UNIVERSIDADE FEDERAL DE SANTA CATARINA
Centro de Ciências Físicas e Matemáticas
Curso de Licenciatura em Matemática

REDUÇÃO DO ÚLTIMO TEOREMA DE FERMAT PARA EXPOENTE PRIMO

Autora: Carla Mörschbächer
Orientador: Prof. Dr. Oscar Ricardo Janesch
Florianópolis
Outubro 2007

Carla Mörschbächer

Redução do Último Teorema de Fermat para expoente primo

Trabalho acadêmico de graduação apresentado
à disciplina Trabalho de Conclusão de Curso II,
do Curso de Matemática - Habilitação Licenciatura,
do Centro Ciências Físicas e Matemáticas da
Universidade Federal de Santa Catarina

Professora: Carmem Suzane Comitre Gimenez

Florianópolis
Outubro 2007

Agradecimentos

Nestes quatro anos de muitos aprendizados gostaria de agradecer a muitas pessoas que estiveram do meu lado: À Deus, por sempre ter iluminado meus passos e ter confiado a mim a tarefa de ensinar. Ao verdadeiro mestre, Oscar, pela orientação, não apenas do TCC, mas também pelos conselhos que ajudaram-me a superar dificuldades e crescer como pessoa. À minha família que, mesmo distante, sempre manteve-se presente. Ao Professor Pinho e ao Pet-Matemática, pelos dois anos e meio de convivência e aprendizado, que sem dúvida, permanecerão para sempre na lembrança. Ao meu namorado, Rafael, pela compreenssão e companheirismo. E também, agradecer aos amigos, minha segunda família, que tornaram estes quatro anos muito alegres e inesquecíveis.

Redução do Último Teorema de Fermat para expoente primo
por
Carla Mörschbächer

Esta monografia foi julgada adequada como **TRABALHO DE CONCLUSÃO DE CURSO** no Curso de Matemática - Habilitação Licenciatura, e aprovada em sua forma final pela Banca Examinadora designada pela Portaria nº 49/CCM/07.

Profª Carmem Suzane Comitre Gimenez
Professora da disciplina

Banca Examinadora:

Prof. Dr. Oscar Ricardo Janesch (Orientador)

Profª Carmem Suzane Comitre Gimenez (UFSC)

Prof. José Luiz Rosas Pinho (UFSC)

Sumário

Introdução

O Último Teorema de Fermat assegura que a equação diofantina $X^n + Y^n = Z^n$, $n \geq 3$, não tem solução não trivial em $\mathbb{Q}^*$. Este teorema, enunciado em 1637 por Fermat e provado em 1994 pelo inglês Andrew Wiles, tem suas raízes em um problema já conhecido antes do século VI a.c., o *Teorema de Pitágoras*:

" *Em um triângulo retângulo, o quadrado da hipotenusa é igual a soma dos quadrados dos catetos* ".

Pitágoras de Samos foi um matemático que contribuiu muito para o desenvolvimento da matemática. Em particular, está o profundo estudo da equação $X^2 + Y^2 = Z^2$.

Acredita-se que Pitágoras tenha aprendido "seu" teorema em viagens pelo mundo antigo, mais precisamente no Egito e na Babilônia. Estes povos usavam matemática, em especial o Teorema de Pitágoras, para resolver problemas do dia-a- dia, como por exemplo, refazer demarcações de terras após as enchentes que ocorriam anualmente no Rio Nilo.

Os cálculos eram feitos e funcionavam perfeitamente, porém, não havia o interesse em saber porque funcionavam, ou, se haveria algum caso em que o método não se aplicaria.

Pitágoras, ao contrário, durante vinte anos junto a estes povos, tentou compreender a matemática usada, entender os números, analisá-los, ver suas características...

Ao voltar para sua cidade, ela estava tomada por um conservadorismo que hesitou em aceitar suas idéias. Pitágoras fugiu então para o sul da Itália. Recebeu apoio e abriu sua escola, " A Irmandade Pitagórica", que chegou a ter mais de 600 seguidores.

O famoso Teorema de Pitágoras, já usado no mundo antigo, foi muito estudado na Irmandade. Pitágoras deu um passo a frente, levando consigo a matemática, ao provar logicamente que todo triângulo retângulo satisfaz a relação $X^2+Y^2 = Z^2$, e reciprocamente, que quaisquer três números positivos (racionais ou inteiros), que satisfazem a relação, são medidas dos lados de um triângulo retângulo.

Os Pitagóricos descobriram maneiras de encontrar triplas de números inteiros satisfazendo $X^2 + Y^2 = Z^2$. Provaram também, que esta equação possuia infinitas soluções.

Diophantus, um matemático que viveu em Alexandria no século III d.c. aproximadamente, escreveu treze livros, em grego, sobre teoria de números.

Sabe-se muito pouco de sua vida, mas conta-se que em seu túmulo grifou-se um problema que gera uma equação, cuja solução é a idade com que morreu.

Diophantus dedicava-se bastante ao estudo de equações polinomiais, dentre elas o Teorema de Pitágoras. Como conseqüência, estas passaram a chamar-se Equações Diofantinas. Sua obra contém muitos problemas originando equações em uma variável, de primeiro e segundo graus.

Nesta época, e também em épocas passadas, os livros eram submetidos a vinganças políticas, pois a sua destruição significava um grande enfraquecimento da cultura e dos conhecimentos dos povos. Foi em virtude disso, que apenas 6 dos 13 livros de Diophantus sobreviveram. E também por este motivo, estudiosos fugiram com importantes obras para o Ocidente.

Na França, em 1621, o intelectual Claude Gaspar Bachet de Mézeriac, fez uma tradução do livro de Diophantus, " Aritmética", para o latim. Bachet, por conhecer bastante matemática, acrescentou problemas e comentários à sua tradução.

