon_2 i$ e $r = \epsilon w$, resulta que $r = z - wq \in \mathbb{Z}[i]$ e $\lambda(r) = \lambda(\epsilon)\lambda(w) = (\epsilon_1^2 + \epsilon_2^2)\lambda(w) \leq \frac{1}{2}\lambda(w) < \lambda(w)$.

Para mostrar que $\mathbb{Z}[i]$ é domínio de ideais principais, tomaremos $\mathbb{I} \neq \{0\}$ um ideal de $\mathbb{Z}[i]$, escolhendo um $z \in \mathbb{I}$, tal que $\lambda(z) = min\{\lambda(x)/x \in \mathbb{I} - \{0\}\}$, fica claro que $< z > \subseteq \mathbb{I}$, reciprocamente, se $w \in \mathbb{I}$, resulta que existem $s, r \in \mathbb{Z}[i]$ com $z = ws + r$ e $\lambda(r) < \lambda(w)$, porém $r = z - ws \in \mathbb{I}$ com $\lambda(r) < \lambda(w)$ o que implica que $r = 0$, pela escolha de z, daí, temos $w \in < z >$, logo $\mathbb{I} = < z >$, então podemos concluir que $\mathbb{Z}[i]$ é um DIP.

Seja então $\mathbb{I} \subseteq \mathbb{Z}[i]$ ideal e defina $\mathbb{I}_+ = \{\lambda(z) : z \in \mathbb{I}\} \cap \mathbb{N}$, escolhendo um $\delta \in \mathbb{I}$, tal que $\lambda(z)$ seja o menor elemento em $\mathbb{I}_+$. Queremos mostrar que $\mathbb{I} = (\delta)$, de fato, seja $z \in \mathbb{I}$, pelo exposto anteriormente, $z = q\delta + r$, com $q, r \in \mathbb{Z}[i]$ e $r = 0$ ou $0 \leq \lambda(r) \leq \lambda(\delta)$.
Se $r \neq 0$, $r = z - q\delta \in \mathbb{I}$ e $\lambda(r) < \lambda(\delta)$, viola o fato de escolher δ tal que seja o menor elemento em $\mathbb{I}_+$, logo $r = 0$ e $z = q\delta \Rightarrow Z \in (\delta) \Rightarrow \mathbb{I} \subseteq (\delta)$, como $\delta \in \mathbb{I} \Rightarrow (\delta) \leq \mathbb{I}$,

segue que $\mathbb{I} = (\delta)$.
Observamos que o essencial à demonstração foi encontrar no anel considerado ($\mathbb{Z}$ ou $\mathbb{Z}[i]$) uma função $\lambda : A \to \mathbb{Z}^+$ com propriedades da divisão euclidiana, ou seja, "dados $a, b \in A,\ b \neq 0,\ \exists q, r \in A$, tal que $a = qb + r$ e $r = 0$ ou $\lambda(r) < \lambda(b)$".

Anéis munidos de funções com propriedades da divisão euclidiana são ditos "Domínios Euclidianos".

Proposição 3.6 *$\mathbb{Z}[w]$ é domínio euclidiano.*

Demonstração: Definindo $\lambda(a + bw) : a^2 + b^2 - ab$ e precisamos mostrar que são válidas as propriedades euclidiana em $\mathbb{Z}[w]$. Dado $z = a + bw$, com $z \in \mathbb{Z}[w]$, sabemos que $\lambda(z) = z.\overline{z}$ e que $\overline{z} = a + bw^2$, definindo um α e β em $\mathbb{Z}[w]$ e supondo $\beta \neq 0$, temos $\dfrac{\alpha}{\beta} = \dfrac{\alpha.\overline{\beta}}{\beta.\overline{\beta}} = r + sw$, onde r e s são números racionais, mas $\lambda(\beta) = \beta.\overline{\beta}$ é um número inteiro positivo, logo, $\alpha.\overline{\beta} \in \mathbb{Z}[w]$, desde que, $\alpha,\ \overline{\beta} \in \mathbb{Z}[w]$. Definiremos m e n tais que $|r - m| \leq \dfrac{1}{2}$ e $|s - n| \leq \dfrac{1}{2}$, então, fazendo $\theta = m + n$, temos $\lambda\left(\dfrac{\alpha}{\beta} - \theta\right) = (r-m)^2 - (r-m)(s-n) + (s-n)^2 \leq \dfrac{1}{4} + \dfrac{1}{4} + \dfrac{1}{4} < 1$ permitindo $\delta = \alpha - \theta.\beta$, teremos assim, $\delta = 0$ ou $\lambda(\delta) = \lambda\left[\beta\left(\dfrac{\alpha}{\beta} - \theta\right)\right] = \lambda(\beta)\,\lambda\left(\dfrac{\alpha}{\beta} - \theta\right) < \lambda(\beta)$.

Mostrando que $\lambda\left[\beta\left(\dfrac{\alpha}{\beta} - \theta\right)\right] = \lambda(\beta)\,\lambda\left(\dfrac{\alpha}{\beta} - \theta\right) < \lambda(\beta)$, são válidas essas propriedades em $\mathbb{Z}[w]$

Exemplo 3.4 *Prove que todo domínio euclidiano é domínio de ideais principais como corolário, prove que $\mathbb{Z}[w]$ é domínio de ideais principais.*

Resolução: Sejam A um domínio euclidiano, com norma λ e $\mathbb{I}$ um ideal em A, se $\mathbb{I} = \{0\} = (0)$ fica fácil perceber que ele é principal, no entanto, se $\mathbb{I} \neq (0)$ e considerarmos o conjunto $\{\lambda(a)/a \in \mathbb{I}, a \neq 0\} \subseteq N$, pelo princípio da boa ordenação, este conjunto tem um mínimo k_o, de modo que $a_o \in \mathbb{I}$ e $\lambda(a_o) = k_o$, $a_o \neq 0$, o que implica $(a_o) \subseteq \mathbb{I}$. Se $(a_o) \in \mathbb{I}$, com $a_o \neq 0$, então existem $q, s \in A$ tais que $a = qa_o + r$, com

$r = 0$ ou $\lambda(r) < \lambda(a_o)$, implicando que $r = a - qa_o \in \mathbb{I}$, então, pela minimalidade de a_o, temos $r = 0$, de modo que $a = qa_o \in (a_o)$, logo $\mathbb{I} \subseteq (a_o)$, daí segue que $\mathbb{I} = (a_o)$, concluindo que A é um DIP.

Para mostrar que $\mathbb{Z}[w]$ é domínio de ideais principais, tomaremos $\mathbb{I} \neq \{0\}$ um ideal de $\mathbb{Z}[w]$, escolhendo um $z \in \mathbb{I}$, tal que $\lambda(z) = min\{\lambda(x)/x \in \mathbb{I} - \{0\}\}$, fica claro que $< z > \subseteq \mathbb{I}$, reciprocamente, se $k \in \mathbb{I}$, resulta que existem $s, r \in \mathbb{Z}[w]$ com $z = ks + r$ e $\lambda(r) < \lambda(k)$, porém $r = z - ks \in \mathbb{I}$ com $\lambda(r) < \lambda(k)$ o que implica que $r = 0$, pela escolha de z, daí, temos $k \in < z >$, logo $\mathbb{I} = < z >$, então podemos concluir que $\mathbb{Z}[w]$ é um DIP.

Já vimos que $\mathbb{Z}[i]$ e $\mathbb{Z}[w]$, são domínios de integridade, mais ainda que eles são domínios euclidianos.

Dados $(\mathbb{A}, +, .)$ domínio de integridade, diremos que $u \in A$ é unidade se $u|a$, $\forall a \in A$ é fácil ver que as unidades em $\mathbb{Z}$ são ± 1, em $\mathbb{Z}[i]$, são ± 1 e $\pm i$ e em $\mathbb{Z}[w]$, são são ± 1, $\pm w$ e são $\pm w^2$, para verificar esse fato, lembramos que em $\mathbb{Z}$, $\lambda(a) = |a|$, em $\mathbb{Z}[i]$, $\lambda(a) = a.\overline{a}$ e em $\mathbb{Z}[w]$, $\lambda(x + wy) = x^2 + y^2 - xy$ e que u é unidade nestes anéis se, e somente se, $\lambda(u) = 1$, (de fato, em todos os casos acima,
$\lambda(ab) = \lambda(a)\lambda(b)$, logo $\lambda(u) = \lambda(u.u) = \lambda^2(u) \Rightarrow (\lambda(u) - 1)\lambda(u) = 1$, se $\lambda(u) = 0$ então $u = 0$ e não é unidade, logo $(\lambda(u) - 1) = 0$ então $\lambda(u) = 1$. Quanto a recíproca, se $\lambda(u) = 1$, queremos mostrar que u é unidade, conforme sabemos que cada anél acima é domínio euclidiano, logo dado $a \in A$, $\exists q, r \in A$, onde $a = qu + r$ e $r = 0$ ou $\lambda(r) < \lambda(u) = 1$, logo $r = 0$ ou $\lambda(r) = 0 \Rightarrow r = 0$ donde $a = qu$, portanto $u|a$).

Dado $\pi \in \mathbb{A}$, $(\mathbb{A}, +, .)$ domínio de integridade, diremos que irredutível (se dado $a \in A$, com $a|\pi$, então $a = u\pi$ e u unidade em $\mathbb{A}$), *"dois elementos em um anel que diferem por um produto por unidade são ditos elementos associados, assim, um irredutível é um elemento em um anel divisível apenas por seus associados"*.

Dados $p \in \mathbb{A}$, diremos que p é primo quando $p|ab \Rightarrow p|a$ ou $p|b$. Em $\mathbb{Z}$, irredutível e primo são termos intercembiavel, em geral, isso não ocorre, mas vale o resultado.

Proposição 3.7 *Seja $(\mathbb{A}, +, .)$ domínio de integridade, então todo elemento primo de $\mathbb{A}$ é também irredutível em $\mathbb{A}$.*

Demonstração: Seja $p \in \mathbb{A}$ primo e suponha $p = ab$ com $a, b \in \mathbb{A}$, então $p|ab$ logo $p|a$ ou $p|b$, pois p é primo, suponhamos sem perda de generalidade que $p|a$, então $a = cp$, logo $p = ab = cpb = p(cb)$ como $\mathbb{A}$ é domínio de integridade, temos $1 = cb$ e portanto c e b são unidades, em particular $p = ab$ daí a é associado de p e b é unidade logo p é irredutível.

