Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

# Inteiros que se escrevem na forma $x^2 + qy^2$, $q = 1, 2, 3, \ldots$ .

**Ricardo de Jesus Caldas Assis**

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Cuiabá - MT

Agosto de 2015

# Inteiros que se escrevem na forma $x^2 + qy^2,\ q = 1, 2, 3, \ldots$ .

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Ricardo de Jesus Caldas Assis e aprovada pela comissão julgadora.

Cuiabá, 10 de setembro de 2015.

Prof. Dr. Martinho da Costa Araújo
Orientador

**Banca examinadora:**

Prof. Dr. Martinho da Costa Araújo
Prof. Dr. José de Arimatéia Fernandes
Prof. Dr. Daniel Carlos Leite.

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**.

**Dados Internacionais de Catalogação na Fonte.**

J58i Jesus Caldas Assis, Ricardo de.
Inteiros que se escrevem na forma x^2+q.y^2, q=1,2,3,... / Ricardo de Jesus Caldas Assis. -- 2015
x, 48 f. : il. color. ; 30 cm.

Orientador: Martinho da Costa Araújo.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2015.
Inclui bibliografia.

1. Soma de dois quadrados. 2. Aritmética dos Inteiros. 3. Resíduos Quadráticos. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

**Dissertação de Mestrado defendida em 10 de Agosto de 2015 e aprovada pela banca examinadora composta pelos Professores Doutores**

Prof. Dr. Martinho da Costa Araújo

Prof. Dr. José de Arimatéia Fernandes

Prof. Dr. Daniel Carlos Leite

*À minha doce amada e meu amado filho.*

# Agradecimentos

Agradeço primeiramente a Deus, que tem nos iluminado e dado a nós a sua infinita graça. Agradeço a minha esposa e meu filho que me ajudaram, de forma valiosa, para que eu chegasse até aqui. Agradeço ao meu orientador que me ajudou grandemente e também aos professores do Profmat de Cuiabá. Agradeço a minha família (pai, mãe e irmão), que colaboraram nessa vitória. Enfim, muito obrigado a todos.

Aos que aqui chegaram,
vale lembrar as palavras
do apóstolo Paulo:

*Posso todas as coisas,*
*naquele que me fortalece*
*(Filipenses* 4 : 13*).*

Versículo biblíco.

# Resumo

Nesta dissertação estamos interessados nos inteiros $n$ que se escrevem na forma $x^2 + 2y^2$ e $x^2 + 3y^2$. Problema proposto por Fermat em 1654. A prova do teorema sobre os inteiros que se escrevem como soma de dois quadrados $x^2 + y^2$ pode ser adaptada para determinar os inteiros que se escrevem na forma $x^2 + 2y^2$ e $x^2 + 3y^2$. Neste caso, precisamos do teorema da fatoração única em produto de primos para números da forma $a + b\sqrt{-2}; a + b\xi_3 \left(\xi_3 = \frac{-1+\sqrt{-3}}{2}\right)$, juntamente com alguns tópicos de teoria dos números.

**Palavras chave:** Soma de dois quadrados; aritmética dos inteiros; resíduos quadráticos.

# Abstract

In this work we are interested in the integers $n$ that are written in the form $x^2 + 2y^2$ and $x^2 + 3y^2$. This problem was proposed by Fermat in 1654. The proof of the theorem about the integers that are written as the sum of two squares $x^2 + y^2$ can be adapted in order to determine the integers that can be writing in the forms $x^2 + 2y^2$ and $x^2 + 3y^2$. In this case, we need to use the theorem of unique factorization on the product of primes for numbers of the form $a + b\sqrt{-2}; a + b\xi_3 \left(\xi_3 = \frac{-1+\sqrt{-3}}{2}\right)$, together with some topics of Number Fields.

**Keywords:** Sum of two squares; arithmetic of integers ; quadratic residues.

# Sumário

# Introdução

Os números primos que se escrevem na forma $x^2 + y^2$ foram estudados, primeiramente, por Fermat, em 1654, e são abordados em vários cursos de Teoria dos Números até os dias de hoje. Em seus estudos, Fermat caracterizou os números primos que se escrevem como soma de dois quadrados e, posteriormente, outros matemáticos formularam novas demonstrações que caracterizaram tais primos. Na atualidade, vem sendo estudados os primos da forma $rx^2 + qy^2$, onde $r$ e $q$ são inteiros livres de quadrados. Abordaremos os primos na forma $x^2 + qy^2$ com $q = 1, 2$ e 3, buscando uma caracterizacão para tais, conforme Clark (2003), de forma que os leitores compreendam esta caracterização. Faremos a fundamentação teórica baseada em alguns tópicos elementares de teoria dos números como, por exemplo, inteiros gaussianos, reciprocidade quadrática, fatoração única, etc. Posteriomente, à fundamentação teórica, caracterizaremos os primos na forma $x^2 + y^2$, e, logo após, os primos na forma $x^2 + 2y^2$ e $x^2 + 3y^2$.

Como este tema é alvo de muitos estudos na atualidade, é interessante apresentá-lo aos leitores interessados, por meio deste trabalho. Serão desenvolvidas algumas etapas, as quais tem como objetivo nos levar a caracterização de primos que se escrevem na forma $x^2 + qy^2$ com $q = 1, 2$ e 3. Cada etapa depende da teoria feita anteriormente e por meio de casos particulares conjecturaremos um resultado e o demonstraremos. Esperamos que todos os leitores entendam o desenvolvimento de cada etapa, e juntos possamos obter uma caracterizacão dos números primos que estamos procurando.

Trataremos no Capítulo 1 sobre os conjuntos $\mathbb{Z}[i]$ e $\mathbb{Z}[\sqrt{-2}]$, deixando claro as suas definições e destacando algumas de suas propriedades. Este capítulo serve de alicerce para o resultado principal do trabalho e a teoria desenvolvida pode ser encontrada nas seguintes referências bibliográficas: Vitorino e ao (2013), Dias (2001), Stillwell (2003) e Moreira et al. (2012).

No Capítulo 2, abordaremos alguns resultados básicos de teoria do números como *Critério*

*de Euler, Lei de Reciprocidade Quadrática de Gauss, entre outros.* Estes conceitos de teoria dos números serão valiosos para o desenvolvimento do trabalho e podem ser encontrados nas seguintes referências bibliográficas: Hefez (2011) e Santos (2007).

Finalmente, no Capítulo 3, trataremos do assunto principal deste trabalho conforme (Clark, 2003). Com base na teoria formulada para a caracterização dos primos que se escrevem como soma de dois quadrados, faremos algumas adaptações para caracterizarmos os primos que se escrevem na forma $x^2 + 2y^2$ e $x^2 + 3y^2$.

# Capítulo 1

# Os conjuntos $\mathbb{Z}[i]$ e $\mathbb{Z}[\sqrt{-2}]$

Neste trabalho vamos usar os seguintes conjuntos:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, .....\}$$

$$\mathbb{Z}_+ = \{x \in \mathbb{Z}; x \geq 0\} = \{0, 1, 2, 3, 4, .....\}.$$

Neste capítulo destacaremos alguns resultados sobre os conjuntos $\mathbb{Z}[i]$ e o $\mathbb{Z}[\sqrt{-2}]$. Estes resultados nos auxiliarão no resultado desejado do trabalho.

## 1.1 O conjunto $\mathbb{Z}[i]$

**Definição 1.1** *O conjunto dos inteiros de Gauss (ou inteiros Gaussianos) é o* $\mathbb{Z}[i] = \{a + bi |\ a, b \in \mathbb{Z}\}$, *onde* $i^2 = -1$.

Dados $z = a + bi, w = c + di \in \mathbb{Z}[i]$, definimos $z + w \in \mathbb{Z}[i]$ e $z.w \in \mathbb{Z}[i]$, por:

1. $z + w = (a + bi) + (c + di) = (a + c) + (b + d)i$

2. $z.w = (a + bi).(c + di) = (ac - bd) + (ad + bc)i$.

As operações de adição e multiplicação em $\mathbb{Z}[i]$ tem as seguintes propriedades, e para todo $z, w, u \in \mathbb{Z}[i]$, temos

1. **Associativa da adição:** $z + (w + u) = (z + w) + u$;

2. **Elemento neutro da adição:** $\exists 0 \in \mathbb{Z}[i]$ tal que $z + 0 = 0 + z = z$;

3. **Elemento oposto da adição:** $\exists -z \in \mathbb{Z}[i]$ tal que $z + (-z) = 0 = (-z) + z$;

4. **Comutativa da adição:** $z + w = w + z$;

5. **Associativa da multiplicação:** $z.(w.u) = (z.w).u$;

6. **Comutativa da multiplicação:** $z.w = w.z$;

7. **Valem as leis distributivas da multiplicação:** $z.(w + u) = (z.w) + (z.u)$ e $(w + u).z = (w.z) + (u.z)$;

8. **Elemento neutro da multiplicação:** $\exists 1 \in \mathbb{Z}[i]$ tal que $z.1 = 1.z = z$.

**Observação 1.1** *Os elementos* $0 = 0+0.i, 1 = 1+0.i$ *e* $-a-bi$ *são ditos, respectivamente, elemento neutro da adição, elemento neutro da multiplicação e elemento oposto em* $\mathbb{Z}[i]$.

**Exemplo 1.1** *Sejam* $z = 3 - i, w = 5 + 2i \in \mathbb{Z}[i]$, *temos:*
$z + w = (3 - i) + (5 + 2i) = 8 + i$
$z.w = (3 - i).(5 + 2i) = 17 + i.$

**Definição 1.2** *Dado* $z = a + bi \in \mathbb{Z}[i]$, *dizemos que* $\overline{z} = a - bi$ *é o seu conjugado em* $\mathbb{Z}[i]$.

**Exemplo 1.2** *Sejam* $z = 2 - i, w = 3 + 2i \in \mathbb{Z}[i]$, *temos:*
$\overline{z} = 2 + i$ *e* $\overline{w} = 3 - 2i$.

**Exemplo 1.3** *Verificar que para todo* $z, w \in \mathbb{Z}[i]$ *tem-se* $\overline{z.w} = \overline{z}.\overline{w}$.

*Com efeito, sejam* $z = a + bi, w = c + di \in \mathbb{Z}[i]$, *temos*
$\overline{z.w} = \overline{(ac - bd) + (ad + bc)i} = (ac - bd) - (ad + bc)i = (a - bi).(c - di) = \overline{z}.\overline{w}.$

Veremos, agora, algumas propriedades e resultados importantes dos *Inteiros Gaussianos.* Por questões didáticas, dividiremos o que vem a seguir em subseções. Começaremos com a definição de norma.

### 1.1.1 Norma em $\mathbb{Z}[i]$

**Definição 1.3** *A função* $N : \mathbb{Z}[i] \to \mathbb{Z}_+$ *dada por* $N(z) = z.\overline{z}, \forall z \in \mathbb{Z}[i]$, *é dita norma em* $\mathbb{Z}[i]$.

**Observação 1.2** *Dado $z = a + bi$, temos $N(z) = z.\overline{z} = (a + bi).(a - bi) = a^2 + b^2$.*

**Exemplo 1.4** *Dado $z = 3 + 4i \in \mathbb{Z}[i]$, temos $N(z) = N(3 + 4i) = 3^2 + 4^2 = 25$.*

Na proposição a seguir, veremos que a norma é multiplicativa em $\mathbb{Z}[i]$.

**Proposição 1.1** *Se $z, w \in \mathbb{Z}[i]$, então $N(z.w) = N(z).N(w)$.*
*Demonstração:*

*De fato, temos que $N(zw) = zw\overline{zw} = z\overline{z}w\overline{w} = N(z)N(w)$.*

■

### 1.1.2 Elementos Invertíveis em $\mathbb{Z}[i]$

No conjunto dos números inteiros $\mathbb{Z}$ os números invertíveis são $\pm 1$ com as operações usuais. Agora, vamos definir elementos invertíveis em $\mathbb{Z}[i]$ e determinar o conjunto dos elementos invertíveis de $\mathbb{Z}[i]$.

**Definição 1.4** *Um elemento $z \in \mathbb{Z}[i], z \neq 0$, é dito invertível se existe $0 \neq w \in \mathbb{Z}[i]$, tal que $z.w = 1$.*

**Afirmação:** O conjunto $(\mathbb{Z}[i])^* = \{z|\ N(z) = 1\} = \{\pm 1,\ \pm i\}$ é o conjunto dos elementos invertíveis de $\mathbb{Z}[i]$.
De fato, se $z = a + bi$ é invertível em $\mathbb{Z}[i]$, então $1 = N(z.w) = N(z)N(w)$, daí
$N(z) = 1 \Leftrightarrow a^2 + b^2 = 1 \Leftrightarrow a = \pm 1,\ b = 0$ ou $a = 0,\ b = \pm 1$, daí $z = \pm 1, \pm i$. Então, como os quatros possuem inverso temos, $(\mathbb{Z}[i])^* = \{z|\ N(z) = 1\} = \{\pm 1,\ \pm i\}$ é o conjunto dos elementos invertíveis de $\mathbb{Z}[i]$.

### 1.1.3 Divisibilidade em $\mathbb{Z}[i]$

De maneira inteiramente análoga a divisibilidade em $\mathbb{Z}$ podemos definir a divisibilidade em $\mathbb{Z}[i]$. Vamos, então, à definição e algumas propriedades da divisibilidade em $\mathbb{Z}[i]$.

**Definição 1.5** *Para $z, w \in \mathbb{Z}[i]$, dizemos que $z$ divide $w$ se existe $u \in \mathbb{Z}[i]$, não-nulo, tal que $w = z.u$.*

Escrevemos que $z$ divide $w$ da seguinte forma: $z|w$.

**Exemplo 1.5** *Note que* $-1|i$ *pois,* $i = (-1)(-i)$ *e* $3 + 4i|25$ *pois,* $25 = (3 + 4i)(3 - 4i)$.

Vejamos algumas propriedades da divisibilidade em $\mathbb{Z}[i]$ na seguinte proposição:

**Proposição 1.2** *Sejam* $z, w, u \in \mathbb{Z}[i]$. *Então,*

1. $1|z$ *e* $z|z$;
2. *Se* $z|1$, *então* $z = 1, -1, i$ *ou* $-i$;
3. *Se* $z|w$ *e* $w|u$, *então* $z|u$;
4. *Se* $z|w$, *então* $N(z)|N(w)$.

*Demonstração:*

*De fato, como* $z = 1.z$, *assim provamos* 1. *Se* $z|1$, *temos que existe* $v \in \mathbb{Z}[i]$ *tal que* $1 = z.v$, *logo* $1 = N(z).N(v)$, *o que significa dizer que* $z \in (\mathbb{Z}[i])^*$, *isto é,*
$z = 1, -1, i$ *ou* $-i$, *com isso provamos* 2. *Agora, se* $z|w$ *e* $w|u$, *tem-se que existem* $v, s \in \mathbb{Z}[i]$ *tais que* $w = z.v$ *e* $u = w.s$, *logo* $u = z.v.s = (v.s).z$, *ou seja,* $z|u$. *Finalmente, se* $z|w$, *existe* $v \in \mathbb{Z}[i]$ *tal que* $w = z.v$, *logo* $N(w) = N(z).N(v)$, *ou seja,* $N(z)|N(w)$, *o que conclui a demonstração.*

■

### 1.1.4 Divisão Euclidiana em $\mathbb{Z}[i]$

Nesta subseção vamos descrever a chamada *divisão euclidiana.* Primeiramente, vamos relembrar o conceito de *divisão euclidiana,* ou divisão com resto, nos números inteiros, que é uma das quatro operações que toda criança aprende na escola, e estenderemos o conceito para os inteiros gaussianos. Sua formulação precisa é: dados $a, b \in \mathbb{Z}$ com
$b \neq 0$, existem $q, r \in \mathbb{Z}$ com $a = bq + r$ e $0 \leq r < |b|$.
Tais $q$ e $r$ estão unicamente determinados pelas duas condições acima e são chamados, respectivamente, *quociente* e *resto* da divisão de $a$ por $b$. No conjunto $\mathbb{Z}[i]$ a divisão euclidiana funciona da mesma forma, a única diferença em relação aos números inteiros é que a norma do resto fica compreendida entre 0 e a norma do dividendo. Daí, em $\mathbb{Z}[i]$ temos a seguinte formulação para a divisão euclidiana:

**Proposição 1.3** *Dados $z, w \in \mathbb{Z}[i]$ com $w \neq 0$, existem $q, r \in \mathbb{Z}[i]$ com $z = wq + r$ e $0 \leq N(r) < N(w)$.*

*Demonstração:*

*Basta dividir $z = x + yi, w = a + bi$, onde $x, y, a, b \in \mathbb{Z}$. Então,*

$$\frac{z}{w} = \frac{x+yi}{a+bi}.\frac{a-bi}{a-bi} = \frac{xa - xbi + yai - ybi^2}{a^2+b^2} = \frac{xa+yb}{a^2+b^2} + \frac{ya-xb}{a^2+b^2}i.$$

*Tomando $m$ e $n$ como os inteiros mais próximos de $\frac{xa+yb}{a^2+b^2}$ e $\frac{ya-xb}{a^2+b^2}$, respectivamente, temos que :*

$$\left|m - \frac{xa+yb}{a^2+b^2}\right|, \left|n - \frac{ya-xb}{a^2+b^2}\right| \leq \frac{1}{2}.$$

*Se $q = m + ni$, então:*

$$r = z - wq = w\left(\frac{z}{w} - q\right) = w\left(\frac{xa+yb}{a^2+b^2} - m + \left(\frac{ya-xb}{a^2+b^2} - n\right)i\right),$$

*o que implica,*

$$N(r) \leq N(w)\left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right) = \frac{N(w)}{2} < N(w).$$

■

### 1.1.5 Lema de Euclides

Utilizaremos a divisão euclidiana para demonstrar o *Lema de Euclides,* mas, primeiramente, daremos uma definição de primo em $\mathbb{Z}[i]$.