Foi através destas traduções que o francês Pierre de Fermat, que enunciou o Último Teorema de Fermat, veio a estudar teoria de números.

Pierre de Fermat nasceu em 20 de agosto de 1601, na cidade de Beaumont-de-Lomagne, no sudoeste da França. Estudou desde cedo e passou pela Universidade, pois seu pai era um rico comerciante de couro. Ocupou cargo público a partir de 1631, tendo como passatempo estudar matemática.

Fermat estudava matemática por prazer, não tinha preocupação em divulgar suas descobertas. Raramente fazia uma demonstração com todos os detalhes. Jul-

gava isso desnecessário.

Foram poucos os matemáticos com quem Fermat manteve contato em sua vida, como exemplo de contatos, pode-se citar o Padre Mersene e Pascal. Ressalta-se que em seu cargo público, Fermat tinha que condenar pessoas a morte na fogueira, exigindo então que se relacionasse com o menor número possível de pessoas.

Ao estudar as traduções de Bachet da " Aritmética", mais precisamente o livro II, Fermat encontrou o Teorema de Pitágoras e os trios pitagóricos. Parecia que tudo a este respeito já havia sido desvendado pelos seguidores de Pitágoras. Já sabia-se inclusive que haviam infinitas soluções e como calculá-las.

O livro II possuia vários problemas que chamaram a atenção do matemático. Dentre eles está o problema 8, intimamente relacionado ao Teorema de Pitágoras:

"Dado um número que é um quadrado, é possível escrevê-lo como soma de dois quadrados?".

É claro que a resposta é sim, pois basta escrever $a^2 = a^2 + 0^2$. O "Problema 8 generalizado" é saber quando um número natural qualquer é a soma de dois de dois quadrados.

Fermat fez uma variação do Teorema de Pitágoras, elevando o expoente 2 da equação $X^2+Y^2 = Z^2$ para 3. Percebendo que não haviam soluções, generalizou suas idéias para um número $n \geq 3$.

Estas observações foram feitas nas margens do livro "Aritmética", ao lado do problema 8. Ele complementou afirmando possuir uma prova para este fato.
Mais precisamente ele escreveu:

"É impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta ser escrita como a soma de dois números elevados a quatro, ou, em geral, para qualquer número que seja elevado para uma potência maior do que dois ser escrito como a soma de duas potências semelhantes. Eu tenho uma demonstração realmente maravilhosa para esta proposição mas esta margem é muito estreita para contê-la."

Esta afirmação pode ser interpretada como uma generalização do problema 8. Um número que é um cubo, pode ser escrito como a soma de dois cubos? Um número que é uma potência de quatro, pode ser escrito como a soma de duas

potências de quatro?

Três décadas mais tarde, Fermat adoeceu e morreu. Suas descobertas, só não foram esquecidas porque seu filho mais velho, Clément-Samuel, percebendo a notória importância, reuniu, organizou e publicou-as em uma edição especial da "Aritmética".

Infelizmente, como era de esperar-se, um grande número de teoremas continham apenas um indício de sua desmonstração ou nem as possuiam. Esse era o caso da afirmação feita ao lado do problema 8.

O teorema a seguir, encontrado nas notas de Fermat, responde ao problema 8, mas ele também não continha sua demonstração.

"Um número n é a soma de dois quadrados se, e somente se, todo primo da forma $4k+3$ que divide n, tem expoente par".

Este teorema foi provado pelo suiço Leonhard Euler, em 1749, depois de 7 anos de trabalho. Aproximadamente 1 século após a morte de seu criador.

Euler encontrou em rabiscos de Fermat, uma prova sem detalhes, através do método da descida infinita, de que $X^4+Y^4=Z^4$ não possuia solução não trivial. Adaptou a prova para $n=3$, mas ela não funcionou para $n \geq 5$.

Aos poucos todos os teoremas de Fermat foram sendo desmonstrados, com excessão daquele rabiscado ao lado do problema 8. Esta conjectura, foi a última que ficou por ser demonstrada. Por isso ficou conhecida mundialmente como "*O Último Teorema de Fermat*".

A afirmação da existência de uma prova para o Último Teorema de Fermat trouxe muitas inquietudes para os matemáticos precedentes durante séculos. Ele foi provado, apenas em 1994, pelo matemático inglês Andrew Wiles, após 8 anos de dedicação exclusiva. E a prova foi uma conseqüência da unificação de dois ramos distintos da matemática: Equações Elípticas e Funções Modulares.

O objetivo principal deste trabalho é abordar dois teoremas de Fermat, que estão relacionados. O primeiro resultado é o teorema que responde ao problema 8 e o segundo é o Último Teorema de Fermat. Provaremos o primeiro e reduziremos o segundo ao caso onde n é um número primo.

Também provaremos que todo número natural pode ser escrito como a soma

de quatro quadrados.

Para tanto, dividimos o trabalho em quatro capítulos.

No primeiro, apresentaremos os conceitos de álgebra necessários para alcançar nossos objetivos. Salienta-se que neste capítulo, admitiremos que o leitor esteja familiarizado com os conceitos básicos de álgebra, sobre Teoria de Anéis (disciplina da licenciatura).

No segundo, após provarmos alguns resultados auxiliares, demonstraremos o teorema que responde ao problema 8 do livro II da "Aritmética".

No terceiro, reduziremos o Último Teorema de Fermat para o caso onde n é um número primo.

Para finalizar, no quarto capítulo, provaremos que todo número natural pode ser escrito como a soma de quatro quadrados de inteiros.

Capítulo 1

Noções Básicas

Neste capítulo, apresentaremos as ferramentas que serão utilizadas no decorrer do trabalho. Tais ferramentas, são resultados clássicos de álgebra sobre teoria de anéis: domínios euclidianos, principais e fatoriais.