Teorema 3.2 *Todo domínio euclidiano é domínio de ideais principais.*

Demonstração: Seja $(\mathbb{A}, +, .)$ domínio euclidiano, ou seja, $\exists \lambda : \mathbb{A} \to \mathbb{Z}^+$, tal que dados $a, b \in \mathbb{A}$, $b \neq 0$, $\exists q, r \in \mathbb{A}$, tal que $a = qb + r$ e $r = 0$ ou $\lambda(r) < \lambda(b)$, seja $\mathbb{I}$ ideal de $\mathbb{A}$ e consideremos $\mathbb{I}_+ = \{\lambda(a) : a \in \mathbb{A}\} \cap \mathbb{N}$, tomemos $d \in \mathbb{A}$, tal que $\lambda(d)$ seja o menor elemento em $\mathbb{I}_+$ que existe pelo princípio da boa ordem, então dado $a \in \mathbb{I}$, $a = qd + r$, onde $q, r \in A$, $r = 0$ ou $\lambda(r) < \lambda(d)$, $\Rightarrow r = a - qd \in \mathbb{I}$, logo $r = 0$, pois $\lambda(d)$ é o menor possível em $\mathbb{I}_+ \cap \mathbb{N}$, logo $\forall a \in \mathbb{I}$, $d|a \Rightarrow \mathbb{I} \subseteq (d)$ e como $d \in \mathbb{I}$ é trivial que $(d) \subseteq \mathbb{I}$, portanto $\mathbb{I} = (d)$ e o ideal $\mathbb{I}$ é principal. Isso vale para qualquer ideal, logo o anel $\mathbb{A}$ é um domínio de ideais principais.

Corolário 3.1 *$\mathbb{Z}$, $\mathbb{Z}[i]$ e $\mathbb{Z}[w]$ são domínios de ideais principais.*

Lema 3.1 *Em um domínio de ideais principais toda cadeia ascendente de ideais é estacionária, ou seja, dado $\{\mathbb{I}_n\}_n \in \mathbb{N}$, sequência de ideais tais que $\mathbb{I}_n \subseteq \mathbb{I}_{n+1}$, $(\mathbb{I}_1 \subseteq \mathbb{I}_2 \subseteq \mathbb{I}_3 \cdots)$, então existe $N \in \mathbb{N}$, tal que $\mathbb{I}_m = \mathbb{I}_n$, $\forall m \geq N$.*

Demonstração: Seja $\mathbb{I} = \bigcup_{i=1}^{\infty} \mathbb{I}_i$ é fácil ver que $\mathbb{I}$ é ideal em A com efeito, sejam $x, y \in \mathbb{I}$, então $x, y \in \bigcup_{i=1}^{\infty} \mathbb{I}_i$, logo $\exists\ m, n \in \mathbb{N}$, tais que $x \in \mathbb{I}_n$ e $y \in \mathbb{I}_m$, logo $x, y \in \mathbb{I}_{max}(m, n)$,

pois $\mathbb{I}_m \subseteq \mathbb{I}_{max}(m,n)$ e $\mathbb{I}_n \subseteq \mathbb{I}_{max}(m,n)$, donde $x+y \in \mathbb{I}_{max}(m,n)$, pois $\mathbb{I}_{max}(m,n)$ é ideal, portanto $x+y\bigcup_{i=1}^{\infty}\mathbb{I}_i \supseteq \mathbb{I}_{max}(m,n)$.

Dado $a \in \mathbb{A}$, $x \in \mathbb{I}$, queremos mostrar que $ax \in \mathbb{I}$, com efeito, $x \in \mathbb{I} = \bigcup_{i=1}^{\infty}\mathbb{I}_i$ implicando que existe $m \in \mathbb{N}$, tal que $x \in \mathbb{I}_m$, pois $\mathbb{I}_m$ é ideal e portanto $x \in \bigcup_{i=1}^{\infty}\mathbb{I}_i \supseteq \mathbb{I}_m$. Como $\mathbb{A}$ é domínio de ideais principais, existe $d \in \mathbb{A}$, tal que $\mathbb{I} = (d)$, em particular $d \in \mathbb{I} = \bigcup_{i=1}^{\infty}\mathbb{I}_i$ tomando $N \in \mathbb{N}$ tal que $d \in \mathbb{I}_N$ daí segue $(d) \subseteq \mathbb{I}_N \subseteq \bigcup_{i=1}^{\infty}\mathbb{I}_i = (d)$ implicando em $\mathbb{I}_N = (d)$. Dado $\mathbb{I}_m$, $m \geq N$, note que $\mathbb{I}_m \subseteq \bigcup_{i=1}^{\infty}\mathbb{I}_i = (d)$, implica que $\mathbb{I}_m \subseteq (d)$, mas $\mathbb{I}_N \subseteq \mathbb{I}_m$ então, $(d) \subseteq \mathbb{I}_m$, logo $\mathbb{I}_m = (d) = \mathbb{I}_N$, $\forall m \geq N$. ∎

Lema 3.2 *Em um domínio de ideais principais todo irredutível é primo, em particular, nestes tipos de domínios, primos e irredutíveis são os mesmos.*

Demonstração: Seja π elemento irredutível e suponha que $\pi|ab$ queremos mostrar que $\pi|a$ ou $\pi|b$, suponhamos que $\pi \nmid b$, então consideremos $\mathbb{I} = (b,\pi)$, é claro que $(b,\pi) \subseteq \mathbb{A}$, contudo dado que $\mathbb{A}$ é domínio de ideais principais segue $(b,\pi) = (d)$, em particular, d é divisor de b e de π, π é irredutível, logo d é unidade ou associado de π, mas $\pi \nmid b$, logo d não pode ser associado de π, portando d é unidade em $\mathbb{A}$, logo $(d) \supseteq (1) = \mathbb{A}$, ou seja $(b,\pi) = \mathbb{A}$, portanto existem $r,s \in \mathbb{A}$, tal que $1 = rb + s\pi \Rightarrow a = r(ab) + (sa)\pi = (r+sa)\pi$, portanto $\pi|a$. ∎

Proposição 3.8 *Em um domínio de ideais principais todo elemento pode ser escrito como produto de irredutíveis (ou primos).*

Demonstração: Seja a elemento qualquer não unidade nem nulo do domínio de ideais principais $(\mathbb{A},+,.)$, sendo $x_1 = a$, se x_1 é irredutível, nada temos a demonstrar, do contrário $x_1 = a_1.x_2$, onde x_2 não é unidade e nem associado de x_1, a_1 e x_2 são iredutíveis, nada temos a demonstrar, do contrário, após eventual mudança de variáveis, podemos, assumir que x_2 não é irredutível, logo $x_2 = a_2.x_3$ e o processo continua em particular, se o processo "parar" em algumas etapas, teremos $a = a_1.a_2.a_3.a_4.\cdots.a_{x-1}.x_k$, com x_k

irredutível ou seja, "qualquer a não unidade nem nulo é divisível por algum irredutível", se o processo pudesse proseguir indefinidamente, teriamos $(x_1) \subseteq (x_2) \subseteq (x_3) \subseteq (x_4) \subseteq \cdots \subseteq$, cadeias ascendentes infinita de ideais o que não é possível pelo Lema 3.2.
Seja, finalmente, $a \in \mathbb{A}$ não unidade nem nulo pelo exposto acima, $a = \pi_1 a_1$, com π_1 irredutível, se a_1 é irredutível nada temos a demonstrar, do contrário $a_1 = \pi_2 a_2$, com π_2 irredutível, o que em última análise conduz à sequência $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq (a_4) \subseteq \cdots$ que é estacionária, logo existe $k \in \mathbb{N}$, tal que $a = \pi_1.\pi_2.\pi_3.\pi_4.\cdots.\pi_k.u$, onde $(u) = \mathbb{A}$, logo u é unidade. ■

Teorema 3.3 *Todo domínio de ideais principais é também domínio de fatoração única, ou seja, dado $a \in \mathbb{A}$ (a não nulo nem unidade) existe um único conjunto finito de irredutíveis $\pi_1.\pi_2.\pi_3.\pi_4.\cdots.\pi_k$, tal que,*
(i) $a = \pi_1^{e_1}.\pi_2^{e_2}.\pi_3^{e_3}.\pi_4^{e_4}.\cdots.\pi_k^{e_k}$
(ii) $u, e_1, e_2, e_3, e_4, \ldots, e_k$, *são unicamente determinados pela ordem imposta a,*

$$\{\pi_1.\pi_2.\pi_3.\pi_4.\cdots.\pi_k\}.$$

Demonstração: Já vimos que, um domínio de ideais principais qualquer elemento não nulo nem unidade é produto de irredutíveis. Seja π irredutível tal que $\pi|a$ então existe $n \in \mathbb{N}$ tal que $\pi^n|a$, mas $\pi^{n+1} \nmid b$, (n é dito ordem π-ádica de a e é denotado por $a = ord_\pi(a)$), de fato $\pi^i|\pi^{i+1}$ implicando em $\left(\pi^i\right) \subseteq \left(\pi^{i+1}\right)$ e se não houvesse limite para $ord_\pi(a)$ teriamos a cadeia ascendente de ideais $(\pi) \subseteq (\pi^2) \subseteq (\pi^3) \subseteq (\pi^4)\cdots$, o que não é possível pois $\mathbb{A}$ é domínio de ideais principais. Pela mesma razão é fácil ver que o conjunto dos irredutíveis que divide a é finito e temos, portanto, que existe $\pi_1.\pi_2.\pi_3.\pi_4.\cdots.\pi_k$, conjunto finito de irredutíveis tal que $a = u\pi_1^{\alpha_1}.\pi_2^{\alpha_2}.\pi_3^{\alpha_3}.\pi_4^{\alpha_4}.\cdots.\pi_k^{\alpha_k}$ com $\alpha_i = ord_{\pi_i}(a)$, $i = 1, 2, \ldots, k$ e u uinidade.
Seja então δ outro irredutível em $\mathbb{A}$, (δ não associado de π_i, com $i = 1, 2, \ldots, k$), tal que $\alpha|a$, então
$ord_\delta(a) = ord_\delta\left(u\pi_1^{\alpha_1}.\pi_2^{\alpha_2}.\pi_3^{\alpha_3}.\pi_4^{\alpha_4}.\cdots.\pi_k^{\alpha_k}\right)$
$ord_\delta(a) = ord_\delta(u) + \alpha_1 ord_\delta(\pi_1)\,\alpha_2 ord_\delta(\pi_2) + \alpha_3 ord_\delta(\pi_3) + \ldots + \alpha_k ord_\delta(\pi_k)$
$ord_\delta(a) = 0$
pois os divisores de π_i são seus associados. ■

