UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL

INSTITUTO DE MATEMÁTICA

PROGRAMA DE PÓS GRADUAÇÃO

MATEMÁTICA EM REDE NACIONAL

MESTRADO PROFISSIONAL

DONIZETE ROCHA DE BRITTES

NÚMEROS PRIMOS COMO SOMA DE DOIS QUADRADOS

CAMPO GRANDE

AGOSTO DE 2014

UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL

INSTITUTO DE MATEMÁTICA

PROGRAMA DE PÓS GRADUAÇÃO

MATEMÁTICA EM REDE NACIONAL

MESTRADO PROFISSIONAL

DONIZETE ROCHA DE BRITTES

NÚMEROS PRIMOS COMO SOMA DE DOIS QUADRADOS

Orientadora: Profa. Dra. ELISABETE SOUSA FREITAS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Instituto de Matemática – INMA/UFMS, como parte dos requisitos para obtenção do Título de Mestre.

CAMPO GRANDE

AGOSTO DE 2014

NÚMEROS PRIMOS COMO SOMA DE DOIS QUADRADOS

DONIZETE ROCHA DE BRITTES

Dissertação submetida ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Instituto de Matemática, da Universidade Federal de Mato Grosso do Sul, como parte dos requisitos para obtenção do título de Mestre.

Aprovado pela Banca Examinadora:

Profa. Dra. Elisabete Sousa Freitas - UFMS

Prof. Dr. Claudemir Aniz - UFMS

Prof. Dr. Lino Sanabria - UFGD

CAMPO GRANDE

AGOSTO DE 2014

Dedico este trabalho aos meus pais Sônia Aparecida da Rocha e Donizete João de Brittes por todo apoio que me deram durante toda a minha vida escolar, acadêmica e pessoal. Agradeço por nunca medirem esforços para que eu tivesse as melhores condições possíveis de vida.

Epígrafe

"A matemática, percebida corretamente, possui não apenas a verdade, mas a suprema beleza uma beleza fria e austera com uma escultura, sem apelar para as fraquezas humanas e sem as maravilhosas armadilhas da pintura ou da música, e ainda assim sublimemente pura e capaz de uma perfeição absoluta que apenas a mais elevada das artes pode mostrar." Bertrand Russell

AGRADECIMENTOS

Agradeço primeiramente a Deus por sempre estar ao meu lado em todos os momentos de fraqueza e me ajudar a seguir em frente. Agradeço a minha orientadora Elisabete Sousa Freitas que com sua imensa sabedoria e paciência me guiou muito bem durante o trabalho. Agradeço aos meus pais por nunca medirem esforços para que eu tivesse as melhores condições de estudo.

Agradeço também, todos os meus professores, desde a educação básica até o ensino superior, principalmente aos meus professores do curso de licenciatura em matemática da UFMS, profissionais fantásticos que mudaram a minha vida.

Por último, quero agradecer aos meus colegas de mestrado pelo companheirismo, principalmente ao Rogério que nos ajudou bastante disponibilizando exercícios durante o curso, o programa LyX e um vídeo explicando as funcionalidades do mesmo.

Resumo

O presente trabalho tem como objetivo estabelecer condições para que um número primo p possa ser escrito como soma de dois quadrados tanto do ponto de vista aritmético como do ponto de vista algébrico. Primeiramente, trabalharemos com o conjunto dos números inteiros onde admitiremos alguns resultados bem conhecidos. Do ponto de vista algébrico estudaremos algumas estruturas algébricas e em particular o domínio Euclidiano formado pelos inteiros Gaussianos.

Palavras-chave: Números Primos, Inteiros Gaussianos, Soma de dois Quadrados.

Abstract

This work aims to establish conditions for a prime number p can be written as a sum of two squares from two points of view: the arithmetical point of view and from the algebraic point of view. First, we will work with the set of integers which admit some well-known results. From the algebraic point of view we will study some algebraic and in particular the Euclidean domain structures formed by Gaussian integers.

Keywords: Prime Numbers, Gaussian integers, Sum of two squares.

Sumário

Capítulo 1

Introdução

Quando um primo p pode ser escrito como soma de dois quadrados? Isto é, quando existem inteiros a e b tais que $p = a^2 + b^2$? Ao longo do trabalho, responderemos esta pergunta aritmeticamente e algebricamente.

Vejamos alguns exemplos de primos que podem ou não ser escritos como soma de dois quadrados:

1) Considere os primos 13 e 17. Observe que $13 = 2^2 + 3^2$ e $17 = 1^2 + (-4)^2$, portanto 13 e 17 podem ser escritos como soma de dois quadrados.

2) Já os primos 7 e 11 não podem ser escritos como soma de dois quadrados, pois não existem inteiros a e b tais que $7 = a^2 + b^2$ ou $11 = a^2 + b^2$.

Com exceção do 2, todos os primos deixam resto 1 ou 3 quando divididos por 4. Observamos no $1^{\underline{o}}$ exemplo que os primos 13 e 17 são tais que $13 = 4.3 + 1$ e $17 = 4.4 + 1$, ou seja, ambos deixam resto 1 quando divididos por 4. No capítulo 3, após admitir conhecidas algumas propriedades dos números inteiros, provaremos que existem infinitos primos que deixam resto 1 quando divididos por 4, e que todos os primos deste tipo podem ser escritos como soma de dois quadrados. Além disso, provaremos que existem infinitos primos que deixam resto 3 quando divididos por 4 e que nenhum deles pode ser escrito como soma de dois quadrados. Além disso, veremos um caso particular de naturais como soma de dois

quadrados, os ternos pitagóricos. Um terno pitagórico (a, b, c) é formado por naturais tais que $a^2 + b^2 = c^2$. Usaremos o método de Euclides para encontrar ternos pitagóricos (a, b, c) tais que o máximo divisor comum entre a e b é 1.

No capítulo 4, estudaremos algumas estruturas algébricas, com exemplos que serão usados posteriormente. No capítulo 5, primeiramente buscaremos condições para um primo p ser soma de dois quadrados no conjunto dos inteiros Gaussianos ($\mathbb{Z}[i]$). Posteriormente, caracterizaremos novamente os ternos pitagóricos usando o conjunto dos inteiros Gaussianos ($\mathbb{Z}[i]$) e generalizaremos o resultado estabelecido para números primos para um número natural qualquer.

Capítulo 2

Resultados Básicos sobre Números Primos

Neste capítulo vamos apresentar alguns resultados sobre números primos. Admitiremos alguns fatos conhecidos dos números inteiros, necessários para o desenvolvimento do trabalho. O Algoritmo da Divisão de Euclides e o Teorema Fundamental da Aritmética não serão demonstrados.

Teorema 1. *(Algoritmo da divisão de Euclides) Dados a e b números inteiros com $b \neq 0$, então existem únicos q e r, inteiros, tais que:*

$$a = bq + r, \quad 0 \leq r < |b|.$$

Dados dois inteiros a e b, usaremos a notação $a \mid b$ para indicar que a é um divisor de b, isto é, existe um inteiro c tal que $b = ac$ e $a \nmid b$ indicará que a não é divisor de b.

A notação $mdc(a, b)$ indicará o máximo divisor comum entre os inteiros a e b, não simultaneamente nulos. Lembramos que, se $d = mdc(a, b)$ então existem r e s inteiros tais que $d = ra + sb$.

Definição 1. Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado de número primo.

Segue da definição os seguintes fatos:

•Se p e q são primos tais que $p \mid q$ então $p = q$.

•Se p é primo e $p \nmid a$ então o $mdc(p, a) = 1$.

Lema 1. *(Lema de Gauss) Sejam a, b e c números inteiros. Se $a \mid bc$ e $mdc(a, b) = 1$, então $a \mid c$.*

Demonstração. Como $mdc(a, b) = 1$ segue que existem inteiros r e s tais que

$$ra + sb = 1$$

Multiplicando a equação por c, obtemos

$$rac + sbc = c$$

onde $a \mid rac$ e $a \mid sbc$, portanto $a \mid c$. □

Proposição 1. *(Propriedade Fundamental dos Números Primos) Sejam a, b, p inteiros com p primo. Se $p \mid ab$ então $p \mid a$ ou $p \mid b$.*

Demonstração. Suponhamos que $p \mid ab$ e que $p \nmid a$. Segue que $mdc(p, a) = 1$ e assim, usando o lema de Gauss, concluímos que $p \mid b$. □

Teorema 2. *(Teorema Fundamental da Aritmética) Dado um número inteiro $n \neq 0, -1, 1$, existem primos $p_1 < \ldots < p_n$, e números naturais $\alpha_1, \ldots, \alpha_n$ univocamente determinados, tais que $n = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n}$.*

Lema 2. *Seja p um número primo. Os números inteiros combinatórios $\begin{pmatrix} p \\ i \end{pmatrix}$, onde $0 < i < p$, são todos divisíveis por p.*

Demonstração. Considere o inteiro $\begin{pmatrix} p \\ i \end{pmatrix} = p \cdot \frac{(p-1)\cdot\ldots\cdot(p-i+1)}{i!}$. Para $i = 1$ temos $\begin{pmatrix} p \\ 1 \end{pmatrix} = p$, portanto o resultado vale trivialmente. Para $1 < i < p$, vale que $i! \mid p\,(p-1)\cdot\ldots\cdot(p-i+1)$. Como $mdc(i!, p) = 1$ (pois $i < p$), segue do Lema de Gauss que, $i! \mid (p-1)\cdot\ldots\cdot(p-i+1)$, assim $p \mid \begin{pmatrix} p \\ i \end{pmatrix}$. □

Teorema 3. *(Pequeno Teorema de Fermat) Dado um número primo p, tem-se que, para todo inteiro a, p divide o número $a^p - a$.*

Demonstração. Para o primo $p = 2$ temos que $2 \mid a^2 - a$, pois $a^2 - a = a(a-1)$ é sempre par.

Suponhamos p primo ímpar. Nesse caso, como $(-a)^p - (-a) = -a^p + a = -(a^p - a)$, basta mostrar o resultado para $a \geq 0$. Vamos provar o resultado usando indução sobre a.

O resultado vale para $a = 0$, pois p é um divisor de 0.

Suponhamos o resultado válido para a, vamos provar que continua válido para $a+1$. Usando a fórmula do binômio de Newton, temos que

$$(a+1)^p - (a+1) = a^p - a + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1} + \ldots + \begin{pmatrix} p \\ p-1 \end{pmatrix} a$$

Usando o lema e a hipótese de indução, concluímos que $p \mid (a+1)^p - (a+1)$. □

Corolário 1. *Se p é um número primo e a e um número natural tal que $p \nmid a$, então $p \mid a^{p-1} - 1$.*

Demonstração. Usando o Pequeno Teorema de Fermat temos que $p \mid a(a^{p-1} - 1)$ e como $p \nmid a$, pela propriedade fundamental dos números primos concluímos que

$$p \mid a^{p-1} - 1$$

□

Teorema 4. *Existem infinitos números primos.*

Demonstração. Suponhamos que exista apenas um número finito de números primos, digamos $p_1, p_2, \ldots p_n$. Considere o número natural $a = p_1 p_2 \cdot \ldots \cdot p_n + 1$ (o produto de todos os primos mais 1). Pelo Teorema Fundamental da Aritmética, o número a possui um divisor primo p e portanto $p = p_i$, com $1 \leq i \leq n$. Consequentemente $p \mid p_1 p_2 \cdot \ldots \cdot p_n$ e daí $p \mid 1 = a - p_1 p_2 \cdot \ldots \cdot p_n$ o que é um absurdo. □

Observação 1. Essa demonstração dada por Euclides, considerada uma das pérolas da matemática, é o primeiro exemplo de prova por redução ao absurdo.

Observamos que todo primo ímpar p é da forma $4k+1$ ou $4k+3$, ou seja, dividindo um primo ímpar por 4 encontraremos resto 1 ou 3.

De fato, considerando a divisão euclidiana de um número inteiro por 4 obteremos restos $0, 1, 2$ ou 3, assim $p = 4k, 4k+1, 4k+2$ ou $4k+3$ e como p é ímpar concluímos que $p = 4k+1$ ou $4k+3$. Mostraremos a seguir que existe uma infinidade de primos das duas formas: $4k+1$ e $4k+3$.

Proposição 2. *Existe uma infinidade de primos da forma* $4k+3$.

Demonstração. Primeiro, observe que o conjunto $A = \{4k+1 \mid k \epsilon \mathbb{N}\}$ é fechado em relação a multiplicação. De fato, $(4k_1+1)(4k_2+1) = 4(4k_1k_2 + k_1 + k_2) + 1 \; \epsilon \; A$.

Usando a mesma ideia de Euclides, suponhamos que exista apenas um número finito de números primos da forma $4k+3$, digamos $3 < p_2 < \ldots < p_n$. Considere $a = 4(p_2 p_3 \cdots p_n) + 3$ e um p primo divisor de a. 8Segue que p é diferente dos primos $3, p_2, \ldots, p_n$.

De fato, se $p = 3$ segue que $3 \mid a - 3 = 4(p_2 p_3 \cdots p_n)$, o que é uma contradição. Analogamente se $p = p_i$, $2 \leq i \leq n$, segue que $p_i \mid a - 4(p_2 p_3 \cdots p_n) = 3$, o que é novamente uma contradição.

Assim a decomposição de a em fatores primos só pode ter elementos do conjunto A, fechado em relação a multiplicação. Chegamos a um absurdo pois a é da forma $4k+3$. □

Vamos usar o lema seguinte para demonstrar que existe uma infinidade de primos da forma $4k+1$.

Lema 3. *Todo divisor primo ímpar de x^2+1, com x natural maior do que 1, é da forma $4k+1$.*

Demonstração. Observamos inicialmente que $4 \nmid (x^2+1)$. De fato, se $x = 2k$, então $x^2+1 = (2k)^2+1 = 4(k^2)+1$, e, se $x = 2k+1$ então $x^2+1 = (2k+1)^2+1 = 4(k^2+k)+2$, logo nos dois casos, $4 \nmid (x^2+1)$. Segue que x^2+1 não é potência de 2 e portanto possui um divisor primo ímpar, digamos p. Temos que $\frac{p-1}{2} \epsilon \mathbb{N}$ e, para algum $t \epsilon \mathbb{N}$,

$$x^2 = tp - 1$$

Elevando a potência $\frac{p-1}{2}$ ambos os lados da equação anterior e usando a fórmula do binômio de Newton obtemos:

$$x^{p-1} = \begin{cases} kp+1 & se \quad \frac{p-1}{2} \quad \acute{e} \ par \\ kp-1 & se \quad \frac{p-1}{2} \quad \acute{e} \ ímpar \end{cases}$$

Suponhamos $x^{p-1} = kp-1$, logo $x^{p-1}-1 = kp-2$. Como $p \mid x^2+1$, segue que $p \nmid x$. Agora pelo Pequeno Teorema de Fermat, temos que $p \mid x^{p-1}-1$ e portanto $p \mid kp-(x^{p-1}-1) = 2$, o que é uma contradição.

Portanto $\frac{p-1}{2}$ tem que ser par, ou equivalentemente, $p = 4k+1$. □

Proposição 3. *Existe uma infinidade de primos da forma $4k+1$.*

Demonstração. Suponhamos por absurdo que exista apenas um número finito de primos da forma $4k+1$, digamos $p_1, p_2, \ldots, p_n$. Considere

$$a = 4(p_1 \cdot p_2 \cdots p_n)^2 + 1$$

Como $p_i \nmid a$, para todo $i = 1, \ldots, n$, caso contrario $p \mid 1$, concluímos que a possui um divisor primo da forma $4k + 3$, o que contraria o lema. $\square$

Capítulo 3

Ternos Pitagóricos e primos como soma de dois quadrados

3.1 Ternos pitagóricos

Nesta seção estudamos os triângulos retângulos com lados inteiros. Se indicarmos por a, b as medidas dos lados dos catetos e c a medida da hipotenusa em um triângulo retângulo, o Teorema de Pitágoras nos diz que $a^2 + b^2 = c^2$. Vale também a recíproca, se a, b e c são as medidas dos lados de um triângulo e $a^2 + b^2 = c^2$ então o triângulo é retângulo e a hipotenusa mede c.