**Definição 1.6** *Dizemos que $p$ é um primo em $\mathbb{Z}[i]$, quando $p$ não pode ser escrito como produto de dois inteiros de $\mathbb{Z}[i]$ cujas normas são maiores que* 1.

**Exemplo 1.6** *Verificar que $z = 1 + i$ é primo em $\mathbb{Z}[i]$.*

*De fato, suponha que existam $w, u \in \mathbb{Z}[i]$ tais que $1 + i = w.u$, então $2 = N(w).N(u)$. Logo, $w$ ou $u$ tem norma igual a* 1. *Portanto, $z = 1 + i$ é um primo em $\mathbb{Z}[i]$.*

Veremos, mais adiante, que os produtos de $1 + i$ pelos elementos de $(\mathbb{Z}[i])^*$ são

todos primos.

O próximo resultado nos auxília na verificação de primalidade em $\mathbb{Z}[i]$.

**Proposição 1.4** *Se $N(z)$ é primo em $\mathbb{Z}$, então $z$ é primo em $\mathbb{Z}[i]$.*
*Demonstração:*

*Suponha que $z$ não é primo em $\mathbb{Z}[i]$. Então, existem $w, u \in \mathbb{Z}[i], w, u \neq 0$, tais que $z = wu$ e $N(w), N(u) > 1$. Isto é uma contradição pois, $N(z)$ é primo em $\mathbb{Z}$.*

■

**Exemplo 1.7** *Verificar que $1 - i$ é primo de $\mathbb{Z}[i]$.*

*Com efeito, como $N(1 - i) = 2$ e $2$ é primo em $\mathbb{Z}$ então $z$ é primo em $\mathbb{Z}[i]$.*

O próximo resultado, *Lema de Euclides,* nos garante que se um primo em $\mathbb{Z}[i]$ divide um produto de dois inteiros gaussianos, então ele divide um dos fatores.

**Lema 1.1 (Lema de Euclides)** *Se $p$ é um primo em $\mathbb{Z}[i]$, com $a, b \in \mathbb{Z}[i]$ e $p|ab$, então $p|a$ ou $p|b$.*
*Demonstração:*

*Para demonstrá-lo, vamos fazer sucessivas divisões euclidianas, sendo $x_0 = a$ e $x_1 = p$. Seja $x_{k+2}$ o resto da divisão euclidiana de $x_k$ por $x_{k+1}$. Temos então as divisões:*

$$x_0 = q_1 x_1 + x_2$$

$$x_1 = q_2 x_2 + x_3$$

$$x_2 = q_3 x_3 + x_4$$

.....

$$x_{n-2} = q_{n-1} x_{n-1} + x_n$$

$$x_{n-1} = q_n x_n + x_{n+1}$$

*Observe que como $x_k \neq 0 \Rightarrow N(x_{k+1}) < N(x_k)$, podemos tomar $n$ tal que $N(x_{n+1}) = 0$, ou seja, $x_{n+1} = 0$. Logo $x_n|x_{n-1}$. Observe que $x_n|x_{k-1}$ e $x_n|x_k$. Logo, $x_n|x_n$ e $x_n|x_{n-1}$, então indutivamente, $x_n|x_k, \forall k, 0 \leq k \leq n$, particularmente*

$x_n|x_0 = a$ *e* $x_n|x_1 = p$. *Tomando as* $j+1$ *primeiras equações e realizando substituições adequadas, temos que* $x_j = a_j x_1 + y_j x_0 = a_j p + y_j a$; *particularmente* $x_n = a_n p + y_n a$. *Se* $p|a$ *então o lema está demonstrado. Se* $p$ *não divide* $a$, *então, como* $x_n|p, x_n|a$ *e* $x_n = a_n p + y_n a$, *então* $x_n \in \{\pm 1, \pm i\}$ *e temos:* $x_n = a_n p + y_n a$ *se, e somente se,* $b = (x_n)^{-1}(ba_n p + y_n ab)$ *implicando que* $p|b$, *o que conclui a demonstração.*

■

### 1.1.6 Fatoração Única em $\mathbb{Z}[i]$

A fatoração única é uma das propriedades mais usadas em problemas envolvendo números inteiros. Vamos prová-la para os inteiros de Gauss. Primeiramente provaremos que todo inteiro $z$ de Gauss com norma maior do que 1 pode ser escrito como o produto de um ou mais primos em $\mathbb{Z}[i]$. Se $N(z) = 2$, como 2 é primo e a norma é multiplicativa, então $z$ é primo, portanto está provado. Considere $N(z) > 2$. Se $z$ é primo a fatoração é imediata. Se $z$ não é primo, então $z = ab$ implicando que $N(z) = N(a).N(b),$ onde $N(a), N(b) > 1,$ e $N(a), N(b) < N(z)$. Podemos supor, por indução, que se $N(x) < N(z)$, então $x$ é fatorável. Logo, $a$ e $b$ são fatoráveis, e portanto $z$ o é. Para provar que esta fatoração é única, basta considerar as duas fatorações $p_1 p_2 ... p_n$ e $q_1 q_2 ... q_m$. Suponha, por indução, $p_1 p_2 ... p_n = \xi q_1 q_2 ... q_m$, sendo $\xi$ um invertível, implica que a sequência $(p_i)$ é uma permutação (a menos que sejam multiplicações pelos invertíveis) da $(q_i)$. Se máx$\{n; m\} = 1$, então o resultado é imediato. Supondo que ele vale se máx$\{n'; m'\} <$ máx$\{n; m\}$, pelo *Lema de Euclides,* vemos que para algum $i, p_n|q_i$. Sem perda de generalidade, podemos supor $i = m$. Como $p_n$ e $q_m$ são primos, então $q_m = \xi' p_n$, onde $\xi'$ é um invertível. Logo $p_1 p_2 ... p_n = \xi q_1 q_2 ... q_m \Leftrightarrow p_1 p_2 .. p_{n-1} = \xi\xi' q_1 q_2 .. q_{m-1}$. Por indução, $p_1, p_2, ..., p_{n-1}$ é uma permutação( a menos que seja multiplicações pelos invertíveis) de $q_1, q_2, ..., q_m$, portanto a fatoração é única. Com isso, provamos a seguinte proposição:

**Proposição 1.5** *Seja* $z \in \mathbb{Z}[i]$, *então existem* $z_1, z_2, ..., z_n \in \mathbb{Z}[i]$, *únicos e primos, tais que* $z = z_1 . z_2 ... z_n$.

**Exemplo 1.8** *Considere as seguintes fatorações*

1. *Para* $z = 2$, *temos* $2 = (1+i)(1-i)$ *onde* $1+i$ *e* $1-i$ *são primos;*

2. *Para* $z = 5$, *temos* $5 = (2+i)(2-i)$ *onde* $2+i$ *e* $2-i$ *são primos.*

### 1.1.7 Congruências Módulo $n$ e o Conjunto $\mathbb{Z}_n$

O conceito de congruência de inteiros foi introduzido e estudado por Gauss e é utilizado para enfatizar o resto da divisão euclidiana. Está seção será útil pois a linguagem de congruência módulo $n$ e classes de equivalência serão utilizadas com muita frequência.

**Definição 1.7 (Congruência módulo $n$)** *Seja $n \geq 2$ um inteiro e $a, b \in \mathbb{Z}$. Dizemos que $a$ é congruente a $b$ módulo $n$ se, e somente se, $n|(a-b)$.*

Quando $a$ é congruente a $b$ módulo $n$ escrevemos $a \equiv b(mod\ n)$. Caso contrário, escrevemos $a \not\equiv b(mod\ n)$. A expressão $a \equiv b(mod\ n)$ lê-se $a$ é congruente a $b$ módulo $n$.

**Exemplo 1.9** *Veja as congruências*

1. $25 \equiv 37(mod\ 6)$, *pois* $25 - 37 = -12$ *e* $6|-12$

2. $13 \not\equiv 22(mod\ 5)$, *pois* $13 - 22 = -9$ *e* $5$ *não divide* $-9$.

A seguir veremos uma propriedade muito interessante da congruência módulo $n$.

**Proposição 1.6** *A congruência módulo $n$ é uma relação de equivalência em $\mathbb{Z}$. Ou seja, para todo $a, b, c \in \mathbb{Z}$ a congruência módulo $n$ satisfaz:*

1. $a \equiv a(mod\ n)$;

2. *Se* $a \equiv b(mod\ n)$, *então* $b \equiv a(mod\ n)$;

3. *Se* $a \equiv b(mod\ n)$ *e* $b \equiv c(mod\ n)$, *então* $a \equiv c(mod\ n)$.

*Demonstração:*

*Vide Villela (2000).*

■

Veremos agora que o conceito de congruência de inteiros módulo $n$ pode ser utilizado para enfatizar o resto da divisão euclidiana por $n$.

**Proposição 1.7** *Seja $n \geq 2$. Então $a \equiv b(mod\ n)$ se, e somente se, $a$ e $b$ têm o mesmo resto na divisão euclidiana por $n$.*

*Demonstração:*

*Vide Villela (2000).*

■

**Exemplo 1.10** *Os números* 25 *e* 100 *deixam resto* 0 *na divisão por* 5, *logo* $25 \equiv 100(mod\ 5)$.

As seguintes propriedades adicionais das congruências são muito úteis nas aplicações do conceito de congruência.

**Proposição 1.8 (Propriedades das congruências)** *Sejam* $a, b, c, d \in \mathbb{Z}$ *e seja* $n \geq 2$.

1. *se* $a \equiv b(mod\ n)$ *e* $c \equiv d(mod\ n)$, *então* $a + c \equiv b + d(mod\ n)$
2. *se* $a \equiv b(mod\ n)$ *e* $c \equiv d(mod\ n)$, *então* $ac \equiv bd(mod\ n)$
3. *se* $a \equiv b(mod\ n)$, *então* $am \equiv bm(mod\ n)$, *para todo* $m \geq 1$.

*Demonstração:*

*Vide Villela (2000).* ∎

**Exemplo 1.11** *Qual o resto da divisão de* $7^{47}$ *por* 9?

*Temos* $7^2 = 49 \equiv 4(mod\ 9)$, *então* $7^3 = 7^2.7 \equiv 4.7 = 28 \equiv 1(mod\ 9)$. *Portanto,* $7^{47} = 7^{3.15+2} = (7^3)^{15}.7^2 \equiv 1^{15}.4 = 4(mod\ 9)$, *ou seja, o resto é* 4.

Seja $n \geq 2$ um inteiro. Pela *Proposição* 1.6 a congruência módulo $n$ é uma relação de equivalência. A classe de equivalência de um inteiro $a$ na congruência módulo $n$ é chamada de classe residual módulo $n$ ou, simplesmente, classe de resíduos módulo $n$. Assim, escrevemos a classe de resíduos módulo $n$ da seguinte forma:

$$[a] = \{x \in \mathbb{Z}/\ x \equiv a(mod\ n)\} = \{x \in \mathbb{Z}/\ n|(x - a)\}.$$

**Exemplo 1.12** *Seja* $n = 2$. *Dado* $a \in \mathbb{Z}$, *pela divisão euclidiana, existem* $q$ *e* $r$, *unicamente determinados, tais que* $a = 2.q + r$, *com* $0 \leq r \leq 1$. *Logo,*

$$[a] = \begin{cases} [0] & \text{se, e somente se, } a \text{ é par} \\ [1] & \text{se, e somente se, } a \text{ é ímpar.} \end{cases}$$

Logo, só há duas classes distintas módulo 2, a saber [0] e [1]. Das propriedades de relação de equivalência, $\mathbb{Z} = [0] \cup [1]$, onde $[0] = 2.\mathbb{Z} = \{2t/\ t \in \mathbb{Z}\}$ e
$[1] = 2.\mathbb{Z} + 1 = \{2s + 1/\ s \in \mathbb{Z}\}$.

**Proposição 1.9** *Seja $n \geq 2$. Para cada $a \in \mathbb{Z}$ existe um único $r \in \mathbb{Z}$, com $0 \leq r \leq n-1$, tal que $[a] = [r]$. Logo, há $n$ classes de resíduos módulo $n$ distintas, a saber, $[0], [1], ..., [n-1]$, onde $[r] = n\mathbb{Z} + r$ e $\mathbb{Z} = [0] \cup [1] \cup .... \cup [n-1]$.*

*Demonstração:*

*Seja $a \in \mathbb{Z}$. Dividindo $a$ por $n$, existem $q, r \in \mathbb{Z}$ unicamente determinados, com $0 \leq r \leq n-1$, tais que*

$$a = qn + r.$$

*De $a = qn + r$, concluímos que $a \equiv r(mod\ n)$, ou seja, $[a] = [r]$, em outras palavras existe tal $r$. Agora, sejam $r, s \in \mathbb{Z}$ tais que $0 \leq r, s \leq n-1$ e $[r] = [s]$. Vamos mostrar que $r = s$. De fato, de $-(n-1) \leq r, s \leq (n-1)$ e $n|(r-s)$, concluímos que $r - s = 0$, isto é, $r = s$. Portanto, $r$ é único.*

■

**Definição 1.8 (Conjunto das Classes de Resíduos Módulo $n$)** *O conjunto $\mathbb{Z}_n$ é chamado de conjunto das classes de resíduos módulo $n$, ou seja,*

$$\mathbb{Z}_n = \{[0], [1], ...., [n-1]\}.$$

**Exemplo 1.13** *Vejamos para alguns valores de $n$ o conjunto $\mathbb{Z}_n$ correspondente.*

1. *Para $n = 2$, temos $\mathbb{Z}_2 = \{[0], [1]\}$;*
2. *Para $n = 3$, temos $\mathbb{Z}_3 = \{[0], [1], [2]\}$;*
3. *Para $n = 5$, temos $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$;*
4. *Para $n = 8$, temos $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$.*

Vamos definir em $\mathbb{Z}_n$ as operações de adição e multiplicação entre seus elementos.

**Definição 1.9 (Adição e Multiplicação em $\mathbb{Z}_n$)** *Sejam $n \geq 2$ e $a, b \in \mathbb{Z}$. Definimos*

1. $[a] + [b] = [a + b]$
2. $[a].[b] = [a.b]$.