As propriedades de anéis específicos, usados nos capítulos seguintes, serão apresentados na forma de proposições e teoremas.

Iniciamos então, a fim de fixar notação, com a definição de anel.

Definição 1.1. Um **anel** $(A, +, \cdot)$ é um conjunto A, munido com uma operação denotada por $+$ e de uma operação denotada por $\cdot$, que satisfazem as seis condições a seguir:

$S_1)$ $(x + y) + z = x + (y + z), \forall x, y, z \in A$ (a operação $+$ é associativa).

$S_2)$ $\exists\, 0 \in A$ tal que $0 + x = x + 0 = x, \forall x \in A$ (existência de elemento neutro para a operação +).

$S_3)$ $\forall\, x \in A$, $\exists$ único $y \in A$, denotado por $y = -x$, tal que $x + y = y + x = 0$ (existência de elemento inverso para a operação +).

$S_4)$ $a + b = b + a$ (a operação + é comutativa).

$S_5)$ $a.(b.c) = (a.b).c$ (a operação $\cdot$ é associativa).

$S_6)$ $a.(b + c) = a.b + a.c$ e $(a + b).c = a.c + b.c$ (a operação $\cdot$ é distributiva com relação a operação +).

Observação 1.1. Podemos apresentar ainda as seguintes condições:

$S_7)$ $\exists\, 1 \in A$ tal que $1.x = x.1 = x, \forall x \in A$ (existência de elemento neutro para a operação $\cdot$).

$S_8)$ $a.b = b.a$ (comutatividade da operação $\cdot$).

Se $(A, +, \cdot\ )$ é um anel e satisfizer S_7 então A é um **anel com unidade**; e se $(A, +, \cdot)$ é um anel e satisfazer S_8 então A é um **anel comutativo**.

Definição 1.2. Se $(A, +, \cdot\ )$ é um anel comutativo, com unidade e satisfizer a condição a seguir, então $(A, +, \cdot)$ é um **domínio de integridade** (ou simplesmente domínio):

$S_9)$ Dados $x, y \in A$. Se $x \neq 0$ e $y \neq 0$ então $x.y \neq 0$.

Observação 1.2. Um anel, com unidade, que satisfaz o axioma S_9 é chamado de **anel sem divisores de zero**.

Definição 1.3. Se $(A, +, \cdot\ )$ é um anel comutativo, com unidade e satisfizer a condição a seguir, então $(A, +, \cdot\ )$ é um **corpo**:

$S_{10}) \forall x \in A, x \neq 0, \exists y \in A$ tal que $x.y = y.x = 1$.

É facil verificar que todo corpo é um domínio.

Definição 1.4. Seja A um anel com unidade. Um elemento $a \in A$ é **invertível** em A se existe $b \in A$ tal que $a.b = b.a = 1$. Denotaremos o conjunto dos elementos invertíveis de um anel A por $\mathcal{U}(A)$.

Com o objetivo de familiarizar-se com alguns exemplos concretos de anéis, domínios e corpos, que serão úteis nos capítulos seguintes, apresentaremos a definição e os exemplos a seguir.

Exemplo 1.1. $(\mathbb{Z}, +, \cdot\ )$, onde $+, \cdot$ são as operações usuais em $\mathbb{Z}$, é um domínio.

Exemplo 1.2. $(\mathbb{Q}, +, \cdot\ ), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot\ )$ onde $+, \cdot$ são as operações usuais em $\mathbb{C}$, são corpos e, em particular domínios.

Exemplo 1.3. $(\mathbb{Z}_n, +, \cdot\ )$ é anel e $(\mathbb{Z}_p, +, \cdot\ )$, onde p é um número primo, é um corpo e em particular é um domínio de integridade.

Definição 1.5. Sejam A um anel e X uma indeterminada. Um polinômio em X com coeficientes em A é uma expressão da forma:

$$p(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + ...$$

onde $a_i \in A, \forall i \in \mathbb{N}$ e $\exists j \in \mathbb{N}$ tal que $a_i = 0, \forall i > j$.

Teremos $p(X) = q(X)$ quando $a_i = b_i,\ \forall i \in \mathbb{N}$.

O conjunto dos polinômios na variável X com coeficientes em A será denotado por $A[X]$.

Exemplo 1.4. $(A[X], +, \cdot\ )$ é anel, onde + e $\cdot$ estão definidos da seguinte forma:
Dados $p(X), q(X) \in A[X]$

$p(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + ...$

$q(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + ...$

$p(X) + q(X) = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + ... \in A[X].$

$p(X).q(X) = c_0 + c_1X + c_2X^2 + ... \in A[X]$, onde $c_k = \sum_{i+j=k} a_ib_j.$

Além do mais, se A é um anel com unidade então $A[X]$ é um anel com unidade; e se A é um anel comutativo então $A[X]$ é um anel comutativo.

Definição 1.6. Seja A um anel. Um subconjunto B, não vazio, de A é um **subanel** de A se for fechado para as operações $+, \cdot$ e se $(B, +, \cdot\ )$ for um anel com as operações de A.

Lema 1.1. Seja A um anel e B um subconjunto de A. Então B é um subanel de A se, e somente se, valem as seguintes condições:

a) $B \neq \emptyset$.

b) Se $a, b \in B$ então $a - b \in B$ e $a.b \in B$.

Demonstração. $(\Rightarrow)$ Se B é um subanel então $B \neq \emptyset$ e, dados $a, b \in B$ temos que $a.b \in B$. Resta então mostrar que $a - b \in B$.
Como $a \in B$ e $b \in B$, temos que $a \in B$ e $-b \in B$. Logo $a + (-b) = a - b$ pertence a B.