Definição 2. Um terno pitagórico (a, b, c) é formado por três números naturais tais que $a^2 + b^2 = c^2$.

Exemplo 1. Os números 3, 4, e 5 formam um terno pitagórico,

pois $3^2 + 4^2 = 5^2$.

Exemplo 2. .Os números 6, 8, e 10 formam um terno pitagórico,

pois $6^2 + 8^2 = 10^2$.

Observação 2. *i*) Se $n \in N$ é um número ímpar, então $a = n$, $b = \frac{n^2-1}{2}$ e $c = \frac{n^2+1}{2}$ formam um terno pitagórico.

ii) Se $n \in N$ é um número par, então $a = n$, $b = \left(\frac{n}{2}\right)^2 - 1$ e $c = \left(\frac{n}{2}\right)^2 + 1$ formam um terno pitagórico.

De fato,

i) Tomando n é ímpar, temos que b e c são inteiros.

Segue que $c^2 = \left(\frac{n^2+1}{2}\right)^2 = \frac{n^4+2n^2+1}{4}$.

Além disso, $a^2 = n^2$, $b^2 = \left(\frac{n^2-1}{2}\right)^2 = \frac{n^4-2n^2+1}{4}$ e $a^2+b^2 = n^2 + \frac{n^4-2n^2+1}{4} = \frac{4n^2}{4} + \frac{n^4-2n^2+1}{4} = \frac{n^4+4n^2-2n^2+1}{4} = \frac{n^4+2n^2+1}{4}$.

Portanto $a^2 + b^2 = c^2$.

ii) Tomando n é par, temos que b e c são inteiros.

Segue que $c^2 = \left(\left(\frac{n}{2}\right)^2 + 1\right)^2 = \frac{n^4}{16} + \frac{n^2}{2} + 1$.

Além disso, $a^2 = n^2$, $b^2 = \left(\left(\frac{n}{2}\right)^2 - 1\right)^2 = \frac{n^4}{16} - \frac{n^2}{2} + 1$ e $a^2 + b^2 = n^2 + \left(\frac{n^4}{16} - \frac{n^2}{2} + 1\right) = \frac{2n^2}{2} + \frac{n^4}{16} - \frac{n^2}{2} + 1 = \frac{n^4}{16} + \frac{2n^2-n^2}{2} + 1 = \frac{n^4}{16} + \frac{n^2}{2} + 1$.

Portanto $a^2 + b^2 = c^2$.

Exemplo 3. Tomando $a = n = 7$,

temos que $b = \frac{7^2-1}{2} = 24$ e $c = \frac{7^2+1}{2} = 25$, satisfazendo $a^2 + b^2 = c^2$.

Exemplo 4. Tomando $a = n = 6$,

temos que $b = \left(\frac{6}{2}\right)^2 - 1 = 8$ e $c = \left(\frac{6}{2}\right)^2 + 1 = 10$, satisfazendo $a^2 + b^2 = c^2$.

Definição 3. Um terno pitagórico (a, b, c) é denominado primitivo quando a e b são primos entre si, isto é, $mdc\,(a, b) = 1$.

Observação 3. (i) Se (a, b, c) é um terno pitagórico primitivo então $mdc(a, c) = mdc(b, c) = 1$.

(ii) Se (a, b, c) é um terno pitagórico e k é um inteiro, então (ka, kb, kc) também é um terno pitagórico.

(iii) Se (a, b, c) é um terno pitagórico onde $a = ka_1$, $b = kb_1$ e $c = kc_1$, k inteiro não nulo, então (a_1, b_1, c_1) também é um terno pitagórico.

(i) De fato, suponhamos por contradição que exista um primo p que divida a e c, segue que p divide $b^2 = c^2 - a^2$ e portanto divide b, o que é um absurdo pois $mdc\,(a, b) = 1$. Logo $mdc\,(a, c) = 1$. De maneira análoga provamos que $mdc\,(b, c) = 1$.

(ii) De fato, $(ka)^2 + (kb)^2 = k^2\,(a^2 + b^2) = k^2c^2 = (kc)^2$.

(iii) De fato, como $(ka_1)^2 + (kb_1)^2 = (kc_1)^2$ temos que $k^2a_1^2 + k^2b_1^2 = k^2c_1^2 \Rightarrow k^2\,(a_1^2 + b_1^2) = k^2c_1^2 \Rightarrow a_1^2 + b_1^2 = c_1^2$.

Observação 4. Seja (a, b, c) um terno pitagórico. Considerando $d = mdc(a, b)$, segue que $a = da_1$ e $b = db_1$, onde $(a_1, b_1) = 1$.

Como $(da_1)^2 + (db_1)^2 = c^2$, temos que d^2 divide c^2, assim $c^2 = kd^2$. Segue que (analisando a decomposição em fatores primos dos inteiros k, c e d), k é um quadrado perfeito, digamos $k = (c_1)^2$, assim temos $c^2 = (c_1d)^2$ e daí $c = c_1d$. Concluímos que um terno qualquer (a, b, c) pode ser obtido do terno primitivo (a_1, b_1, c_1). Assim, conhecendo os ternos pitagóricos primitivos, conhecemos todos os outros.

Método de Euclides para encontrar ternos pitagóricos primitivos

Proposição 4. *Um ponto $P = (x, y)$ pertencente a circunferência centrada na origem com raio igual a 1 tem coordenadas racionais, se, e somente se, $P = (-1, 0)$ ou $P = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ com $t \in \mathbb{Q}$.*

Demonstração. ($\Leftarrow$) *i*) Temos que $P = (-1, 0)$ pertence a circunferência centrada na origem de raio igual a 1, pois $(0 - (-1))^2 + (0 - 0)^2 = 1$.

ii) Se $t \in \mathbb{Q}$, temos que $P = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ tem ambas as coordenadas racionais.

Além disso, segue que $\left(0-\left(\frac{1-t^2}{1+t^2}\right)\right)^2+\left(0-\frac{2t}{1+t^2}\right)^2=\left(\frac{1-2t^2+t^4}{\left(1+t^2\right)^2}\right)+\left(\frac{4t^2}{\left(1+t^2\right)^2}\right)=\frac{1+2t^2+t^4}{\left(1+t^2\right)^2}=\frac{\left(1+t^2\right)^2}{\left(1+t^2\right)^2}=1$. Logo P pertence a circunferência centrada na origem de raio igual a 1.

($\Rightarrow$) Consideremos a circunferência C centrada em $(0,0)$ de raio 1, o ponto $P=(-1,0)$ e as retas $y=t\,(x+1)$, com $t\,\epsilon\,\mathbb{R}$. As retas citadas passam por $P=(-1,0)$, tem inclinação t e as suas interseções com C são dadas pelo sistema:

$$\begin{cases} y=t\,(x+1) & (1) \\ x^2+y^2=1 & (2) \end{cases}, \text{ substituindo (1) em (2) temos:}$$

$x^2+(t\,(x+1))^2=1 \iff$

$x^2+t^2\,(x^2+2x+1)=1 \iff$

$x^2+t^2x^2+2t^2x+t^2-1=0 \iff$

$x^2\,(1+t^2)+2t^2x+(t^2-1)=0$

Segue que:

$$x_t=\frac{-2t^2\pm\sqrt{4t^4-4\left(t^2+1\right)\left(t^2-1\right)}}{2\left(1+t^2\right)}=\frac{-2t^2\pm\sqrt{4t^4-4(t^4-1)}}{2\left(1+t^2\right)}=\frac{-2t^2\pm\sqrt{4t^4-4t^4+4}}{2\left(1+t^2\right)}=$$

$$\frac{-2t^2\pm\sqrt{4}}{2\left(1+t^2\right)}=\frac{-2t^2\pm2}{2\left(1+t^2\right)}=\begin{cases}\frac{2\left(1-t^2\right)}{2\left(1+t^2\right)}\\ \\ \frac{-2\left(1+t^2\right)}{2\left(1+t^2\right)}\end{cases}=\begin{cases}\frac{1-t^2}{1+t^2}\\ \\ -1\end{cases} \quad (3)$$

Substituindo (3) em (1), temos

$$\begin{cases} y=t\left(\frac{1-t^2}{1+t^2}+1\right) \\ y=t\,(-1+1) \end{cases} \Rightarrow \begin{cases} y=t\left(\frac{1-t^2+\left(1+t^2\right)}{1+t^2}\right) \\ y=0 \end{cases} \Rightarrow \begin{cases} y=t\left(\frac{2}{1+t^2}\right) \\ y=0 \end{cases} \Rightarrow$$

$$\begin{cases} y=\frac{2t}{1+t^2} \\ y=0 \end{cases}.$$

Ou seja, o outro ponto de interseção da reta que tem inclinação t e passa por $(-1,0)$, e a circunferência C é o ponto $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$. Se t é um número racional, então o ponto $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ tem ambas as coordenadas racionais.

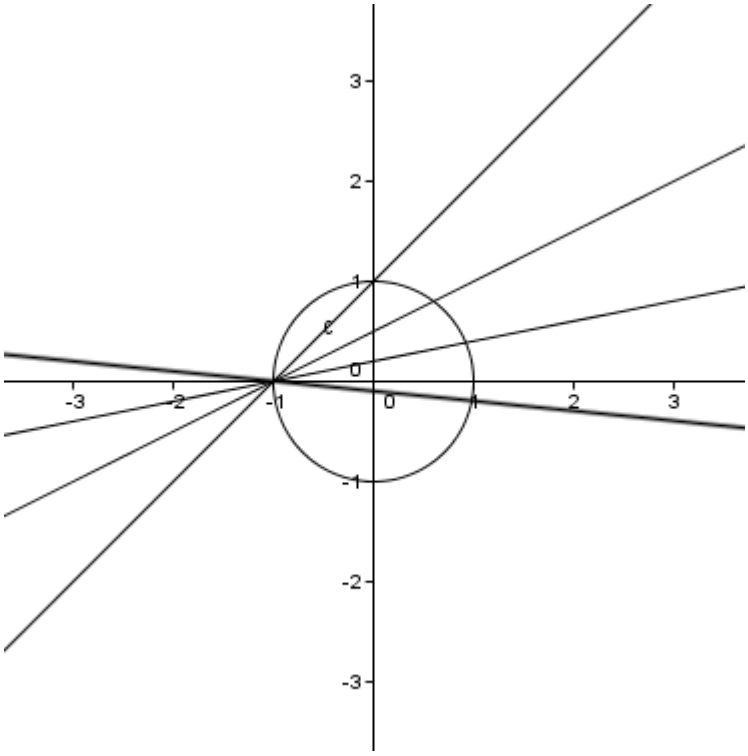

Figura 3.1.1: Circunferência centrada em (0,0) com raio 1 e retas com inclinação t passando por (-1,0).

Considere o ponto $(x_t, y_t) \neq (-1,0)\ \epsilon\ C$ com ambas as coordenadas racionais. Tomando a reta que passa por $(-1,0)$ e tem inclinação $t = \frac{y_t}{x_t+1}\ \epsilon\ \mathbb{Q}$, temos que a sua interseção com C é o ponto

$$\left(\frac{1-\left(\frac{y_t}{x_t+1}\right)^2}{1+\left(\frac{y_t}{x_t+1}\right)^2}, \frac{2\left(\frac{y_t}{x_t+1}\right)}{1+\left(\frac{y_t}{x_t+1}\right)^2}\right) = \left(\frac{\frac{(1+x_t)^2-y_t^2}{(x_t+1)^2}}{\frac{(1+x_t)^2+y_t^2}{(x_t+1)^2}}, \frac{\frac{2y_t}{x_t+1}}{\frac{(x_{t+1})^2+y_t^2}{(x_t+1)^2}}\right) =$$

$$\left(\frac{(1+x_t)^2-y_t^2}{(1+x_t)^2+y_t^2}, \frac{2y_t(x_t+1)^2}{\left((x_{t+1})^2+y_t^2\right)(x_t+1)}\right) = \left(\frac{1+2x_t+x_t^2-y_t^2}{1+2x_t+x_t^2+y_t^2}, \frac{2y_t(x_t+1)}{1+2x_t+x_t^2+y_t^2}\right),$$

como $y_t^2 = 1 - x_t^2$, temos que

$$\left(\frac{1+2x_t+x_t^2-y_t^2}{1+2x_t+x_t^2+y_t^2}, \frac{2y_t(x_t+1)}{1+2x_t+x_t^2+y_t^2}\right) = \left(\frac{1+2x_t+x_t^2-\left(1-x_t^2\right)}{1+2x_t+x_t^2+\left(1-x_t^2\right)}, \frac{2y_t(x_t+1)}{1+2x_t+x_t^2+\left(1-x_t^2\right)}\right) =$$
$$\left(\frac{2x_t+2x_t^2}{2+2x_t}, \frac{y_t 2(x_t+1)}{2x_t+2}\right) = \left(\frac{x_t(2+2x_t)}{2+2x_t}, \frac{y_t(2x_t+2)}{2x_t+2}\right) = (x_y, y_t).$$

Portanto, todo ponto $P \neq (-1, 0)$ com ambas as coordenadas racionais de C é da forma $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$. □

Observação 5. Sejam a, b, $c \in \mathbb{N}$ com $c \neq 0$, temos que $a^2+b^2=c^2 \iff \left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=1 \iff \left(\frac{a}{c}-0\right)^2+\left(\frac{b}{c}-0\right)^2=1$.

Ou seja, a caracterização de ternos pitagóricos pode ser obtida através da caracterização de pontos da circunferência C centrada em $(0, 0)$ de raio 1, com ambas as coordenadas racionais.

Proposição 5. *Todos os ternos pitagóricos primitivos (a, b, c) são dados por $a = n^2 - m^2$, $b = 2mn$, $c = n^2 + m^2$, onde $mdc(m, n) = 1$, m e n tem paridades opostas e $m < n$.*

Demonstração. Considere a, b, $c \in \mathbb{N}$ com $c \neq 0$ e $mdc(a, b) = 1$, tais que $a^2 + b^2 = c^2$, pela observação 5 e pela proposição 4, temos que $\left(\frac{a}{c}, \frac{b}{c}\right) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) = \left(\frac{1-\left(\frac{m}{n}\right)^2}{1+\left(\frac{m}{n}\right)^2}, \frac{2\left(\frac{m}{n}\right)}{1+\left(\frac{m}{n}\right)^2}\right) = \left(\frac{\frac{n^2-m^2}{n^2}}{\frac{n^2+m^2}{n^2}}, \frac{\frac{2m}{n}}{\frac{n^2+m^2}{n^2}}\right) = \left(\frac{n^2-m^2}{n^2+m^2}, \frac{2mn}{n^2+m^2}\right)$, onde consideramos $t = \frac{m}{n}$ com $mdc\,(m, n) = 1$.

Da igualdade dos pares ordenados, temos $\frac{a}{c} = \frac{m^2-n^2}{n^2+m^2}$ e $\frac{b}{c} = \frac{2mn}{n^2+m^2}$. Como $mdc\,(a, b) = 1$ e $a^2 + b^2 = c^2$, concluímos que $mdc\,(a, c) = 1$ e $mdc\,(b, c) = 1$ (observação 3).

Como $mdc\,(m, n) = 1$, temos dois casos a considerar:

1) m e n tem paridades opostas.