Observamos que essas definições não dependem dos representantes das classes de resíduos. De fato, pelas propriedades das congruências, temos

$$a \equiv a_1 (mod\ n) \text{ e } b \equiv b_1 (mod\ n) \Leftrightarrow$$

$$a + b \equiv a_1 + b_1 (mod\ n) \text{ e } a.b \equiv a_1.b_1 (mod\ n) \Leftrightarrow$$

$$[a + b] = [a_1 + b_1] \text{ e } [a.b] = [a_1.b_1] \Leftrightarrow$$

$$[a] + [b] = [a_1] + [b_1] \text{ e } [a].[b] = [a_1].[b_1].$$

Portanto, a adição e a multiplicação das classes de resíduos independem do inteiro que é representante da classe.
Vejamos as tabelas das operações em $\mathbb{Z}_2$.

**Exemplo 1.14** *Tabelas das operações em* $\mathbb{Z}_2$

| $+$ | $[0]$ | $[1]$ |
|---|---|---|
| $[0]$ | $[0]$ | $[1]$ |
| $[1]$ | $[1]$ | $[0]$ |

| $.$ | $[0]$ | $[1]$ |
|---|---|---|
| $[0]$ | $[0]$ | $[0]$ |
| $[1]$ | $[0]$ | $[1]$ |

**Proposição 1.10 (Propriedades da adição e multiplicação de $\mathbb{Z}_n$)** *Seja $n \geq 2$. A adição e a multiplicação de $\mathbb{Z}_n$ têm as seguintes propriedades, para quaisquer $[a], [b], [c] \in \mathbb{Z}_n$ :*

1. *(Associativa da adição)* $([a] + [b]) + [c] = [a] + ([b] + [c])$;
2. *(Comutativa da adição)* $[a] + [b] = [b] + [a]$;
3. *(Existência de elemento neutro da adição)* $[0]$ *é o elemento neutro aditivo* $[0] + [a] = [a]$;
4. *(Existência do oposto da adição) O oposto de* $[a]$ *é* $[-a]$ *tal que* $[a] + [-a] = [0]$;
5. *(Associativa da multiplicação)* $([a].[b]).[c] = [a].([b].[c])$;
6. *(Comutativa da multiplicação)* $[a].[b] = [b].[a]$;
7. *(Existência da unidade)* $[1]$ *é a unidade de* $\mathbb{Z}_n$ *tal que* $[1].[a] = [a]$;

*8. (Distributiva da multiplicação)* $([a]+[b]).[c] = [a].[c] + [b].[c]$.

*Demonstração:*

*Vide Villela (2000).*

■

O próximo resultado nos dá um critério para determinar se um elemento é invertível ou não em $\mathbb{Z}_n$.

**Proposição 1.11** *Seja* $n \geq 2$. *Um elemento* $[a] \in \mathbb{Z}_n$ *é invertível se, e somente se,* $mdc(a, n) = 1$.

*Demonstração:*

*Seja* $[a] \in \mathbb{Z}_n$ *um elemento invertível. Então, existe* $[b] \in \mathbb{Z}_n$ *tal que* $[1] = [a][b] = [ab]$. *Logo,* $ab \equiv 1(mod\ n)$, *ou seja,* $n|(ab-1)$. *Portanto, existe* $q \in \mathbb{Z}$ *tal que* $ab-1 = qn$, *isto é,* $a(b)+n(-q) = 1$. *Daí, concluímos que* $mdc(a, n) = 1$. *Por outro lado, suponhamos que* $mdc(a, n) = 1$. *Então, existem* $x, y \in \mathbb{Z}$ *tais que* $ax + ny = 1$. *Portanto,* $[1] = [ax + ny] = [a][x] + [n][y] = [a][x] + [0][y] = [a][x]$, *mostrando que* $[x]$ *é o inverso de* $[a]$.

■

**Exemplo 1.15** *Vamos obter o conjunto dos elementos invertíveis de* $\mathbb{Z}_{10}$.
*Para cada* $i \in \{0, 1, ...., 9\}$, *temos* $mdc(i, 10) = 1$ *se, e somente se,* $i \in \{1, 3, 7, 9\}$. *Portanto,* $(\mathbb{Z}_{10})^* = \{[1], [3], [7], [9]\}$.

**Exemplo 1.16** *Vamos obter o conjunto dos elementos invertíveis de* $\mathbb{Z}_{11}$.
*Note que se* $i \in \{1, ...., 9, 10\}$, *então* $mdc(i, 11) = 1$. *Portanto,*
$(\mathbb{Z}_{11})^* = \{[1], [2], ...., [10]\} = \mathbb{Z}_{11} - \{[0]\}$.

**Corolário 1.1** *Todo elemento não-nulo de* $\mathbb{Z}_p$, *com p primo, é invertível.*
*Demonstração:*

*De fato, pela proposição anterior para cada* $i \in \{1, 2, ....., p-1\}$ *temos que* $mdc(i, p) = 1$. *Portanto,* $(\mathbb{Z}_p)^* = \mathbb{Z}_p - \{[0]\}$.

■

**Exemplo 1.17** *Em* $\mathbb{Z}_3 = \{[0], [1], [2]\}$, *os inversos de* $[1]$ *e* $[2]$ *são, respectivamente,* $[1]$ *e* $[2]$, *pois* $[1]^2 = [1]$ *e* $[2]^2 = [1]$.

**Observação 1.3** *Representaremos o símbolo* $[x] \in \mathbb{Z}_n$ *por* $x \in \mathbb{Z}_n$. *Por exemplo,* $5 \in \mathbb{Z}_7$.

### 1.1.8 Elementos Primos em $\mathbb{Z}[i]$

Agora vamos caracterizar os primos em $\mathbb{Z}[i]$. Pela *Proposição* 1.4 se $N(z)$ é primo em $\mathbb{Z}$, então $z$ é um primo em $\mathbb{Z}[i]$ ( pois se $z$ fatora então $N(z)$ fatora). Observe que todo primo $z$ divide $N(z)$, portanto ele deve dividir ao menos um fator primo em $\mathbb{Z}$ de $N(z)$. Se $z$ dividir ao menos dois números distintos(absolutamente) $x$ e $y$ primos em $\mathbb{Z}$, como sempre é possível tomar $a, b \in \mathbb{Z}$ tal que $ax + by = 1$, teríamos $z|1$, um absurdo. Logo, todo primo em $\mathbb{Z}[i]$ divide exatamente um primo inteiro positivo (e seu elemento oposto da soma) em $\mathbb{Z}$. Seja esse primo inteiro positivo $p$. Temos 3(três) casos:

1. Se $p$ é par, então $p = 2$. Sendo $z = a + bi$, então $N(z) = a^2 + b^2 = 2$, ou seja, $z = \pm 1 \pm i$, e obtemos os quatro primos $1 + i, 1 - i, -1 + i$ e $-1 - i$.

2. Se $p \equiv 3(mod\ 4)$. Note que $x \equiv 0, 1, 2$ ou $3(mod\ 4)$, então $x^2 \equiv 0$ ou $1(mod\ 4)$. Queremos mostrar que $p$ é um primo em $\mathbb{Z}[i]$. Suponha que $p$ não é primo de $\mathbb{Z}[i]$, então existem $z = c + di, w = a + bi \in \mathbb{Z}[i],$ com $1 < N(z), N(w) < p^2$, tais que $p = zw$. Como $p$ é um inteiro primo, devemos ter $w = \overline{z} = c - di$, logo $p = c^2 + d^2$. Agora, $p = c^2 + d^2 \equiv 0, 1$ ou $2(mod\ 4)$, o que é um absurdo, pois por hipótese $p \equiv 3(mod\ 4)$. Portanto, $p$ é um primo em $\mathbb{Z}[i]$.

3. Se $p \equiv 1(mod\ 4)$. Dado $x = 1.2..... \left(\frac{p-1}{2}\right)$ , temos que:

$$x^2 \equiv 1.2..... \left(\frac{p-1}{2}\right).1.2..... \left(\frac{p-1}{2}\right) \equiv 1.2..... \left(\frac{p-1}{2}\right).\left(\frac{p+1}{2}\right)...(p-2).(p-1) \equiv$$

$$1.(p-1) \equiv -1(mod\ p).$$

Logo, $p|x^2 + 1 = (x + i)(x - i)$. Suponha que $p$ é um primo de $\mathbb{Z}[i]$, então pelo *Lema de Euclides* $p|(x + i)$ ou $p|(x - i)$. Daí, existem $z_1, z_2 \in \mathbb{Z}[i]$ tais que $x + i = p.z_1$ ou $x - i = pz_2$. Mas, teríamos $z_1 = \frac{1}{p}x + \frac{1}{p}i$ ou $z_2 = \frac{1}{p}x - \frac{1}{p}i$ e $\frac{1}{p}$ não é inteiro. Logo, $p$ não é primo de $\mathbb{Z}[i]$, daí existem $z = a + bi, w = c + di \in \mathbb{Z}[i],$ com
$1 < N(z), N(w) < p^2$, tais que $p = wz = (a + bi)(c + di) = (ac - bd) + (bc + ad)i$. Como $p \in \mathbb{Z}$, então $bc = -ad$, ou seja, $a = c$ e $b = -d$ ou $a = -c$ e $b = d$, com isso concluímos que $w = \pm\overline{z}$. Logo, como $p > 0$ segue que $w = \overline{z}$ e $N(z) = p$ $(p = a^2 + b^2)$, portanto concluímos que $z$ é primo e mais $z$ e seu conjugado são os únicos primos em $\mathbb{Z}[i]$ que dividem $p$.

Com base no exposto acima, vimos que os únicos primos em $\mathbb{Z}[i]$ são:

(a) O primo $1+i$ e seus produtos pelos invertíveis.

(b) Os primos $p$ em $\mathbb{Z}$ tal que $p \equiv 3(mod\ 4)$ e seus produtos pelos invertíveis.

(c) Para cada primo $p$ em $\mathbb{Z}$ tal que $p \equiv 1(mod\ 4)$, os primos $a+bi, a-bi$ e seus produtos pelos invertíveis, sendo $p = a^2 + b^2$.

### 1.1.9 Elementos Irredutíveis em $\mathbb{Z}[i]$

Em $\mathbb{Z}$, os conceitos de elemento irredutível e elemento primo coincidem, ou seja, um elemento $p$ é irredutível se, e somente se, é primo. No conjunto $\mathbb{Z}[i]$ veremos que os conceitos de primo e irredutível também coincidem, isto segue do fato de que em $\mathbb{Z}[i]$ a fatoração é única.

**Definição 1.10** *Um elemento $z \in \mathbb{Z}[i]$, não-nulo e não-invertível, é dito irredutível quando $z = wu$ com $w$ ou $u$ invertível em $\mathbb{Z}[i]$.*

**Exemplo 1.18** *Verificar que $z = 1+i$ é irredutível em $\mathbb{Z}[i]$.*

*De fato, escrevendo $1+i = wu$, com $w, u \in \mathbb{Z}[i]$, temos $2 = N(w)N(u)$. Logo, $N(w) = 1$ ou $N(u) = 1$ e daí concluímos que $w$ ou $u$ é invertível em $\mathbb{Z}[i]$. Portanto, $z = 1+i$ é irredutível em $\mathbb{Z}[i]$.*

**Observação 1.4** *É facil verificar que os produtos de $1+i$ pelos invertíveis também são irredutíveis em $\mathbb{Z}[i]$.*

O próximo resultado mostra que um elemento $p$ é primo em $\mathbb{Z}[i]$ se, e somente se, $p$ é irredutível em $\mathbb{Z}[i]$.

**Proposição 1.12** *Seja $p \in \mathbb{Z}[i]$, com $p$ não-nulo e não-invertível. Então $p$ é um elemento primo de $\mathbb{Z}[i]$ se, e somente se, $p$ é um elemento irredutível de $\mathbb{Z}[i]$.*
*Demonstração:*

*Se $p = wu$ com $w, u \in \mathbb{Z}[i]$, então $p|wu$ e, como $p$ é primo, temos que $p|w$ ou $p|u$. Por outro lado, $u|p$ e $w|p$. Logo $w$ ou $u$ é invertível, mostrando assim que $p$ é um elemento irredutível de $\mathbb{Z}[i]$. Por outro lado, seja $p \in \mathbb{Z}[i]$ um elemento irredutível. Então $p$ é não-nulo e não-invertível. Se $w, u \in \mathbb{Z}[i]$ são tais que $p|wu$, escrevendo $w = w_1...w_r$ e*

*$u = u_1...u_s$, com $w_i$ e $u_j$ elementos irredutíveis de $\mathbb{Z}[i]$, temos que uma fatoração para $ab$ é*

$$ab = w_1....w_r.u_1....u_s.$$

*Como $p|wu$, temos que $wu = pz$, para algum $z \in \mathbb{Z}[i]$. Pela unicidade da fatoração de $wu$, temos que $p = w_i v$ ou $p = u_j v$, com $v$ invertível, para algum índice $i, j$. Agora, se $p|w_i$ e $w_i|w$, implica que $p|w$, por outro lado se $p|u_j$ e $u_j|u$, implica que $p|u$, o que mostra que $p$ é primo.*

■

## 1.2 O conjunto $\mathbb{Z}[\sqrt{-2}]$

**Definição 1.11** *O conjunto dos inteiros quadráticos é dado por*
$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2}|\ a, b \in \mathbb{Z}\} = \{a + b\sqrt{2}i|\ a, b \in \mathbb{Z}$ *onde* $i^2 = -1\}$.

Dados $z = a + b\sqrt{-2}, w = c + d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, definimos $z + w \in \mathbb{Z}[\sqrt{-2}]$ e $z.w \in \mathbb{Z}[\sqrt{-2}]$, por:

1. $z + w = (a + b\sqrt{-2}) + (c + d\sqrt{-2}) = (a + c) + (b + d)\sqrt{-2}$
2. $z.w = (a + b\sqrt{-2}).(c + d\sqrt{-2}) = (ac - 2bd) + (ad + bc)\sqrt{-2}$.

As operações de adição e multiplicação em $\mathbb{Z}[\sqrt{-2}]$ tem as seguintes propriedades: Para todo $z, w, u \in \mathbb{Z}[\sqrt{-2}]$, temos

1. **Associativa da adição:** $z + (w + u) = (z + w) + u$;
2. **Elemento neutro da adição:** $\exists 0 \in \mathbb{Z}[\sqrt{-2}]$ tal que $z + 0 = 0 + z = z$;
3. **Elemento oposto da adição:** $\exists - z \in \mathbb{Z}[\sqrt{-2}]$ tal que $z + (-z) = 0 = (-z) + z$;
4. **Comutativa da adição:** $z + w = w + z$;
5. **Associativa da multiplicação:** $z.(w.u) = (z.w).u$;
6. **Comutativa da multiplicação:** $z.w = w.z$;
7. **Valem as leis distributivas da multiplicação:** $z.(w + u) = (z.w) + (z.u)$ e $(w + u).z = (w.z) + (u.z)$;

8. **Elemento neutro da multiplicação:** $\exists 1 \in \mathbb{Z}[\sqrt{-2}]$ tal que $z.1 = 1.z = z$.

**Observação 1.5** *Os elementos* $0 = 0 + 0.\sqrt{-2}, 1 = 1 + 0.\sqrt{-2}$ *e* $-a - b\sqrt{-2}$ *são ditos, respectivamente, elemento neutro da adição, elemento neutro da multiplicação e elemento oposto em* $\mathbb{Z}[\sqrt{-2}]$.

**Exemplo 1.19** *Sejam* $z = 2 - \sqrt{-2}, w = 3 + 2\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, *temos que:*
$z + w = (2 - \sqrt{-2}) + (3 + 2\sqrt{-2}) = 5 + \sqrt{-2}$
$z.w = (2 - \sqrt{-2}).(3 + 2\sqrt{-2}) = 10 + \sqrt{-2}.$

**Definição 1.12** *Dado* $z = a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, *dizemos que* $\overline{z} = a - b\sqrt{-2}$ *é o seu conjugado em* $\mathbb{Z}[\sqrt{-2}]$.

**Exemplo 1.20** *Sejam* $z = 5 - 2\sqrt{-2}, w = -1 + 6\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, *temos:*
$\overline{z} = 5 + 2\sqrt{-2}$ *e* $\overline{w} = -1 - 6\sqrt{-2}$.

De modo análogo a $\mathbb{Z}[i]$, podemos verificar que para todo $z, w \in \mathbb{Z}[\sqrt{-2}]$ tem-se $\overline{z.w} = \overline{z}.\overline{w}$. Veremos, agora, algumas propriedades e resultados importantes dos *Inteiros Quadráticos.* Por questões didáticas, dividiremos o que vem a seguir em subseções. Começaremos com a definição de norma.