$(\Leftarrow)$ Precisamos verificar que se B satisfaz os itens a) e b) implica que B satisfaz as condições de subanel, ou seja, temos que verificar que $B \neq \emptyset$, B é fechado para as operações $+$ e $\cdot$, e que valem em B os seis axiomas de anel.
De fato, pelo item a) temos que $B \neq \emptyset$, e pelo item b) temos que a operação $\cdot$ é fechada em B.
Como, pelo item b), dados $a, b \in B$ vem que $a - b \in B$, tomando $a = b$, temos que $0_A \in B$. Então $0_A - b = -b$ pertence a B. Portanto $a - (-b) = a + b$ pertence

a B, ou seja a operação $+$ é fechada em B.
Agora, vamos verificar que valem os axiomas de anel em B.
Perceba que os axiomas S_1, S_4, S_5 e S_6 valem para todos os elementos de A. Podemos concluir então que eles valem para todos os elementos de B, pois eles são, em particular, elementos de A.
Resta então verificar os axiomas S_2 e S_3.
Já vimos que o elemento neutro de A, 0_A, pertence a B. Logo, dado $a \in B$ temos que $a + 0_A = a$, pois a, em particular, pertence a A. Assim, $0_A = 0_B$, pois 0_A é único para todo elemento de A; o axioma S_2 está verificado.
Dado $b \in B$ temos, pelo item b), que $0_A - b = (-b)_A$ pertence a B. Este elemento é único, caso contrário A não seria anel. Logo S_3 está verificado e portanto B é um subanel de A.

■

Definição 1.7. Seja D um domínio. Um subconjunto B, não vazio, de D é um **subdomínio** de D se $(B, +, \cdot)$ é um subanel, com unidade de D.

Como a comutatividade e a inexistência de divisores de zero são propriedades hereditárias (se valem no anel também valerão em todo subanel), temos que um subdomínio é um domínio.

Definição 1.8. Seja K um corpo. Um subconjunto B, não vazio, de K é um **subcorpo** de K se, $(B, +, \cdot)$ além de ser um subanel com as operações de K, é também um corpo.

Proposição 1.1. O conjunto $\mathbb{Q}[i] = \{a + bi; a, b \in \mathbb{Q}\}$ é um subcorpo de $\mathbb{C}$.

Demonstração. Note que $0 + 0i \in \mathbb{Q}[i]$, basta tomar $a = 0$ e $b = 0$. Logo $\mathbb{Q}[i] \neq \emptyset$.
Se $x, y \in \mathbb{Q}[i]$ então $x = a + bi$ e $y = c + di$, onde $a, b, c, d \in \mathbb{Q}$.
Logo, como $a, b, c, d \in \mathbb{Q}$ e $\mathbb{Q}$ é anel temos:

$$x - y = (a - c) + (b - d)i \in \mathbb{Q}[i]$$

e

$$x.y = (ac - bd) + (ad + bc) \in \mathbb{Q}[i].$$

A unidade de $\mathbb{Q}[i]$ é $(1 + 0i)$.
De fato, dado $a + bi \in \mathbb{Q}[i]$ temos:

$$(1 + 0i).(a + bi) = (1.a - 0.b) + (1.b + 0.a)i$$

$$= a + bi.$$

Se $x = a + bi \in \mathbb{Q}[i]$, $x \neq 0$ então $a^2 + b^2 \neq 0$ e portanto existe $y \in \mathbb{Q}[i]$ tal que

$$x.y = 1.$$

De fato, tome $y = \dfrac{a}{a^2+b^2} - \dfrac{b}{a^2+b^2}.i \in \mathbb{Q}[i]$.

Então $x.y = (a+bi).\left(\dfrac{a}{a^2+b^2} - \dfrac{b}{a^2+b^2}.i\right)$

$$= \left(\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}\right) + \left(\frac{-a.b}{a^2+b^2} + \frac{b.a}{a^2+b^2}\right) i$$

$$= 1 + 0i$$

Portanto $\mathbb{Q}[i]$ é um subcorpo de $\mathbb{C}$.

■

Proposição 1.2. O conjunto $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ é um subdomínio de $\mathbb{Q}[i]$.

Demonstração. Note que $0 + 0i \in \mathbb{Z}[i]$, basta tomar $a = 0$ e $b = 0$. Assim $\mathbb{Z}[i] \neq \emptyset$.
Se $x, y \in \mathbb{Z}[i]$ então $x = a_1 + ib_1$ e $y = a_2 + ib_2$, onde a_1, a_2, b_1 e $b_2 \in \mathbb{Z}$.
Logo, como $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ e $\mathbb{Z}$ é anel, temos:

$$x - y = (a_1 - a_2) + i(b_1 - b_2) \in \mathbb{Z}[i]$$

e

$$x.y = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i \in \mathbb{Z}[i].$$

A unidade de $\mathbb{Z}[i]$ é $(1 + 0i)$.
De fato, dado $a + bi \in \mathbb{Z}[i]$ temos:

$$(1 + 0i).(a + bi) = (1a - 0b) + (1b + 0a)i$$

$$= a + bi.$$

■

Observação 1.3. O anel $\mathbb{Z}[i]$ é chamado anel de inteiros de Gauss.

A partir de agora, vamos introduzir uma condição a mais aos domínios de integridade: uma divisão similar a euclidiana.

Já temos definidas nos domínios duas operações ($+$ e $\cdot$), no entanto, para podermos fazer divisões com resto menor que o divisor, necessitamos de uma ferramenta que possibilite comparar o tamanho dos elementos.

Por exemplo, quando dividimos em $\mathbb{Z}$, comparamos os números atráves de sua distância à origem. Perceba que podemos associar a distância de um número à origem com a função módulo.

Essa nova ferramenta, como pode-se prever, trata-se de uma função

$$\varphi : D \to \mathbb{N}$$

e é através dela que compararemos os elementos.