Corolário 3.2 $\mathbb{Z}$, $\mathbb{Z}[i]$ *e* $\mathbb{Z}[w]$ *são domínios de fatoração única.*

Proposição 3.9 *As soluções diofantinas (isto é, $x, y, z \in \mathbb{Z}$) da equação pitagórica $x^2 + y^2 = z^2$ podem ser parametrizadas por,*

$$\begin{cases} x = a^2 - b^2 \\ y = 2ab \qquad com\ a, b \in \mathbb{Z} \\ z = a^2 + b^2 \end{cases}$$

Demonstração: É fácil a verificação que cada valor de x, y e z, obtidos pela parametrização acima, é de fato, uma solução da equação pitagórica. Queremos mostrar que não existem outras, com efeito,
$x^2 + y^2 = z^2 \Rightarrow (x + iy)(x - iy) = z^2$, considerando agora a equação em $\mathbb{Z}[i]$, seja $\pi \in \mathbb{Z}[i]$ irredutível tal que $\pi | (x + iy)$ e $\pi | (x - iy)$, então,
(i) $\pi | [(x + iy) + (x - iy)] \Rightarrow \pi | 2x$
(ii) $\pi | [(x + iy) - (x - iy)] \Rightarrow \pi | 2iy$, como i é unidade, temos que $\pi | 2y$.

Note que eliminando os fatores primos (em $\mathbb{Z}$) em comum na equação $x^2 + y^2 = z^2$, temos z ímpar, assim, se $\pi | 2$, teriamos,
$\pi | (1 + i) \Rightarrow \pi.\overline{\pi} = 2 | z^2$ ou $\pi = 2 \Rightarrow 2 | z^2$ que é uma contradição, pois z é ímpar, assim $\pi | x$ e $\pi | y \Rightarrow \lambda(\pi) | \lambda(x)$ e $\lambda(\pi) | \lambda(y)$, mas $\lambda(\pi) = p$, pois a norma de um irredutível em $\mathbb{Z}[i]$ é um primo em $\mathbb{Z}$ e $\lambda(x) = x^2$, $\lambda(y) = y^2$ e teremos p fator primo em comum a x^2 e a y^2, logo também a z^2, considerando a escolha de $x^2 + y^2 = z^2$, com o $\text{mdc}(x, y) = 1$, assim, $x + iy$ e $x - iy$ são coprimos em $\mathbb{Z}[i]$.

Fatorando z em $\mathbb{Z}[i]$, temos, pela fatoração única em $\mathbb{Z}[i]$ que $x + iy$ e $x - iy$ são quadrados em $\mathbb{Z}[i]$, logo $x + iy = u\beta^2$, escrevendo $\beta^2 = a + bi$ e $u = 1$, teremos,

$$\begin{cases} x = a^2 - b^2 \\ y = 2ab \\ z = a^2 + b^2. \end{cases}$$

■

A importância da demonstração acima é que ela sugere generalizações para o caso $x^n + y^n = z^n$, com $n \geq 3$, conforme veremos adiante, o uso das propriedades de $\mathbb{Z}[w]$ é crucial para verificar a existência de soluções em $x^{3n} + y^{3n} = z^{3n}$, com $n \geq 1$ inteiro que é o mesmo que $(x^n)^3 + (y^n)^3 = (z^n)^3$.

Continuando a abordagem sobre o teorema de Fermat, enunciaremos e demonstraremos o teorema de **Sophie Germain**.

Sophie Germain nasceu em Paris em 01 de Abril de 1776, no seio de uma família da classe média. O seu pai era mercador e mais tarde tornou-se diretor do Banco de França. Nesse mesmo ano começou a Revolução Americana e treze anos mais tarde iniciou-se a Revolução Francesa. Os seus pais consideravam que este interesse pela matemática era inapropriado para uma rapariga e fizeram tudo o que podiam para desencorajá-la, chegando ao ponto de lhe tirarem as roupas quando ela ia para cama e de a privarem de aquecimento e luz para que ela fosse forçada a permanecer na cama em vez de ir estudar. Contudo, estes esforços falharam. Sophie embrulhava-se nos cobertores e usava velas que tinha escondido para poder estudar à noite. Deste modo, os pais acabaram por concluir que a sua paixão pela matemática era incurável. Assim, a sua época foi marcada por um espírito revolucionário que caracteriza também a sua personalidade. Contra os preconceitos da sua família e da sociedade da época, Sophie trabalhou arduamente e lutou com perseverança para se tornar matemática reconhecida.

Sophie resolveu alguns casos particulares do último teorema de Fermat, donde nasceu a definição de "números primos de Sophie Germain"e, em 1816, ganhou um concurso promovido pela Academia de Ciências da França, resolvendo um problema que foi proposto na época sobre vibrações de membranas. De seus trabalhos e pesquisas nesta área é de onde nasceu o conceito de curvatura média de superfícies, conceito este, que é hoje objeto de pesquisa de vários matemáticos na área de Geometria Diferencial.

Embora com algumas falhas matemáticas, devidas talvez ao seu autodidatismo e ao seu isolamento do meio acadêmico matemático, Sophie Germain foi sem dúvida, a primeira mulher a fazer um trabalho matemático inédito e de grande importância.

Antes de enunciarmos o teorema de Fermat, observe a tabela abaixo.

Teorema de Sophie Germain	
p	$2p+1$
2	5
3	7
5	11
7	15
11	23
13	27
17	35
19	39
23	47

Em muitos casos, se p é primo, $2p+1$ também é primo. Se um primo p é tal que $2p+1$ é primo chamamos p de primo de Sophie Germain.

Teorema 3.4 *Seja p primo ímpar de Sophie Germain, então $x^p + y^p + z^p = 0$ não possui solução diofantina na qual $p \nmid xyz$.*

Demonstração: Suponha, por absurdo, que existe solução e que após eventuais cancelamentos, que não haja fatores primos em comum a x, y e z, escrevendo então,
$-x^p = y^p + z^p$
$-x^p = (y+z)\left(z^{p-1} - z^{p-2}y + \ldots + y^{p-1}\right).$
Seja então,
$r|y+z$
$r|\left(z^{p-1} - z^{p-2}y + \ldots + y^{p-1}\right)$
$y + z \equiv mod r$ implica que $y \equiv -z mod r$ e $z^{p-1} - z^{p-2}y + \ldots + y^{p-1} \equiv 0 mod r$, substituindo $y \equiv -z mod r$ de modo que, $z^{p-1} + z^{p-1} + z^{p-1} + \ldots + z^{p-1} \equiv 0 mod r$ logo, $pz^{p-1} \equiv 0 mod r$. Como $r \nmid p$, pois p é primo segue que $r|z$ então $r|x$ pois $r|y+z$, $r|y$, pois $y \equiv -z mod r$ e $r|z$, portanto r é fator comum a x, y, z, então $r = 1$.
Assim, $-x^p = (y+z)\left(z^{p-1} - z^{p-2}y + \ldots + y^{p-1}\right)$ pela fatoração única em $\mathbb{Z}$, implica que,

$$\begin{cases} x+y=A^p \\ z^{p-1}-z^{p-2}y+\ldots+y^{p-1}=T^p, \quad com\ A,T\in\mathbb{Z}. \end{cases}$$

escrevendo,

$$\begin{cases} -z^p=x^p+y^p \\ -y^p=x^p+z^p \end{cases}$$

e usando o mesmo argumento anterior concluímos também que existem $B,C\in\mathbb{Z}$ tais que,

$$\begin{cases} x+y=B^p \\ x+z=C^p. \end{cases}$$

Definimos agora $q=2p+1$, com q primo , vale o pequeno teorema de Fermat, ou seja se $\alpha\in\mathbb{Z}$ e $q\nmid\alpha$, então $\alpha^{q-1}\equiv 1 mod q$ implica que $\alpha^{q-1}\equiv 0 mod q$ de modo que $\left(\alpha^{\frac{q-1}{2}}-1\right)\left(\alpha^{\frac{q+1}{2}}+1\right)\equiv 0 mod q$ então, $(\alpha^p-1)(\alpha^p+1)\equiv 0 mod q$ logo, $\alpha^p\equiv 1 mod q$ ou $\alpha^p\equiv -1 mod q$. E uma outra demonstração do resultado acima pode ser encontrada no Teorema 1.19.
Em particular , dado que $x^p+y^p+z^p=0$ de modo que $x^p+y^p+z^p\equiv 0 mod q$ então $(\pm1)+(\pm1)+(\pm1)\equiv 0 mod q$, o que não é possivel, pois o lado esquerdo da última equação é ±1 ou ±3 e $q>5$, se $q\nmid xyz$, assim $q|xyz$ e podemos sem perda de generalidade que $q|x$, como,

$$\begin{cases} y+z=A^p \\ x+y=B^p \\ x+z=C^p. \end{cases}$$

então $B^p+C^p-A^p=2x$ e $q|x$, logo $B^p+C^p-A^p\equiv 0 mod q$ e argumento análogo de $x^p+y^p+z^p\equiv 0 mod q$, concluimos que $q|ABC$, como $x+y=B^p$, se $q|B$, teriamos $x+y\equiv y\equiv 0 mod q$ e q seria assim fator comum a x e a y, logo também a z contradizendo a escolha inicial. Similarmente $q\nmid C$ ou seja, $q\nmid BC$, assim, $q|ABC$, $q\nmid BC$ então $q|A$, como $A^p=y+z$, teremos $y\equiv -z mod q$, pois $A^p\equiv 0 mod q$ e $T^p\equiv z^{p-1}+z^{p-1}+z^{p-1}+z^{p-1}+\ldots+z^{p-1}\equiv pz^{p-1} mod q$, se $q|T$ então q seria

fator comum a A e a T o que já vimos não ser possível, logo $T^p \equiv \pm 1 mod q$ logo, $pz^{p-1} \equiv \pm 1 mod q$, acontece que $q = 2p + 1$ implicando que $2p \equiv -1 mod q$ de modo que, $2pz^{p-1} \equiv (-1) z^{p-1} \equiv \pm 2 mod q$ então, $z^{p-1} \equiv \pm 2 mod q$, mas se $q|x$ daí, temos $q \nmid z$ por que do contrário q seria fator comum a x, y e z, mas $p-1$ é par e $x + z = C^p$ então, $z \equiv C^p mod q$, pois $q|x$, logo $z^{p-1} \equiv \pm 2 mod q$ dai segue, $(C^p)^{p-1} \equiv \pm 2 mod q$ então, $(\pm 1)^{p-1} \equiv \pm 2 mod q$ implacando em $1 \equiv \pm 2 mod q$ o que não é possível. ■