### 1.2.1 Norma em $\mathbf{Z}[\sqrt{-2}]$

**Definição 1.13** *A função* $N : \mathbb{Z}[\sqrt{-2}] \to \mathbb{Z}_+$ *dada por* $N(z) = z.\overline{z}, \forall z \in \mathbb{Z}[\sqrt{-2}]$, *é dita norma em* $\mathbb{Z}[\sqrt{-2}]$.

**Observação 1.6** *Dado* $z = a + b\sqrt{-2}$, *temos*

$$N(z) = z.\overline{z} = (a + b\sqrt{-2}).(a - b\sqrt{-2}) = a^2 + 2.b^2.$$

**Exemplo 1.21** *Dado* $z = -3 + 2\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, *temos*
$N(z) = N(-3 + 2\sqrt{-2}) = (-3)^2 + 2.2^2 = 17.$

Na proposição a seguir, veremos que a norma é multiplicativa em $\mathbb{Z}[\sqrt{-2}]$.

**Proposição 1.13** *Se* $z, w \in \mathbb{Z}[\sqrt{-2}]$, *então* $N(z.w) = N(z).N(w)$.
*Demonstração:*

*De fato, temos que* $N(zw) = zw\overline{zw} = z\overline{z}w\overline{w} = N(z)N(w)$.

■

### 1.2.2 Elementos Invertíveis em $\mathbf{Z}[\sqrt{-2}]$

No conjunto $\mathbb{Z}[i]$ os elementos invertíveis são $\pm 1$ e $\pm\, i$. Agora, vamos definir elementos invertíveis em $\mathbb{Z}[\sqrt{-2}]$ e determinar o conjunto dos elementos invertíveis de $\mathbb{Z}[\sqrt{-2}]$.

**Definição 1.14** *Um elemento $z \in \mathbb{Z}[\sqrt{-2}], z \neq 0$, é dito invertível se existe $0 \neq w \in \mathbb{Z}[\sqrt{-2}]$ tal que $z.w = 1$.*

**Afirmação:** O conjunto $(\mathbb{Z}[\sqrt{-2}])^* = \{z|N(z) = 1\} = \{\pm 1\}$ é o conjunto dos elementos invertíveis de $\mathbb{Z}[\sqrt{-2}]$.
De fato, se $z = a + b\sqrt{-2}$ é invertível em $\mathbb{Z}[\sqrt{-2}]$, então $1 = N(z.w) = N(z)N(w)$ implicando que $N(z) = 1 \Leftrightarrow a^2 + 2b^2 = 1 \Leftrightarrow a = \pm 1, b = 0,$ daí $z = \pm 1$. Então, como os dois possuem inverso são $\pm 1$ temos, $(\mathbb{Z}[\sqrt{-2}])^* = \{z|N(z) = 1\} = \{\pm 1\}$ é o conjunto dos elementos invertíveis de $\mathbb{Z}[\sqrt{-2}]$.

### 1.2.3 Divisibilidade em $\mathbf{Z}[\sqrt{-2}]$

De maneira inteiramente análoga a divisibilidade em $\mathbb{Z}[i]$ podemos definir a divisibilidade em $\mathbb{Z}[\sqrt{-2}]$. Vamos, então, a definição e algumas propriedades da divisibilidade em $\mathbb{Z}[\sqrt{-2}]$ que são semelhantes a $\mathbb{Z}[i]$.

**Definição 1.15** *Para $z, w \in \mathbb{Z}[\sqrt{-2}]$, dizemos que $z$ divide $w$ se existe $u \in \mathbb{Z}[\sqrt{-2}]$, não-nulo, tal que $w = z.u$.*

Denotaremos que $z$ divide $w$ da seguinte forma: $z|w$.

**Exemplo 1.22** *Note que $2 - \sqrt{-2}|6$ pois, $6 = (2 - \sqrt{-2})(2 + \sqrt{-2})$.*

Vejamos algumas propriedades da divisibilidade em $\mathbb{Z}[\sqrt{-2}]$ na seguinte proposição:

**Proposição 1.14** *Sejam $z, w, u \in \mathbb{Z}[\sqrt{-2}]$. Então,*

1. *$1|z$ e $z|z$;*
2. *Se $z|1$, então $z = 1$ ou $-1$;*
3. *Se $z|w$ e $w|u$, então $z|u$;*

*4. Se $z|w$, então $N(z)|N(w)$.*

*Demonstração:*

*De fato, como $z = 1.z$, assim provamos 1. Se $z|1$, temos que existe $v \in \mathbb{Z}[\sqrt{-3}]$ tal que $1 = z.v$, logo $1 = N(z).N(v)$, o que significa dizer que $z \in (\mathbb{Z}[\sqrt{-3}])^*$, isto é, $z = 1$ ou $-1$, com isso provamos 2. Agora, se $z|w$ e $w|u$, tem-se que existem $v, s \in \mathbb{Z}[\sqrt{-2}]$ tais que $w = z.v$ e $u = w.s$, logo $u = z.v.s = (v.s).z$, ou seja, $z|u$. Finalmente, se $z|w$, existe $v \in \mathbb{Z}[\sqrt{-2}]$ tal que $w = z.v$, logo $N(w) = N(z).N(v)$, ou seja, $N(z)|N(w)$, o que conclui a demonstração.*

■

### 1.2.4 Divisão Euclidiana em $\mathbf{Z}[\sqrt{-2}]$

Assim como no conjunto $\mathbb{Z}[i]$, a divisão euclidiana em $\mathbb{Z}[\sqrt{-2}]$ funciona da mesma forma. Portanto, em $\mathbb{Z}[\sqrt{-2}]$ temos a seguinte formulação para a divisão euclidiana:

**Proposição 1.15** *Dados $z, w \in \mathbb{Z}[\sqrt{-2}]$ com $w \neq 0$, existem $q, r \in \mathbb{Z}[\sqrt{-2}]$ com $z = wq + r$ e $0 \leq N(r) < N(w)$.*

*Demonstração:*

*Basta dividir $z = x + y\sqrt{-2}, w = a + b\sqrt{-2}$, onde $x, y, a, b \in \mathbb{Z}$. Então,*

$$\frac{z}{w} = \frac{x + y\sqrt{-2}}{a + b\sqrt{-2}}.\frac{a - b\sqrt{-2}}{a - b\sqrt{-2}} = \frac{xa - xb\sqrt{-2} + ya\sqrt{-2} - yb\left(\sqrt{-2}\right)^2}{a^2 + 2b^2} = \frac{xa + 2yb}{a^2 + 2b^2} + \frac{ya - xb}{a^2 + 2b^2}\sqrt{-2}.$$

*Tomando $m$ e $n$ como os inteiros mais próximos de $\frac{xa + 2yb}{a^2 + 2b^2}$ e $\frac{ya - xb}{a^2 + 2b^2}$, respectivamente, temos que*

$$\left|m - \frac{xa + 2yb}{a^2 + 2b^2}\right|, \left|n - \frac{ya - yb}{a^2 + 2b^2}\right| \leq \frac{1}{2}.$$

*Se $q = m + n\sqrt{-2}$, então:*

$$r = z - wq = w\left(\frac{z}{w} - q\right) = w\left(\frac{xa + 2yb}{a^2 + 2b^2} - m + \left(\frac{ya - yb}{a^2 + 2b^2} - n\right)\sqrt{-2}\right),$$

*o que implica,*

$$N(r) \leq N(w)\left(\left(\frac{1}{2}\right)^2 + 2.\left(\frac{1}{2}\right)^2\right) = \frac{3}{4}.N(w) < N(w).$$

■

### 1.2.5 Lema de Euclides

Utilizaremos a divisão euclidiana para demonstrar o *Lema de Euclides,* mas, primeiramente, daremos uma definição de primo em $\mathbb{Z}[\sqrt{-2}]$.

**Definição 1.16** *Dizemos que $p$ é primo em $\mathbb{Z}[\sqrt{-2}]$, quando $p$ não pode ser escrito como produto de dois inteiros de $\mathbb{Z}[\sqrt{-2}]$ cujas normas são maiores que* 1.

**Exemplo 1.23** *Verificar que $z = 0 + \sqrt{-2}$ é primo em $\mathbb{Z}[\sqrt{-2}]$.*

*De fato, suponha que existam $w, u \in \mathbb{Z}[\sqrt{-2}]$ tais que $0 + \sqrt{-2} = w.u$, então $2 = N(w).N(u)$. Logo, $w$ ou $u$ tem norma igual a* 1. *Portanto, $z = 0 + \sqrt{-2}$ é um primo em $\mathbb{Z}[\sqrt{-2}]$.*

Veremos, mais adiante, que os produtos de $0+\sqrt{-2}$ pelos elementos de $(\mathbb{Z}[\sqrt{-2}])^*$ são todos primos.

O próximo resultado nos auxilia na verificação da primalidade em $\mathbb{Z}[\sqrt{-2}]$.

**Proposição 1.16** *Se $N(z)$ é primo em $\mathbb{Z}$, então $z$ é primo em $\mathbb{Z}[\sqrt{-2}]$.*
*Demonstração:*

*Suponha que $z$ não é primo em $\mathbb{Z}[\sqrt{-2}]$. Então, existem $w, u \in \mathbb{Z}[\sqrt{-2}], w, u \neq 0$, tais que $z = wu$ e $N(w), N(u) > 1$. Isto é uma contradição pois, $N(z)$ é primo em $\mathbb{Z}$.*

■

**Exemplo 1.24** *Verificar que $3 - \sqrt{-2}$ é primo de $\mathbb{Z}[\sqrt{-2}]$.*

*Com efeito, como $N(3 - \sqrt{-2}) = 11$ e 11 é primo em $\mathbb{Z}$ temos $z$ primo em $\mathbb{Z}[\sqrt{-2}]$.*

O próximo resultado, *Lema de Euclides,* nos garante que se um primo em $\mathbb{Z}[\sqrt{-2}]$ divide um produto de dois inteiros quadráticos, então ele divide um dos fatores.

**Lema 1.2 (Lema de Euclides)** *Se $p$ é um primo em $\mathbb{Z}[\sqrt{-2}]$, com $a, b \in \mathbb{Z}[\sqrt{-2}]$ e $p|ab$, então $p|a$ ou $p|b$.*

*Demonstração:*

*Para demonstrá-lo, vamos fazer sucessivas divisões euclidianas, sendo $x_0 = a$ e $x_1 = p$. Seja $x_{k+2}$ o resto da divisão euclidiana de $x_k$ por $x_{k+1}$. Temos então as divisões:*

$$x_0 = q_1 x_1 + x_2$$

$$x_1 = q_2 x_2 + x_3$$

$$x_2 = q_3 x_3 + x_4$$

.....

$$x_{n-2} = q_{n-1} x_{n-1} + x_n$$

$$x_{n-1} = q_n x_n + x_{n+1}$$

*Observe que como $x_k \neq 0 \Rightarrow N(x_{k+1}) < N(x_k)$, podemos tomar $n$ tal que $N(x_{n+1}) = 0$, ou seja, $x_{n+1} = 0$. Logo $x_n|x_{n-1}$. Observe que $x_n|x_{k-1}$ e $x_n|x_k$. Logo, $x_n|x_n$ e $x_n|x_{n-1}$, então indutivamente, $x_n|x_k, \forall k, 0 \leq k \leq n$, particularmente $x_n|x_0 = a$ e $x_n|x_1 = p$. Tomando as $j+1$ primeiras equações e realizando substituições adequadas, temos que $x_j = a_j x_1 + y_j x_0 = a_j p + y_j a$; particularmente $x_n = a_n p + y_n a$. Se $p|a$ então o lema está demonstrado. Se $p$ não divide $a$, então, como $x_n|p, x_n|a$ e $x_n = a_n p + y_n a$, então $x_n \in \{\pm 1\}$ e temos: $x_n = a_n p + y_n a$ se, e somente se, $b = (x_n)^{-1}(b a_n p + y_n ab)$ implicando que $p|b$, o que conclui a demonstração.*

■

### 1.2.6 Fatoração Única em $\mathbf{Z}[\sqrt{-2}]$

A fatoração única é uma das propriedades mais usadas em problemas envolvendo números inteiros. Vamos prová-la para o conjunto $\mathbb{Z}[\sqrt{-2}]$. Primeiramente provaremos que todo inteiro $z \in \mathbb{Z}[\sqrt{-2}]$ com norma maior que 1 pode ser escrito como o produto de um ou mais primos de $\mathbb{Z}[\sqrt{-2}]$. Se $N(z) = 2$, como 2 é primo e a norma é multiplicativa, então $z$ é primo, o resultado está provado. Considere $N(z) > 2$. Se $z$ é primo a fatoração é imediata. Se $z$ não é primo, então $z = ab$ implicando que $N(z) = N(a).N(b)$, onde

$N(a), N(b) > 1$, portanto $N(a), N(b) < N(z)$. Podemos supor, por indução, que se $N(x) < N(z)$, então $x$ é fatorável. Logo, $a$ e $b$ são fatoráveis, e portanto $z$ o é. Para provar que esta fatoração é única, basta considerar as duas fatorações $p_1p_2...p_n$ e $q_1q_2...q_m$. Suponha, por indução, $p_1p_2...p_n = \xi q_1q_2...q_m$, sendo $\xi$ uma unidade, implica que a sequência $(p_i)$ é uma permutação( a menos que sejam multiplicações pelos invertíveis) da $(q_i)$. Se máx$\{n; m\} = 1$, então o resultado é imediato. Supondo que ele vale se
máx$\{n'; m'\} <$ máx$\{n; m\}$, pelo *Lema de Euclides,* vemos que para algum $i, p_n|q_i$. Sem perda de generalidade, podemos supor $i = m$. Como $p_n$ e $q_m$ são primos, então $q_m = \xi' p_n$, onde $\xi'$ é uma unidade. Logo $p_1p_2...p_n = \xi q_1q_2...q_m \Leftrightarrow p_1p_2..p_{n-1} = \xi\xi' q_1q_2..q_{m-1}$. Por indução, $p_1, p_2, ..., p_{n-1}$ é uma permutação( a menos que seja multiplicações pelos invertíveis) de $q_1, q_2, ..., q_m$, portanto a fatoração é única. Com isso, provamos a seguinte proposição:

**Proposição 1.17** *Seja $z \in \mathbb{Z}[\sqrt{-2}]$, então existem $z_1, z_2, ..., z_n \in \mathbb{Z}[\sqrt{-2}]$, únicos e primos, tais que $z = z_1.z_2...z_n$.*

**Exemplo 1.25** *Considere as seguintes fatorações*

1. *Para $z = 3$, temos $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$ onde $1 + \sqrt{-2}$ e $1 - \sqrt{-2}$ são primos;*
2. *Para $z = 11$, temos $11 = (3 + \sqrt{-2})(3 - \sqrt{-2})$ onde $3 + \sqrt{-2}$ e $3 - \sqrt{-2}$ são primos.*

### 1.2.7 Elementos Primos em Z$[\sqrt{-2}]$

Agora vamos procurar os primos em $\mathbb{Z}[\sqrt{-2}]$. Note que se $N(z)$ é primo em $\mathbb{Z}$, então $z$ é um primo de $\mathbb{Z}[\sqrt{-2}]$ (pois se $z$ fatora então $N(z)$ fatora). Observe que todo primo $z$ divide $N(z)$, portanto ele deve dividir ao menos um fator primo em $\mathbb{Z}$ de $N(z)$. Se $z$ dividir ao menos dois números distintos (absolutamente) $x$ e $y$ primos em $\mathbb{Z}$, como sempre é possível tomar $a, b \in \mathbb{Z}$ tal que $ax + by = 1$, teríamos $z|1$, um absurdo. Logo, todo primo de $\mathbb{Z}[\sqrt{-2}]$ divide exatamente um primo inteiro positivo (e seu oposto da soma) em $\mathbb{Z}$. Seja esse primo inteiro positivo $p$. Temos 3(três) casos:

1. Se $p$ é par, então $p = 2$. Sendo $z = a + b\sqrt{-2}$, então $N(z) = a^2 + 2b^2 = 2$, ou seja, $z = \pm\sqrt{-2}$, e obtemos os dois primos $0 + \sqrt{-2}$ e $0 - \sqrt{-2}$.