Neste caso, $mdc\,(m^2 - n^2, n^2 + m^2) = 1$ e $mdc\,(2mn, m^2 + n^2) = 1$.

De fato, suponhamos por contradição que $mdc\,(m^2 - n^2, n^2 + m^2) \neq 1$. Considere p primo que divide n^2-m^2 e n^2+m^2. Como m e n tem paridades opostas, temos que n^2-m^2 e n^2+m^2 são ímpares, portanto $p \neq 2$. Além disso, p divide a soma $(n^2 - m^2)+(n^2 + m^2) = 2n^2$

e a diferença $(n^2+m^2)-(n^2-m^2)=2m^2$. Logo, p divide m e n, o que é uma contradição, pois m e n são primos entre si.

Suponhamos agora que $mdc\,(2mn, n^2+m^2) \neq 1$. Considere p primo que divide $2mn$ e n^2+m^2. Como n^2+m^2 é ímpar, temos que $p \neq 2$. Assim, $p \neq 2$ e p divide $2mn$, logo p divide m ou p divide n. Sem perda de generalidade, suponhamos que p divide m, segue que p divide m^2, como p divide n^2+m^2, concluímos que p divide n^2 e portanto divide n, o que é novamente uma contradição, pois m e n são primos entre si. Assim, podemos concluir que nas igualdades $\frac{a}{c} = \frac{m^2-n^2}{n^2+m^2}$ e $\frac{b}{c} = \frac{2mn}{n^2+m^2}$ todas as frações são irredutíveis. Portanto $a = m^2-n^2$, $b = 2mn$ e $c = n^2+m^2$.

2) m e n são ambos ímpares:

Considere $p = \frac{m+n}{2}$ e $q = \frac{n-m}{2}$, temos que p e q são inteiros primos entre si com paridades opostas. Se existisse um natural divisor comum diferente de 1 que dividisse p e q, este natural dividiria a soma (n) e a diferença (m) entre eles , o que é um absurdo. Se tivessem a mesma paridade, 2 dividiria a soma (n) e a diferença (m) entre eles, o que é novamente um absurdo.

Usando $p = \frac{m+n}{2} \Longleftrightarrow 2p = m+n$ e $q = \frac{n-m}{2} \Longleftrightarrow 2q = n-m$ em $\left(\frac{a}{c}, \frac{b}{c}\right) = \left(\frac{n^2-m^2}{n^2+m^2}, \frac{2mn}{n^2+m^2}\right)$, temos:

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \left(\frac{n^2-m^2}{n^2+m^2}, \frac{2mn}{n^2+m^2}\right) = \left(\frac{(n-m)(n+m)}{n^2+m^2}, \frac{2mn}{n^2+m^2}\right) =$$

$$= \left(\frac{(2q)(2p)}{(p+q)^2+(p-q)^2}, \frac{2(p-q)(p+q)}{(p+q)^2+(p-q)^2}\right) = \left(\frac{(2q)(2p)}{2\left(p^2+q^2\right)}, \frac{2(p-q)(p+q)}{2\left(p^2+q^2\right)}\right) =$$

$$= \left(\frac{2pq}{p^2+q^2}, \frac{p^2-q^2}{p^2+q^2}\right),$$ com p e q com paridades opostas e $mdc\,(p,q)=1$, o que nos faz retornar ao caso 1). Portanto, é legítimo tomar $a = 2pq$, $b = p^2-q^2$ e $c = p^2+q^2$. □

Vejamos alguns exemplos que essa máquina de ternos pitagóricos com elementos primos entre si dois a dois nos fornece:

Exemplo 5. Tomando $t = \frac{1}{2}$, temos que $a = 2^2-1^2 = 3$, $b = 2.1.2 = 4$ e $c = 2^2+1^2 = 5$.

E assim $5^2 = 3^2+4^2$, com $mdc\,(3,4) = 1$.

Exemplo 6. Tomando $t = \frac{3}{7}$, devemos tomar $p = \frac{3+7}{2} = 5$ e $q = \frac{7-3}{2} = 2$. Assim, temos $a = 2.5.2 = 20$, $b = 5^2 - 2^2 = 21$ e $c = 5^2 + 2^2 = 29$,

obtendo $29^2 = 20^2 + 21^2$, com $mdc\,(20, 21) = 1$.

3.2 Primos como soma de dois quadrados

Proposição 6. *Se p é um número primo ímpar e $p = a^2 + b^2$, então $p = 4k + 1$ com $k \in \mathbb{N}$.*

Demonstração. Temos três casos a considerar: a e b pares, a e b ímpares ou a e b com paridades opostas,

(i) Se a e b fossem ambos pares, teríamos que $a^2 + b^2 (= p)$ seria um número par, contrariando a hipótese.

(ii) Se a e b fossem ambos ímpares, novamente teríamos que $a^2 + b^2 (= p)$ seria um número par, contrariando a hipótese.

(iii) Se a e b tem paridades opostas, suponhamos sem perda de generalidade $a = 2k$ um número par e $b = 2t + 1$ um número ímpar, temos que $a^2 = 4k^2$ e $b^2 = 4t^2 + 4t + 1$ e $a^2 + b^2 = 4k^2 + (4t^2 + 4t + 1) = 4\,(k^2 + t^2 + t) + 1$. Portanto $p = a^2 + b^2$ é da forma $4k + 1$. □

Para cada natural n, seja $r(n)$ o número de modos distintos de se escrever n como soma de dois quadrados, $n = x^2 + y^2$, com x e y inteiros. Ao calcularmos $r(n)$, pensaremos nas soluções inteiras (a, b) de $n = x^2 + y^2$ como um par ordenado de inteiros. Por exemplo,

$8 = 2^2 + (-2)^2$ e $8 = (-2)^2 + 2^2$, são duas maneiras *distintas* de escrever 8 como soma de dois quadrados.

Vejamos alguns exemplos:

Exemplo 7. $r(8) = 4$, pois

$8 = 2^2 + 2^2$

$8 = (-2)^2 + (-2)^2$

$$8 = (-2)^2 + 2^2$$
$$8 = 2^2 + (-2)^2$$

Exemplo 8. $r(10) = 8$, pois

$$10 = 3^2 + 1^2 = 1^2 + 3^2 = (-1)^2 + 3^2 = 3^2 + (-1)^2 = 1^2 + (-3)^2 = (-3)^2 + 1^2 = (-1)^2 + (-3)^2 = (-3)^2 + (-1)^2$$

Exemplo 9. $r(17) = 8$, pois

$$17 = 1^2 + 4^2 = 4^2 + 1^2 = (-1)^2 + 4^2 = 4^2 + (-1)^2 = 1^2 + (-4)^2 = (-4)^2 + 1^2 = (-1)^2 + (-4)^2 = (-4)^2 + (-1)^2.$$

Observamos que o primo 2 pode ser escrito como soma de dois quadrados, pois $2 = 1^2 + 1^2$. Além disso, $r(2) = 4$, já que as únicas escritas de 2 como soma de dois quadrados são $2 = (-1)^2 + (-1)^2$, $2 = (-1)^2 + 1^2$, $2 = 1^2 + (-1)^2$ e $2 = 1^2 + 1^2$. O primo 5 também pode ser escrito como soma de dois quadrados pois $5 = 1^2 + 2^2 = (-1)^2 + 2^2 = 1^2 + (-2)^2 = (-1)^2 + (-2)^2 = 2^2 + 1^2 = (-2)^2 + 1^2 = 2^2 + (-1)^2 = (-2)^2 + (-1)^2$, portanto $r(5) = 8$. Já o primo 3 não pode ter tal escrita, logo $r(3) = 0$.

Observação 6. Observamos que se p é um número primo ímpar e $p = a^2 + b^2$, então $a \neq b$ e $ab \neq 0$.

De fato, se $a = b$, teríamos que $p = 2a^2$, ou seja, teríamos que p é um número par.

Se $a = 0$ ou $b = 0$, teríamos $p = a^2$ ou $p = b^2$, que não são primos.

Lema 4. *Se p é um número primo ímpar e $p = a^2 + b^2$, então $r(p) = 8$.*

Demonstração. Pela observação 6 nós concluímos que $a \neq b$, assim podemos escrever p como soma de dois quadrados de pelo menos 8 maneiras, usando os pares ordenados do conjunto $X = \{(a,b), (-a,b), (a,-b), (-a,-b), (b,a), (-b,a), (b,-a), (-b,-a)\}$.

Suponhamos que exista $(c,d) \notin X$, tal que $p = a^2 + b^2 = c^2 + d^2$. Como p é ímpar, a e b têm paridades opostas e c e d também têm paridades opostas, sem perda de generalidade suponhamos a e c pares, logo b e d ímpares. Temos que $a^2 + b^2 = c^2 + d^2$, logo $a^2 - c^2 = d^2 - b^2$,

assim $(a-c)(a+c) = (d-b)(d+b)$ (1). Como a soma ou a diferença entre números de mesma paridade resulta em um número par, concluímos que $(a-c)$, $(a+c)$, $(d-b)$ e $(d+b)$ são todos números pares. Como $c \neq \pm a$ e $d \neq \pm b$, considerando $D = mdc(a-c, d-b)$ e $E = mdc(a+c, d+b)$, segue que D e E são ambos números pares, e existem:

i) l_1, $l_2 \in \mathbb{N}$, tais que $a - c = l_1 D$ e $d - b = l_2 D$ (2), onde $mdc(l_1, l_2) = 1$.

ii) k_1, $k_2 \in \mathbb{N}$, tais que $a + c = k_1 E$ e $d + b = k_2 E$ (3), onde $mdc(k_1, k_2) = 1$.

De (1), (2) e (3) temos, $(a-c)(a+c) = (d-b)(d+b) \Rightarrow l_1 D k_1 E = l_2 D k_2 E \Rightarrow l_1 k_1 = l_2 k_2 \Rightarrow \frac{k1}{k_2} = \frac{l_2}{l_1}$. Nesta última igualdade temos duas frações equivalentes nas suas formas irredutíveis, portanto, temos $k_1 = l_2$ e $k_2 = l_1$ (4).

Assim, temos que,

$a - c = l_1 D$ e $d - b = l_2 D$ (2).

$a + c = l_2 E$ e $d + b = l_1 E$ (3) e (4).

Segue que, $(a-c) + (a+c) = l_1 D + l_2 E \Rightarrow 2a = l_1 D + l_2 E \Rightarrow a = \frac{l_1 D + l_2 E}{2}$ e,

$(d+b) - (d-b) = l_1 E - l_2 D \Rightarrow 2b = l_1 E - l_2 D \Rightarrow b = \frac{l_1 E - l_2 D}{2}$.

Daí, $p = a^2 + b^2 = \left(\frac{l_1 D + l_2 E}{2}\right)^2 + \left(\frac{l_1 E - l_2 D}{2}\right)^2 = \frac{l_1^2 D^2 + 2 l_1 D l_2 E + l_2^2 E^2}{4} + \frac{l_1^2 E^2 - 2 l_1 D l_2 E + l_2^2 D^2}{4} =$

$$\frac{l_1^2 D^2 + l_1^2 E^2 + l_2^2 E^2 + l_2^2 D^2}{4} = \frac{l_1^2\left(D^2 + E^2\right) + l_2^2\left(D^2 + E^2\right)}{4} = \frac{\left(l_1^2 + l_2^2\right)\left(D^2 + E^2\right)}{4} =$$

$$\left(l_1^2 + l_2^2\right)\left[\frac{\left(D^2 + E^2\right)}{4}\right] = \left(l_1^2 + l_2^2\right)\left[\frac{D^2}{4} + \frac{E^2}{4}\right] = \left(l_1^2 + l_2^2\right)\left[\left(\frac{D}{2}\right)^2 + \left(\frac{E}{2}\right)^2\right].$$

Como $\left(l_1^2 + l_2^2\right)$ e $\left[\left(\frac{D}{2}\right)^2 + \left(\frac{E}{2}\right)^2\right]$ são números naturais maiores que 1, teríamos p composto, o que é um absurdo. Portanto, se p pode ser escrito como soma de dois quadrados, então $r(p) = 8$. □

Demonstramos que se $p = a^2 + b^2$ com p primo, então $p = 4k+1$ com $k \in \mathbb{N}$ (deixa resto 1 quando dividido por 4), logo primos da forma $4k + 3$ não podem ser escritos como soma de dois quadrados. Além disso, provamos que se $p = a^2 + b^2$ então $r(p) = 8$.

O teorema conhecido como grande teorema de Fermat afirma que todo primo p da forma $4k+1$ pode de fato ser escrito como soma de dois quadrados e portanto $r(p) = 8$. Para completar a demonstração do teorema usaremos um tipo de função, chamada involução, definida a seguir.

Definição 4. Seja S um conjunto finito, uma função $f : S \to S$ é uma involução se $fof = I_S$, onde $I_S : S \to S$ é a função identidade.

Observamos que a condição $fof = I_S$ é equivalente a afirmação "f é bijetiva e coincide com sua inversa".

Definição 5. Um ponto fixo de uma função $f : S \to S$, é um ponto x_0 tal que $f(x_0) = x_0$.

Proposição 7. *Seja S um conjunto finito e f uma involução. O número de elementos de S e o número dos pontos fixos de f têm mesma paridade.*

Demonstração. Provaremos essa proposição por indução. Suponha que S tenha n elementos e que o conjunto dos pontos fixos de f em S seja designado por F_{f_S}.

Passo 1) Se $n = 1$, temos que $S = \{a_1\}$ e $f(a_1) = a_1$. Assim $n = 1 = F_{f_S}$.

Se $n = 2$ ($S = \{a_1, a_2\}$), como f é uma involução temos apenas duas possibilidades: $f(a_1) = a_1$ e $f(a_2) = a_2$ ou $f(a_1) = a_2$ e $f(a_2) = a_1$. No primeiro caso F_{f_S} tem 2 elementos, no segundo caso F_{f_S} tem 0 elementos, em ambos os casos F_{f_S} tem mesma paridade que S.

Passo 2) Suponhamos a proposição válida para quando um conjunto tenha até n elementos, temos que mostrar que o mesmo é válido para quando f tenha $n+1$ elementos.

Sejam $S = \{a_1, a_2, ..., a_{n+1}\}$ e $f : S \to S$ uma involução. Temos dois casos:

i) $f(a_{n+1}) = a_{n+1}$. Considere f restrita ao conjunto $S_1 = S - \{a_{n+1}\}$, com esta restrição f continua sendo uma involução, pela hipótese de indução, o número de elementos de S_1 e do conjunto dos pontos fixos de f em S_1 tem igual paridade. Se S_1 e $F_{f_{S_1}}$ tem quantidade ímpar de elementos, então S e F_{f_S} tem uma quantidade par de elementos. Se S_1 e $F_{f_{S_1}}$ tem quantidade par de elementos, então S e F_{f_S} tem quantidade ímpar de elementos.

$ii) f(a_{n+1}) = a_k$, com $1 \leq k \leq n$. Como $f : S \to S$ é uma involução, $f(a_k) = a_{n+1}$. Considere $S_2 = S - \{a_k, a_{n+1}\}$, com esta restrição f continua sendo uma involução, pela hipótese de indução, temos que S_2 e $F_{f_{S_2}}$ tem igual paridade. Temos que S_2 tem mesma paridade que S, como a quantidade de pontos fixos não mudará na passagem do domínio de S_2 para S, podemos concluir que S e F_{f_S} tem igual paridade. □

Teorema 5. *(Grande teorema de Fermat) Se p é primo da forma $4k+1$ com $k \epsilon \mathbb{N}$, então $r(p) = 8$.*

Demonstração. Seja p um número primo da forma $4k+1$, com $k \epsilon \mathbb{N}$. Consideremos o conjunto $S = \{(x, y, z) \epsilon \mathbb{N}^3 \setminus x^2 + 4yz = p\}$. S é um conjunto não vazio, pois $(1, 1, k) \epsilon S$. Além disso, S é finito, já que os valores de x, y e z estão entre 1 e p.