Definição 1.9. Um **domínio euclidiano** $(D, +, \cdot, \varphi)$ é um domínio de integridade $(D, +, \cdot)$ com uma função

$$\varphi : D\backslash\{0\} \to \mathbb{N} = \{0, 1, 2, 3, ...\}$$

que satisfaz as seguintes propriedades:

$$\begin{cases} a) \forall\, a, b \in D, b \neq 0, \text{existem} \\ \qquad\qquad t, r \in \mathbb{Z} \text{ tais que:} \\ \qquad a = bt + r \text{ com} \begin{cases} \varphi(r) & < & \varphi(b) \\ \text{ou} & r & = 0 \end{cases} \\ b) \forall\, a, b \in D\backslash\{0\}, \varphi(a) \leq \varphi(ab). \end{cases}$$

Utilizando esta definição, vamos provar agora que, alguns domínios que serão utilizados nos capítulos seguintes, são também domínios euclidianos.

Teorema 1.1. *Seja* $|\ | : \mathbb{Z} \to \mathbb{N}$ *a função valor absoluto. Então:*

a) $(\mathbb{Z}, +, \cdot, |\ |)$ *é um domínio euclidiano, isto, é:*

$$\begin{cases} i)\ (\mathbb{Z}, +, \cdot\ ) \textit{ é um domínio}. \\ ii) \forall\ a, b \in \mathbb{Z}, b \neq 0, \textit{existem}\ \ t, r \in \mathbb{Z} \textit{ tais que:} \\ \qquad\qquad a = bt + r \textit{ com } |r| < |b|. \\ iii) \forall\, a, b \in \mathbb{Z}\backslash\{0\}, |a| \leq |ab|. \end{cases}$$

b) Tais t e r podem ser efetivamente calculados.

c) Em geral, t e r não são únicos.

d) Se exigirmos $r \geq 0$, então t e r são únicos.

Demonstração. a) i) Já sabemos que $\mathbb{Z}$ é domínio.

ii) Sejam $a, b \in \mathbb{Z}, b \neq 0$. Precisamos encontrar $t, r \in \mathbb{Z}$ tais que

$$a = bt + r \quad \text{com} \quad |r| < |b|,$$

ou seja, procuramos os números $t, r \in \mathbb{Z}$ tais que

$$|a - bt| < |b|.$$

Se a é um múltiplo de b, então tome $t = \frac{a}{b}$ e $r = 0$.
Se a não é um múltiplo de b então a está entre dois múltiplos de b, a saber, hb e $(h+1)b$, onde $h \in \mathbb{Z}$. Dessa forma temos que:

$$|a - bh| < |b| \quad \text{e} \quad |a - b(h+1)| < |b|.$$

Logo, tome $t = h$ e $r = (a - bh)$ ou $t = (h+1)$ e $r = (a - b(h+1))$.

iii) Note ainda que, se $b \in \mathbb{Z}\backslash\{0\}$, temos $|b| \geq 1$, e então:

$$|a| \leq |a|\,|b| = |ab|, \; \forall\, a \in \mathbb{Z}.$$

b) Basta calcular o múltiplo de b à direita de a e o múltiplo de b à esquerda de a, que estão mais próximos de a.

c) Em geral tais t, e r não são únicos, pois se a não for um múltiplo de b, então $t = h$ e $r = (a - bh)$ ou $t = (h+1)$ e $r = (a - b(h+1))$ são soluções.

d) Sejam $t_1, t_2, r_1, r_2 \in \mathbb{Z}$ tais que

$$bt_1 + r_1 = a = bt_2 + r_2, \quad \text{com} \quad 0 \leq r_1, r_2 < |b|.$$

Segue que $r_1 - r_2 < |b|$ e $r_2 - r_1 < |b|$. Logo $|r_1 - r_2| < |b|$.

Suponha que $t_1 \neq t_2$. Então $|t_1 - t_2| \geq 1$ e daí $|b||t_1 - t_2| \geq |b|$.
De $bt_1 + r_1 = bt_2 + r_2$ temos $r_2 - r_1 = b(t_1 - t_2)$.
Tomando módulo:

$$|r_2 - r_1| = |b||t_1 - t_2| \geq |b|.$$

Contradição com $|r_2 - r_1| < |b|$.
Logo $t_1 = t_2$ e conseqüentemente $r_1 = r_2$.

■

Definição 1.10. Um elemento $a \in A\backslash\{0\}$ é **irredutível** em A se a não é invertível e se $a = bc$, com $b, c \in A$, implica que $b \in \mathcal{U}(A)$ ou $c \in \mathcal{U}(A)$.

Definição 1.11. A função $N : \mathbb{Z}[i] \to \mathbb{N}$, onde $N(a+bi) = a^2+b^2$, é denominada função norma.

Lema 1.2. Sejam N a função norma e $\alpha = a + bi,\ \beta = c + di \in \mathbb{Z}[i]$. Então:

a) $N(\alpha) = \alpha.\overline{\alpha}$, onde $\overline{\alpha} = a - bi$.

b) $N(\alpha) \geq 0$, para todo $\alpha \in \mathbb{Z}[i]$.

c) $N(\alpha) = 0$ se e somente se $\alpha = 0$.

d) $N(\alpha.\beta) = N(\alpha).N(\beta)$.

e) $N(\alpha) = 1$ se e somente se $\alpha \in \mathcal{U}(\mathbb{Z}[i])$.

f) Se $N(\alpha) = p, p$ primo em $\mathbb{Z}$, então α é irredutível em $\mathbb{Z}[i]$.