Corolário 3.3 *A equação $x^3 + y^3 = z^3$ não possui solução diofantina, não triviais, na qual $3 \nmid xyz$.*

Para finalizar nossas considerações sobre as equações de Fermat, vamos utilizar as propriedades de $\mathbb{Z}[w]$, para mostrar que não há soluções diofantinas para a equação $x^3 + y^3 = z^3$ e em particular não haverá solução para $x^n + y^n = z^n$ se $3|n$. Relembrando, $\mathbb{Z}[w]$ é domínio de fatoração única, cujas unidades são ± 1, $\pm w$ e $\pm w^2$, denotando $\rho = 1 - w$, teremos $\rho^2 = 1 - 2w + w^2$ e como $w^2 = -(1 + w)$, teremos $\rho^2 = 1 - 2w - 1 - w = -3w$, logo $(\rho^2) = (3w) = (3)$ que são ideais, mais ainda, lembrando que $\lambda(x + wy) = x^2 + y^2 - xy$, onde $\lambda : \mathbb{Z}[w] \to \mathbb{Z}^+$ é tal que, dados $\alpha, \beta \in \mathbb{Z}[w]$, $\beta \neq 0$, existem $q, r \in \mathbb{Z}[w]$, tal que $\alpha = q\beta + r$ e $r = 0$ ou $\lambda(r) < \lambda(\beta)$, temos $\lambda(\rho) = 1^2 + 1^2 - (1)(-1) = 3$, se $\lambda(\rho) = \lambda(z)\lambda(w)$, com $\lambda(\rho) = 3$ primo em $\mathbb{Z}$, então z ou w são unidades em $\mathbb{Z}[w]$, pois $\lambda(z)$ ou $\lambda(w)$ é igual a ± 1 e, portanto ρ é irredutível em $\mathbb{Z}[w]$, mais ainda, dado $x + w \in \mathbb{Z}[w]$, teremos $x + yw = (x - y)\rho y$ e $x + yw \equiv (x - y) mod \rho$, como $\lambda(\rho) = 3$ e $x, y \in \mathbb{Z}$, segue que $x + yw \equiv (\pm 1) mod \rho$ ou $x + yw \equiv 0 mod \rho$.

Lema 3.3 *A equação $x^3 + y^3 = uz^3$ não possui solução $x, y, z \in \mathbb{Z}[w]$, na qual $\rho|xyz$, (u é unidade qualquer em $z \in \mathbb{Z}[w]$), em particular $x^3 + y^3 = z^3$ não possui solução diofantina, não triviais em $\mathbb{Z}[w]$ o qual $\rho \nmid xyz$.*

Demonstração: Como ρ é irredutível, $\rho \nmid xyz$ logo, $\rho \nmid x$, $\rho \nmid y$ e $\rho|z$, assim,

$$\begin{cases} x \equiv \pm 1 \, (mod \rho) \\ y \equiv \pm 1 \, (mod \rho) \\ z \equiv \pm 1 \, (mod \rho) \end{cases}$$

sem perda de generalidade, suponhamos que $x \equiv \pm 1\,(mod\rho)$ então, $x = 1 + \tau\rho$, de modo que,

$x^3 - 1 = (x-1)(x-w)(x-w^2)$

$x^3 - 1 = \tau\rho(1 - w + \tau\rho)(1 - w^2 + \tau\rho)$

$x^3 - 1 = \tau\rho(\rho + \tau\rho)((1+w)\rho + \tau\rho)$

$x^3 - 1 = [\rho^3(1+\tau)(\tau - w^2)]$

como $w^2 \equiv mod\rho$ segue $x^3 - 1 \equiv 0 mod\rho^4$ então $x^3 \equiv 1 mod\rho^4$, se $x \equiv -1 mod\rho$ usando esse raciocíno conclui-se que $x^3 \equiv -1 mod\rho^4$, donde $x^3 + y^3 = uz^3$ que implica $x^3 + y^3 \equiv uz^3 \equiv mod\rho^4$ daí temos, $(\pm 1) + (\pm 1) \equiv u(\pm 1)\, mod\rho^4$ o que não é possível.

■

Lema 3.4 *Se a equação $x^3 + y^3 = uz^3$, $x, y, z \in \mathbb{Z}[w]$ e $\rho \nmid xy$ e $\rho | z$ então $\rho^2 | z$.*

Demonstração: Sabemos que $x^3 + y^3 = uz^3$, como $\rho \nmid x$, $\rho \nmid y$, temos,

$$\begin{cases} x \equiv \pm 1\,(mod\rho^4) \\ y \equiv \pm 1\,(mod\rho^4) \end{cases}$$

De modo que, $(\pm 1) + (\pm 1) \equiv uz^3 mod\rho^4$ então $uz^3 \equiv 0 mod\rho^4$ ou $uz^3 \equiv \pm 2 mod\rho^4$. Se $uz^3 \equiv \pm 2 mod\rho^4$ e se $\rho^2 \nmid z$, teriamos $z = \rho\beta$, $\rho \nmid \beta$ e $uz^3 \pm 2 = u\rho^3\beta^3 \pm 2 = \tau\rho^4$ logo, $\rho | 2$ o que não é verdade, de modo que $uz^3 \equiv 0 mod\rho^4$. Escrevendo $z = \rho^3\beta^3$, teremos $uz^3 = \tau\rho^4$ dai segue, $u\rho^3\beta^3 = \tau\rho^4$ logo, $u\beta^3 = \tau\rho$ logo $\rho | \beta^3$ implica $\rho | \beta$ temos que, $\rho^2 | z$. ■

Lema 3.5 *Se a equação $x^3 + y^3 = uz^3$, possui solução não triviais, com $mdc(x,y) = 1$, $\rho \nmid xy$ e $ord_\rho z \geq 2$. Então existem $x_1, y_1, z_1 \in \mathbb{Z}[w]$ e $u_1 \in \mathbb{Z}[w]$ unidade, tais que $\rho \nmid x_1 y_1$, $ord_\rho z_1 = ord_\rho z - 1$ e $x_1^3 + y_1^3 = u_1 z_1^3$.*

Demonstração: Sabemos que,

$$x^3 + y^3 = (x+y)(x+wy)(x+w^2y) = uz^3, \qquad \textbf{(1)}$$

como $ord_\rho z \geq 2$ então, $ord_\rho uz^3 \geq 6$ segue que algumas das parcelas de **(1)** é tal que ρ^2 aparece como fator definindo y para wy ou w^2y se necessário, podemos supor, sem perda de generalidade que tal fator ρ^2 aparece em $x + y$. Observe que $ord_\rho(x+y) \geq 2$ então, $ord_\rho(x+wy) = ord_\rho((x+y) - (1-w)y) = ord_\rho((x+y) - \rho y)$, como

$\rho \nmid y$ segue que $ord_\rho(x+wy) = 1$, similarmente $ord_\rho(x+w^2y) = 1$, portanto $ord_\rho(x+y) + ord_\rho(x+wy) + ord_\rho(x+w^2y) = 3ord_\rho z$, implica que $3ord_\rho z - 2 = ord_\rho(x+y)$.
Seja então π irredutível em $\mathbb{Z}[w]$, se $\pi|(x+y)$ e $\pi|(x+wy)$, segueria que $\pi|(1-w)y$, como $\rho = 1-w$, teriamos $\pi|\rho y$, assumindo $(\pi) \neq (\rho)$, implicaria que $\pi|y$ portanto, como $\pi|(x+y)$, teriamos que $\pi|x$ o que viola, pois o mdc$(x,y) = 1$, donde mdc$(x+y, x+wy) = \rho$, análogamente o mdc$(x+wy, x+w^2y) = (x+y, x+w^2y) = \rho$. Pela fatoração única em $\mathbb{Z}[w]$, temos portanto,

$$x+y = u_1\alpha^3\rho^T,\ T = 3ord_\rho z - 2,\ \rho \nmid \alpha \qquad \textbf{(2)}$$
$$x+wy = u_2\beta^3\rho,\ \rho \nmid \beta \qquad \textbf{(3)}$$
$$x+w^2y = u_3\delta^3\rho,\ \rho \nmid \delta \qquad \textbf{(4)}$$

onde u_1, u_2 e u_3 são unidades e $mdc(\alpha,\beta) = mdc(\alpha,\delta) = mdc(\beta,\delta) = 1$, multiplicando a equação **(2)** por w e a equação **(3)** por w^2 e somando-as, obtemos,
$u_1\alpha^3\rho^T + wu_2\beta^3\rho + w^2u_3\delta^3\rho = 0$
$u_1\alpha^3\rho^{T-1} + wu_2\beta^3 + w^2u_3\delta^3 = 0$
ora, $T-1 = 3ord_\rho z - 3 = 3(ord_\rho z - 1)$ e podemos fazer $x_1 = \beta$, $y_1 = \delta$ e $z_1 = \alpha\delta^{ord_\rho z - 1}$, obtemos, assim,
$u_1z_1^3 + wu_2x_1^3 + w^2u_3y_1^3 = 0$
dividindo pela unidade wu_2, podemos reescrever a equação, assim,
$x_1^3 + \epsilon_1y_1^3 + \epsilon_2z_1^3 = 0$, com ϵ_1 e ϵ_2 unidades.
Observe que,
$ord_\rho z_1 \geq 2 \Rightarrow x_1^3 + \epsilon_1y_1^3 \equiv \epsilon_2z_1^3 \equiv 0 mod\rho^2 \Rightarrow (\pm1)^3 + \epsilon_1(\pm1) \equiv 0 mod\rho^2$, donde $\epsilon_1 = (\pm1)$, podemos então, após renomear as variáveis, se necessário reescrever $x_1^3 + y_1^3 = \epsilon z_1^3$, como $\rho \nmid xy$, ϵ unidade e $ord_\rho z_1 = ord_\rho z - 1$. ■