Seja $f : S \to S$ uma função dada por

$$f(x,y,z) = \begin{cases} (x+2z, z, y-x-z), & se \quad x < y-z \\ (2y-x, y, x-y+z), & se \quad y-z < x < 2y \\ (x-2y, x-y+z, y), & se \quad x > 2y \end{cases}$$

A função f está bem definida, já que os planos $x = y - z$ e $x = 2y$ não intersectam S (se intersectassem, teríamos elementos de S sem correspondente). De fato, substituindo $x = y - z$ em $x^2 + 4yz = p$, teríamos $(y-z)^2 + 4yz = p \Rightarrow y^2 - 2yz + z^2 + 4yz = p \Rightarrow y^2 + 2yz + z^2 = p \Rightarrow (y+z)^2 = p$, o que é um absurdo, pois p é primo e não pode ser quadrado de nenhum natural. Substituindo $x = 2y$ em $x^2 + 4yz = p$, teríamos $p = (2y)^2 + 4yz = 4(y^2 + yz)$, o que é um absurdo, pois p é primo da forma $4k+1$. Além disso, observe que a imagem de f realmente está em S, pois $(x+2z)^2 + 4(z)(y-x-z) = (2y-x)^2 + 4(y)(x-y+z) = (x-2y)^2 + 4(x-y+z)(y) = x^2 + 4yz$.

Vamos provar agora que a função f é uma involução. Temos que

$$f(x,y,z)=\begin{cases}(x+2z,z,y-x-z) & , \quad se \quad (x,y,z) \quad \epsilon \quad S_1\\ (2y-x,y,x-y+z) & , \quad se \quad (x,y,z) \quad \epsilon \quad S_2\\ (x-2y,x-y+z,y) & , \quad se \quad (x,y,z) \quad \epsilon \quad S_3\end{cases}$$

onde $S_1 = \{(x,y,z)\,\epsilon S / x < y-z\}$, $S_2 = \{(x,y,z)\,\epsilon S / y-z < x < 2y\}$ e $S_3 = \{(x,y,z)\,\epsilon S / x > 2y\}$.

Observamos que $f(S_1) \subset S_3$, $f(S_3) \subset S_1$ e $f(S_2) \subset S_2$, logo

$$f(f(x,y,z)) = \begin{cases}((x+2z)-2(z),(x+2z)-(z)+(y-x-z),z)\\ (2y-(2y-x),y,(2y-x)-(y)+(x-y+z))\\ (x-2y)+2(y),y,(x-y+z)-(x-2y)-(y)\end{cases} = \begin{cases}(x,y,z)\\ (x,y,z)\\ (x,y,z)\end{cases}$$

Afirmação: $\left(1,1,\frac{p-1}{4}\right)\,\epsilon\, S_2$ é o único ponto fixo de f.

Primeiramente, $f\left(1,1,\frac{p-1}{4}\right) = \left(2-1,1,1-1+\frac{p-1}{4}\right) = \left(1,1,\frac{p-1}{4}\right)$.

Unicidade do ponto fixo:

Como $f(S_1) \subset S_3$ e $f(S_3) \subset S_1$, a função f não possui pontos fixos em S_1 e S_3 ($S_1 \cap S_3 = \emptyset$).

Suponhamos então $(x,y,z)\,\epsilon\, S_2$ tal que $f(x,y,z) = (x,y,z)$, ou seja,

$(2y-x,y,x-y+z) = (x,y,z)$. Assim,

$$\begin{cases}2y-x=x\\ y=y\\ x-y+z=z\end{cases} \qquad \text{e daí obtemos } x=y.$$

Assim, o possível ponto fixo é da forma $(x,x,z)\,\epsilon\, S_2 \subset S$. Segue que $x^2+4xz = p \Rightarrow p = x(x+4z)$. Como p é primo, concluímos que $x=1$, logo $p=4z+1$, isto é, $z=\frac{p-1}{4}$. Portanto, $(x,y,z) = \left(1,1,\frac{p-1}{4}\right)$ é o único ponto fixo.

Pela **proposição** 7, podemos concluir que S tem quantidade ímpar de elementos.

Considere agora a aplicação $g : S \to S$, $g(x, y, z) = (x, z, y)$. A função g é uma involução, pois $gog(x, y, z) = g(g(x, y, z)) = g(x, z, y) = (x, y, z)$. Como S tem quantidade ímpar de número de elementos, novamente pelo **Proposição** 7, concluímos que g possui pelo menos um ponto fixo. Considere então (x, y, z) em S tal que $g(x, y, z) = (x, y, z)$, logo $(x, z, y) = (x, y, z)$ e assim $y = z$. Como $(x, y, y) \epsilon S$, temos $p = x^2 + 4y.y = x^2 + (2y)^2$. Portanto, provamos que um primo p da forma $4k + 1$ pode ser escrito como soma de dois quadrados. O fato de que $r(p) = 8$ já foi demonstrado no lema 4. □

Neste capítulo, usando aritmética dos números inteiros, provamos que somente o primo 2 e primos da forma $4k + 1$ podem ser escritos como soma de dois quadrados.

No capítulo 5 esse fato será provado usando a estrutura algébrica dos inteiros Gaussianos.

Capítulo 4

Estruturas algébricas e fatoração

4.1 Definições, exemplos e propriedades

Definição 6. Um conjunto A com pelo menos 2 elementos, munido de duas operações denotadas por $+$ (chamada *adição*) e $\cdot$ (chamada *multiplicação*) é um *Anel Comutativo com unidade*, ou simplesmente *Anel* se satisfaz as seguintes propriedades:

A1) A adição é associativa, isto é, $\forall\ x, y, z \in A$, $(x + y) + z = x + (y + z)$.

A2) Existe um elemento neutro com respeito a adição, isto é, $\exists\ 0 \in A$ tal que, $\forall\ x \in A$, $0 + x = x + 0 = x$.

A3) Todo elemento de A possui um oposto com respeito a adição, isto é, $\forall\ x \in A$, $\exists z \in A$ tal que, $x + z = z + x = 0$.

A4) A adição é comutativa, isto é, $\forall\ x, y \in A$, $x + y = y + x$.

M1) A multiplicação é associativa, isto é, $\forall\ x, y, z \in A$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

M2) Existe um elemento neutro (unidade) com respeito a multiplicação, isto é, $\exists\ 1 \in A$ tal que, $\forall\ x \in A$, $1 \cdot x = x \cdot 1 = x$.

M3) A multiplicação é comutativa, isto é, $\forall\ x, y \in A$, $x \cdot y = y \cdot x$.

M4) A multiplicação é distributiva relativamente a adição, isto é, $\forall\ x, y, z \in A$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

Por comodidade, indicaremos a multiplicação $a \cdot b$ simplesmente por ab.

Exemplo 10. O conjunto dos números inteiros $\mathbb{Z}$ munido das operações usuais de adição e multiplicação é um *Anel*.

Definição 7. Um anel A será chamado de domínio de integridade ou simplesmente domínio se for verificada a seguinte propriedade:

Dados a e $b \epsilon A$, se $a \neq 0$ e $b \neq 0$ então $ab \neq 0$ (ou equivalentemente dados a e $b \epsilon A$, se $ab = 0$ então $a = 0$ ou $b = 0$).

Exemplo 11. O conjunto dos números inteiros $\mathbb{Z}$ munido das operações usuais de adição e multiplicação é um *Domínio*.

Observação 7. Em todo *Domínio* D vale a lei do cancelamento, isto é, se $a \cdot b = a \cdot c$ com $a \neq 0$ então $b = c$.

De fato, $a \cdot b = a \cdot c \Rightarrow a \cdot b + (-a \cdot c) = 0 \Rightarrow a \cdot b + (-1)\, a \cdot c = 0 \Rightarrow a \cdot (b - c) = 0 \Rightarrow a = 0$ ou $b - c = 0$, como $a \neq 0$, concluímos que $b - c = 0$, ou seja, $b = c$.

Definição 8. Um elemento a de um *Anel* A é invertível, se existe $b \epsilon A$ tal que $a \cdot b = b \cdot a = 1$. Indicaremos o inverso de a por a^{-1} ou $\frac{1}{a}$. Por conveniência, indicaremos por $\frac{a}{b}$ a multiplicação $a \cdot \frac{1}{b} = ab^{-1}$.

Note que o inverso de um elemento a, se existir, é único.

Exemplo 12. O número 2 é invertível no *Anel* $\mathbb{Q}$ (seu inverso é o $\frac{1}{2}$), e não é invertível no anel $\mathbb{Z}$.

Definição 9. Um *Anel* A tal que todo elemento diferente de 0 (não nulo) é invertível é chamado de corpo.

Observação 8. O conjunto dos inteiros $\mathbb{Z}$ é exemplo de um domínio que não é um corpo.

Exemplo 13. O conjunto dos números reais $\mathbb{R}$ e o conjunto dos números complexos $\mathbb{C}$ munidos das operações usuais são exemplos de corpos.

Observação 9. Todo corpo K também é um Domínio.

De fato, sejam a e b pertencentes a K com $a \cdot b = 0$. Se $a \neq 0$, temos que $a \cdot b = 0 \Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \Rightarrow b = 0$.

Definição 10. Sejam a e b, elementos de um anel A. Se existir um elemento $c \epsilon A$ tal que $b = ac$, dizemos que a divide b. Neste caso, dizemos também que a é um divisor de b, b é um múltiplo de a, b é divisível por a, ou ainda que a é um fator de b.

Denotaremos a afirmação a divide b por $a \mid b$ e a sua negação por $a \nmid b$.

Proposição 8. *(Propriedades da divisibilidade) Sejam a, b, c e d elementos de um anel A. As seguintes afirmações são verdadeiras:*

1) $a \mid 0$ *e* $a \mid a$.

2) Se $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

3) Se $a \mid b$ *e* $c \mid d$, *então* $ac \mid bd$.

4) Se $a \mid b + c$ *e* $a \mid b$, *então* $a \mid c$.

5) Se u *é invertível, então* $u \mid a$.

As demonstrações seguem diretamente da definição de divisibilidade e das propriedades de anel, de modo inteiramente análogo as propriedades de divisibilidade em $\mathbb{Z}$.

Definição 11. Dois elementos a e b de um *Anel* A são ditos associados se existir um elemento invertível u de A tal que $a = ub$ $(b = u^{-1}a)$.

Proposição 9. *Sejam D um domínio e* $a, b \epsilon D \setminus \{0\}$. *Temos que* $a \mid b$ *e* $b \mid a$, *se e somente se, a e b são associados.*

Demonstração. ($\Rightarrow$) Como $a \mid b$ e $b \mid a$, temos que $b = ak$ e $a = bt$, com $k, t \epsilon D$. Assim, $b = (bt)\, k$, pela lei do cancelamento, $1 = tk$. Logo, t e k são invertíveis. Portanto, a e b são associados.

($\Leftarrow$) Como a e b são associados, temos que $a = bk$, com k invertível. Segue que, $ak^{-1} = b$. Assim, concluímos que $a \mid b$ e $b \mid a$. □

Definição 12. Seja um *Anel* A e a, b, d elementos de A, d é um máximo divisor comum de a e b (não simultaneamente nulos) se:

1) $d \mid a$ e $d \mid b$.

2) $\forall\ d' \epsilon A$ tal que $d' \mid a$ e $d' \mid b$, tem-se que $d' \mid d$.

Proposição 10. *Num domínio D, dois máximos divisores comuns de dois elementos a e b não simultaneamente nulos são associados e todo associado de um máximo divisor comum destes elementos é também um máximo divisor comum deles.*

Demonstração. Sejam d e d' dois máximos divisores comuns de a e b. Temos que $d \mid a$ e $d \mid b$. Portanto $d \mid d'$. Além disso, $d' \mid a$ e $d' \mid b$. Portanto $d' \mid d$. Pela proposição 9, concluímos que d e d' são associados.

Considere agora, d um máximo divisor comum de a e b, e t um associado de d. Segue que $d = tu$ e $t = du^{-1}$.

Temos que $d \mid a$ e $d \mid b$. Assim, $a = dk_1$ e $b = dk_2$, com $k_1, k_2 \epsilon D$.

Daí, $a = tuk_1$ e $b = tuk_2$. Logo $t \mid a$ e $t \mid b$.

Seja c, tal que $c \mid a$ e $c \mid b$, temos que $c \mid d$. Assim, $d = ck$, com $k \epsilon D$. Logo $t = du^{-1} = cku^{-1}$. Portanto, c divide t e t é um máximo divisor comum de a e b. □

Definição 13. Seja A um *Anel*, um subconjunto não vazio I de A é um *Ideal* se

(i) $\forall\ x, y \epsilon I$, $x + y \epsilon I$

(ii) $\forall\ x \epsilon I$, $\forall\ a \epsilon A$, $a \cdot x \epsilon I$.

Exemplo 14. Seja A um anel e a um elemento de A. O conjunto $I(a) = \{a \cdot k \setminus k \epsilon A\}$ é um ideal de A.

Neste caso, dizemos que $I(a)$ é gerado por a.

De fato,

(i) $\forall\ x, y \epsilon I(a)$, $x + y = ak_1 + ak_2 = a(k_1 + k_2) \epsilon I$.

(ii) $\forall\ x \epsilon I(a)$, $\forall\ b \epsilon A$, $b \cdot x = bak_1 = a(bk_1) \epsilon I$.

Observamos que $I(0) = \{0\}$, denominado ideal nulo e denotado simplesmente por 0.

Exemplo 15. Sejam A um anel e $a, b \in A$. O conjunto $I(a,b) = \{na + mb \mid m, n \epsilon A\}$ é um ideal de A.

Neste caso, dizemos que o ideal $I(a,b)$ é gerado por a e b.

A demonstração é análoga a do exemplo 14.

Exemplo 16. Sejam A um anel e $a_1, \ldots, a_t \in A$.

O conjunto $I(a_1, \ldots, a_t) = \{n_1a_1 + \ldots + n_ta_t / n_1, \ldots, n_t \epsilon A\}$ é um ideal de A gerado pelos elementos $a_1, \ldots, a_t$.

A demonstração é análoga a do exemplo 14.

Exemplo 17. Seja $(I_n)_{n\epsilon\mathbb{N}}$ uma família de ideais de um anel A. Então

(i) $\bigcap_{n\epsilon\mathbb{N}} I_n$ é um ideal de A;

De fato, sejam a e $b \in \bigcap_{n\epsilon\mathbb{N}} I_n$. Segue que $a, b \in I_k$ para todo $k \in \mathbb{N}$. Assim $a + b \in I_k$ para todo $k \in \mathbb{N}$, logo $a + b$ pertence a $\bigcap_{n\epsilon\mathbb{N}} I_n$.

Além disso, sendo $a \in \bigcap_{n\epsilon\mathbb{N}} I_n$ e $x \in A$, temos que $a \in I_k$ para todo $k \in \mathbb{N}$. Assim, $ax \in I_k$ para todo $k \in \mathbb{N}$. Logo ax pertence a $\bigcap_{n\epsilon\mathbb{N}} I_n$.

(ii) Se $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$, então $\bigcup_{n\epsilon\mathbb{N}} I_n$ é um ideal de A.

De fato, sejam a e $b \in \bigcup_{n\epsilon\mathbb{N}} I_n$. Segue que a pertence a algum I_j e b pertence a algum I_k com $i, j \in \mathbb{N}$.