Demonstração. a) $N(\alpha) = a^2 + b^2 = (a + bi).(a - bi) = \alpha.\overline{\alpha}$.

b) $N(\alpha) = a^2 + b^2 \geq 0$.

c) ($\Rightarrow$) Se $N(\alpha) = 0$ então $a^2 + b^2 = 0$. Mas $a^2 \geq 0$ e $b^2 \geq 0$.
Logo, se $a^2 + b^2 = 0$ implica que $a^2 = 0$ e $b^2 = 0$, ou seja, $a = 0$ e $b = 0$.
Portanto, neste caso $\alpha = 0 + 0i$.

($\Leftarrow$) Se $\alpha = 0 + 0i$ então $N(\alpha) = 0^2 + 0^2 = 0$.

d) $N(\alpha.\beta) = N((ac - bd) + (ad + bc)i)$

$$= (ac - bd)^2 + (ad + bc)^2$$

$$= (ac)^2 + (bd)^2 - 2acbd + (ad)^2 + (bc)^2 + 2adbc$$

$$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$$

$$= c^2(a^2 + b^2) + d^2(a^2 + b^2)$$

$$= (a^2 + b^2)(c^2 + d^2)$$

$$= N(\alpha).N(\beta).$$

e) ($\Rightarrow$)
$1 = N(\alpha) = \alpha\overline{\alpha} \Longrightarrow \alpha^{-1} = \overline{\alpha}$.

($\Leftarrow$) Por hipótese, existe $\alpha^{-1} \in \mathbb{Z}[i]$ tal que $\alpha\alpha^{-1} = 1$. Segue que:

$$\begin{aligned} 1 = N(1) &= N(\alpha\alpha^{-1}) \\ &= N(\alpha).N(\alpha^{-1}) \\ &\Longrightarrow N(\alpha) = 1, \text{ pois } N(\alpha) \in \mathbb{N}. \end{aligned}$$

f) Pelos itens c) e e) temos que $\alpha \neq 0$ e $\alpha \notin \mathcal{U}(\mathbb{Z}[i])$.
Suponha que existam $\beta, \delta \in \mathbb{Z}[i]$, tais que $\alpha = \beta.\delta$.
Sejam $\beta = c + di$ e $\delta = e + fi$, então $\alpha = (ce - df) + (cf + de)i$ e portanto

$$\begin{aligned} N(\alpha) &= (ce - df)^2 + (cf + de)^2 \\ &= (e^2 + f^2).(c^2 + d^2) \\ &= p. \end{aligned}$$

Inferimos daí que $(e^2 + f^2) = 1$ ou $(c^2 + d^2) = 1$. Caso contrário p não seria primo. Conseqüentemente, pelo item e), temos que $\beta \in \mathcal{U}(\mathbb{Z}[i])$ ou $\delta \in \mathcal{U}(\mathbb{Z}[i])$. Logo α é irredutível em $\mathbb{Z}[i]$.

■

Exemplo 1.5. $\mathcal{U}(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$, pois $N(1) = N(-1) = N(i) = N(-i) = 1$.

Exemplo 1.6. $\{1+i, 2+i, 1+2i, 3+2i\}$ está contido no conjunto dos elementos irredutíveis de $\mathbb{Z}[i]$.

Teorema 1.2. *Seja $N : \mathbb{Z}[i] \to \mathbb{N}$, onde $N(a + bi) = a^2 + b^2$, a função norma. Então:*

a) $(\mathbb{Z}[i], +, \cdot, N)$ *é um domínio euclidiano, isto, é:*

$$\begin{cases} i)\ (\mathbb{Z}[i], +, \cdot) \text{ é um domínio.} \\ ii) \forall\ \alpha, \beta \in \mathbb{Z}[i], \beta \neq 0, \text{existem } t, r \in \mathbb{Z}[i] \text{ tais que:} \\ \qquad \alpha = \beta t + r \text{ com } N(r) < N(\beta). \\ iii) \forall\, \alpha, \beta \in \mathbb{Z}[i]\backslash\{0\}, N(\alpha) \leq N(\alpha\beta). \end{cases}$$

b) Tais t e r podem ser efetivamente calculados.

c) Em geral, t e r não são únicos.

Demonstração. a) i) Já demonstramos que $(\mathbb{Z}[i], +, \cdot)$ é um domínio.

ii) Dados $\alpha = a+bi$, $\beta = c+di \in \mathbb{Z}[i] \subset \mathbb{Q}[i]$, $\beta \neq 0$. Queremos encontrar $t, r \in \mathbb{Z}[i]$ tais que:

$$\alpha = \beta t + r \text{ com} \begin{cases} N(r) & < & N(\beta) \\ \text{ou} & r & = 0 \end{cases}$$

Vamos fazer esta divisão em $\mathbb{Q}[i]$, que é corpo, e depois, trazer o resultado para ser analisado em $\mathbb{Z}[i]$.
Como $\mathbb{Q}[i]$ é corpo, $\beta^{-1} \in \mathbb{Q}[i]$, e então existe $x + yi \in \mathbb{Q}[i]$ tal que:

$$\alpha\beta^{-1} = x + yi.$$

Considere agora $u, v \in \mathbb{Z}$ tais que:

$$|x - u| \leq \frac{1}{2} \quad \text{e} \quad |y - v| \leq \frac{1}{2}.$$

Reescrevendo $\alpha\beta^{-1} = x + iy$ em função de u, v temos:

$$\alpha\beta^{-1} = (u + vi) + ((x - u) + (y - v)i). \quad (*)$$

Denote $(u + vi) = t$ e $((x - u) + (y - v)i) = r'$. E note que $t \in \mathbb{Z}[i]$, pois $u, v \in \mathbb{Z}$.
Multiplicando por β em ambos os lados de $(*)$ vem que:

$$\alpha = t\beta + \beta r'.$$

Note que $\beta r' = (\alpha - t\beta) \in \mathbb{Z}[i]$, pois $\mathbb{Z}[i]$ é subanel de $\mathbb{Q}[i]$, ou seja, a subtração é fechada nele. Então tome

$$t = (u + vi) \text{ e } r = \beta r'.$$

Precisamos verificar ainda que, $N(r) = N(\alpha - \beta t) < N(\beta)$.
Mas antes note que:

$$\begin{aligned} N(\alpha - \beta t) &= N(\beta(\alpha\beta^{-1} - t)) \\ &= N(\beta).N(\alpha\beta^{-1} - t). \end{aligned}$$