Teorema 3.5 *Não exite solução de $x^3+y^3 = uz^3$ em $\mathbb{Z}[w]$ com unidade em $\mathbb{Z}[w]$ e $xyz \neq 0$.*

Demonstração: Pelo Lema 3.3, não há solução de $x^3+y^3 = uz^3$ em $\mathbb{Z}[w]$ se $\rho \nmid xyz$, logo se houvesse solução de $x^3+y^3 = uz^3$ em $\mathbb{Z}[w]$, teriamos $\rho|xyz$, cancelando fatores em comum, se necessário em x, y em $\mathbb{Z}$, podemos supor que $\rho|z$ e $\rho \nmid xy$. Pelo Lema

3.4, se há solução de $x^3 + y^3 = uz^3$, com $\rho \nmid xy$ e $\rho | z$, então há solução com $\rho^2 | z$ e pelo Lema 3.5, isso implica numa solução $x_1^3 + y_1^3 = \epsilon z_1^3$, com $ord_\rho z_1 = ord_\rho z - 1 \geq 1$ o que viola, obtendo assim, novas soluções da equação original por repetidas aplicações dos Lema 3.4 e Lema 3.5 o que não é obviamente possível. ■

Corolário 3.4 *(Equação de Fermat, $n = 3$) Não existem soluções de $x^3 + y^3 = z^3$ com $x, y, z \in \mathbb{Z}$ e $xyz \neq 0$.*

Demonstração: Como $\mathbb{Z} \subset \mathbb{Z}[w]$ e 1 unidade em $\mathbb{Z}[w]$, isto implicaria numa solução para $x^3 + y^3 = uz^3$ em $\mathbb{Z}[w]$, com $xyz \neq 0$ e que não é possível. ■

Capítulo 4

SOMA DE QUADRADOS

Em 1770, Waring publicou um artigo na Meditationes Algebraical no qual é proposto o seguinte problema "Existe, para um k fixo, algum $s = s(k)$ tal que $n = x_1^k + x_2^k + x_3^k + \ldots + x_s^k$ é solúvel para todo n?" Neste mesmo trabalho, Waring conjecturou a resposta afirmativa, para alguns valores de k, enunciando, sem demonstração que todo inteiro é a soma de quatro quadrados, de nove cubos e de dezenove biquadrados (muitos dos quais podem ser nulos), 100 anos mais tarde, Hibert provou a veracidade destas afirmações e diversas outras têm sido apresentadas desde então.

Neste capítulo, provaremos os teoremas relativos ao caso $k = 2$ e $s = 2$ (neste caso, caracterizaremos quais números inteiros são soma de dois quadrados) e $s = 4$, (mostraremos que qualquer número inteiro é soma de quatro quadrados). Outros casos de k e s são, igualmente, bem mais difíceis que estes e exigem uma ferramenta matemática mais elaborada. Em um apêndice a este capítulo, forneceremos para k fixo, cotas para o menor s, para o qual a afirmação de Warimg é verdadeira (este número será denotado por $g(k)$ e cotas para o menor s para o qual a afirmação é falsa apenas um número finito de cotas, (tal número será denotado por $G(k)$).

Ainda neste capítulo, serão demonstrados alguns resultados interessantes sobre a quantidade de representações de um número como soma de quadrados.

4.1 Soma de dois quadrados

Seja p primo ímpar, então $p \equiv 1\,(mod\ 4)$ ou $p \equiv 3\,(mod\ 4)$, é fácil ver que o produto de primos que são congruentes a um módulo quatro é ainda congruente a um módulo quatro. A proposição seguinte fornece a primeira diferênça significante entre estas duas classes de primos.

Proposição 4.1 *Para p primo a congruência $x^2 \equiv -1\,(mod\ p)$, tem solução se, e somente se, $p = 2$ ou $p \equiv 1\,(mod\ 4)$.*

Demonstração: Fica claro que para $x = 1$, temos uma solução se $p = 2$, precisamos construir uma solução no caso de $p \equiv 1 mod 4$, para um p primo ímpar, podemos recorrer ao teorema de de Wilson, maiores detalhes ver Teorema 1.18, onde podemos escrevê-lo da seguinte forma,
$\left(1.2.3...j...\dfrac{p-1}{2}\right)\left(\dfrac{p+1}{2}...\,(p-j)\,...\,(p-2)\,(p-1)\right) \equiv -1\,(mod p)$

Observamos que o produto $(p-1)!$, está dividido em duas partes, cada uma com o mesmo número de fatores. Podemos reescrever esse produto formando pares, uma vez que para cada fator j na primeira parte temos o fator $(p-j)$ na segunda, então o teorema de Wilson pode ser escrito assim,
$\prod_{j=1}^{(p-1)/2} j\,(p-j) \equiv -1\,(mod p)$, como $j\,(p-j) \equiv -j^2\,(p-j)\,(mod p)$, temos,
$-1 \equiv \prod_{j=1}^{(p-1)/2} (-j)^2 \equiv (-1)^{(p-1)/2}\left(\prod_{j=1}^{(p-1)/2} j\right)^2 (mod p)$, mas $p \equiv 1\,(mod\ 4)$, $(p-1)/2$ é par e, portanto,
$x = \prod_{j=1}^{(p-1)/2} j = \left(\dfrac{p-1}{2}\right)!$, e é uma solução de $x^2 \equiv -1\,(mod\ p)$.

Suponhamos agora que a congruência $x^2 \equiv -1 mod p$ tenha solução e que $p > 2$, elevando ambos os membros à potência $(p-1)/2$, obtêm-se,
$(x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2}\,(mod p)$, como $(x^2)^{(p-1)/2} \equiv x^{(p-1)}\,(mod p)$, pelo Teorema 1.19 (observe que $p \nmid x$ pois $x^2 \equiv -1\,(mod p)$), temos que $(-1)^{(p-1)/2} \equiv 1\,(mod p)$, logo $(p-1)/2$ é par, ou seja $p = 2$ ou $p \equiv 1\,(mod\ 4)$. ■

Exemplo 4.1 *Represente se for possível os números* 13 *e* 7 *como soma de dois quadrados.*

Resolução:

- $13 \equiv 1\,(mod\ 4)$, logo $13 = 3^2 + 2^2$
- $7 \not\equiv 1\,(mod\ 4)$, logo não podemos escerver 7, como soma de dois quadrados.

Teorema 4.1 *Seja* $n \in \mathbb{Z}$, n *é soma de dois quadrados se, e somente se,* $n = n_1^2.n_2$, *onde* $mdc\,(n_1, n_2) = 1$ *e a decomposição em fatores primos de* n_2 *é composta apenas de primos congruentes a um módulo quatro e potências de dois.*

Demonstração: Inicialmente se $p \equiv 3mod4$, afirmaremos $x^2 + y^2 = n$ não possui solução se $ord_p(n)$ é ímpar, com efeito, se houvesse solução de $x^2 + y^2 = n$, então suponha $mdc\,(x, y) = d$, logo podemos escrever $x = x_1 d$ e $y = y_1 d$, obtendo assim, $x_1^2 + y_1^2 = \left(\frac{n}{d^2}\right)$, solução de $x_1^2 + y_1^2 = n_1$, fazendo $n_1 = \left(\frac{n}{d^2}\right)$, com $mdc\,(x_1, y_2) = 1$ e $p|n_1$, pois $ord_p\,(n)$ é ímpar e $ord_p\,(d^2) = 2ord_p\,(d)$ é par, observe que $p \nmid x_1$ e $p \nmid y_1$.

Sabemos que a congruência linear $ax \equiv bmodm$ tem solução se, e somente se, $mdc\,(a, m) = 1$, logo seja ℓ a solução da congruência $\ell x_1 \equiv y_1 modp$ implica $\ell^2 x_1^2 \equiv y_1^2 modp$ implica $x_1^2 + \ell^2 x_1^2 \equiv x_1^2 + y_1^2 modp$ logo $x_1^2\,(1 + \ell^2) \equiv x_1^2 + y_1^2 modp$, mas $p|x_1^2 + y_1^2$ então, $x_1^2 + y_1^2 \equiv 0modp$ donde $x_1^2\,(1 + \ell^2) \equiv 0modp$, como $p \nmid x_1^2$, segue que $p|\,(1 + \ell^2)$ daí temos, $1 + \ell^2 \equiv 0modp$ segue, $\ell^2 \equiv -1modp$ o que contradiz a Proposição 4.1, se $p \equiv 3mod4$. Assim, se $x^2 + y^2 = n$ possui solução, necessariamente, os primos congruentes a três módulo quatro na decomposição de n aparecem com potências pares e podemos escrever $n = n_1^2.n_2$, com $mdc\,(n_1, n_2) = 1$ e todos os primos ímpares em n_2 congruentes a um módulo quatro, agora se $p \equiv 1mod4$, note que existe solução de $\ell^2 \equiv 1modp$, seja $n_1 = \lfloor\sqrt{p}\rfloor$ e escolhendo $a, b \in \mathbb{Z}$ tais que $o < b < n_1$ e $\left|\frac{\ell}{p} + \frac{a}{b}\right| < \frac{1}{bn_1}$, escrevendo $c = \ell b + pa$, logo,

$|c| = \left|bp\left(\frac{\ell}{p} + \frac{a}{b}\right)\right| = |bp|\left|\frac{\ell}{p} + \frac{a}{b}\right| < |bp|\frac{1}{bn_1} \leq \sqrt{p}$ com $0 < c^2 < p$ então, $0 < b^2 + c^2 < 2p$ mas, $c \equiv \ell modp$, donde $b^2 + c^2 = b^2 + \ell^2 b^2 \equiv b^2\,(\ell + 1) \equiv 0modp$, logo $p|b^2 + c^2$ e $0 < b^2 + c^2 < 2p$, donde $b^2 + c^2 = p$ ou seja, se $p \equiv 1mod4$, então $x^2 + y^2 = p$ solução da identidade,

$(x_1^2 + y_1^2)\,(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2$, segue que se $n = n_1^2.n_2$ onde

todos os fatores primos ímpares de n_2 são congruentes a um módulo quatro, então $x^2 + y^2 = n$, possui solução. (Note que $2 = 1^2 + 1^2$ e que $n_1^2 = 0^2 + n_1^2$) o que prova este teorema. ■

Exemplo 4.2 *Represente se for possível os números* $7^2.13$ *e* 7.13 *como soma de dois quadrados.*

Resolução:

- $7^2.13 = 637 = 21^2 + 14^2$
- $7.13 = 91$, logo não pode ser escrito como soma de dois quadrados.