Suponhamos sem perda de generalidade que $j \leq k$. Assim a, $b \in I_k$, logo $a + b \in I_k$ e portanto $a + b$ pertence a $\bigcup_{n\epsilon\mathbb{N}} I_n$.

Seja $a \in \bigcup_{n\epsilon\mathbb{N}} I_n$ e $x \in A$, temos que a pertence a algum I_k com $k \in \mathbb{N}$. Assim, $ax \in I_k$ com $k \in \mathbb{N}$, logo ax pertence a $\bigcup_{n\epsilon\mathbb{N}} I_n$.

Definição 14. Se um ideal I de um anel A é da forma $I(a)$ para algum $a \in A$, dizemos que I é um ideal principal.

Definição 15. Um *Domínio D* é dito *Domínio Principal* se todo *Ideal* de D é principal.

Exemplo 18. O domínio $\mathbb{Z}$, dos números inteiros, é um domínio principal.

De fato os subconjuntos que são ideais de $\mathbb{Z}$ são exatamente os conjuntos $I(m) = \{mk \mid k \epsilon Z\}$, onde $m \epsilon \mathbb{Z}$.

Proposição 11. *Sejam A um anel e a, b elementos de A. Se $d \epsilon A$ é tal que $I(a,b) = I(d)$, então d é um máximo divisor de a e b.*

Demonstração. Como $a, b \epsilon I(a,b) = I(d)$, segue que $a = k_1 d$ e $b = k_2 d$, com $k_1, k_2 \epsilon A$, donde $d \mid a$ e $d \mid b$. Suponhamos agora que c seja um divisor comum de a e b, logo $I(a,b) \subset I(c)$. Consequentemente $I(d) \subset I(c)$, daí $d = kc$ e portanto $c \mid d$. □

Corolário 2. *Sejam D um domínio principal e a, b elementos de D. Então existe o máximo divisor comum destes elementos e todo máximo divisor comum é da forma $na + mb$, com $n, m \epsilon D$.*

Demonstração. Sejam $a, b \epsilon D$. Como D é principal, segue que $I(a,b) = I(d)$, para algum $d \epsilon D$. Como $d \epsilon I(d) = I(a,b)$ segue que $d = ma + nb$ com $m, n \epsilon D$. □

Definição 16. Um elemento não nulo e não invertível de um anel é dito irredutível se os seus únicos divisores são os elementos invertíveis do anel e os seus próprios associados. Por exemplo, 2 é irredutível em $\mathbb{Z}$, pois seus divisores são

$$\pm 1 \text{ e } \pm 2.$$

Definição 17. Um domínio D é um *Domínio de fatoração única* (DFU), se todo elemento não nulo e não invertível de D se fatora como produto de um número finito de elementos irredutíveis. Além disso, tal fatoração é única a menos da ordem dos fatores e de elementos associados, isto é, se

$$p_1 \cdots p_r = q_1 \cdots q_s$$

onde $p_1, \ldots, p_r, q_1, \ldots, q_s$ são irredutíveis, então $r = s$ e após um reordenamento temos que p_i e q_i são associados para todo $i = 1, \ldots, r$.

Chamaremos um *Domínio de fatoração única* simplesmente de *Domínio Fatorial*.

Definição 18. Um elemento p não nulo e não invertível de um anel é dito primo se toda vez que p divide o produto de dois elementos de A, ele divide um dos fatores.

$p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.

Observamos que, se p é primo e $p \mid a_1 \cdots a_n$ então existe $1 \leq i \leq n$ tal que $p \mid a_i$, além disso todo associado de p também é primo.

Proposição 12. *Num domínio de integridade D, todo elemento primo é irredutível.*

Demonstração. Seja p um elemento primo de um domínio de integridade D. Suponha $a \epsilon D$ tal que $a \mid p$. Vamos provar que a é invertível ou a é um associado de p. Existe $b \epsilon D$, não nulo, tal que $p = ab$, logo $p \mid ab$ e como p é primo temos que $p \mid a$ ou $p \mid b$.

Suponhamos inicialmente que $p \mid a$. Como por hipótese $a \mid p$ segue que p e a são associados. Agora, suponhamos que $p \mid b$, segue que $b = pk$, com $k \epsilon D$. Temos que $p = ab \Rightarrow p = apk \Rightarrow p = pak$, pela lei do cancelamento, logo $1 = ak$, portanto a é invertível. □

Corolário 3. *Sejam $p, p_1, \ldots, p_n$ elementos primos de um domínio de integridade.*

Se $p \mid p_1 \cdots p_n$ então p é associado de p_i para algum $i = 1, \ldots, n$.

Demonstração. Suponhamos que $p \mid p_1 \cdots p_n$. Como p é primo, existe i tal que $p \mid p_i$. Pela proposição, p é irredutível, logo p e p_i são associados. □

Proposição 13. *Num domínio principal, todo elemento irredutível é primo.*

Demonstração. Seja p um elemento irredutível de um domínio principal D. Suponhamos que $p \mid ab$ e que $p \nmid a$. Temos que provar que $p \mid b$.

De fato, como D é principal, existe $c \epsilon D$ tal que $I(a,p) = I(c)$, logo $c \mid a$ e $c \mid p$. Como p é irredutível, temos que c é associado de p ou c é invertível. Mas c não é associado de p, caso contrario teríamos $p \mid c$, como $c \mid a$, teríamos que $p \mid a$, o que é uma contradição.

Temos portanto que c é invertível e consequentemente

$$I\left(a,p\right) = I\left(c\right) = D$$

Segue daí que existem elementos $m, n \epsilon D$ tais que

$$1 = n \cdot a + n \cdot p$$

Multiplicando a equação acima por b obtemos

$$b = n \cdot a \cdot b + n \cdot p \cdot b$$

Como $p \mid ab$, concluímos que $p \mid b$. □

Lema 5. *Num domínio principal D, toda cadeia ascendente de ideais*

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

é estacionária, isto é, existe um índice m tal que

$$I_m = I_{m+1} = \cdots$$

Demonstração. Como $\bigcup_{j\geq 1} I_j$ é um ideal de D e D é domínio principal, existe $a \epsilon D$ tal que

$$\bigcup_{j\geq 1} I_j = I\,(a)$$

Segue daí que $a \epsilon \bigcup_{j\geq 1} I_j$ e portanto $a \epsilon I_m$, para algum m. Segue que $a \epsilon I_n$ para todo $n \geq m$ e consequentemente

$I\,(a) \subset I_n$ para todo $n \geq m$. Como para todo n, temos que

$$I_n \subset \bigcup_{j\geq 1} I_j = I\,(a)$$

Concluímos que $I_n = I(a)$, para todo $n \geq m$. □

Lema 6. *Todo elemento não nulo e não invertível de um domínio principal possui pelos menos um fator irredutível.*

Demonstração. Sejam D um domínio principal e a um elemento de D não nulo e não invertível. Se a é irredutível, já temos que a é fator irredutível de a. Suponhamos agora que a é redutível, isto é, a tem um fator a_1 que não é invertível e nem associado de a. Segue que

$$I(a) \subsetneqq I(a_1) \subsetneqq D$$

onde $I(a) \neq I(a_1)$ pois a e a_1 não são associados e $I(a_1) \neq D$ pois a_1 não é invertível. Se a_1 é irredutível, o resultado é válido. Caso contrário, a_1 tem um fator a_2 que não é invertível e nem associado de a_1, logo

$$I(a) \subsetneqq I(a_1) \subsetneqq I(a_2) \subsetneqq D$$

Se não encontrarmos um fator irredutível de a, chegaremos numa cadeia infinita de ideais

$$I(a) \subsetneqq I(a_1) \subsetneqq \ldots \subsetneqq I\,(a_i) \ldots$$

o que não é possível, pelo lema demonstrado anteriormente. □

Teorema 6. *Se D é um Domínio Principal então D é um Domínio Fatorial.*

Demonstração. Sejam D um domínio principal e a um elemento não nulo e não invertível em D. Pelo lema anterior, o elemento a possui um fator irredutível p_1 e assim, existe $a_1 \epsilon D$ tal que $a = p_1 \cdot a_1$.

Se a_1 não é invertível, então ele também possui um fator irredutível $p_2 \epsilon D$, logo existe $a_2 \epsilon D$ tal que

$$a = p_1 \cdot a_1 = p_1 \cdot p_2 \cdot a_2$$

Assim sucessivamente,

$$a = p_1 \cdot a_1 = p_1 \cdot p_2 \cdots p_i a_i$$

Este procedimento tem que parar após um número finito de passos, isto é, para algum n temos que a_n é invertível. De fato, se nenhum dos $a_1, a_2, \ldots, ai, \ldots$ fosse invertível teríamos uma cadeia infinita de ideais

$$I(a) \subsetneqq I(a_1) \subsetneqq \ldots \subsetneqq I\,(a_i) \ldots$$

o que é uma contradição pelo lema demonstrado anteriormente.

Portanto, para algum n obtemos a_n invertível. Denotando $a_n = u$ temos que

$$a = p_1 \cdot \ldots \cdot p_n \cdot u$$

com $p_1, \ldots, p_n$ irredutíveis.

Provaremos a unicidade por indução sobre r.

Suponhamos que $r = 1$ e $p_1 = q_1.q_2 \cdot \ldots \cdot q_s$, com $p_1, q_1.q_2 \cdot \ldots \cdot q_s$ irredutíveis e portanto primos. Segue que $p_1 \mid q_1.q_2 \cdot \ldots \cdot q_s$, e pelo corolário 3 p_1 é associado a q_i, para

algum i. Após uma reordenação, se necessário, podemos supor $i = 1$ e assim $p_1 = u \cdot q_1$ com u invertível obtendo $p_1 = u \cdot p_1 \cdot q_2 \cdot \ldots \cdot q_s$.

Se $s > 1$, pela lei do cancelamento, obtemos $1 = u \cdot q_2 \cdot \ldots \cdot q_s$, o que é uma contradição.

Suponhamos a unicidade verdadeira para $r-1$ e consideremos $p_1.p_2 \cdot \ldots \cdot p_r = q_1.q_2 \cdot \ldots \cdot q_s$. Temos que $p_1/q_1.q_2 \cdot \ldots \cdot q_s$ e portanto é associado a algum q_i. Após uma reordenação, se necessário, podemos supor $i = 1$ e assim $p_1 = u \cdot q_1$ com u invertível obtendo $p_1.p_2 \cdot \ldots \cdot p_r = u \cdot p_1 \cdot q_2 \cdot \ldots \cdot q_s$. Pela lei do cancelamento, temos $p_2 \cdot \ldots \cdot p_r = (u.q_2) \cdot \ldots \cdot q_s$. Usando a hipótese de indução, podemos concluir que $r - 1 = s - 1$ e que $(uq_2) \cdot \ldots \cdot q_{s-1}$ pode ser ordenado de forma que p_i seja associado a q_i para $2 \leq i \leq r$. Portanto $r = s$ e após reordenação, p_i é associado a q_i para $1 \leq i \leq r$. □

Definição 19. Um *Domínio D* recebe o nome de *Domínio Euclidiano* se possui uma função $\varphi: D\backslash\{0\} \to \{0, 1, 2, 3, ...\}$ que satisfaz as seguintes propriedades:

1) $\forall a, b \in D$, $b \neq 0$, $\exists q, r \in D$, tais que

$a = bq + r$ com $\varphi(r) < \varphi(b)$ ou $r = 0$.

2) $\varphi(a) \leq \varphi(a, b)$, $\forall a, b \in D\backslash\{0\}$.

Denotaremos um domínio Euclidiano por (D, φ).

O algoritmo da divisão em $\mathbb{Z}$ nos diz que dados a e b números inteiros com $b \neq 0$, então existem únicos q e r, inteiros, tais que $a = bq + r, \quad 0 \leq r < |b|$. Domínio Euclidiano é uma generalização desta ideia. Para isto ocorrer, além das duas operações (adição e subtração) temos a função φ, usada para comparar os elementos de D.

Proposição 14. *Um elemento a de um domínio Euclidiano (D, φ) é invertível se, e somente se a é não nulo e $\varphi(ab) = \varphi(b)$, onde $b \in D$ e $b \neq 0$.*

Demonstração. Seja $a \in D$ invertível, isto é, $a \neq 0$, $a^{-1} \in D$ e $a \cdot a^{-1} = 1$. Assim $\varphi(b) = \varphi(baa^{-1}) \geq \varphi(ba) \geq \varphi(b)$, logo $\varphi(ab) = \varphi(b)$.

Reciprocamente, suponhamos $a \epsilon D$ não nulo e $\varphi(ab) = \varphi(b)$, onde $b \epsilon D$ e $b \neq 0$. Como D é domínio Euclidiano e $ab \neq 0$ existem $t, r \epsilon D$ tais que $b = (ab)t + r$ com $\varphi(r) < \varphi(ab)$ ou $r = 0$. Afirmamos que $r = 0$. De fato, se $r \neq 0$, como $r = b - (ab)t$ obtemos

$$\varphi(r) = \varphi(b(1 - at)) \geq \varphi(b)$$

o que é uma contradição. Segue que $b = (ab)t$, como $b \neq 0$ e D é um domínio, temos $1 = at$, logo a é invertível. □

Corolário 4. *Num domínio Euclidiano (D, φ) valem as seguintes afirmações:*

(i) $\{a \epsilon D : a$ é invertível$\} = \{a \epsilon D : \varphi(a) = \varphi(1)\}$

(ii) Dado $a \epsilon D$, $\{b \epsilon D : b$ é associado a $a\} \subset \{b \epsilon D : \varphi(b) = \varphi(a)\}$.

Demonstração. (i) $\varphi(a) = \varphi(a \cdot 1) = \varphi(1)$ equivale a dizer que a é invertível.

(ii) Se b é associado a a, isto é, $b = ua$, com u invertível, então $\varphi(b) = \varphi(ua) = \varphi(a)$. □

Teorema 7. *Se D é um Domínio Euclidiano então D é um Domínio Principal.*

Demonstração. Como D é um *Domínio Euclidiano*, existe $\varphi: D\backslash\{0\} \to \{0, 1, 2, 3, ...\}$ que satisfaz as seguintes propriedades:

1) $\forall a, b \epsilon D$, $b \neq 0$ $\exists q, r \epsilon D$, tais que

$a = b.q + r$ com $\varphi(r) < \varphi(b)$ ou $r = 0$.

2) $\varphi(a) \leq \varphi(ab)$, $\forall a, b \epsilon D\backslash\{0\}$.

Seja $I \neq 0$ um *Ideal* de D. Considere o conjunto $A = \{\varphi(t) \mid t \epsilon I\} \subset \{0, 1, 2, 3, ...\}$. Como $A \neq \varnothing$, pelo princípio da boa ordenação, A possui um menor elemento. Seja $a \epsilon I$, tal que $\varphi(a)$ seja o menor elemento de A. Vamos provar que $I = I(a)$. Como $a \epsilon I$, temos que $I(a) \subset I$.

Considere agora b um elemento qualquer de I. Como D é domínio euclidiano, existem q e $r \epsilon D$ tais que, $b = a \cdot q + r$ com $\varphi(r) < \varphi(a)$ ou $r = 0$. Observe que $a \cdot q \epsilon I$ e $a \cdot q \cdot (-1) = -a \cdot q$ também pertence a I. Logo, $b + (-a \cdot q) = r \epsilon I$ com $\varphi(r) < \varphi(a)$ ou $r = 0$.