2. Se $p \equiv 5$ ou $7(mod\,8)$. Note que $x \equiv 0, 1, ..,$ ou $7(mod\,8)$, então $x^2 \equiv 0, 1$ ou $4(mod\,8)$. Queremos mostrar que $p$ é um primo em $\mathbb{Z}[\sqrt{-2}]$. Suponha que $p$ não é primo de $\mathbb{Z}[\sqrt{-2}]$, então existem $z = c + d\sqrt{-2}, w = a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, com $1 < N(z), N(w) < p^2$, tais que $p = zw$. Como $p$ é um inteiro primo, devemos ter $w = \overline{z} = c - d\sqrt{-2}$, logo $p = c^2 + 2d^2$. Agora, $p = c^2 + 2d^2 \equiv 0, 1, 2, 3$ ou $6(mod\ 8)$, o que é um absurdo, pois por hipótese $p \equiv 5$ ou $7(mod\ 8)$. Portanto, $p$ é um primo em $\mathbb{Z}[\sqrt{-2}]$.

3. Se $p \equiv 1$ ou $3\ mod\ 4$. Dado $x = 1.2.....(p-1)$, temos:

$$x^2 \equiv 1.2.....(p-1).1.2.....(p-1) \equiv -2(mod\ p).$$

Logo, $p|x^2 + 2 = (x + \sqrt{-2})(x - \sqrt{-2})$. Suponha que $p$ é um primo de $\mathbb{Z}[\sqrt{-2}]$, então pelo *Lema de Euclides* $p|(x + \sqrt{-2})$ ou $p|(x - \sqrt{-2})$. Daí, existem $z_1, z_2 \in \mathbb{Z}[\sqrt{-2}]$ tais que $x + \sqrt{-2} = p.z_1$ ou $x - \sqrt{-2} = pz_2$. Mas, teríamos $z_1 = \frac{1}{p}x + \frac{1}{p}\sqrt{-2}$ ou $z_2 = \frac{1}{p}x - \frac{1}{p}\sqrt{-2}$ e $\frac{1}{p}$ não é inteiro. Logo, $p$ não é primo de $\mathbb{Z}[\sqrt{-2}]$, daí existem $z = a + b\sqrt{-2}, w = c + d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, com $1 < N(z), N(w) < p^2$, tais que $p = wz = (a+bi)(c+di) = (ac-2bd)+(bc+ad)\sqrt{-2}$. Como $p \in \mathbb{Z}$, então $bc = -ad$, ou seja, $a = c$ e $b = -d$ ou $a = -c$ e $b = d$, com isso concluímos que $w = \pm\overline{z}$. Logo, como $p > 0$ segue que $w = \overline{z}$ e $N(z) = p(p = a^2+2b^2)$, portanto concluímos que $z$ é primo e mais $z$ e seu conjugado são os únicos primos em $\mathbb{Z}[\sqrt{-2}]$ que dividem $p$.
Com base no exposto acima, vimos que os únicos primos em $\mathbb{Z}[\sqrt{-2}]$ são:

   (a) O primo $0 + \sqrt{-2}$ e seus produtos pelos invertíveis.

   (b) Os primos $p$ em $\mathbb{Z}$ tal que $p \equiv 5$ ou $7(mod\ 8)$ e seus produtos pelos invertíveis.

   (c) Para cada primo $p$ em $\mathbb{Z}$ tal que $p \equiv 1$ ou $3(mod\ 8)$, os primos $a + b\sqrt{-2}$, $a - b\sqrt{-2}$ e seus produtos pelos invertíveis, sendo $p = a^2 + 2b^2$.

### 1.2.8 Elementos Irredutíveis em $\mathbb{Z}[\sqrt{-2}]$

De maneira inteiramente análoga a $\mathbb{Z}[i]$ veremos que os conceitos de primo e irredutível também coincidem em $\mathbb{Z}[\sqrt{-2}]$, pois em $\mathbb{Z}[\sqrt{-2}]$ a fatoração também é única.

**Definição 1.17** *Um elemento $z \in \mathbb{Z}[\sqrt{-2}]$, não-nulo e não-invertível, é dito irredutível quando $z = wu$ com $w$ ou $u$ invertíveil em $\mathbb{Z}[\sqrt{-2}]$.*

**Exemplo 1.26** *Verificar que $z = 0 + \sqrt{-2}$ é irredutível em $\mathbb{Z}[\sqrt{-2}]$.*

*De fato, escrevendo $0 + \sqrt{-2} = wu$, com $w, u \in \mathbb{Z}[\sqrt{-2}]$, temos $2 = N(w)N(u)$. Logo, $N(w) = 1$ ou $N(u) = 1$ e daí, concluimos que $w$ ou $u$ é invertível em $\mathbb{Z}[\sqrt{-2}]$. Portanto, $z = 0 + \sqrt{-2}$ é irredutível em $\mathbb{Z}[\sqrt{-2}]$.*

**Observação 1.7** *É facil verificar que os produtos de $0 + \sqrt{-2}$ pelos invertíveis também são irredutíveis em $\mathbb{Z}[\sqrt{-2}]$.*

O próximo resultado mostra que um elemento $p$ é primo em $\mathbb{Z}[\sqrt{-2}]$ se, e somente se, $p$ é irredutível em $\mathbb{Z}[\sqrt{-2}]$.

**Proposição 1.18** *Seja $p \in \mathbb{Z}[\sqrt{-2}]$, com $p$ não-nulo e não-invertível. Então $p$ é um elemento primo de $\mathbb{Z}[\sqrt{-2}]$ se, e somente se, $p$ é um elemento irredutível de $\mathbb{Z}[\sqrt{-2}]$.*
*Demonstração:*

*Se $p = wu$ com $w, u \in \mathbb{Z}[\sqrt{-2}]$, então $p|wu$ e, como $p$ é primo, temos que $p|w$ ou $p|u$. Por outro lado, $u|p$ e $w|p$. Logo $w$ ou $u$ é invertível, mostrando assim que $p$ é um elemento irredutível de $\mathbb{Z}[\sqrt{-2}]$. Por outro lado, seja $p \in \mathbb{Z}[\sqrt{-2}]$ um elemento irredutível. Então $p$ é não-nulo e não-invertível. Se $w, u \in \mathbb{Z}[\sqrt{-2}]$ são tais que $p|wu$, escrevendo $w = w_1...w_r$ e $u = u_1...u_s$, com $w_i$ e $u_j$ elementos irredutíveis de $\mathbb{Z}[\sqrt{-2}]$, temos que uma fatoração para $ab$ é*

$$ab = w_1....w_r.u_1....u_s.$$

*Como $p|wu$, temos que $wu = pz$, para algum $z \in \mathbb{Z}[\sqrt{-2}]$. Pela unicidade da fatoração de $wu$, temos que $p = w_i v$ ou $p = u_j v$, com $v$ invertível, para algum índice $i, j$. Agora, se $p|w_i$ e $w_i|w$, implica que $p|w$, por outro lado se $p|u_j$ e $u_j|u$, implica que $p|u$, o que mostra que $p$ é primo.*

■

# Capítulo 2

# Reciprocidade Quadrática

Neste capítulo destacaremos o símbolo de Legendre, o critério de Euler e a Lei de Reciprocidade Quadrática de Gauss.

## 2.1 Resíduos quadráticos e não-quadráticos

**Definição 2.1** *Sejam $m$ um inteiro positivo e $a$ um inteiro com $mdc(m, a) = 1$. Dizemos que $a$ é um inteiro resíduo quadrático $(mod\ m)$ se existe $x \in \mathbb{Z}$ tal que $x^2 \equiv a(mod\ m)$. Caso não exista tal inteiro, dizemos que $a$ é um resíduo não-quadrático $(mod\ m)$.*

**Exemplo 2.1** *Resíduos quadráticos mod 7.*

| | | |
|---|---|---|
| $1^2 \equiv 1(mod\ 7)$ | $2^2 \equiv 4(mod\ 7)$ | $3^2 \equiv 2(mod\ 7)$ |
| $4^2 \equiv 2(mod\ 7)$ | $5^2 \equiv 4(mod\ 7)$ | $6^2 \equiv 1(mod\ 7)$. |

*Note que, como $(a, 7) = 1, a \in \{1, 2, 3, 4, 5, 6\}$, os resíduos quadráticos $(mod\ 7)$ são $1, 2$ e $4$ e os resíduos não-quadráticos são $3, 5$ e $6$. Podemos escrever também $RQ_7 = \{1, 2, 7\}$ e $RNQ_7 = \{3, 5, 6\}$.*

## 2.2 Símbolo de Legendre

**Definição 2.2** *Seja $p$ um primo ímpar e $a$ um inteiro tal que $p$ não divide $a$. O símbolo de Legendre $\left(\frac{a}{p}\right)$ é definido por:*

$$\left(\tfrac{a}{p}\right) = \begin{cases} 1 \text{ se } a \text{ é resíduo quadrático módulo } p \\ -1 \text{ se } a \text{ é resíduo não-quadrático módulo } p. \end{cases}$$

**Exemplo 2.2** $\left(\frac{3}{11}\right) = 1$, *pois existe* $x \in \mathbb{Z}$ *tal que* $x^2 \equiv 3(mod\ 11)$; *por exemplo,* $x = 5$ *ou* $6$.

**Exemplo 2.3** $\left(\frac{2}{11}\right) = -1$, *pois não existe* $x \in \mathbb{Z}$ *tal que* $x^2 \equiv 2(mod\ 11)$; *de fato, se* $x \equiv 1, 2, ...., 10(mod\ 11)$, *então* $x^2 \not\equiv 2(mod\ 11)$.

## 2.3 Critério de Euler

Nesta seção, veremos um resultado importante, que nos ajudará a decidirmos se $a$ é um resíduo quadrático ou não.

**Teorema 2.3 (Critério de Euler)** *Seja* $p$ *um primo ímpar e* $a$ *um inteiro positivo com* $p$ *não dividindo* $a$. *Então* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(mod\ p)$.
*Demonstração:*

*Suponha* $\left(\frac{a}{p}\right) = 1$, *ou seja, a congruência* $x^2 \equiv a(mod\ p)$ *tem solução: digamos que* $x = x_0$ *seja uma solução, daí* $(x_0)^2 \equiv a(mod\ p)$. *Pelo teorema de Fermat:*

$$a^{p-1} \equiv 1(mod\ p) \Rightarrow a^{\frac{p-1}{2}} \equiv [(x_0)^2]^{\frac{p-1}{2}} \equiv (x_0)^{p-1} \equiv 1(mod\ p) \Rightarrow a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(mod\ p).$$

*Para* $\left(\frac{a}{p}\right) = -1$, *ou seja, a congruência* $x^2 \equiv a(mod\ p)$ *não tem solução. Logo, para cada* $1 \leq k \leq p-1$ *existe uma única solução* $1 \leq l \leq p-1$ *tal que* $kl \equiv a(mod\ p)$. *Como* $x^2 \equiv a(mod\ p)$ *não tem solução, então* $k \neq l(k$ *incongruente* $l(mod\ p)$, *pois, caso contrário teríamos* $k^2 \equiv a(mod\ p)(ou\ l^2 \equiv a(mod\ p))$. *Agrupando os inteiros* $1, 2, 3, ...., p-1$ *em* $\left(\frac{p-1}{2}\right)$ *pares* $(k, l)$ *com*

$$kl \equiv a(mod\ p) \Rightarrow 1.2.3...(p-2)(p-1) \equiv a^{\frac{p-1}{2}}(mod\ p) \Rightarrow (p-1)! \equiv -1 \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(mod\ p).$$

*Portanto,* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(mod\ p)$.

■

**Exemplo 2.4** *Pelo critério de Euler,* $\left(\frac{5}{23}\right) \equiv 5^{11} \equiv -1(mod\ 23)$, *então* $5$ *é um resíduo não-quadrático mod* $23$, *daí* $\left(\frac{5}{23}\right) = -1$.

**Teorema 2.4** *Seja* $p$ *um primo ímpar e* $a, b$ *inteiros não divisíveis por* $p$, *então*

1. *Se* $a \equiv b(mod\ p)$, *então* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2. $\left(\frac{a}{p}\right).\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

3. $\left(\frac{a^2}{p}\right) = 1$.

*Demonstração:*

1. *se* $a \equiv b(mod\ p)$, *então* $x^2 \equiv a(mod\ p)$ *tem sol.* $\Leftrightarrow x^2 \equiv b(mod\ p)$ *tem sol., daí,* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2. *De* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(mod\ p)$ *e* $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}}(mod\ p)$, *temos que:*

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(mod\ p) \Rightarrow \left(\frac{a}{p}\right).\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

3. $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right).\left(\frac{a}{p}\right) = 1$

■

**Exemplo 2.5** *Note que* $\left(\frac{75}{97}\right) = \left(\frac{3.5^2}{97}\right) = \left(\frac{3}{97}\right).\left(\frac{5^2}{97}\right) = 1$, *pois* $10^3 \equiv 3(mod\ 97)$. *Logo,* $\left(\frac{75}{97}\right) = 1$.

**Teorema 2.5** *Se* $p$ *é um primo ímpar então*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & , se\ p \equiv 1(mod\ 4) \\ -1 & , se\ p \equiv -1(mod\ 4) \end{cases}$$

*Demonstração:*

*Pelo critério de Euler:* $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}(mod\ p)$. *Se* $p \equiv 1(mod\ 4)$, *então* $p-1 = 4k, k \in \mathbb{Z}$. *Logo,* $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{4k}{2}}(-1)^{2k} \equiv 1(mod\ p) \Rightarrow \left(\frac{-1}{p}\right) = 1$. *Se* $p \equiv -1(mod\ 4)$, *então* $p+1 = 4k, k \in \mathbb{Z}$, *logo,* $p-1 = 2(2k-1)$.
*Logo,* $\left(\frac{-1}{p}\right) \equiv (-1)^{2k-1} \equiv -1(mod\ p) \Rightarrow \left(\frac{-1}{p}\right) = -1$.

■

**Exemplo 2.6** *Note que* $\left(\frac{-5}{23}\right) = \left(\frac{5}{23}\right).\left(\frac{-1}{23}\right)$. *Pelo critério de Euler,* $\left(\frac{5}{23}\right) \equiv 5^{11} \equiv -1(mod\ 23)$, *então* 5 *é um resíduo não-quadrático* $(mod\ 23)$, *daí* $\left(\frac{5}{23}\right) = -1$. *Como* $23 \equiv -1(mod\ 4)$, *temos que* $\left(\frac{-1}{23}\right) = -1$. *Portanto,* $\left(\frac{5}{23}\right).\left(\frac{-1}{23}\right) = (-1).(-1) = 1$, *ou seja,* $-5$ *é um resíduo quadrático* $(mod\ 23)$.

## 2.4 Lei de Reciprocidade Quadrática de Gauss

Vamos iniciar esta seção com a demonstração do seguinte resultado:

**Lema 2.1 (Lema de Gauss)** *Seja* $p$ *um primo ímpar e* $a$ *um inteiro com* $mdc(a,p) = 1$. *Seja* $s$ *o número dos menores resíduos quadráticos positivos dos inteiros* $a, 2a, 3a, ....., \frac{p-1}{2}a$ *que são maiores que* $\frac{p}{2}$, *então* $\left(\frac{a}{p}\right) = (-1)^s$.