Note que utilizamos a função norma N definida em $\mathbb{Q}[i]$, isto é,

$$N : \mathbb{Q}[i] \longrightarrow \mathbb{N}, \quad N(a + bi) = a^2 + b^2.$$

Então, para verificar que $N(r) = N(\alpha - \beta t) < N(\beta)$, basta verificar que

$$N(\alpha\beta^{-1} - t) < 1.$$

De fato, $N(\alpha\beta^{-1} - t) = N((x + yi) - (u + vi))$

$$= N((x - u) + i(y - v))$$
$$= (x - u)^2 + (y - v)^2$$
$$\leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2} < 1.$$

Então $N(r) < N(\beta)$ e portanto $t = (u + vi)$ e $r = \beta r'$.

iii) A imagem da função norma está contida no conjunto dos números naturais, e se $\beta = c + di \neq 0$ então $N(\beta) = c^2 + d^2$ é maior do que zero, ou seja, é maior ou igual do que um (propriedade c) da função norma.
Logo $N(\alpha) \leq N(\alpha).N(\beta) = N(\alpha\beta)$.

b) Tais t e r podem ser efetivamente calculáveis, pois u, v podem ser calculados a partir de x e y e, r pode ser calculado a partir de u, v, x, y.

c) Tais t e r não são únicos, veja o exemplo:

$2 + 3i = (1 + i).3 - 1;$

$2 + 3i = (1 + i).(3 + i) - i;$

$2 + 3i = (1 + i).(2 + i) + 1;$

$2 + 3i = (1 + i).2 + i.$

■

Definição 1.12. Sejam D um domínio e $D[X]$ o conjunto dos polinômios com coeficientes em D. A função grau: $A[X]\backslash\{0\} \longrightarrow \mathbb{N}$, onde grau $f(X) =$ grau de $f(X)$, é denominada função grau.

Lema 1.3. Sejam D um domínio, e $f(X), g(X) \in D[X]^*$. Então temos as seguintes propriedades da função grau:

a) grau $(f(X).g(X)) =$ grau $(f(X))+$ grau $(g(X))$.

b) grau $(f(X) + g(X)) \leq$ max { grau $f(X)$, grau $g(X)$}, se $f(X) + g(X) \neq 0$.

c) grau $(f(X) - g(X)) \leq$ max { grau $f(X)$, grau $g(X)$}, se $f(X) - g(X) \neq 0$.

Demonstração. Vamos denotar

$$f(X) = a_nX^n + \cdots + a_1X + a_0, \text{ com } a_n \neq 0 \text{ e}$$

$$g(X) = b_mX^m + \cdots + b_1X + b_0, \text{ com } b_m \neq 0.$$

Deste modo, grau $(f(X)) = n$ e grau $(g(X)) = m$.

a) Usando a notação acima para $f(X)$ e $g(X)$ temos:

$$f(X).g(X) = c_0 + c_1X + c_2X^2 + \cdots, \text{ onde } c_k = \sum_{i+j=k} a_ib_j.$$

Note que, para todo $k \geq (m+n)+1$, $c_k = 0$, já que neste caso $a_i = 0$ ou $b_j = 0$.
Note ainda que $c_{n+m} \neq 0$, pois

$$c_{n+m} = \sum_{i+j=n+m} a_ib_j =$$

$$= a_0b_{m+n} + a_1b_{m+n-1} + \cdots + a_{n-1}b_{m+1} + a_nb_m + a_{n+1}b_{m-1} + \cdots + a_{m+n}b_0,$$

todas as parcelas anteriores e posteriores a a_nb_m são nulas e a parcela $a_nb_m \neq 0$, pois $a_n \neq 0$, $b_m \neq 0$ e D é um domínio.
Logo, podemos concluir que grau $(f(X).g(X)) = n + m$

$$= \text{grau } (f(X)) + \text{ grau } (g(X)).$$

b) Temos três possibilidades para analisar:

$$\text{grau } f(X) > \text{ grau } g(X),$$

$$\text{grau } f(X) = \text{ grau} g(X) \text{ e}$$

$$\text{grau } f(X) < \text{ grau } g(X).$$

1º caso: grau $f(X) >$ grau $g(X)$.
Neste caso temos:

$$f(X)+g(X) = a_nX^n+\cdots+a_{m+1}X^{m+1}+(a_m+b_m)X^m+\cdots+(a_1+b_1)X+(a_0+b_0)$$

e então como $a_n \neq 0$, vem que

$$\text{grau } (f(X) + g(X)) = n = \text{ max } \{ \text{ grau } f(X), \text{ grau } g(X)\}.$$

2º caso: grau $f(X) =$ grau $g(X)$.
Neste caso temos $n = m$ e:

$$f(X) + g(X) = (a_n + b_m)X^n + \cdots + (a_1 + b_1)X + (a_0 + b_0).$$

Note que, neste caso $a_n + b_m$ pode ser nulo. No entanto, como $(f(X) + g(X)) \neq 0$, algum coeficiente $(a_i + b_i), 0 \leq i \leq n$, é não nulo. Então:

grau $(f(X)+g(X)) \leq$ grau $f(X)$

$= \max\{\text{grau } f(X), \text{grau } g(X)\}.$

3^{o} caso: grau $f(X) <$ grau $g(X)$.