Como $\varphi(a)$ é o menor elemento de A concluímos que $r = 0$ e assim $b+(-a.q) = 0 \Rightarrow b = a \cdot q$ ϵ $I(a)$. Portanto $I = I(a)$. □

Teorema 8. *Todo Domínio Euclidiano é Domínio Fatorial.*

Demonstração. Teoremas 6 e 7. □

4.2 Os Anéis $\mathbb{Z}_m$

Definição 20. Seja $m > 1$ um inteiro. Dizemos que dois inteiros a e b são congruentes módulo m, se a e b deixam o mesmo resto quando divididos por m. Se a e b são congruentes módulo m, escrevemos $a \equiv b \ mod \ m$.

Proposição 15. *Tem-se que a e b são congruentes módulo m se, e somente se $m \mid a - b$.*

Demonstração. De fato, segue da definição que $a = mq_1 + r$ e $b = mq_2 + r$, assim $a - b = m(q_1 - q_2)$. Portanto $m \mid a - b$.

Por outro lado, considere $a = mq_1 + r_1$ e $b = mq_2 + r_2$ com $0 \leq r_1, r_2 < m$. Como $a-b = m(q_1 - q_2)+(r_1 - r_2)$ e $m \mid a-b$, temos que m divide $\mid r_1-r_2 \mid < m$. Logo $r_1-r_2 = 0$, ou seja, $r_1 = r_2$. □

Proposição 16. *(Propriedades da Congruência) Para todos a, b, c, d, m e $n \epsilon \mathbb{Z}$, com $n \geq 0$ e $m > 1$, valem as seguintes propriedades:*

(1) $a \equiv a \ mod \ m$;

(2) Se $a \equiv b \ mod \ m$, então $b \equiv a \ mod \ m$;

(3) Se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, então $a \equiv c \ mod \ m$;

(4) Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $a + c \equiv b + d \ mod \ m$;

(5) Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $ac \equiv bd \ mod \ m$;

(6) Se $a \equiv b \ mod \ m$, então $a^n \equiv b^n \ mod \ m$.

Demonstração. (1) Temos que $m \cdot 0 = 0 = a - a$, logo $m \mid a - a$. Portanto $a \equiv a \ mod \ m$.

(2) Como $a \equiv b \; mod \; m$, temos que $m \mid a - b$. Assim, existe k tal que $mk = a - b \Rightarrow m \cdot (-k) = b - a$. Logo $m \mid b - a$. Portanto $b \equiv a \; mod \; m$.

(3) Como $a \equiv b \; mod \; m$ e $b \equiv c \; mod \; m$, temos que $m \mid a - b$ e $m \mid b - c$. Assim, existem k_1 e k_2 tais que $mk_1 = a - b$ e $mk_2 = b - c$. Somando as duas equações, temos $m\,(k_1 + k_2) = a - c$. Logo, $m \mid a - c$. Portanto $a \equiv c \; mod \; m$.

(4) Como $a \equiv b \; mod \; m$ e $c \equiv d \; mod \; m$, temos que $m \mid a - b$ e $m \mid c - d$. Assim, existem k_1 e k_2 tais que $mk_1 = a - b$ e $mk_2 = c - d$. Somando as duas equações, temos $m\,(k_1 + k_2) = (a + c) - (b + d)$. Logo $m \mid (a + c) - (b + d)$. Portanto $a + c \equiv b + d \; mod \; m$.

(5) Como $a \equiv b \; mod \; m$ e $c \equiv d \; mod \; m$, temos que $m \mid a - b$ e $m \mid c - d$. Segue que, existem k_1 e k_2 tais que $mk_1 = a - b$ e $mk_2 = c - d$. Multiplicando as duas equações, temos $m\,(mk_1k_2) = ac - ad - bc + bd \Rightarrow ac - bd + bd - ad + bd - bc \Rightarrow ac - bd + d\,(b - a) + b\,(d - c)$. Assim, existem k_3 e k_4 tais que $m\,(mk_1k_2) = ac - bd + mk_3 + mk_4 \Rightarrow m\,(mk_1k_2 - k_3 - k_4) = ac - bd$. Logo, $m \mid ac - bd$. Portanto, $ac \equiv bd \; mod \; m$.

(6) $n = 1$, válida trivialmente.

Suponhamos $a^n \equiv b^n$ válida, como $a \equiv b$, por (5) temos $a^n a \equiv b^n b$, logo $a^{n+1} \equiv b^{n+1}$. □

Segue das propriedades (1), (2) e (3) que a congruência modulo m define uma relação de equivalência em $\mathbb{Z}$.

Definição 21. Dado $a \in \mathbb{Z}$, a classe de equivalência de a, denotada por $\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a\}$, chama-se classe residual do elemento a módulo m.

Como a relação de congruência módulo m é uma relação de equivalência, são válidas as seguintes propriedades:

1) $\overline{a} \neq \varnothing$, $\forall \; a \in \mathbb{Z}$.

2) $a \equiv b \; mod \; m \iff \overline{a} = \overline{b}$.

3) $\overline{a} \cap \overline{b} \neq \varnothing \Rightarrow \overline{a} = \overline{b}$.

4) $\bigcup\limits_{a \in \mathbb{Z}} \overline{a} = \mathbb{Z}$.

Proposição 17. *Existem exatamente m classes residuais módulo m distintas, a saber:* $\overline{0}, \overline{1}, \ldots, \overline{m-1}$.

Demonstração. Observe que os elementos do conjunto $A = \{0, 1, \ldots, m-1\}$ não são congruentes entre si módulo m, pois na divisão por m, eles mesmos são os restos.

Considere $n \in \mathbb{Z}$, tal que $n \geq m$, pelo algoritmo da divisão, temos que $\exists q, r$ tais que $n = mq + r$, com $0 \leq r < m$. Logo n é congruente a $r \in A$. Portanto existem exatamente m classes residuais módulo m distintas: $\overline{0}, \overline{1}, \ldots, \overline{m-1}$. □

Definição 22. O conjunto de todas as classes residuais módulo m chama-se conjunto dos inteiros módulo m e é denotado por $\mathbb{Z}_m$.

Em $\mathbb{Z}_m$, definimos duas operações :

Adição: $\overline{a_1} + \overline{a_2} = \overline{a_1 + a_2}$

Multiplicação: $\overline{a_1} \cdot \overline{a_2} = \overline{a_1 \cdot a_2}$

Segue das propriedades (4) e (5) de congruência que estas operações estão bem definidas.

Proposição 18. *O conjunto $\mathbb{Z}_m$, munido das operações de adição e multiplicação tem uma estrutura de Anel.*

Demonstração. As propriedades associativa e comutativa da adição e multiplicação, assim como a propriedade distributiva são herdadas das propriedades de $\mathbb{Z}$. Por exemplo,

$$\overline{a_1} + \overline{a_2} = \overline{a_1 + a_2} = \overline{a_2 + a_1} = \overline{a_2} + \overline{a_1}$$

O elemento neutro da adição é o $\overline{0}$. O elemento oposto de cada elemento $\overline{a}$ é o elemento $\overline{-a}$. O elemento unidade da multiplicação é o elemento $\overline{1}$. □

Proposição 19. *Seja $\overline{a} \in \mathbb{Z}_m$. Então $\overline{a} \neq \overline{0}$ é invertível se, e somente se, $mdc(a, m) = 1$.*

Demonstração. ($\Rightarrow$) $\exists \overline{b} \in \mathbb{Z}_m$ tal que $\overline{ab} = \overline{1}$, assim $ab \equiv 1 \; mod \; m \Rightarrow m \mid ab-1 \Rightarrow ab-1 = mk$ (1) com k inteiro. Seja d, tal que $d \mid a$ e $d \mid m$, de (1) temos que $d \mid 1$. Logo $mdc(a, m) = 1$.

($\Leftarrow$) Como $mdc(a,m) = 1$, temos que $\exists r, s \,\epsilon\, \mathbb{Z}$, tais que $ra + sm = 1 \Rightarrow ra + sm \equiv 1 \; mod \; m \Rightarrow ra \equiv 1 \; mod \; m$. Logo, $\overline{ra} = \overline{1}$, isto é, $\overline{r} \cdot \overline{a} = \overline{1}$. Portanto a é invertível. □

Proposição 20. *O anel $\mathbb{Z}_m$ é um corpo se, e somente se, m é um número primo.*

Demonstração. ($\Rightarrow$) Como $\mathbb{Z}_m$ é corpo, todos os seus elementos não nulos são invertíveis, pela proposição 19, temos que o máximo divisor comum entre m e qualquer elemento de $A = \{1, \ldots, m-1\}$ é 1, ou seja, não existe número menor que m que o divida, a não ser o 1, logo m é primo.

($\Leftarrow$) Como m é primo, para todo $a \,\epsilon\, A = \{1, \ldots, m-1\}$, temos $mdc\,(a,m) = 1$, pela proposição 19, concluímos que $\overline{a}$ é invertível. Portanto $\mathbb{Z}_m$ é um corpo. □

4.3 O anel dos Polinômios K[x]

Definição 23. Seja K um corpo. Chamamos de polinômio sobre K em uma indeterminada x a uma expressão formal

$$a_0 + a_1 x + \cdots + a_n x^n + \cdots$$

onde $a_k \,\epsilon\, A$, $\forall k \geq 0$, e existe $m \geq 0$ tal que $a_j = 0$ para $j > m$.

Dizemos que dois polinômios $p(x) = a_0 + a_1 x + \cdots + a_m x^m + \ldots$ e $q(x) = a_0 + b_1 x + \cdots + b_m x^m + \ldots$ são iguais se, e somente se $a_i = b_i$ para todo $i \geq 0$.

O polinômio $p(x) = 0 + 0x + \cdots + 0x^m + \cdots$ onde $a_i = 0$ para todo $i \geq 0$, será indicado por $p(x) = 0$ (polinômio nulo) e o polinômio $p(x) = a + 0x + \cdots + 0x^m + \cdots$, onde $a_i = 0$ para todo $i > 0$, por $p(x) = a$ (polinômio constante).

Vamos denotar por $K[x]$ o conjunto de todos os polinômios sobre K, em uma indeterminada x.

Definição 24. Se $p(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ é tal que $a_n \neq 0$ e $a_j = 0$ para todo $j > n$, dizemos que a_n é o coeficiente líder de $p(x)$, n é o grau do polinômio $p(x)$, e nesse caso, escrevemos

$p(x) = a_0 + a_1x + \cdots + a_nx^n$ e o grau de $p(x)$ por $\delta p(x) = n$.

Agora vamos definir operações soma e produto no conjunto $K[x]$. Sejam $f(x) = a_0 + a_1x + \cdots + a_rx^r + \cdots$ e $g(x) = b_0 + b_1x + \cdots + b_sx^s + \cdots$ dois elementos de $K[x]$.

Definimos a soma como

$f(x) + g(x) = c_0 + c_1x + \cdots + c_kx^k + \cdots$, onde $c_i = (a_i + b_i) \epsilon K$

e o produto como

$f(x) \cdot g(x) = c_0 + c_1x + \cdots + c_kx^k + \ldots$, onde $c_0 = a_0 \cdot b_0$, $c_1 = a_0 \cdot b_1 + a_1 \cdot b_0$, $c_2 = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0$,..., $c_k = a_0 \cdot b_k + a_1 \cdot b_{k-1} + \cdots + a_k \cdot b_0$, ...

Proposição 21. *(i) Sejam $f(x)$ e $g(x)$ polinômios não nulos de $K[x]$, tais que $f(x)+g(x)$ também é não nulo. Então*

$$\delta(f(x) + g(x)) \leq máx\{\delta f(x), \delta g(x)\}$$

.

(ii) Sejam $f(x)$ e $g(x)$ polinômios não nulos de $K[x]$. Então $f(x) \cdot g(x)$ também é não nulo e

$$\delta(f(x) \cdot g(x)) = \delta f(x) + \delta g(x)$$

.

Demonstração. (i) Suponhamos $\delta f(x) = r$, $\delta g(x) = s$ e, sem perda de generalidade, $r \leq s$. Daí, com as notações dadas acima, $f(x)+g(x) = (a_0 + b_0)+(a_1 + b_1)x+\cdots+(a_s + b_s)x^s + 0x^{s+1} + 0x^{s+2} + \cdots$, portanto

$\delta(f(x) + g(x)) \leq s = máx\{r, s\} = máx\{\delta f(x), \delta g(x)\}$.

(ii) Suponhamos $\delta f(x) = r$ e $\delta g(x) = s$.

Daí, $f(x) \cdot g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \ldots + a_r b_s x^{r+s} + 0x^{r+s+1} + 0x^{r+s+2} + \ldots$

Como $a_r \neq 0$ e $b_s \neq 0$, temos que $a_r . b_s \neq 0$. Assim, $f(x) g(x)$ é não nulo e

$$\delta(f(x) \cdot g(x)) = r + s = \delta f(x) + \delta g(x).$$

□

Proposição 22. *O conjunto $K[x]$ com as operações soma e produto é um domínio.*

Demonstração. As propriedades associativa e comutativa da adição e multiplicação, assim como a propriedade distributiva são herdadas das propriedades de K. Por exemplo,

$f(x).g(x) = (a_0 + \cdots + a_s x^s).(b_0 + \cdots + b_r x^r) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \cdots +$ $(a_0 b_{s+r} + \cdots + a_{s+r} b_0) x^{s+r} =$

$b_0 a_0 + (b_0 a_1 + b_1 a_0) x + \cdots + (b_0 a_{s+r} + \cdots + b_{s+r} a_0) x^{s+r} = (b_0 + \cdots + b_r x^r).(a_0 + \cdots + a_s x^s) =$ $g(x).f(x)$.

O elemento neutro da adição é o $0 = 0 + 0x + \cdots + 0x^m + \cdots$, onde $a_i = 0$ para todo $i \geq 0$. O elemento oposto de cada elemento $a_0 + \cdots + a_s x^s$ é o elemento $(-a_0) + \cdots + (-a_s) x^s$. O elemento unidade da multiplicação é o elemento $1 = 1 + 0x + \cdots + 0x^m + \cdots$, onde $a_i = 0$ para todo $i > 0$.

Além disso, dados $f(x), g(x)$ ambos não nulos pertencentes a $K[x]$, temos que pela parte (ii) da proposição 21 que $f(x) g(x)$ também é não nulo. Portanto $K[x]$ é um domínio. □

Observe que os únicos elementos invertíveis de $K[x]$ são os polinômios constantes não nulos. De fato, se $f(x)g(x) = 1$ então $\delta f(x) + \delta g(x) = 0$ e assim $f(x) = a_0$ e $g(x) = b_0 = a_0^{-1}$.

Proposição 23. *Se K é um corpo então $K[x]$ é um Domínio Euclidiano.*

Demonstração. Primeiramente, consideremos a função φ:$K[x]\backslash\{0\}\rightarrow\mathbb{N}\cup\{0\}$, definida por

$\varphi(p(x))$ = grau de $p(x)$.

Sejam dois polinômios $f(x) = a_0 + \cdots + a_n x^n$ e $g(x) = b_0 + \ldots + b_m x^m$ com $g(x) \neq 0$ e $\delta g(x) = m$. Vamos mostrar que existem únicos $q(x)$ e $r(x)\ \epsilon\ K[x]$, tais que

$$f(x) = q(x) \cdot g(x) + r(x)$$

com $\delta r(x) < \delta g(x)$ ou $r(x) = 0$.

Existência: Se $f(x) = 0$ ou se $\delta a(x) < \delta b(x)$, tomamos $q(x) = 0$ e $r(x) = f(x)$.

Vamos demonstrar a afirmação por indução completa (segunda forma) sobre n, o grau de $f(x)$, onde $n \geq m$.

Se $n = 0$ então, $m = 0$, $f(x) = a_0 \neq 0$, $g(x) = b_0 \neq 0$ e temos que $f(x) = a_0 b_0^{-1} g(x)$. Assim, basta tomar $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$.