*Demonstração:*

*Considere os inteiros* $a, 2a, 3a, ....., \frac{p-1}{2}a(*)$. *Sejam* $u_1, u_2, ...., u_s$ *os maiores resíduos positvos destes inteiros* $(*)$ *que são maiores que* $\frac{p}{2}$ *e* $v_1, v_2, ...., v_t$ *os menores resíduos positvos destes inteiros* $(*)$ *que são menores que* $\frac{p}{2}$. *Vamos mostrar que*

$$p - u_1, ...., p - u_s, v_1, ...., v_t(1)$$

*são exatamente os inteiros* $a, 2a, 3a, ....., \frac{p-1}{2}a(mod\ p)$. *De fato, dados quaisquer dois inteiros de* $(1)$, *nenhum deles são congruentes mod* $p$*(pois, são menores que* $p-1$*). Ou seja,* $u_i \not\equiv u_j(mod\ p)$ *e* $v_i \not\equiv v_j(mod\ p), \forall i \neq j$. *Digamos que ocorra uma dessas congruências, teríamos* $ma \equiv na(mod\ p)$, *onde* $m$ *e* $n$ *são inteiros com* $1 \leq m, n \leq \frac{p-1}{2}$. *Também se* $p - u_i \not\equiv v_j(mod\ p)$, *caso venha acontecer teríamos* $p - ma \equiv na(mod\ p)$, *o que implica,* $m \equiv -n(mod\ p)$*(impossível). Portanto,* $p - u_1, ...., p - u_s, v_1, ...., v_t(1)$ *são os inteiros* $(*)$ *em alguma ordem. Portanto,*

$$(p - u_1)....(p - u_s).v_1....v_t = 1.2..... \left(\frac{p-1}{2}\right) = \left(\frac{p-1}{2}\right)! \Rightarrow$$

$$(-u_1)(-u_2)...(-u_s).v_1....v_t \equiv \left(\frac{p-1}{2}\right)!(mod\ p) \Rightarrow$$

$$(-1)^s u_1.u_2...u_s.v_1.v_2...v_t \equiv \left(\frac{p-1}{2}\right)!(mod\ p).$$

*Sabemos que* $u_1, u_2, ...., u_s, v_1, ...., v_t$ *são os menores resíduos positivos de* $(*)$, *então*

$$u_1.u_2...u_s.v_1.v_2...v_t \equiv a.2a.3a... \left(\frac{p-1}{2}\right) a \equiv a^{\frac{p-1}{2}}.\left(\frac{p-1}{2}\right)!(mod\ p).$$

*Portanto,* $(-1)^s \equiv a^{\frac{p-1}{2}}(mod\ p)$,*e pelo critério de Euler,* $\left(\frac{a}{p}\right) = (-1)^s$.

■

**Teorema 2.6** *Se* $p$ *é um primo ímpar então*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & , se\ p \equiv \pm 1(mod\ 8) \\ -1 & , se\ p \equiv \pm 3(mod\ 8) \end{cases}$$

*Demonstração:*

*No Lema de Gauss, tome* $a = 2$. *Se* $p \equiv 1(mod\ 4)$, *digamos* $p = 4k+1$, *temos* $\frac{p-1}{2} = 2k$. *Como* $1 \leq 2j \leq \frac{p-1}{2}$ *para* $j \leq k$ *e* $\frac{p-1}{2} < 2j \leq p-1$ *para* $k+1 \leq j \leq 2k$, *temos*

$$\left(\frac{2}{p}\right) = (-1)^k = \begin{cases} 1 & , se\ p \equiv 1(mod\ 8) \\ -1 & , se\ p \equiv 5(mod\ 8) \end{cases}$$

*Se* $p \equiv 3(mod\ 4)$, *digamos* $p = 4k+3$, *temos* $\frac{p-1}{2} = 2k+1$.
*Para* $1 \leq j \leq k$ *temos* $1 \leq 2j \leq \frac{p-1}{2}$ *e para* $k+1 \leq j \leq 2k+1$ *temos* $\frac{p-1}{2} < 2j \leq p-1$ *donde*

$$\left(\frac{2}{p}\right) = (-1)^{k+1} = \begin{cases} 1 & , se\ p \equiv 3(mod\ 8) \\ -1 & , se\ p \equiv 7(mod\ 8) \end{cases}$$

*Portanto,*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & , se\ p \equiv \pm 1(mod\ 8) \\ -1 & , se\ p \equiv \pm 3(mod\ 8) \end{cases}$$

■

**Exemplo 2.7** *Note que* $\left(\frac{-2}{569}\right) = \left(\frac{-1}{569}\right).\left(\frac{2}{569}\right) = 1.1 = 1$, *logo* $-2$ *é um resíduo quadrático* $(mod\ 569)$( *observe que,* $569 \equiv 1(mod\ 4)$ *e* $569 \equiv 1(mod\ 8)$).

**Teorema 2.7** *Se $p$ é um primo ímpar e $a$ um inteiro ímpar não-divisível por $p$, então,*

$$\left(\frac{a}{p}\right) = (-1)^M$$

*onde*

$$M = \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2a}{p} \right\rfloor + ..... + \left\lfloor \frac{p-1}{2}.\frac{a}{p} \right\rfloor .$$

*Demonstração:*

*Pelo Algoritmo da divisão podemos obter os menores resíduos positivos de* $a, 2a, 3a, ...., \dfrac{(p-1)a}{2}$ *através das divisões seguintes:*

$$a = p\left\lfloor \frac{a}{p} \right\rfloor + r_1$$

$$2a = p\left\lfloor \frac{2a}{p} \right\rfloor + r_2$$

$$3a = p\left\lfloor \frac{3a}{p} \right\rfloor + r_3$$

$$.....$$

$$\frac{p-1}{2}a = p\left\lfloor \frac{p-1}{2}.\frac{a}{p} \right\rfloor + r_{\frac{p-1}{2}}$$

*onde* $r_1, r_2, ....., r_{\frac{p-1}{2}}$ *são os* $u_i$ *e* $v_i$ *definidos na demonstração do Lema* 2.1. *Se somarmos, membro a membro, as* $\dfrac{p-1}{2}$ *igualdades acima obteremos*

$$a\left(1+2+3+...+\frac{p-1}{2}\right) = p\left(\left\lfloor \frac{a}{p} \right\rfloor + p\left\lfloor \frac{2a}{p} \right\rfloor + ... + \left\lfloor \frac{p-1}{2}.\frac{a}{p} \right\rfloor\right) + r_1 + r_2 + ... + r_{\frac{p-1}{2}}$$

*ou seja*

$$\frac{p^2-1}{8}a = pM + I + S(*)$$

*onde* $I$ *e* $S$ *são, respectivamente, as somas dos resíduos inferiores e superiores a* $\frac{p}{2}$, *isto é,*

$$I = u_1 + u_2 + .... + u_s$$

*e*

$$S = v_1 + v_2 + .... + v_t.$$

*Vimos, também, na demonstração do Lema* 2.1 *que os números* $p-u_1, ...., p-u_s, v_1, ...., v_t$

*são, a menos da ordem, os números* $a, 2a, 3a, ....., \frac{p-1}{2}$. *Logo,*

$$a + 2a + 3a + .... + \frac{p-1}{2} = \frac{p^2-1}{8} = v_1 + v_2 + .... + v_t + sp - (u_1 + u_2 + .... + u_s)$$

*isto é,*

$$\frac{p^2-1}{8} = S + sp - I.(**)$$

*Subtraindo, membro a membro, as equações* $(*)$ *e* $(**)$ *obtemos* $\frac{p^2-1}{8}(a-1) = p(M-s)+2I$. *Como, por hipótese,* $a$ *e* $p$ *são ímpares o termo* $\frac{p^2-1}{8}(a-1)$ *será par e, portanto,* $p(M-s)$ *também. Logo,* $M-s$ *é par. Mas, se esta diferença é par, é porque ambos são pares ou ambos são ímpares. Portanto, pelo Lema* 2.1, *concluímos que*

$$\left(\frac{a}{p}\right) = (-1)^s = (-1)^M$$

*uma vez que* $M$ *e* $s$ *possuem a mesma paridade.*

■

O próximo resultado, que se chama *Lei de Reciprocidade de Gauss* já fora demonstrado de muitas maneiras distintas. A lei nos diz: para $p$ e $q$ primos ímpares, as congruências $x^2 \equiv p(mod\ q)$ e $x^2 \equiv q(mod\ p)$ são ambas solúveis ou ambas insolúveis, a menos que $p$ e $q$ sejam congruentes a 3 módulo 4, caso em que uma terá solução e a outra não. Vejamos, então, esse resultado.

**Teorema 2.8 (Lei de Reciprocidade Quadrática de Gauss)** *Se* $p$ *e* $q$ *são primos ímpares distintos, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

*Demonstração:*

*Consideremos um retângulo de vértices* $A = (0,0), B = (p/2, 0), C = (p/2, q/2)$ *e* $D = (0, q/2)$. *Marcamos, em seu interior, os pontos que pertencem ao produto catesiano dos conjuntos* $\{1, 2, 3, ..., (p-1)/2\}$ *e* $\{1, 2, 3, ..., (q-1)/2\}$. *É claro que o número de pontos interiores a este retângulo, cujas coordenadas são números inteiros, é igual a*

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right).$$

*Consideremos a equação da reta que passa por* $A$ *e* $C$, *isto é,* $y = (q/p)x$. *Como os*

*números* $1, 2, 3, ..., \frac{(p-1)}{2}$ *são todos primos com* $p$, *esta reta não contém nenhum dos pontos interiores que contamos acima. Esta reta,* $y = (q/p)x$, *intercepta as retas* $x = k$, *paralelas ao eixo* $y$, *nos pontos* $(K, kq/p)$. *Como* $\dfrac{kq}{p}$ *não é inteiro, para* $k \in \{1, 2, 3, ..., (p-1)/2\}$, *o número* $\left\lfloor \dfrac{kq}{p} \right\rfloor$ *é número de pontos da reta* $x = k$ *que estão acima do eixo* $x$ *e abaixo da reta* $y = (q/p)x$. *Logo, o total* $M$ *de pontos do nosso reticulado no interior do triângulo* $ABC$ *é dado por*

$$M = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + ..... + \left\lfloor \frac{p-1}{2}.\frac{q}{p} \right\rfloor .$$

*Se considerarmos, agora, as inteseções das retas* $y = k$, *paralelas ao eixo* $x$, *com a reta* $y = (q/p)x$, *obteremos, através de raciocínio análogo ao anterior, que o número* $N$ *dos pontos, que estamos considerando, no interior do triângulo* $ACD$ *é igual a*

$$N = \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + ..... + \left\lfloor \frac{q-1}{2}.\frac{p}{q} \right\rfloor .$$

*Portanto, temos a seguinte igualdade,*

$$M + N = \frac{p-1}{2}\frac{q-1}{2}.$$

*Mas, pelo Teorema* 2.7,

$$\left(\frac{p}{q}\right) = (-1)^M \ e \ \left(\frac{q}{p}\right) = (-1)^N$$

*o que implica*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

■

**Exemplo 2.8** *Vamos calcular* $\left(\dfrac{5}{p}\right)$, $p$ *primo ímpar maior que* 5.

*Pelo Teorema* 3.7, *temos* $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).(-1)^{2\left(\frac{p-1}{2}\right)} = \left(\frac{p}{5}\right)$. *Como*

$$\left(\frac{p}{5}\right) = \begin{cases} \left(\frac{1}{5}\right) = 1 & , \text{ se } p \equiv 1(mod\ 5) \\ \left(\frac{2}{5}\right) = -1 & , \text{ se } p \equiv 2(mod\ 5) \\ \left(\frac{3}{5}\right) = -1 & , \text{ se } p \equiv 3(mod\ 5) \\ \left(\frac{4}{5}\right) = 1 & , \text{ se } p \equiv 4(mod\ 5) \end{cases}$$

*então*

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & , \text{ se } p \equiv \pm 1(mod\ 5) \\ -1 & , \text{ se } p \equiv \pm 2(mod\ 5) \end{cases}$$

**Teorema 2.9** *Se* $p > 3$ *é um primo então*

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & , \text{ se } p \equiv \pm 1(mod\ 12) \\ -1 & , \text{ se } p \equiv \pm 5(mod\ 12) \end{cases}$$

*Demonstração:*

*De fato, pela* ***LRQ***

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{(p-1)}{2}}.$$

*Agora, note que*

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 & \text{se } p \equiv 1(mod\ 3) \\ \left(\frac{2}{3}\right) = -1 & \text{se } p \equiv 2(mod\ 3) \end{cases}$$

*Por outro lado,*

$$(-1)^{\frac{(p-1)}{2}} = \begin{cases} 1 & \text{se } p \equiv 1(mod\ 4) \\ -1 & \text{se } p \equiv 2(mod\ 4) \end{cases}$$

*Assim,*

$\left(\frac{3}{p}\right) = 1$ *se, e somente se,* $p \equiv 1(mod\ 3)$ *e* $p \equiv 1(mod\ 4)$ *ou* $p \equiv 2(mod\ 3)$ *e* $p \equiv 2(mod\ 4)$ *se, e somente se,* $p \equiv 1(mod\ 12)$ *e* $p \equiv 11(mod\ 12)$ *se, e somente se,* $p \equiv \pm 1(mod\ 12)$. *Logo,* $\left(\frac{3}{p}\right) = -1$ *se, e somente se,* $p \equiv \pm 5(mod\ 12)$. *O que demonstra*

*o teorema.*

■

**Teorema 2.10** *Se $p$ é um primo ímpar então*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & , \text{ se } p \equiv 1 \text{ ou } 5(mod\ 12) \\ -1 & , \text{ se } p \equiv 7 \text{ ou } 11(mod\ 12) \end{cases}$$

*Demonstração:*

*Pelo critério de Euler:* $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}(mod\ p)$. *Para* $p \equiv 1$ *ou* $5(mod\ 12)$, *temos que* $\frac{p-1}{2}$ *é par, logo* $\left(\frac{-1}{p}\right) = 1$. *Agora, para* $p \equiv 7$ *ou* $11(mod\ 12)$ *temos que* $\frac{p-1}{2}$ *é ímpar, logo* $\left(\frac{-1}{p}\right) = -1$, *o que conclui a demonstração.*

■

# Capítulo 3

# Inteiros que se escrevem na forma $x^2 + qy^2,\ q = 1, 2$ e $3$.

Neste capítulo faremos a caracterização dos números primos ímpares que se escrevem como a soma de dois quadrados e os que se escrevem na forma $x^2 + 2y^2$ ou $x^2 + 3y^2$. Também caracterizaremos os primos ímpares que não são soma de dois quadrados e aqueles que não se escrevem na forma $x^2 + 2y^2$ ou na forma $x^2 + 3y^2$.

## 3.1 Inteiros que se escrevem na forma $x^2 + y^2$

Está seção irá tratar dos primos ímpares que se escrevem na forma $x^2 + y^2$, problema proposto e provado por Fermat em 1654. Faremos a caracterização destes números utilizando os seguintes passos:

*Passo* 1 : Concluir que um inteiro $n$ é da forma $x^2 + y^2$ se, e somente se, $n$ é da forma $N(x + yi)$.

**Proposição 3.1** *Um número $n$ é da forma $(x^2 + y^2)$ se, e somente se, $n$ é da forma $N(x + yi)$.*

*Demonstração:*

*De fato, temos* $N(x + yi) = (x + yi)(x - yi) = x^2 + y^2$

■

*Passo* 2 : Podemos utilizar o *Lema de Euclides* em $\mathbb{Z}[i]$, como vimos anteriormente.

*Passo* 3 : Experimentaremos valores inteiros $n$ para ver se podemos encontrar um padrão quanto aos que são da forma $x^2 + y^2$ e os que não são.
Vamos considerar a situação para valores pequenos de $n$, na seguinte tabela:

| | |
|---|---|
| $n = 1 : 2 = 0^2 + 1^2$ | $n = 2$ (primo) $: 2 = 1^2 + 1^2$ |
| $n = 3$ (primo) não é soma de dois quadrados | $n = 4 : 4 = 2^2 + 0^2$ |
| $n = 5$ (primo) $: 5 = 2^2 + 1^2$ | $n = 6$ não é soma de dois quadrados |
| $n = 7$ (primo) não é soma de dois quadrados | $n = 8 : 8 = 2^2 + 2^2$ |
| $n = 9 : 9 = 3^2 + 0^2$ | $n = 10 : 10 = 3^2 + 1^2$ |
| $n = 11$ (primo) não é soma de dois quadrados | $n = 12$ não é soma de dois quadrados |
| $n = 13$ (primo) $: 13 = 3^2 + 2^2$ | $n = 14$ não é soma de dois quadrados |
| $n = 15$ não é soma de dois quadrados | $n = 16 : 16 = 4^2 + 0^2$ |
| $n = 17$ (primo) $: 17 = 4^2 + 1^2$ | $n = 18 : 18 = 3^2 + 3^2$ |
| $n = 19$ (primo) não é soma de dois quadrados | $n = 20 : 20 = 4^2 + 2^2$ |
| $n = 21$ não é soma de dois quadrados | $n = 22$ não é soma de dois quadrados |
| $n = 23$ (primo) não é soma de dois quadrados | $n = 24$ não é soma de dois quadrados |
| $n = 25 : 25 = 5^2 + 0^2$ | $n = 26 : 26 = 5^2 + 1^2$ |
| $n = 27$ não é soma de dois quadrados | $n = 28$ não é soma de dois quadrados |
| $n = 29$ (primo) $: 29 = 5^2 + 2^2$ | $n = 30$ não é soma de dois quadrados |
| $n = 31$ (primo) não é soma de dois quadrados | $n = 32 : 32 = 4^2 + 4^2$. |

Nós podemos continuar a lista, no entanto, o padrão aparente já é fácil de imaginar: $5, 13$ e $17$ são da forma $x^2 + y^2$, qualquer primo $p \equiv 1(mod\ 4)$ é da forma $x^2 + y^2$, e qualquer primo $p \equiv 3(mod\ 4)$ não é da forma $x^2 + y^2$, por exemplo, os primos 3 e 7.