4.2 Soma de quatro quadrados

Lema 4.1 *Se* p *é primo ímpar (sempre assumindo primos positivos) então existem* $m, x, y \in \mathbb{Z}$, *com* $0 < m < p$ *tais que* $1 + x^2 + y^2$.

Demonstração: Seja $S = \{x^2 : 0 \leq x \leq 1/2\,(p-1)\,, x \in \mathbb{Z}\}$ e $T = \{y^2 : 0 \leq y \leq 1/2\,(p-1)\,, y \in \mathbb{Z}\}$, dois elementos quaisquer de S são incongruentes módulo p, pois $x_1^2 \equiv x_2^2\,(mod p)$ então $p|\,(x_1^2 - x_2^2)$, ou seja $p|\,(x_1 - x_2)\,(x_1 + x_2)$ implica $x_1 \equiv x_2\,(mod p)$, $x_1 \equiv -x_2\,(mod p)$, como $0 \leq x_1, x_2 \leq 1/2\,(p-1)$, segue que nenhum dos casos é possível. De forma análoga, também os elementos de T são incongruentes módulo p. S e T possuem, em conjunto, $p+1$ elementos em S e em T que são "o mesmo módulo p", ou seja, existem $0 \leq x, y \leq 1/2\,(p-1)$ tal que $x^2 \equiv -\,(1 + y^2)\,(mod p) \Rightarrow p|\,(1 + x^2 + y^2)$ de modo que existe $m \in \mathbb{Z}$, tal que $1+x^2+y^2 = mp$ como $x^2 \leq 1/4\,(p-1)^2$ e $y^2 \leq 1/4\,(p-1)^2$, segue que $1+x^2+y^2 < p^2$ então, $m < p$. ■

Proposição 4.2 *Todo primo é soma de quatro quadrados.*

Demonstração: Pelo Lema 4.1, dado p primo ímpar (se $p = 2$, temos $2 = 1^2 + 1^2 + 0^2 + 0^2$ e a proposição é verdadeira), existem $m < p$ e $x, y \in \mathbb{Z}$, tal que $x^2+y^2+1 = mp$, em particular mp é a soma de quatro quadrados. Seja então m o menor inteiro para o qual mp é soma de quatro quadrados, isto é, $mp = x^2 + y^2 + z^2 + w^2$, se $m = 1$, então

nada temos a demonstrar, logo podemos assumir que $m > 1$.

Se m for par, então os inteiros x, y, z, w são todos pares ou x, y, z, w são todos ímpares ou exatamente dois deles (podemos assumir z e w) são ímpares, em qualquer caso, podemos escrever a identidade,

$\left(\frac{1}{2}m\right) p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2$.

como nem todos x, y, z, w podem ser múltiplos de p, segue que a equação acima escreve um múltiplo, menor que m de p como soma de quatro quadrados o que contradiz a escolha de m, logo m é ímpar. Se todos x, y, z e w fossem múltiplos de m, teriamos, $mp = x^2 + y^2 + z^2 + w^2 = m^2 k$ implica $p = mk$, logo $m|p$, o que não é possível pois $m < 1$, sendo $x = b_1 m + x_1$, podemos então fazer,

$x_1 = x - b_1 m$

$x_2 = x - b_2 m$

$x_3 = x - b_3 m$

$x_4 = x - b_4 m$

onde os b_i são os quocientes da divisão por m, escolhendo $|x_i| < \frac{1}{2}m$, assim,

$0 < x_1^2 + x_2^2 + x_3^2 + x_4^2 < 4\left(\frac{1}{2}m\right)^2 = m^2$, observe que,

$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0\,(mod\, m)$, donde $x_1^2 + x_2^2 + x_3^2 + x_4^2 = km$, com $0 < k < m$. Mas, $(x_1^2 + x_2^2 + x_3^2 + x_4^2)\,(x^2 + y^2 + z^2 + w^2)$, temos,

$m^2 kp = z_1^2 + z_2^2 + z_3^2 + z_4^2$ e como $Z_i = \sum x_i\,(x_i - b_i m) \equiv 0\,(mod\, m)$, teremos $Z_i = mT_i \Rightarrow kp = T_1^2 + T_2^2 + T_3^2 + T_4^2$ e dado $k < m$, isto contradiz a escolha de m. ■

Exemplo 4.3 *Represente se for possível os números* 7 *e* 5 *como soma de quatro quadrados.*

Resolução:

- $7 = 2^2 + 1^2 + 1^2 + 1^2$
- $5 = 2^2 + 1^2 + 0^2 + 0^2$.

Teorema 4.2 *Todo inteiro positivo é soma de quatro quadrados.*

Demonstração: $(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2$

■

Exemplo 4.4 *Represente se for possível os números* 7, 5 *e* 35 *como soma de quatro quadrados.*

Resolução:

- $7 = 2^2 + 1^2 + 1^2 + 1^2$
- $5 = 2^2 + 1^2 + 0^2 + 0^2$
- $7.5 = 35 = 4^2 + 3^2 + 3^2 + 1^2$

Logo podemos concluir que todo inteiro positivo pode ser representado como soma de quadrados, haja vista que todo número composto pode ser escrito como produto de primos.

Capítulo 5

EQUAÇÕES DIOFANTINAS CLÁSSICAS E APLICAÇÕES

5.1 Aplicações

Aplicação: 01

ELEIÇÕES 2008 - A eleição para o cargo de diretor do CEFET-MA, o fato inusitado que aconteceu foi que o professor Alexandre era amigo dos dois principais candidatos, professor Zé Costa da chapa 100 e o professor Agenor da chapa 300, a eleição se aproximava e Alexandre não se decidia em quem votar, foi quando o mesmo teve a idéia de mandar uma mensagem criptografada para o gabinete de Zé Costa com o seguinte conteúdo, 380439422853269630651721 9, esta sequência numérica revelaria o seu candidato, apenas um funcionário tinha como desvendar esse código uma vez que o professor usou recursos da Teoria dos Números e criptografia RSA, devido a sua segurança e querendo total sigilo sobre a mensagem enviada. Mostraremos os procedimentos adotados pelo professor.

Num primeiro momento, iremos identificar a chave pública, um número n inteiro positivo, tal que $n = p.q$, onde $p = 23$ e $q = 31$ primos, logo $n = 713$ e $\alpha = 7$, as funções de codificação $D(b_i) \equiv (b_i)^{\alpha}\,(mod\ n)$ e de decodificação $D(c_i) \equiv (c_i)^{d}\,(mod\ n)$ e i que representa o bloco a ser decodificado. A escolha do α é feita aleatória em $\mathbb{Z}_{\phi(n)}$,

isto é, α é um inteiro entre 1 e $\phi(n)$ ver Teorema 1.20, que seja relativamente coprimo com $\phi(n)$ que é a função Euler.

Para calcular o valor de d, ele precisou recorrer ao Algoritmo Euclidiano Estendido, ver Exemplo 1.2, uma vez que o valor d é o inverso de $\alpha\,(mod\ \phi(n))$.

Neste caso $\alpha = 7$ e $\phi(713) = (p-1).(q-1) = (23-1).(31-1) = 660$ e $mdc(7, 660) = 1$, logo,
$1 = 660.(-3) + 7.(283) \Rightarrow 283.7 \equiv 7.283 \equiv 1\,(mod\ 660)$, então $d = 283$.

Partiremos para o segundo momento, quando o professor envia a mensagem criptografada 380439422853269630651721 9 e as informações contidas no par (n, d), após essas informações o funcionário segue os procedimentos de decodificação, dividindo essa sequência em blocos c_i de modo que $c_i < n$. Assim,

$$D(c_i) \equiv (c_i)^d\,(mod\ n) \text{ ou seja, } D(c_i) \equiv (c_i)^{283}\,(mod\ 713)$$

Blocos a serem decodificados								
c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9
380	439	42	28	532	696	306	517	219

Seguindo com este procedimento agora com os valores dos blocos definidos aleatoriamente, mas obdecendo os procedimento da criptografia RSA, onde os valores correspondentes aos blocos precisam serem menores que o valor de n, aplicaremos a função de decodificação para identificar a mensagem passada pelo professor.

Decodificação do bloco $c_1 = 308$:
$D(c_i) \equiv (c_i)^d\,(mod\ n)$
$D(380) \equiv (380)^{283}\,(mod\ 713)$
$D(380) \equiv (380)^{283} \equiv (380)^{256+16+8+2+1}\,(mod\ 713)$
$D(380) \equiv (380)^{283} \equiv (380)^{256}(380)^{16}(380)^{8}(380)^{2}(380)^{1}\,(mod\ 713)$
$D(380) \equiv (380)^{283} \equiv ((380)^2)^{128}\,((380)^2)^{8}\,((380)^2)^{4}\,(380)^2(380)\,(mod\ 713)$
$D(380) \equiv (380)^{283} \equiv ((374)^2)^{64}\,((374)^2)^{4}\,((374)^2)^{2}\,(374)(380)\,(mod\ 713)$

$D(380) \equiv (380)^{283} \equiv ((128)^2)^{32}\,((128)^2)^2\,(128)^2(233)\,(mod\ 713)$

$D(380) \equiv (380)^{283} \equiv ((698)^2)^{16}\,(698)^2(698)(233)\,(mod\ 713)$

$D(380) \equiv (380)^{283} \equiv 698\,(mod\ 713)$

Logo, o bloco decodificado é $b_1 = 698$.