Consideremos o polinômio $f_1(x)$ definido por $f(x) = a_n b_m^{-1} x^{n-m} g(x) + f_1(x)$. Observamos que $\delta f_1(x) < \delta f(x)$.

Temos que $f_1(x) = f(x) - a^n b_m^{-1} x^{n-m} g(x)$ e pela hipótese de indução, existem $q_1(x)$, $r_1(x)$ tais que

$$f_1(x) = q_1(x) g(x) + r_1(x)$$

onde $r_1(x) = 0$ ou $\delta r_1(x) < \delta g(x)$.

Daí, segue que

$$f(x) = (q_1(x) + a^n b_m^{-1} x^{n-n}) g(x) + r_1(x)$$

onde $r_1(x) = 0$ ou $\delta r_1(x) < \delta g(x)$. Portanto, tomando $q(x) = q_1(x) + a^n b_m^{-1} x^{n-n}$ e $r(x) = r_1(x)$ temos a afirmação válida para n.

Unicidade: Suponhamos $f(x) = q_1(x) \cdot g(x) + r_1(x) = f(x) = q_2(x) \cdot g(x) + r_2(x)$ nas condições exigidas.

Daí, $g(x) \cdot (q_1(x) - q_2(x)) = r_2(x) - r_1(x)$.

Mas, se $q_1(x) - q_2(x) \neq 0$ o grau do polinômio da esquerda, da igualdade anterior, é maior do que ou igual a $\delta g(x)$ enquanto que o grau do polinômio da direita $r_2(x) - r_1(x)$ é menor do que $\delta g(x)$, o que é uma contradição. Portanto, $q_1(x) = q_2(x)$ e consequentemente $r_1(x) = r_2(x)$.

Finalmente, observamos que $\delta(f(x) \cdot g(x)) = \delta f(x) + \delta g(x) \geq \delta f(x)$, quaisquer que sejam $f(x)$, $g(x)$ pertencentes a $K[x] \setminus \{0\}$.

Portanto $(K[x], \delta)$ é um *Domínio Euclidiano*. □

Corolário 5. *$K[x]$ é Domínio Principal.*

Corolário 6. *$K[x]$ é Domínio fatorial.*

Vimos anteriormente que os elementos invertíveis de um domínio Euclidiano (D, φ) são os elementos $a \in D \setminus \{0\}$ tais que $\varphi(a) = \varphi(1)$.

Aplicando em $K[x]$, que temos $f(x) \neq 0$ é invertível se, e somente se $\delta f(x) = \delta(1) = 0$, obtendo novamente que os invertíveis de $K[x]$ são os polinômios constantes não nulos.

Definição 25. Se $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ é um polinômio não nulo em $K[x]$ e $\alpha \in K$ é tal que $f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0 \in K$, dizemos que α é uma raiz de $f(x)$ em K.

Lema 7. *Sejam K um Corpo, $f(x)$ um polinômio de $K[x]$. Um elemento α de K é uma raiz do polinômio $f(x)$ se, e somente se, $f(x) = (x - \alpha)q(x)$ com $q(x) \in K[x]$.*

Demonstração. ($\Rightarrow$) Como $K[x]$ é um *Domínio Euclidiano*, existem $q(x)$, $r(x) \in K[x]$ tais que $f(x) = (x - \alpha) \cdot q(x) + r(x)$, com $\delta r(x) < \delta(x - \alpha)$ ou $r(x) = 0$, assim $r(x) = k$ com k

constante $\epsilon\ K/\{0\}$ ou $r(x) = 0$. Temos que $f(\alpha) = (\alpha - \alpha) \cdot q(\alpha) + r(\alpha)$, logo $r(\alpha) = 0$, e assim $r(x) = 0$. Portanto, $f(x) = (x - \alpha) \cdot q(x)$ com $q(x)\ \epsilon\ K[x]$.

($\Leftarrow$) Temos que $f(x) = (x - \alpha) \cdot q(x) \Rightarrow f(\alpha) = (\alpha - \alpha) \cdot q(\alpha) = 0 \cdot q(\alpha) = 0$. □

Proposição 24. *Sejam K um Corpo, $f(x)$ um polinômio não nulo de $K[x]$ de grau n. Então o número de raízes de $f(x)$ em K é no máximo igual ao $\delta f(x) = n$.*

Demonstração. Vamos provar usando indução sobre n.

Para $n = 0$, temos que $f(x) = a_0$, com $a_0 \neq 0$, logo $f(x)$ não possui raízes em K.

Para $n = 1$, temos que $f(x) = a_0 + a_1 x$, com $a_1 \neq 0$ e neste caso, $f(x)$ tem uma única raiz dada por $\alpha = -a_0 a_1^{-1}$.

Portanto, para $n = 0,\ 1$ a proposição é verdadeira.

Considere agora $f(x)$ um polinômio de grau n.

Se $f(x)$ não possui raízes em K, a proposição é verdadeira.

Suponhamos então que α seja raiz de $f(x)$. Segue do lema que $f(x) = (x-\alpha)q(x)$, com $q(x)\ \epsilon\ K[x]$.

Neste caso temos que $\delta q(x) = n - 1 < \delta f(x)$, e por indução, $q(x)$ possui no máximo $\delta q(x) = n - 1$ raízes em K.

Para $\beta\ \epsilon\ K$ temos que, $f(\beta) = 0$ se, e somente se, $\beta = \alpha$ ou $q(\beta) = 0$, logo as raízes de $f(x)$ são α e as raízes de $q(x)$. Portanto $f(x)$ possui no máximo n raízes. □

4.4 O Anel $\mathbb{Z}[i]$

Definição 26. Um inteiro Gaussiano é um número complexo da forma $a + bi$ com a e b inteiros.

O subconjunto do corpo $\mathbb{C}$, dos números complexos, formado pelos inteiros Gaussianos será denotado por $\mathbb{Z}[i]$.

Proposição 25. *O conjunto dos inteiros Gaussianos, $\mathbb{Z}[i]$, com as operações usuais de números complexos é um Domínio.*

Demonstração. Primeiramente, observamos que $\mathbb{Z}[i]$ é fechado em relação a adição e a multiplicação, pois dados $a+bi$ e $c+di$ pertencentes a $\mathbb{Z}[i]$, temos que $(a+bi)+(c+di) = (a+c)+(b+d)\,i$ e $(a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)\,i$ continuam em $\mathbb{Z}[i]$.

As propriedades associativa e comutativa da adição e multiplicação, assim como a propriedade distributiva são herdadas de $\mathbb{C}$.

O elemento neutro da adição é $0 = 0+0i$. O elemento oposto de cada elemento $a+bi$ é o elemento $-a-bi$. O elemento unidade da multiplicação é o elemento $1 = 1+0i$.

Além disso, como $\mathbb{Z}[i] \subset \mathbb{C}$ e $\mathbb{C}$ é corpo, temos que dados $a+bi \neq 0$ e $c+di \neq 0$ em $\mathbb{Z}[i]$ então $(a+bi)(c+di) \neq 0$.

Portanto $\mathbb{Z}[i]$ é um *Domínio*. □

Definição 27. Definimos a função norma $N : \mathbb{C} \to \mathbb{R}$,

$$N(a+bi) = a^2+b^2$$

Proposição 26. *Seja a função norma* $N : \mathbb{C} \to \mathbb{R}$, *temos que* $N((a+bi)\cdot(c+di)) = N(a+bi)\cdot N(c+di)$.

Demonstração. De fato, $N((a+bi)\cdot(c+di)) = N((ac-bd)+(bc+ad)\,i) = (ac-bd)^2 + (bc+ad)^2 = a^2c^2 - 2acbd + b^2d^2 + b^2c^2 + 2acbd + a^2d^2 =$

$$a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = (a^2+b^2)\cdot(c^2+d^2) = N(a+bi)\cdot N(c+di).$$ □

Corolário 7. *Se* $\alpha \mid \beta$ *em* $\mathbb{Z}[i]$ *então* $N(\alpha) \mid N(\beta)$.

Demonstração. Temos que existe γ em $\mathbb{Z}[i]$ tal que $\alpha\gamma = \beta$. Assim $N(\alpha\gamma) = N(\beta)$ e portanto $N(\alpha)\,N(\gamma) = N(\beta)$. Logo, $N(\alpha) \mid N(\beta)$. □

Corolário 8. *Seja* $\alpha \in \mathbb{Z}[i]$. *As seguintes afirmações são equivalentes:*

(i) α *é invertível em* $\mathbb{Z}[i]$

(ii) $N(\alpha) = 1$

(iii) $\alpha \in \{1, -1, i, -i\}$

Demonstração. (i)⇒(ii) Temos que $\exists\ \beta \in \mathbb{Z}[i]$ tal que $\alpha\beta = 1$, assim $N(\alpha\beta) = N(1)$, logo $N(\alpha)N(\beta) = 1$, e portanto $N(\alpha) = 1$.

(ii)⇒(iii) Considerando $\alpha = a + bi \in \mathbb{Z}[i]$, temos que $N(\alpha) = a^2 + b^2 = 1$, assim $a^2 = 0$ e $b^2 = 1$ ou $a^2 = 1$ e $b^2 = 0$, logo $\alpha \in \{1, -1, i, -i\}$.

(iii)⇒(i) Imediato. □

Proposição 27. *Seja $\alpha \in \mathbb{Z}[i]$. Se a norma de α é primo em $\mathbb{Z}$ então α é primo em $\mathbb{Z}[i]$.*

Demonstração. Suponhamos por contradição α composto em $\mathbb{Z}[i]$, assim $\alpha = (a + bi)(c + di)$ com $N(a + bi) \neq 1$ e $N(c + di) \neq 1$, segue que $N((a + bi)(c + di)) = N(\alpha)$, logo

$$N(a + bi)\,N(c + di) = N(\alpha).$$

Portanto $N(\alpha)$ é composto em $\mathbb{Z}$, o que é uma contradição. □

Proposição 28. *O conjunto $Z[i]$ munido das operações definidas anteriormente é um Domínio Euclidiano.*

Demonstração. Considere a função $N : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N} \cup \{0\}$, restrição da função norma aos inteiros Gaussianos não nulos, isto é, $N(a + bi) = a^2 + b^2$, para todo $a + bi \in \mathbb{Z}[i] \setminus \{0\}$.

Sejam $x = a + bi$ e $y = c + di$ pertencentes a $Z[i]$ com $y \neq 0$, vamos mostrar que existem q e $r \in Z[i]$, tais que $x = y.q + r$, com $N(r) < N(y)$.

Devemos achar $q = g + hi$ tal que $N(x - y \cdot q) < N(y)$. Temos que

$N(x - y \cdot q) < N(y) \iff N\left(y \cdot \left(\frac{x}{y} - q\right)\right) < N(y) \iff N(y) \cdot N\left(\frac{x}{y} - q\right) < N(y) \iff N\left(\frac{x}{y} - q\right) < 1$.

Como $\frac{x}{y} = (a + bi) \cdot (c + di)^{-1} = (a + bi) \cdot \left(\frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}i\right) = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$. Tomando $\frac{ac+bd}{c^2+d^2} = e$ e $\frac{bc-ad}{c^2+d^2} = f$, temos

$N\left(\frac{x}{y} - q\right) < 1 \iff (e - g)^2 + (f - h)^2 < 1$.

Assim, basta tomarmos $q = g + hi \in Z[i]$, tal que $|e - g| \leq \frac{1}{2}$ e $|f - h| \leq \frac{1}{2}$ (observação no final da demonstração), pois assim teremos

$$(e-g)^2 + (f-h)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

Além disso, observamos que $\forall\ x = a + bi \in Z[i] \setminus \{0\}$, $N(x) = a^2 + b^2 \geq 1$. Logo $\forall\ y \in Z[i] \setminus \{0\}$, temos que $N(x) \cdot N(y) \geq N(y) \Rightarrow N(x \cdot y) \geq N(y)$.

Portanto $Z[i]$ é um *Domínio Euclidiano*. □

Observação 10. Dado um racional c, existe um número inteiro no intervalo $(c, c+1]$.

De fato, suponhamos $c = \frac{m}{n}$ com $m \in \mathbb{Z}$ e $n \neq 0$. Considerando a divisão euclidiana de m por n temos

$m = nq + r$ com $r = 0$ ou $0 \leq r < n$.

Segue que $\frac{m}{n} = q + \frac{r}{n}$, logo $q = \frac{m}{n} - \frac{r}{n}$ com $0 \leq \frac{r}{n} < 1$.

Daí $0 < q + 1 - c = 1 - \frac{r}{n} \leq 1$, portanto $c < q + 1 \leq 1 + c$.

Exemplo 19. Considerando $x = 2+3i$ e $y = 1-i$, vamos determinar os possíveis quocientes de x por y (usando as notações da proposição 27).

Indicando $q = g + hi$, temos

$$\frac{x}{y} = \frac{2+3i}{1-i} = \frac{(2+3i)(1+i)}{2} = \frac{-1+5i}{2} = -\frac{1}{2} + \frac{5}{2}i \ (e = -\frac{1}{2},\ f = \frac{5}{2})$$

$| g - e | \leq \frac{1}{2}$ e $| h - f | \leq \frac{1}{2}$

$\left| g + \frac{1}{2} \right| \leq \frac{1}{2} \Longleftrightarrow -\frac{1}{2} \leq g + \frac{1}{2} \leq \frac{1}{2} \Longleftrightarrow -1 \leq g \leq 0$

$\left| h - \frac{5}{2} \right| \leq \frac{1}{2} \Longleftrightarrow -\frac{1}{2} \leq h - \frac{5}{2} \leq \frac{1}{2} \Longleftrightarrow 2 \leq h \leq 3$

logo $g = -1$ ou 0 e $h = 2$ ou 3. Portanto, temos 4 possibilidades para o quociente q: $-1 + 2i$, $-1 + 3i$, $2i$ ou $3i$.

Capítulo 5

Naturais como soma de dois quadrados

Neste capítulo, usando a estrutura algébrica dos inteiros Gaussianos, faremos novamente a caracterização de primos escritos como soma de dois quadrados.

5.1 Primo como soma de dois quadrados: caracterização em $\mathbb{Z}[i]$

Agora reunimos base suficiente para a demonstração do teorema seguinte, o qual estabelece uma caracterização de primos como soma de dois quadrados.

Antes de enunciar o teorema lembraremos alguns resultados estudados.

• Se p é primo, então $\mathbb{Z}_p = \left\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\right\}$ tem uma estrutura de corpo.

• Se p é primo então, o domínio dos polinômios com coeficientes em $\mathbb{Z}_p$, $\mathbb{Z}_p[x]$, é um domínio Euclidiano, portanto também é domínio principal e domínio de fatoração única.

• O domínio $\mathbb{Z}[i]$ é domínio euclidiano, portanto também é domínio principal e domínio de fatoração única.

• Num domínio Euclidiano (D, φ), os elementos invertíveis são os elementos que possuem norma igual à norma do elemento $1 \, \epsilon \, D$.

• Num domínio Principal, um elemento p é primo se, e somente se, p é irredutível.

Teorema 9. *(Fermat) Seja p um primo. As afirmações a seguir são equivalentes:*

(i)$p = 2$ ou p é da forma $4k + 1$ com k natural.

(ii)Existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \ mod \ p$.

(iii)p não é irredutível em $\mathbb{Z}[i]$.

(iv)p é soma de dois quadrados.

Demonstração. $(i) \Rightarrow (ii)$ Se $p = 2$, temos $1^2 \equiv -1 \ mod \ p$.