*Passo* 4 : Demonstrar o *Lema de Fermat:*

**Lema 3.1 (Lema Fermat)** *Para $p \equiv 1(mod\ 4)$, existe algum $x \in \mathbb{Z}$ tal que $p|x^2 + 1$.*

Para demonstrar o *Lema de Fermat* vamos usar o teorema de Wilson.

**Proposição 3.2** *Sejam $a, m \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1(mod\ m)$ possui uma solução $x_0$ se, e somente se, $mdc(a, m) = 1$. Além disso, $x$ é uma solução da congruência se, e somente se, $x \equiv x_0(mod\ m)$.*
*Demonstração:*

*A congruência acima tem uma solução $x_0$ se, e somente se, $m|(ax_0 - 1)$, o que equivale a dizer que a equação diofantina $aX - mY = 1$ possui solução em naturais. Isto ocorre se, e somente se, $mdc(a, m) = 1$. Por outro lado, observe que, se $x$ e $x_0$ são soluções da congruência $aX \equiv 1(mod\ m)$, então $ax \equiv ax_0(mod\ m)$, o que implica, $x \equiv x_0(mod\ m)$ (pois, $mdc(a, m) = 1$). Observe, ainda, que se $x_0$ é solução da congruência $aX \equiv 1(mod\ m)$, e $x \equiv x_0(mod\ m)$, então $x$ também é solução da mesma congruência, pois*

$$ax \equiv ax_0 \equiv 1(mod\ m).$$

■

**Proposição 3.3 (Teorema de Wilson)** *Se $p$ é primo, então $p|(p-1)! + 1$.*
*Demonstração:*

*Para todo $l \in \{1, 2, 3, ..., p-1\}$, pela Proposição 3.2, a congruência $lX \equiv 1(mod\ p)$ possui uma única solução$(mod\ p)$. Ou seja, dado $l \in \{1, 2, 3, ..., p-1\}$ existe $j \in \{1, 2, 3, ..., p-1\}$ tal que $lj \equiv 1(mod\ p)$. Por outro lado, se $l \in \{1, 2, 3, ..., p-1\}$ é tal que $l^2 \equiv 1(mod\ p)$, então $p|(l^2 - 1)$, o que equivale a $p|(l-1)$ ou $p|(l+1)$, o que só pode ocorrer se $l = 1$ ou $l = p - 1$. Logo,*

$$2.3....(p-2) \equiv 1(mod\ p),$$

*e, portanto,*

$$1.2.3....(p-2).(p-1) \equiv (p-1)(mod\ p) \text{ se, e somente se, } p|(p-1)! + 1.$$

■

Agora, nos valendo do teorema de Wilson, podemos demonstrar o *Lema de Fermat.* De fato, se $p = 4n + 1$, então

$$-1 \equiv 1.2.3...4n \equiv (1.2...2n).((2n+1)...(4n-1).(4n)) \equiv$$

$$(1.2...2n).((-2n)....(-2).(-1)) \equiv (1.2...2n)^2(-1)^{2n} \equiv (1.2...2n)^2(mod\ p).$$

Basta tomar $x = (2n)!$ e daí $x^2 \equiv -1(mod\ p)$. Portanto, $p|x^2 + 1$.

**Observação 3.1** *Uma forma alternativa de demonstrar o Lema de Fermat é usando o Teorema* 2.5. *Com efeito, pelo Teorema* 2.5 *temos:*

$$\left(\frac{-1}{p}\right) = 1 \text{ se, e somente se, } p \equiv 1(mod\ 4).$$

*Portanto, de* $\left(\frac{-1}{p}\right) = 1$ *concluímos que existe* $x \in \mathbb{Z}$ *tal que* $x^2 \equiv -1(mod\ p)$, *ou seja,* $p|x^2 + 1$.

*Passo* 5 : Provado o *Lema de Fermat* usaremos o *Lema de Euclides* para mostrar que os primos $p = 4k + 1$, na classe de equivalência módulo 4, não podem ser irredutíveis em $\mathbb{Z}[i]$ e concluir que todos os números primos nessa classe são da forma $x^2 + y^2$.

**Proposição 3.4** *Se* $p \equiv 1(mod\ 4)$, *então p não é irredutível em* $\mathbb{Z}[i]$. *Daí, podemos concluir que p é da forma* $x^2 + y^2$.
*Demonstração:*

*Pelo Lema de Fermat se* $p \equiv 1(mod\ 4)$, *então existe algum* $x \in \mathbb{Z}$ *tal que* $p|(x^2+1)$. *Em* $\mathbb{Z}[i], x^2 + 1$ *tem a seguinte fatoração* $x^2 + 1 = (x + i)(x - i)$. *Queremos mostrar que p não pode ser irredutível em* $\mathbb{Z}[i]$. *Suponha p irredutível em* $\mathbb{Z}[i]$. *Pelo Lema Euclideano concluímos que* $p|(x+i)$ *ou* $p|(x-i)$. *Este fato é um absurdo: pois se* $p|(x+i)$ *ou* $p|(x-i)$, *então* $x + i = p.z_1$ *ou* $x - i = p.z_2$. *Mas,* $\frac{x}{p} + \frac{1}{p}i$ *e* $\frac{x}{p} - \frac{1}{p}i$ *não são inteiros gaussianos, pois certamente* $\frac{1}{p}$ *não é inteiro. Logo, p não é irredutível, então existem* $z = x + yi$, $w = a + bi \in \mathbb{Z}[i]$, *com* $1 < N(x + yi), N(a + bi) < p^2$, *tais que* $p = zw = (x + yi)(a + bi)$. *Desde que* $N(p) = N(p + 0i) = p^2$, *isto significa que*

$$p = N(x + yi) = (x + yi)(x - yi) = x^2 + y^2,$$

*como queríamos demonstrar.* ∎

Com isso, provamos o seguinte teorema:

**Teorema 3.1 (Soma de dois quadrados de Fermat)** *Se* $p = 4k + 1$ *é primo, então* $p = x^2 + y^2$.

*Passo* 6 : Finalmente, vamos mostrar que se $p \not\equiv 1(mod\ 4)$, então $p$ não é da forma $x^2 + y^2$.

**Proposição 3.5** *Se $p \equiv 3(mod\ 4)$, então $p$ não é da forma $x^2 + y^2$.*

*Demonstração:*

*Suponha $p = x^2 + y^2$; então reduzindo para módulo 4 teríamos $3 = x^2 + y^2$ em $\mathbb{Z}_4$. Na verdade isso não é possível: os quadrados em $\mathbb{Z}_4$ são $0 = 0^2 = 2^2$ e $1 = 1^2 = 3^2$. Daí, $x^2 + y^2 \in \{0, 1, 2\}$, ou seja, não podemos obter 3.*

■

**Conclusão 3.1** *Em resumo, temos $p = x^2 + y^2 \Leftrightarrow p \equiv 1(mod\ 4)$.*

O próximo resultado nos mostra como escrever, um número $m$ composto, na forma $x^2 + y^2$.

**Proposição 3.6** *Seja $m = p_1.p_2...p_n$, com $p_1, p_2, ..., p_n$ primos. Se $p_s = {x_s}^2 + {y_s}^2$, $\forall s = 1, 2, ..., n$, então $m = x^2 + y^2$, com $x, y \in \mathbb{Z}$.*

*Demonstração:*

*Vamos mostrar por indução finita sobre $n$. Com efeito, para $n = 2$, temos que: se $p_1 = a^2 + b^2$ e $p_2 = c^2 + d^2$, então $m = p_1.p_2 = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = (a^2c^2 + 2abcd + b^2d^2) + (a^2d^2 - 2abcd + b^2c^2) = (ac + bd)^2 + (ad - bc)^2$. Agora, suponha válido para $n = k$. Devemos mostrar válido para $n = k + 1$. De fato, veja que $m = p_1.p_2...p_k.p_{k+1} = (x^2 + y^2)({x_{k+1}}^2 + {y_{k+1}}^2) = (xx_{k+1} + yy_{k+1})^2 + (xy_{k+1} - yx_{k+1})^2$, ou seja, é válido para $n = k+1$. Portanto, pelo princípio de indução finita é válido para todo $n$ inteiro.*

■

**Exemplo 3.1** *Considere os seguintes valores de $n$ :*

1. *Se $n = 65$, temos $n = 65 = 5.13 = (2^2 + 1^2)(3^2 + 2^2) = 8^2 + 1^2$.*

2. *Se $n = 170$, temos $n = 170 = 2.5.17 = (1^2 + 1^2)(2^2 + 1^2)(4^2 + 1^2) = [(1.2 + 1.1)^2 + (1.1 - 1.2)^2](4^2 + 1^2) = (3^2 + 1^2)(4^2 + 1^2) = 13^2 + 1^2$.*

## 3.2 Inteiros que se escrevem na forma $x^2 + 2y^2$

Esta seção irá tratar dos primos ímpares que se escrevem na forma $x^2 + 2y^2$, problema análogo ao anterior. Faremos a caracterização destes números através dos seguintes

passos:

*Passo* 1*:* Concluir que um inteiro $n$ é da forma $x^2 + 2y^2$ se, e somente se, $n$ é da forma $N(x + y\sqrt{-2})$.

**Proposição 3.7** *Um inteiro $n$ é da forma $x^2 + 2y^2$ se, e somente se, é da forma $N(x + y\sqrt{-2})$.*

*Demonstração:*

*De fato, note que* $N(x + y\sqrt{-2}) = (x + y\sqrt{-2})(x - y\sqrt{-2}) = x^2 + 2y^2$.

■

*Passo* 2 : Podemos utilizar o *Lema de Euclides* em $\mathbb{Z}[\sqrt{-2}]$, como vimos anteriormente.

*Passo* 3 : Experimentaremos inteiros $n$ para ver se podemos encontrar um padrão quanto aos que são da forma $x^2 + 2y^2$ e os que não são.

Vamos considerar a situação para valores pequenos de $n$, na seguinte tabela:

| | |
|---|---|
| $n = 2(primo) : 2 = 0^2 + 2.1^2$ | $n = 3(primo) : 3 = 1^2 + 2.1^2$ |
| $n = 4 : 4 = 2^2 + 2.0^2$ | $n = 5(primo)$ não é da forma $x^2 + 2y^2$ |
| $n = 6 : 6 = 2^2 + 2.1^2$ | $n = 7(primo)$ não é da forma $x^2 + 2y^2$ |
| $n = 8$ não é da forma $x^2 + 2y^2$ | $n = 9 : 9 = 3^2 + 2.0^2$ |
| $n = 10$ não é da forma $x^2 + 2y^2$ | $n = 11(primo) : 11 = 3^2 + 2.1^2$ |
| $n = 12$ não é da forma $x^2 + 2y^2$ | $n = 13(primo)$ não é da forma $x^2 + 2y^2$ |
| $n = 14$ não é da forma $x^2 + 2y^2$ | $n = 15$ não é da forma $x^2 + 2y^2$ |
| $n = 16 : 16 = 4^2 + 2.0^2$ | $n = 17(primo) : 17 = 3^2 + 2.2^2$ |
| $n = 18$ não é da forma $x^2 + 2y^2$ | $n = 19(primo) : 19 = 1^2 + 2.3^2$ |
| $n = 20$ não é da forma $x^2 + 2y^2$ | $n = 21$ não é da forma $x^2 + 2y^2$ |
| $n = 22$ não é da forma $x^2 + 2y^2$ | $n = 23(primo)$ não é da forma $x^2 + 2y^2$ |
| $n = 24$ não é da forma $x^2 + 2y^2$ | $n = 25 : 25 = 5^2 + 2.0^2$ |

| | |
|---|---|
| $n = 26$ não é da forma $x^2 + 2y^2$ | $n = 27 : 27 = 5^2 + 2.1$ |
| $n = 28$ não é da forma $x^2 + 2y^2$ | $n = 29(primo)$ não é da forma $x^2 + 2y^2$ |
| $n = 30$ não é da forma $x^2 + 2y^2$ | $n = 31(primo)$ não é da forma $x^2 + 2y^2$ |
| $n = 32$ não é da forma $x^2 + 2y^2$ | $n = 33 : 33 = 5^2 + 2.2^2$ |
| $n = 34$ não é da forma $x^2 + 2y^2$ | $n = 35$ não é da forma $x^2 + 2y^2$ |
| $n = 36 : 36 = 6^2 + 2.0^2$ | $n = 37(primo)$ não é da forma $x^2 + 2y^2$ |
| $n = 38$ não é da forma $x^2 + 2y^2$ | $n = 39$ não é da forma $x^2 + 2y^2$ |
| $n = 40$ não é da forma $x^2 + 2y^2$ | $n = 41(primo) : 41 = 3^2 + 2.4^2$. |

Nós podemos continuar a lista, no entanto, o padrão aparente já é fácil de imaginar: $3, 11$ e $17$ são da forma $x^2 + 2y^2$, qualquer primo $p \equiv 1$ ou $3(mod\ 8)$ é da forma $x^2 + 2y^2$, e qualquer primo $p \equiv 5$ ou $7(mod\ 8)$ não é da forma $x^2 + 2y^2$, por exemplo 5 e 7.

*Passo* 4 : Com base no *passo* 3, podemos conjecturar um resultado análogo ao Lema de Fermat: Dado um número primo $p$ numa classe de equivalência adequada (neste caso, módulo 8), $p|(x^2 + 2)$.

**Lema 3.2** *Se $p \equiv 1$ ou $3(mod\ 8), p$ primo ímpar, então existe algum $x \in \mathbb{Z}$ tal que $p|(x^2 + 2)$.*

*Demonstração:*

*Pelo Teorema* 2.5 *e* 2.6, *temos*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & , \text{ se } p \equiv 1(mod\ 4) \\ -1 & , \text{ se } p \equiv -1(mod\ 4) \end{cases}$$

*e que*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & , \text{ se } p \equiv \pm 1(mod\ 8) \\ -1 & , \text{ se } p \equiv \pm 3(mod\ 8) \end{cases}$$

*Logo, se* $p \equiv 1(mod\ 8)$, *então* $\left(\frac{2}{p}\right) = 1$ *e, como* $p = 8k + 1 = 4(2k) + 1$, *daí* $\left(\frac{-1}{p}\right) = 1$.
*Então,* $\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right).\left(\frac{-1}{p}\right) = 1$. *Por outro lado, se* $p \equiv 3(mod\ 8)$, *então*
$\left(\frac{2}{p}\right) = -1$ *e, como* $p = 8k + 3 = 4(2k + 1) - 1$, *daí* $\left(\frac{-1}{p}\right) = -1$.
*Então,* $\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = (-1)(-1) = 1$. *Portanto,*

$$\left(\frac{-2}{p}\right) = 1, \text{ se } p \equiv 1 \text{ ou } 3(mod\ 8).$$

*Com isso, concluímos que existe algum* $x \in \mathbb{Z}$, *tal que* $-2 \equiv x^2 (mod\ p)$, *ou seja,* $p|(x^2+2)$.

■

*Passo* 5 : Provado o análogo ao Lema de Fermat usaremos o *Lema de Euclides* para mostrar que os primos ímpares na classe de equivalência módulo 8 não podem ser irredutíveis em $\mathbb{Z}[\sqrt{-2}]$ e concluir que todos os números primos ímpares nessa classe são da forma $x^2+2y^2$.