Decodificação do bloco $c_2 = 439$:

$D(c_i) \equiv (c_i)^d\,(mod\ n)$

$D(439) \equiv (439)^{283}\,(mod\ 713)$

$D(439) \equiv (439)^{283} \equiv (439)^{256+16+8+2+1}\,(mod\ 713)$

$D(439) \equiv (439)^{283} \equiv (439)^{256}(439)^{16}(439)^8(439)^2(439)^1\,(mod\ 713)$

$D(439) \equiv (439)^{283} \equiv ((439)^2)^{128}\,((439)^2)^8\,((439)^2)^4\,(439)^2(439)\,(mod\ 713)$

$D(439) \equiv (439)^{283} \equiv ((211)^2)^{64}\,((211)^2)^4\,((211)^2)^2\,(211)(439)\,(mod\ 713)$

$D(439) \equiv (439)^{283} \equiv ((315)^2)^{32}\,((315)^2)^2\,(315)^2(652)\,(mod\ 713)$

$D(439) \equiv (439)^{283} \equiv ((118)^2)^{16}\,(118)^2(118)(652)\,(mod\ 713)$

$D(439) \equiv (439)^{283} \equiv ((377)^2)^8\,(377)(645)\,(mod\ 713)$

$D(439) \equiv (439)^{283} \equiv 532\,(mod\ 713)$

Logo, o bloco decodificado é $b_2 = 532$.

Decodificação do bloco $c_3 = 42$:

$D(c_i) \equiv (c_i)^d\,(mod\ n)$

$D(42) \equiv (42)^{283}\,(mod\ 713)$

$D(42) \equiv (42)^{283} \equiv (42)^{256+16+8+2+1}\,(mod\ 713)$

$D(42) \equiv (42)^{283} \equiv (42)^{256}(42)^{16}(42)^8(42)^2(42)^1\,(mod\ 713)$

$D(42) \equiv (42)^{283} \equiv ((42)^2)^{128}\,((42)^2)^8\,((42)^2)^4\,(42)^2(42)\,(mod\ 713)$

$D(42) \equiv (42)^{283} \equiv ((338)^2)^{64}\,((338)^2)^4\,((338)^2)^2\,(338)(42)\,(mod\ 713)$

$D(42) \equiv (42)^{283} \equiv ((164)^2)^{32}\,((164)^2)^2\,(164)^2(649)\,(mod\ 713)$

$D(42) \equiv (42)^{283} \equiv ((515)^2)^{16}\,(515)^2(515)(649)\,(mod\ 713)$

$D(42) \equiv (42)^{283} \equiv ((702)^2)^8\,(702)(551)\,(mod\ 713)$

$D(42) \equiv (42)^{283} \equiv 83\,(mod\ 713)$

Logo, o bloco decodificado é $b_3 = 83$.

Decodificação do bloco $c_4 = 28$:

$D(c_i) \equiv (c_i)^d \, (mod \ n)$

$D(28) \equiv (28)^{283} \, (mod \ 713)$

$D(28) \equiv (28)^{283} \equiv (28)^{256+16+8+2+1} \, (mod \ 713)$

$D(28) \equiv (28)^{283} \equiv (28)^{256}(28)^{16}(28)^{8}(28)^{2}(28)^{1} \, (mod \ 713)$

$D(28) \equiv (28)^{283} \equiv ((28)^2)^{128} \, ((28)^2)^{8} \, ((28)^2)^{4} \, (28)^2(28) \, (mod \ 713)$

$D(28) \equiv (28)^{283} \equiv ((71)^2)^{64} \, ((71)^2)^{4} \, ((71)^2)^{2} \, (71)(28) \, (mod \ 713)$

$D(28) \equiv (28)^{283} \equiv ((50)^2)^{32} \, ((50)^2)^{2} \, (50)^2(562) \, (mod \ 713)$

$D(28) \equiv (28)^{283} \equiv ((361)^2)^{16} \, (361)^2(361)(562) \, (mod \ 713)$

$D(28) \equiv (28)^{283} \equiv ((555)^2)^{8} \, (555)(390) \, (mod \ 713)$

$D(28) \equiv (28)^{283} \equiv 7 \, (mod \ 713)$

Logo, o bloco decodificado é $b_4 = 7$.

Decodificação do bloco $c_5 = 532$:

$D(c_i) \equiv (c_i)^d \, (mod \ n)$

$D(532) \equiv (532)^{283} \, (mod \ 713)$

$D(532) \equiv (532)^{283} \equiv (532)^{256+16+8+2+1} \, (mod \ 713)$

$D(532) \equiv (532)^{283} \equiv (532)^{256}(532)^{16}(532)^{8}(532)^{2}(532)^{1} \, (mod \ 713)$

$D(532) \equiv (532)^{283} \equiv ((532)^2)^{128} \, ((532)^2)^{8} \, ((532)^2)^{4} \, (532)^2(532) \, (mod \ 713)$

$D(532) \equiv (532)^{283} \equiv ((676)^2)^{64} \, ((676)^2)^{4} \, ((676)^2)^{2} \, (676)(532) \, (mod \ 713)$

$D(532) \equiv (532)^{283} \equiv ((656)^2)^{32} \, ((656)^2)^{2} \, (656)^2(280) \, (mod \ 713)$

$D(532) \equiv (532)^{283} \equiv ((397)^2)^{16} \, (397)^2(397)(280) \, (mod \ 713)$

$D(532) \equiv (532)^{283} \equiv ((36)^2)^{8} \, (36)(645) \, (mod \ 713)$

$D(532) \equiv (532)^{283} \equiv 98 \, (mod \ 713)$

Logo, o bloco decodificado é $b_5 = 98$.

Decodificação do bloco $c_6 = 696$:

$D(c_i) \equiv (c_i)^d \, (mod \ n)$

$D(696) \equiv (696)^{283} \, (mod \ 713)$

$D(696) \equiv (696)^{283} \equiv (696)^{256+16+8+2+1} \, (mod \ 713)$

$D(696) \equiv (696)^{283} \equiv (696)^{256}(696)^{16}(696)^{8}(696)^{2}(696)^{1} \, (mod \ 713)$

$D(696) \equiv (696)^{283} \equiv ((696)^2)^{128} \, ((696)^2)^{8} \, ((696)^2)^{4} \, (696)^2(696) \, (mod \ 713)$

$D(696) \equiv (696)^{283} \equiv ((289)^2)^{64} \, ((289)^2)^{4} \, ((289)^2)^{2} \, (289)(696) \, (mod \ 713)$

$D(696) \equiv (696)^{283} \equiv ((100)^2)^{32}\,((100)^2)^2\,(100)^2(78)\,(mod\ 713)$

$D(696) \equiv (696)^{283} \equiv ((18)^2)^{16}\,(18)^2(18)(78)\,(mod\ 713)$

$D(696) \equiv (696)^{283} \equiv ((324)^2)^{8}\,(324)(691)\,(mod\ 713)$

$D(696) \equiv (696)^{283} \equiv 524\,(mod\ 713)$

Logo, o bloco decodificado é $b_6 = 524$.

Decodificação do bloco $c_7 = 306$:

$D(c_i) \equiv (c_i)^d\,(mod\ n)$

$D(306) \equiv (306)^{283}\,(mod\ 713)$

$D(306) \equiv (306)^{283} \equiv (306)^{256+16+8+2+1}\,(mod\ 713)$

$D(306) \equiv (306)^{283} \equiv (306)^{256}(306)^{16}(306)^{8}(306)^{2}(306)^{1}\,(mod\ 713)$

$D(306) \equiv (306)^{283} \equiv ((306)^2)^{128}\,((306)^2)^8\,((306)^2)^4\,(306)^2(306)\,(mod\ 713)$

$D(306) \equiv (306)^{283} \equiv ((233)^2)^{64}\,((233)^2)^4\,((233)^2)^2\,(233)(306)\,(mod\ 713)$

$D(306) \equiv (306)^{283} \equiv ((101)^2)^{32}\,((101)^2)^2\,(101)^2(711)\,(mod\ 713)$

$D(306) \equiv (306)^{283} \equiv ((219)^2)^{16}\,(219)^2(219)(711)\,(mod\ 713)$

$D(306) \equiv (306)^{283} \equiv ((190)^2)^{8}\,(190)(275)\,(mod\ 713)$

$D(306) \equiv (306)^{283} \equiv 494\,(mod\ 713)$

Logo, o bloco decodificado é $b_7 = 494$.

Decodificação do bloco $c_8 = 517$:

$D(c_i) \equiv (c_i)^d\,(mod\ n)$

$D(517) \equiv (517)^{283}\,(mod\ 713)$

$D(517) \equiv (517)^{283} \equiv (517)^{256+16+8+2+1}\,(mod\ 713)$

$D(517) \equiv (517)^{283} \equiv (517)^{256}(517)^{16}(517)^{8}(517)^{2}(517)^{1}\,(mod\ 713)$

$D(517) \equiv (517)^{283} \equiv ((517)^2)^{128}\,((517)^2)^8\,((517)^2)^4\,(517)^2(517)\,(mod\ 713)$

$D(517) \equiv (517)^{283} \equiv ((627)^2)^{64}\,((627)^2)^4\,((627)^2)^2\,(627)(517)\,(mod\ 713)$

$D(517) \equiv (517)^{283} \equiv ((266)^2)^{32}\,((266)^2)^2\,(266)^2(457)\,(mod\ 713)$

$D(517) \equiv (517)^{283} \equiv ((169)^2)^{16}\,(169)^2(169)(457)\,(mod\ 713)$

$D(517) \equiv (517)^{283} \equiv ((41)^2)^{8}\,(41)(229)\,(mod\ 713)$

$D(517) \equiv (517)^{283} \equiv 84\,(mod\ 713)$

Logo, o bloco decodificado é $b_8 = 84$.