Seja $p = 4k + 1$ com k natural. Considere o polinômio $x^{p-1} - \overline{1}$ de $\mathbb{Z}_p[x]$. Pelo pequeno teorema de Fermat, se $mdc(a, p) = 1$, então $a^{p-1} \equiv 1 \ mod \ p$, ou equivalentemente, $\overline{a}^{p-1} = \overline{1}$. Segue daí que, para todo $a \in \{1, 2, 3, \ldots, p-1\}$ temos $\overline{a}^{p-1} - \overline{1} = 0$, ou seja $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ são raízes do polinômio $x^{p-1} - 1$.

Como $(p-1)$ é o grau do polinômio $x^{p-1} - 1$, não temos outras raízes e o polinômio se fatora como

$$x^{p-1} - \overline{1} = \left(x - \overline{1}\right) \cdot \left(x - \overline{2}\right) \cdot \ldots \cdot \left(x - \overline{p-1}\right)$$

Por outro lado, como $p - 1 = 4k$, temos que

$$x^{p-1} - \overline{1} = x^{4k} - \overline{1} = \left(x^{2k} - \overline{1}\right) \cdot \left(x^{2k} + \overline{1}\right)$$

e assim

$$\left(x - \overline{1}\right) \cdot \left(x - \overline{2}\right) \cdot \ldots \cdot \left(x - \overline{p-1}\right) = \left(x^{2k} - \overline{1}\right) \cdot \left(x^{2k} + \overline{1}\right)$$

.

Como $\mathbb{Z}_p[x]$ é domínio de fatoração única, segue que existe a, $1 \leq a \leq (p-1)$, tal que $\overline{a}^{2k} + \overline{1} = 0$, portanto existe a, $1 \leq a \leq (p-1)$ tal que $a^{2k} = \left(a^k\right)^2 \equiv -1 \ mod \ p$, como queríamos demonstrar.

$(ii) \Rightarrow (iii)$ Temos que existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \ mod \ p$, ou equivalentemente $p \mid a^2 + 1 = (a + i) \cdot (a - i)$.

Observamos que $p \nmid (a+i)$ em $Z[i]$, caso contrário teríamos $a+i = p(c+di)$ e daí $p.d = 1$, o que é uma contradição.

Analogamente $p \nmid (a-i)$ em $Z[i]$, caso contrário teríamos $a-i = p(c+di)$ e daí $p.d = -1$, o que é uma contradição.

Assim temos que p (não nulo e não invertível em $\mathbb{Z}[i]$) não é primo em $\mathbb{Z}[i]$, portanto p não é irredutível em $\mathbb{Z}[i]$.

$(iii) \Rightarrow (iv)$ Temos que $p = (a+bi) \cdot (c+di)$, com $a+bi$ e $c+di \; \epsilon \; \mathbb{Z}[i]$ não invertíveis. Segue que $N(a+bi) = a^2+b^2 \neq 1$ e $N(c+di) = c^2+d^2 \neq 1$.

Além disso, temos que $N(p) = p^2 = N((a+bi) \cdot (c+di)) = N(a+bi) \cdot N(c+di) = (a^2+b^2) \cdot (c^2+d^2)$. Como p é primo em $\mathbb{Z}$, concluímos que $p = a^2+b^2 = c^2+d^2$, portanto soma de dois quadrados.

$(iv) \Rightarrow (i)$Proposição 6. □

Assim, provamos que um primo $p \; \epsilon \; \mathbb{Z}$ é soma de dois quadrados se, e somente se, p não é irredutível em $\mathbb{Z}[i]$ e, usando a estrutura algébrica de $\mathbb{Z}[i]$, chegamos ao resultado desejado.

5.2 Ternos pitagóricos

Usando a estrutura de $\mathbb{Z}[i]$, domínio Euclidiano formado pelos inteiros Gaussianos, vamos dar uma outra prova da caracterização dos ternos Pitagóricos.

Lembramos que os únicos elementos invertíveis de $\mathbb{Z}[i]$ são $1, -1, i$ e $-i$. Assim, dado um elemento não nulo $z = a+bi \; \epsilon \; \mathbb{Z}[i]$, seus associados são $a+bi, -a-bi, -b+ai$, e $b-ai$.

Note que um e somente um dos quatro associados z' de $a+bi$ é tal que a parte real é positiva e a parte imaginária é não negativa: $Real(z') > 0$ e $Im(z') \geq 0$.

Dados $\alpha, \beta \; \epsilon \; \mathbb{Z}[i]$ não ambos nulos, vamos denotar por $mdc(\alpha, \beta)$, o máximo divisor comum, d, de α e β tal que $Real(d) > 0$ e $Im(d) \geq 0$.

Lema 8. *Sejam x e y inteiros primos entre si, então*

$$mdc\,(x+yi, x-yi) = \begin{cases} 1, & se \quad x^2+y^2 \quad é \quad ímpar \\ 1+i, & se \quad x^2+y^2 \quad é \quad par \end{cases}$$

Demonstração. Temos que x e y são primos entre si em $\mathbb{Z}$, isto é, $mdc\,(x,y) = 1$ em $\mathbb{Z}$, e daí existem inteiros m e n tais que

$$mx + ny = 1$$

logo $mdc\,(x,y) = 1$ também em $\mathbb{Z}\,[i]$.

Como $N\,(x+yi) = N\,(x-yi) = x^2+y^2$ então $x+yi$ e $x-yi$ são ambos invertíveis ou ambos não invertíveis.

Seja $\alpha \,\epsilon\, \mathbb{Z}\,[i]$ tal que $\alpha \mid x+yi$ e $\alpha \mid x-yi$. Segue que α divide a soma $2x$ e a diferença $2yi$, logo $\alpha \mid 2x$ e $\alpha \mid 2y$.

Como x e y são primos entre si em $\mathbb{Z}\,[i]$ segue que $\alpha \mid 2$ e consequentemente α é associado de 1, $1+i$ ou 2.

Descartamos o 2, pois se $2 \mid x+yi$ e $2 \mid x-yi$ implicaria que $4 \mid (x+yi)\,(x-yi) = x^2+y^2$, o que não é possível. De fato, sendo x e y primos entre si, eles são de paridade distinta ou ambos ímpares o que acarreta

$x^2+y^2 = (2k)^2 + (2t+1)^2 = 4\,(k^2+t^2+t) + 1$ ou

$x^2+y^2 = (2k+1)^2 + (2t+1)^2 = 4\,(k^2+t^2+k+t) + 2.$

Suponhamos primeiramente que $x^2+y^2 = N\,(x+yi) = N\,(x-yi)$ seja par.

Segue que $2 \mid (x+yi)\,(x-yi) = x^2+y^2$ e $x+yi$, $x-yi$ não são invertíveis. Além disso, como $2 = (1+i)\,(1-i)$, temos que $(1+i)\,(1-i) \mid (x+yi)\,(x-yi)$, daí $(1+i) \mid (x+yi)\,(x-yi)$. Mas $1+i$ é primo, pois tem norma igual a 2, logo $(1+i)$ divide um dos fatores, digamos $(x+yi)$. Por conjugação, $(1-i) \mid x-yi$ e como $1-i = -i\,(1+i)$, obtemos que $(1+i) \mid (x-yi)$. Neste caso, obtemos

$$mdc\,(x+yi, x-yi) = 1+i.$$

Suponhamos agora que x^2+y^2 seja ímpar.

Se $(1+i) \mid (x+iy)$, segue que $(1-i) \mid (x-yi)$, logo $2 \mid x^2+y^2$, o que é uma contradição. Portanto

$$mdc\,(x+yi, x-yi) = 1.$$

□

Nota: Observe que $(c+di)|(a+bi) \iff (c-di)|(a-bi)$, de fato: $a+bi = (c+di)(e+fi) \iff a-bi = (c-di)(e-fi)$.

Teorema 10. *As soluções de (x,y,z) da equação $x^2+y^2=z^2$ com x e y primos entre si são todas as ternas da forma $(\pm(a^2-b^2), \pm 2ab, \pm(a^2+b^2))$ ou $(\pm 2ab, \pm(a^2-b^2), \pm(a^2+b^2))$ com a, $b \in \mathbb{Z}$, primos entre si e de paridade distinta.*

Demonstração. Seja (x,y,z) uma solução inteira de $x^2+y^2=z^2$ com x e y primos entre si. Como x e y são primos entre si, eles são de paridade distinta, ou são ambos ímpares. No primeiro caso, $x^2+y^2 = (2k_1)^2 + (2k_2+1)^2$ é da forma $4k+1$ e no segundo, $x^2+y^2 = (2k_1+1)^2 + (2k_2+1)^2$ é da forma $4k+2$.

Como todo quadrado z^2 é da forma $4k$ ou $4k+1$, concluímos que x e y são de paridade distinta, logo x^2+y^2 é ímpar.

Segue, pelo lema anterior, que $mdc\,(x+yi, x-yi) = 1$.

Seja $z = z_1^{n_1} \cdots z_r^{n_r}$ a decomposição de z em fatores primos em $\mathbb{Z}[i]$, logo

$$(x+yi)(x-yi) = x^2+y^2 = z^2 = z_1^{2n_1} \cdot \ldots \cdot z_r^{2n_r}$$

Como $x+yi$ e $x-yi$ são primos entre si, temos que $x+yi$ é associado de um quadrado,

$$x + yi = u\,(a + bi)^2 = u\left(a^2 - b^2 + 2abi\right)$$

com u invertível em $\mathbb{Z}[i]$, isto é, u é igual a 1, -1, i ou -1.

Segue daí, conforme os valores de u, que

$$x = \pm\,(a^2 - b^2) \quad e \quad y = \pm 2ab$$

ou

$$x = \pm 2ab \quad e \quad y = \pm\,(a^2 - b^2)$$

Calculando z, a partir da equação $x^2 + y^2 = z^2$, obtemos

$$z = \pm\left(a^2 + b^2\right)$$

.

Reciprocamente, substituindo os valores de x, y e z, dados no enunciado, verificamos que todas as ternas são pitagóricas. □

Finalizamos, generalizando o teorema 9 na próxima seção, estabelecendo condições para um natural n ser soma de dois quadrados.

5.3 Naturais como soma de quadrados

Lema 9. *(i) Tem-se que $n \in \mathbb{Z}$ é soma de dois quadrados se, e somente se, existe $\alpha \in \mathbb{Z}[i]$ tal que $n = N(\alpha)$.*

(ii) Dados inteiros que são somas de quadrados, o seu produto é soma de quadrados.

Demonstração. (i) Temos que $n = a^2 + b^2$ se, e somente se $n = N(a + bi)$.

(ii) Suponha que $n_1, ..., n_r$ são soma de quadrados. Segue que

$$n_1 = N(\alpha_1), \ldots, n_r = N(\alpha_r)$$

e assim

$$n_1 \cdot \ldots \cdot n_r = N(\alpha_1) \cdot \ldots \cdot N(\alpha_r) = N(\alpha_1 \cdot \ldots \cdot a_r)$$

portanto, o produto $n_1 \cdot \ldots \cdot n_r$ é soma de quadrados. □

Teorema 11. *Seja $n \epsilon \mathbb{N}$ com decomposição em fatores primos dada por*

$$n = 2^{\alpha} p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} \cdot q_1^{\beta_1} \cdot \ldots \cdot q_s^{\beta_s}$$

onde cada p_i é um primo da forma $4k+1$ e cada q_j é um primo da forma $4k+3$. A equação $n = x^2 + y^2$ tem solução em $\mathbb{Z}$ se, e somente se, $\beta_1, \ldots, \beta_s$ são pares.

Demonstração. Suponhamos primeiramente que todos os β_j são pares. Como 2 é soma de dois quadrados, cada p_i é soma de dois quadrados e todo inteiro elevado a expoente par é um quadrado, logo soma de quadrados, temos pelo lema anterior que n é soma de quadrados.

Reciprocamente, suponhamos por absurdo $n = a^2 + b^2$ com pelo menos um dos β_j ímpar. Sem perda de generalidade, podemos supor β_1 ímpar.

Tomando $d = mdc(a, b)$, temos que $a = da_1$, $b = db_1$ com $mdc(a_1, b_1) = 1$, e assim

$$n = d^2 \left(a_1^2 + b_1^2\right).$$

Como a maior potência de q_1 que divide d^2 tem expoente par, β_1 é ímpar e $q_1^{\beta_1}$ divide $n = d^2 (a_1^2 + b_1^2)$ temos que

$$q_1 \mid \left(a_1^2 + b_1^2\right).$$

Como $mdc\,(a_1, b_1) = 1$ e $q_1 \mid (a_1^2 + b_1^2)$, temos que $mdc\,(a_1, q_1) = 1$ e $mdc\,(b_1, q_1) = 1$, logo

$q_1 \nmid a_1$ e $q_1 \nmid b_1$.

Considerando o corpo $\mathbb{Z}_{q_1} = \left\{\overline{0}, \overline{1}, \ldots, \overline{q_1 - 1}\right\}$, temos então que $\overline{a_1} \neq \overline{0}$, $\overline{b_1} \neq \overline{0}$ e $\overline{a_1}^2 + \overline{b_1}^2 = \overline{0}$. Multiplicando essa última equação por $\left(\left(\overline{b_1}\right)^{-1}\right)^2$ obtemos

$$\overline{a_1}^2 \left(\overline{b_1}^{-1}\right)^2 + \overline{1} = \overline{0}.$$

Tomando $c \,\epsilon\, \mathbb{Z}$ tal que $\overline{c} = \overline{a_1}\left(\overline{b_1}\right)^{-1}$, temos que $\overline{c}^2 = -\overline{1}$, logo

$c^2 \equiv -1 \; mod \; q_1$.

Consequentemente, pelo teorema 9, temos que $q_1 = 2$ ou $q_1 = 4k+1$, o que é uma contradição. □

Capítulo 6

Considerações finais

No desenvolvimento deste trabalho concluímos que, uma simples pergunta na matemática pode implicar em uma investigação rica para encontrar a sua resposta. Na investigação sobre quando um número primo pode ser escrito como soma de dois quadrados, vários foram os conceitos abordados, como a relação entre aritmética e geometria, congruência, função e até mesmo números complexos. Este trabalho poderia ser reproduzido parcialmente em sala de aula por professores que tenham interesse, por exemplo, em lançar a pergunta: "Quando um número primo p pode ser escrito como soma de dois quadrados?" e desenvolver uma investigação com os alunos observando o resto da divisão do primo p por 4. Vários outros conceitos aqui presentes poderiam ser aplicados em sala de aula, para observação de propriedades matemáticas, ou relação de conceitos que a priori não pareciam estar relacionados.

Referências Bibliográficas

[1] Carlos Correia de Sá, Jorge Rocha, Treze viagens pelo mundo da matemática, Coleção professor de matemática, SBM, U.Porto editorial, 2012.

[2] Arnaldo Garcia, Yves Lequain, Elementos de Álgebra, Projeto Euclides, IMPA, 2010.

[3] W.J. Leveque, Topics in Number Theory, Volume 1, Addison-Wesley, 1956.

[4] I. Niven, H.S. Zuckerman, An Introduction to the Theory of Numbers, Jhon Wiley, 1966.

[5] L.H.J. Monteiro, Elementos de Álgebra, Coleção elementos de matemática, Ao livro técnico 1969.

[6] S. Sidki, Introdução à Teoria dos Números, 10^{o} colóquio de matemática, Poços de Caldas, 1975.

[7] Abramo Hefez, Curso de Álgebra, IMPA, Volume 1, 2013.

[8] Abramo Hefez, Aritmética, Coleção Profmat, SBM, 2013.

[9] Adilson Gonçalves, Introdução à álgebra, Projeto Euclides, IMPA, 2007.

[10] Elon Lages lima, Paulo Cesar Pinto Carvalho, Eduardo Wagner e Augusto César Morgado, A matemática no ensino médio. Volume 3, Coleção professor de matemática, SBM, 2006.