**Proposição 3.8** *Se* $p \equiv 1$ *ou* $3(mod\ 8), p$ *primo ímpar, então* $p$ *não é irredutível em* $\mathbb{Z}[\sqrt{-2}]$. *Daí, podemos concluir que* $p$ *é da forma* $x^2+2y^2$.
*Demonstração:*

*Pelo lema acima, se* $p \equiv 1$ *ou* $3(mod\ 8), p$ *primo ímpar, então existe algum* $x \in \mathbb{Z}$ *tal que* $p|(x^2+2)$. *Em* $\mathbb{Z}[\sqrt{-2}], x^2+2$ *tem a seguinte fatoração* $x^2+2 = (x+\sqrt{-2})(x-\sqrt{-2})$. *Queremos mostrar que* $p$ *não pode ser irredutível em* $\mathbb{Z}[\sqrt{-2}]$. *Suponha* $p$ *irredutível em* $\mathbb{Z}[\sqrt{-2}]$. *Pelo Lema de Euclides podemos concluir que* $p|(x+\sqrt{-2})$ *ou* $p/(x-\sqrt{-2})$. *Este fato é um absurdo: pois se* $p|(x+\sqrt{-2})$ *ou* $p|(x-\sqrt{-2})$, *então* $x+\sqrt{-2} = p.z_1$ *ou* $x-\sqrt{-2} = p.z_2$. *Mas,* $\frac{x}{p}+\frac{1}{p}\sqrt{-2}$ *e* $\frac{x}{p}-\frac{1}{p}\sqrt{-2}$ *não pertencem ao conjunto* $\mathbb{Z}[\sqrt{-2}]$, *pois certamente* $\frac{1}{p}$ *não é inteiro. Logo,* $p$ *não é irredutível, então existem* $z = x+y\sqrt{-2}, w = c+d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, *com* $1 < N(x+y\sqrt{-2}), N(c+d\sqrt{-2}) < p^2$, *tais que* $p = zw = (x+y\sqrt{-2})(c+d\sqrt{-2})$. *Desde que* $N(p) = N(p+0\sqrt{-2}) = p^2$, *isto significa que* $p = N(x+y\sqrt{-2}) = (x+y\sqrt{-2})(x-y\sqrt{-2}) = x^2+2y^2$, *como queríamos demonstrar.*

■

*Passo* 6*:* Finalmente, vamos mostrar que se $p \not\equiv 1$ e $3(mod\ 8)$, $p$ primo ímpar, então $p$ não é da forma $x^2+2y^2$.

**Proposição 3.9** *Se* $p \equiv 5$ *ou* $7(mod\ 8)$, *então* $p$ *não é da forma* $x^2+2y^2$.
*Demonstração:*

*Suponha* $p = x^2+2y^2$; *então reduzindo para módulo* 8 *teríamos* $5 = x^2+2y^2$ *ou* $7 = x^2+2y^2$ *em* $\mathbb{Z}_8$. *Na verdade isso não é possível: os quadrados em* $\mathbb{Z}_8$ *são* $0 = 0^2 = 4^2$, $1 = 1^2 = 3^2 = 5^2$ *e* $4 = 2^2 = 6^2 = 7^2$. *Daí,* $x^2+2y^2 \in \{0,1,2,3,4,6\}$, *ou seja, não podemos obter* 5 *ou* 7.

■

**Conclusão 3.2** *Em resumo, temos* $p = x^2 + 2y^2 \Leftrightarrow p \equiv 1$ *ou* $3(mod\ 8)$.

O próximo resultado nos mostra como escrever, um número $m$ composto, na forma $x^2 + 2y^2$.

**Proposição 3.10** *Seja* $m = p_1.p_2...p_n$, *com* $p_1, p_2, ..., p_n$ *primos. Se* $p_s = {x_s}^2 + 2{y_s}^2$, $\forall s = 1, 2, ..., n$, *então* $m = x^2 + 2y^2$, *com* $x, y \in \mathbb{Z}$.

*Demonstração:*

*Vamos mostrar por indução finita sobre n. Com efeito, para* $n = 2$, *temos que: se* $p_1 = a^2 + 2b^2$ *e* $p_2 = c^2 + 2d^2$, *então* $m = p_1.p_2 = a^2c^2 + 2a^2d^2 + 2b^2c^2 + 4b^2d^2 = (a^2c^2 + 4abcd + 4b^2d^2) + (2a^2d^2 - 4abcd + 2b^2c^2) = (ac + 2bd)^2 + 2(ad - bc)^2$. *Agora, suponha válido para* $n = k$. *Devemos mostrar válido para* $n = k + 1$. *De fato, veja que* $m = p_1.p_2...p_k.p_{k+1} = (x^2 + 2y^2)({x_{k+1}}^2 + 2{y_{k+1}}^2) = (xx_{k+1} + 2yy_{k+1})^2 + 2(xy_{k+1} - yx_{k+1})^2$, *ou seja, é válido para* $n = k + 1$. *Portanto, pelo princípio de indução finita é válido para todo n inteiro.*

■

**Exemplo 3.2** *Considere os seguintes valores de n* :

1. *Se* $n = 22$, *temos* $n = 22 = 2.11 = (0^2 + 2.1^2)(3^2 + 2.1^2) = (0.3 + 2.1.1)^2 + 2(0.1 - 1.3)^2 = 2^2 + 2.3^2$.

2. *Se* $n = 81$, *temos* $n = 81 = 3.3.3.3 = (1^2 + 2.1^2)(1^2 + 2.1^2)(1^2 + 2.1^2)(1^2 + 2.1^2) = [(1.1 + 2.1.1)^2 + 2(1.1 - 1.1)^2][(1.1 + 2.1.1)^2 + 2(1.1 - 1.1)^2] = (3^2 + 2.0^2)(3^2 + 2.0^2) = (3.3 + 2.0.0)^2 + 2(3.0 - 0.3)^2 = 3^2 + 2.0^2$.

3. *Se* $n = 66$, *temos* $n = 66 = 2.3.11 = (0^2 + 2.1^2)(1^2 + 2.1^2)(3^2 + 2.1^2) = (2^2 + 2.1^2)(3^2 + 2.1^2) = (2.3 + 2.1.1)^2 + 2(2.1 - 1.3)^2 = 8^2 + 2.1^2$.

## 3.3 Inteiros que se escrevem na forma $x^2 + 3y^2$

Esta seção irá tratar dos primos ímpares maiores que 3 que se escrevem na forma $x^2 + 3y^2$. Faremos a caracterização destes números em duas etapas: primeiro experimentaremos inteiros $n$ para ver se podemos encontrar um padrão quanto aos que são da forma $x^2 + 3y^2$ e os que não são e segundo conjecturaremos um resultado e o demonstraremos.

*Passo* 1 : Vamos considerar a situação para valores pequenos de $n$, na seguinte tabela:

| | |
|---|---|
| $n = 2(primo)$ não é da forma $x^2 + 3y^2$ | $n = 3(primo) : 3 = 0^2 + 3.1^2$ |
| $n = 4 : 4 = 2^2 + 3.0^2$ | $n = 5(primo)$ não é da forma $x^2 + 3y^2$ |
| $n = 6$ não é da forma $x^2 + 3y^2$ | $n = 7(primo) : 7 = 2^2 + 3.1^2$ |
| $n = 8$ não é da forma $x^2 + 3y^2$ | $n = 9 : 9 = 3^2 + 3.0^2$ |
| $n = 10$ não é da forma $x^2 + 3y^2$ | $n = 11(primo)$ não é da forma $x^2 + 3y^2$ |
| $n = 12 : 12 = 3^2 + 3.1^2$ | $n = 13(primo) : 13 = 1^2 + 3.2^2$ |
| $n = 14$ não é da forma $x^2 + 3y^2$ | $n = 15$ não é da forma $x^2 + 3y^2$ |
| $n = 16 : 16 = 4^2 + 3.0^2$ | $n = 17(primo)$ não é da forma $x^2 + 3y^2$ |
| $n = 18$ não é da forma $x^2 + 3y^2$ | $n = 19(primo) : 19 = 4^2 + 3.1^2$ |
| $n = 20$ não é da forma $x^2 + 3y^2$ | $n = 23(primo)$ não é da forma $x^2 + 3y^2$ |
| $n = 29(primo)$ não é da forma $x^2 + 3y^2$ | $n = 31(primo) : 31 = 2^2 + 3.3^2$ |
| $n = 37(primo) : 37 = 5^2 + 3.2^2$ | $n = 41(primo)$ não é da forma $x^2 + 3y^2$ |

Nós podemos continuar a lista, no entanto, o padrão aparente já é fácil de imaginar: $3, 7, 13, 19, 31$ e $37$ são da forma $x^2 + 3y^2$, qualquer primo $p = 3$ ou $p \equiv 1(mod\ 3)$ é da forma $x^2 + 3y^2$, e qualquer primo $p \equiv 2(mod\ 3)$ não é da forma $x^2 + 3y^2$, por exemplo $5, 11, 17, 23, 29$ e $41$.

*Passo* 2 : Com base no *passo* 1, podemos conjecturar um resultado que trata dos números que se escrevem na forma $x^2 + 3y^2$.

**Teorema 3.2** *Seja $p > 3$ primo. Se $p = x^2 + 3y^2$, então $p \equiv 1(mod\ 3)$.*
*Demonstração:*

*Vamos mostrar que se $p \not\equiv 1(mod\ 3)$, $p > 3$ primo, então $p$ não é da forma $x^2 + 3y^2$. Que equivale dizer: se $p \equiv 2(mod\ 3)$, então $p$ não é da forma $x^2 + 3y^2$. Suponha $p = x^2 + 3y^2$; então reduzindo para módulo 3 teríamos $2 = x^2 + 3y^2$ em $\mathbb{Z}_3$. Na verdade isso não é possível: os quadrados em $\mathbb{Z}_3$ são $0 = 0^2$ e $1 = 1^2 = 2^2$. Daí, $x^2 + 3y^2 \in \{0, 1\}$, ou seja, não podemos obter 2.*

■

**Conclusão 3.3** *Em resumo, temos $p = x^2 + 3y^2 \Rightarrow p \equiv 1(mod\ 3)$.*

**Observação 3.2** *Na realidade para o Teorema* 3.2 *vale a sua recíproca: se* $p \equiv 1(mod\ 3)$, *então* $p = x^2 + 3y^2$. *Mas a prova deste resultado não faz parte do objetivo deste trabalho. Para uma prova ver Martin (2009).*

O próximo resultado nos mostra como escrever, um número $m$ composto, na forma $x^2 + 3y^2$.

**Proposição 3.11** *Seja* $m = p_1.p_2...p_n$, *com* $p_1, p_2, ..., p_n$ *primos. Se* $p_s = {x_s}^2 + 3{y_s}^2$, $\forall s = 1, 2, ..., n$, *então* $m = x^2 + 3y^2$, *com* $x, y \in \mathbb{Z}$.

*Demonstração:*

*Vamos mostrar por indução finita sobre* $n$. *Com efeito, para* $n = 2$, *temos que: se* $p_1 = a^2 + 3b^2$ *e* $p_2 = c^2 + 3d^2$, *então* $m = p_1.p_2 = a^2c^2 + 3a^2d^2 + 3b^2c^2 + 6b^2d^2 = (a^2c^2 + 6abcd + 9b^2d^2) + (3a^2d^2 - 6abcd + 3b^2c^2) = (ac + 3bd)^2 + 3(ad - bc)^2$. *Agora, suponha válido para* $n = k$. *Devemos mostrar válido para* $n = k + 1$. *De fato, veja que* $m = p_1.p_2...p_k.p_{k+1} = (x^2 + 3y^2)({x_{k+1}}^2 + 3{y_{k+1}}^2) = (xx_{k+1} + 3yy_{k+1})^2 + 3(xy_{k+1} - yx_{k+1})^2$, *ou seja, é válido para* $n = k + 1$. *Portanto, pelo princípio de indução finita é válido para todo* $n$ *inteiro.*

■

**Exemplo 3.3** *Considere os seguintes valores de* $n$ :

1. *Se* $n = 21$, *temos* $n = 21 = 3.7 = (0^2+3.1^2)(2^2+3.1^2) = (0.2+3.1.1)^2+3(0.1-1.2)^2 = 3^2 + 3.2^2$.

2. *Se* $n = 81$, *temos* $n = 81 = 3.3.3.3 = (0^2 + 3.1^2)(0^2 + 3.1^2)(0^2 + 3.1^2)(0^2 + 3.1^2) = [(0.0+3.1.1)^2+3(0.1-1.0)^2][(0.0+3.1.1)^2+3(0.1-1.0)^2] = (9^2+3.0^2)(3^2+2.0^2) = (3.3 + 2.0.0)^2 + 2(3.0 - 0.3)^2 = 3^2 + 2.0^2$.

# Considerações finais

Este trabalho foi elaborado para servir de apoio para alunos e professores que buscam conhecer um pouco mais sobre os números primos. Procuramos abordar os temas em linguagem simples e acessível, valorizando os aspectos algébricos das operações e propriedades envolvendo os números inteiros e complexos. Começamos exibindo o contexto histórico e ressaltamos como estão os estudos atuais do tema principal do trabalho.

No capítulo 1, apresentamos os conjuntos dos inteiros gaussianos e inteiros quadráticos destacando suas principais propriedades e seus principais resultados, também incluímos o conjuntos dos resíduos módulo $n$ pois, a linguagem de congruência e classes foram muito utilizadas no texto.

No capítulo 2, expomos alguns fatos relevantes de *Teoria dos Números* que contribuíram no sentido de facilitar as demonstrações feitas nos capítulos subsequentes.

Finalmente, no último capítulo concluímos que os números primos ímpares que se escrevem na forma $x^2 + 2y^2$ são todos os primos tal que $p \equiv 1$ ou $3(mod\ 8)$ e os que não se escrevem são $p \equiv 5$ ou $7(mod\ 8)$, já os números primos ímpares maiores que 3 que se escrevem na forma $x^2 + 3y^2$ são todos os primos tal que $p \equiv 1(mod\ 3)$ e os que não se escrevem são $p \equiv 2(mod\ 3)$. Vimos também que, se $m$ é um número inteiro composto tal que, na sua decomposição em fatores primos, todos os fatores são da forma $a^2+b^2$, $a^2+2b^2$ ou $a^2+3b^2$, então $m$ se escreve na forma $x^2 + y^2, x^2 + 2y^2$ ou $x^2 + 3y^2$.

# Referências Bibliográficas


Clark, P. L. (2003). Sums of two squares. URL: http://math.uga.edu / pete /4400twos-quares.pdf / Acesso em: 09/07/2014.

Dias, I. (2001). Álgebra 2. URL: http://www.icmc.usp.br /iresdias /material /sma306.pdf / Acesso em: 20/10/2014.

Hefez, A. (2011). *Elementos de Aritmética*. Rio de Janeiro: 2 ed., Sociedade brasileira de Matemática.

Martin, K. (2009). Number Theory-Course Information. URL: http://www2.math.ou.edu /kmartin /nti /guidelines.html / Acesso em: 22/03/2015.

Moreira, C. G. T. A., Martínez, F. E. B., e Saldanha, N. C. (2012). *Tópicos de Teoria dos Números*. Rio de Janeiro: 1 ed., Sociedade brasileira de Matemática, (Coleção PROFMAT).

Santos, J. P. O. (2007). *Introdução à Teoria dos Números*. Rio de Janeiro: 1 ed., IMPA,(Coleção Matemática Universitária).

Stillwell, J. (2003). *Elements of Number Theory*. Springer-Verlag New York: 1 ed., Undergraduate Texts in Mathematics.

Villela, M. L. T. (2000). Álgebra Módulo 3. URL: http://www.professores.uff.br /jco-lombo /Algebra_I_Mat_20121/algebra_modulo3.pdf / Acesso em: 15/09/2014.

Vitorino, A. e ao, B. L. R. (2013). Inteiros de Gauss. URL: http://www.ime.unicamp.br /ftorres /ENSINO /MONOGRAFIAS /B_M2_FM_2013.pdf/ Acesso em: 15/12/2014.