Decodificação do bloco $c_9 = 219$:

$D(c_i) \equiv (c_i)^d \, (mod \ n)$

$D(219) \equiv (219)^{283} \, (mod \ 713)$

$D(219) \equiv (219)^{283} \equiv (219)^{256+16+8+2+1} \, (mod \ 713)$

$D(219) \equiv (219)^{283} \equiv (219)^{256}(219)^{16}(219)^{8}(219)^{2}(219)^{1} \, (mod \ 713)$

$D(219) \equiv (219)^{283} \equiv ((219)^2)^{128} \, ((219)^2)^8 \, ((219)^2)^4 \, (219)^2(219) \, (mod \ 713)$

$D(219) \equiv (219)^{283} \equiv ((190)^2)^{64} \, ((190)^2)^4 \, ((190)^2)^2 \, (190)(219) \, (mod \ 713)$

$D(219) \equiv (219)^{283} \equiv ((450)^2)^{32} \, ((450)^2)^2 \, (450)^2(256) \, (mod \ 713)$

$D(219) \equiv (219)^{283} \equiv ((8)^2)^{16} \, (8)^2(8)(256) \, (mod \ 713)$

$D(219) \equiv (219)^{283} \equiv ((64)^2)^8 \, (64)(622) \, (mod \ 713)$

$D(219) \equiv (219)^{283} \equiv 8 \, (mod \ 713)$

Logo, o bloco decodificado é $b_9 = 8$.

Após o processo de decodificação, geramos a tabela com os blocos codificados,

Blocos codificados								
b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9
698	532	83	7	98	524	494	84	8

A sequência codificada em ASCII, "American Standard Code for Information Interchange", pelo professor Alexandre foi 69853283798524494848, dividiremos essa sequência em códigos e caracteres, com o auxílio do resumo abaixo, assim,

Blocos decodificados e codificados								
c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9
380	439	42	28	532	696	306	517	219
b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9
698	532	83	7	98	524	494	84	8

Códigos e Caracteres em ASCII									
69	85	32	83	79	85	32	49	48	48
E	*U*		*S*	*O*	*U*		1	0	0

Após todo esse processo podemos concluir que o professor Alexandre, além de ter votado no candidato Zé Costa quando afirma em sua mensagem cifrada "EU SOU

100", ele demonstrou que o processo de criptografia é uma grande ferramenta com aplicações nos mais diversos sistemas que envolvem sigilo e segurança segurança com o auxílio da Teoria dos Números.

Aplicação: 02

FEIRA DE CIÊNCIAS DO CEFET-MA-2008 A equipe de Design em produto elaborou uma problematização utilizando balões nas cores roxo, azul e vermelho na construção de uma árvore de natal, foi um total de seis balões (três roxos, dois azuis e um vermelho), fazendo uso do conceito de funções geradoras e de equações diofantinas, os alunos lançaram o seguinte desafios: Sabendo que a cor que representa a equipe é o roxo, de quantas maneiras podemos ter na base da "pirâmide" pelo menos um balão roxo?

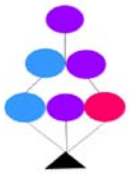


Fig. 5.1: Árvore de Natal

A resolução desse problema $3x_1+2x_2+x_3=6$, inicia-se em definirmos os polinômios $p_1(x)=1+rx+r^2x^2+r^3x^3$, onde $1=r^0x^0$ que indica a ausência do balão de cor roxa, rx indica uma ocorrência do balão de cor roxa, r^2x^2 indica duas ocorrências do balão de cor roxa e r^3x^3 indica três ocorrências do balão de cor roxa e vale o mesmo raciocínio para os balões das cores azul e vermelho, logo $p_2(x)=1+ax+a^2x^2$ e $p_3(x)=1+vx$, sendo $p(x)=p_1(x).p_2(x).p_3(x)$, ou seja,

$p(x)=(1+rx+r^2x^2+r^3x^3)(1+ax+a^2x^2)(1+vx)$

$p(x)=(r^3a^2v)x^6+(r^2a^2v+r^3av+r^3a^2)x^5+(ra^2v+r^2av+r^3v+r^2a^2+r^3a)x^4$

$+(a^2v+rav+r^2v+ra^2+r^2a+r^3)x^3+(av+rv+a^2+ra+r^2)x^2$

$+(r+a+v)x+1$

Analisando o coeficiente $(a^2v + rav + r^2v + ra^2 + r^2a + r^3)$ de x^3, temos as possibilidades de ocorencias dos balões que irão compor a base da "pirâmide", ou seja, a^2v representa dois balões azuis e um vermelho (não satisfaz), rav implica em um balão roxo, um azul e um vermelho, r^2v são dois roxos e um vermelho, ra^2 um roxo e dois azuis, r^2a são dois roxos e um azul e por fim r^3 são os três roxos. No polinômio $p(x)$ o termo independente 1 significa a ausência dos balões nas cores definidas.

Para encontrarmos a listagem das diferentes escolhas possíveis, porém somente o número de tais escolhas, basta tornarmos no produto dos três polinômios $r = a = v = 1$, obtendo assim,

$p(x) = (1 + x + x^2 + x^3)(1 + x + x^2)(1 + x)$

$p(x) = x^6 + 3x^5 + 5x^4 + 6x^3 + 5x^2 + 3x + 1$

Este polinômio é conhecido como Polinômio Gerador ou Função Geradora e os coeficientes $1, 3, 5, 6, 5, 3, 1$, sendo que essa sequência fornece a resposta para a problematização, como é preciso ter pelo menos um balão de cor roxa o coeficiente 6 de x^3 tem uma ocorência que não satisfaz que a base formada pelas cores dois balões azuis e um vermelho, então teremos apenas cinco possibilidades.

Considerações Finais

Dentre todos os campos da matemática e sua importância, este foi um trabalho que a cada página escrita o envolvimento e o entusiasmo com as novas descobertas com a teoria dos números iriam aumentando, uma vez que as Equações Diofantinas não tem um receita própria para estudo da existência, quantidade e/ou propriedades de soluções racionais, assim procuramos desenvolver este, com uma expectativa de como poderíamos contribuir para uma melhor compreensão destes tópicos dentro do processo de ensino e aprendizagem.

Como professor, este trabalho ajudou a ampliar a minha visão das aplicações dos conceitos aprendidos, a avaliar a importância da utilização dos mais diversos conceitos da teoria dos números na análise (ou mesmo resolução) de problemas.

Referências Bibliográficas

[1] G. H. Hardy, An Introduction to the Theory of Numbers. 1959.

[2] Kenneth Ireland, Michael Rosen, AClassical Introduction to Modern Number Theory. Springer, 1990.

[3] José Plínio de Oliveira Santos. Introdução à Teoria dos Números, Coleção Matemática Universitaria, IMPA, 2005, Rio de Janeiro, RJ.

[4] César Polcinio Milies, Sônia Pitta Coelho, Números, Uma intradução à Matemática, 2006.

[5] Edmundo Landau, Teoria Elementar dos Números, Ed. Ciência Moderna,2002, Rio de Janeiro, RJ.

[6] José Plínio de Oliveira Santos, Margarida P. Melo, Idani T. C. Murari. Introdução à Análise Combinatória, ed. Unicamp, 2002, Campinas, SP.

[7] Angela Vidigal, Fundamentos da Álgebra, ed. UFMG, 2005, Belo Horizonte, MG.

[8] Howard Eves, Introdução à Historia da Matemática, ed. Unicamp, 2007, Campinas, SP.

[9] Edward R. Scheinerman, Matemática Discreta, ed. Thomson, 2003, São Paulo, SP.

[10] Herbert S. Wilf, Algorithms Complexity, New Jersey, EUA, 1986.

[11] Donald E. Knuth, The art of Computer Programmingplexity, Second Edition, 1969.

[12] Severino Collier Coutinho. Números Inteiros e Criptografia RSA, ed. IMPA, 2007, Rio de Janeiro, RJ.

Anexos

Dada a importância de consultas às informações complementares, tais como dados fornecidos em tabelas com padrões mundiais, colocaremos a disposição em forma de anexo, texto referente à tabela ASCII, mesmo sabendo que existem outros decimais trataremos em nosso trabalho com a variação de 0 a 105.

Tabela ASCII

A tabela ASCII (American Standard Code for Information Interchange) que em português significa "Código Padrão Americano para o Intercâmbio de Informação"é uma codificação de caracteres de sete bits baseada no alfabeto inglês. Desenvolvida a partir de 1960, grande parte das codificações de caracteres modernas a herdaram como base e tem uma enorme aplicação nas industrias de computadores para troca de informações. Cada caracter é representado por um código de 8 bits (um byte).

Tabela ASCII					
Decimal	*Caracter*	*Decimal*	*Caracter*	*Decimal*	*Caracter*
0	*NUL*	11	*VT*	21	*NAK*
1	*SOH*	11	*VT*	22	*SYN*
2	*STX*	12	*FF*	23	*ETB*
3	*ETX*	13	*CR*	24	*CAN*
4	*EOT*	14	*SO*	25	*EM*
5	*ENQ*	15	*SI*	26	*SUB*
6	*ACK*	16	*DLE*	27	*ESC*
7	*BEL*	17	*D*1	28	*FS*
8	*BS*	18	*D*2	29	*GS*
9	*HT*	19	*D*3	30	*RS*
10	*LF*	20	*D*4	31	*US*

Tabela ASCII					
Decimal	*Caracter*	*Decimal*	*Caracter*	*Decimal*	*Caracter*
31	*US*	56	%	81	*Q*
32	*Espaço*	57	&	82	*R*
33	!	58	:	83	*S*
34	”	59	;	84	*T*
35	#	60	<	85	*U*
36	$	61	=	86	*V*
37	%	62	>	87	*W*
38	&	63	?	88	*X*
39	′	64	–	89	*Y*
40	(	65	*A*	90	*Z*
41	)	66	*B*	91	[
42	*	67	*C*	92	\
43	+	68	*D*	93	]
44	,	69	*E*	94	^
45	–	70	*E*	95	_
46	.	71	*G*	96	‘
47	/	72	*H*	97	*a*
48	0	73	*I*	98	*b*
49	1	74	*J*	99	*c*
50	2	75	*K*	100	*d*
51	3	76	*L*	101	*e*
52	4	77	*M*	102	*f*
53	5	78	*N*	103	*g*
54	6	79	*O*	104	*h*
55	7	80	*P*	105	*i*