Neste caso temos:

$f(X)+g(X) = b_mX^m+\cdots+b_{n+1}X^{n+1}+(a_n+b_n)X^n+\cdots+(a_1+b_1)X+(a_0+b_0).$

E então, como $b_m \neq 0$, vem que,

grau $(f(X)+g(X)) = m$

$=$ grau $g(X)$

$=$ max $\{$ grau $f(X),$ grau $g(X)\}$.

Portanto, grau $(f(X)+g(X)) \leq$ max $\{$ grau $f(X)$, grau $g(X)\}$.

c) Análogo ao item b).

■

Teorema 1.3. *Seja $(R[X],+,\cdot)$ o anel de polinômios numa variável sobre o anel R. Seja $f(X) \in R[X]$ um polinômio. Seja $g(X) = b_mX^m+\cdots+b_1X+b_0 \in R[X]$ um polinômio com b_m invertível em R. Então:*

a) Existem $t(X),\ r(X) \in R[X]$ tais que:

$$f(X) = g(X)t(X)+r(X) \text{ com } \begin{cases} \text{grau } r(X) < \text{grau } g(X) \\ \text{ou } r(X) = 0 \end{cases}$$

b) Tais $t(X)$ e $r(X)$ podem ser efetivamente calculados.

c) Tais $t(X)$ e $r(X)$ são unicamente determinados.

Demonstração. a) Se $f(X) = 0$ ou grau $f(X) <$ grau $g(X)$ então tome

$$t(X) = 0X+0X^2+\cdots \quad \text{e} \quad r(X) = f(X).$$

Agora vamos analisar o caso onde grau $f(X) \geq$ grau $g(X)$.
Considerando que grau $f(X) = n$, podemos escrevê-lo da seguinte maneira:

$$f(X) = a_nX^n+\cdots+a_1X+a_0, \text{ com } a_n \neq 0.$$

Como b_m é invertível em R, vem que $(b_m)^{-1} \in R$ e então $(b_m)^{-1}a_n \in R$, ou seja, $(b_m)^{-1}a_nX^{n-m} \in R[X]$.
Note que, multiplicando $(b_m)^{-1}a_nX^{n-m}$ pelo primeiro termo de $g(X)$ obtemos o primeiro termo de $f(X)$. Dessa forma temos que:

$$f(X) - ((b_m)^{-1}a_nX^{n-m})g(X) =$$
$$= (a_{n-1} - a_nb_{m-1}(b_m)^{-1})X^{n-1} + \cdots + (a_{n-m} - a_nb_0(b_m)^{-1})X^{n-m} + a_{n-m-1}X^{n-m-1} + \cdots + a_0$$
$$= f_1(X).$$

Logo $f(X) = g(X).(b_m)^{-1}a_nX^{n-m} + f_1(X)$.
Note que $(b_m)^{-1}a_n$ e $f_1(X)$ foram efetivamente calculados.
Se $f_1(X) = 0$ ou se grau $f_1(X) <$ grau $g(X)$ então acabou. Tome

$$t(X) = (b_m)^{-1}a_nX^{n-m} \qquad \text{e} \qquad r(X) = f_1(X).$$

Se $p =$ grau $f_1(X) \geq m$ então repita o processo com $f_1(X)$ e $g(X)$ no lugar de $f(X)$ e $g(X)$:
Como grau $f_1(X) = p$, vem que:

$$f_1(X) = c_pX^p + \cdots + c_1X + c_0 \text{ com } c_p \neq 0 \text{ e com } n - 1 \geq p \geq m.$$

Note que, multiplicando $(b_m)^{-1}c_pX^{p-m}$ pelo primeiro termo de $g(X)$, obtemos o primeiro termo de $f_1(X)$:

$$f_1(X) - ((b_m)^{-1}c_pX^{p-m})g(X) =$$
$$= (c_{p-1} - c_pb_{m-1}(b_m)^{-1})X^{p-1} + \cdots + (c_{p-m} - c_pb_0(b_m)^{-1})X^{p-m} + \cdots = f_2(X).$$

Logo

$$f_1(X) = ((b_m)^{-1}c_pX^{p-m})g(X) + f_2(X).$$

Substituindo $f_1(X)$ em $f(X) = g(X).(b_m)^{-1}a_nX^{n-m} + f_1(X)$ vem que:

$$f(X) = g(X)[(b_m)^{-1}a_nX^{n-m} + (b_m)^{-1}c_pX^{p-m}] + f_2(X),$$

onde $(b_m)^{-1}a_n, (b_m)^{-1}c_p$ e $f_2(X)$ são efetivamente calculáveis.
Se $f_2(X) = 0$ ou se grau $f_2(X) <$ grau $g(X)$ então acabou. Tome

$$t(X) = (b_m)^{-1}a_nX^{n-m} + (b_m)^{-1}c_pX^{p-m} \qquad \text{e} \qquad r(X) = f_2(X).$$

Se $s =$ grau $f_2(X) \geq m$ então repita o processo com $f_2(X)$ e $g(X)$ no lugar de $f_1(X)$ e $g(X)$.
Note que, depois de um número finito de passos, chegamos em grau $f_j(X) = 0$ ou grau $f_j(X) < m$, pois grau $f(X) \in \mathbb{N}$ e

$$\text{grau } f(X) > \text{ grau } f_1(X) > \text{ grau } f_2(X) > \cdots .$$

b) Note que no item a) $t(X), r(X)$ foram efetivamente calculados.

c) Suponhamos que existem $t_1(X), r_1(X), t_2(X), r_2(X) \in R[X]$ tais que:

$$f(X) = g(X).t_1(X) + r_1(X) = g(X).t_2(X) + r_2(X), \quad (*)$$

$$\text{com} \begin{cases} \text{grau} \quad r_1(X) \quad < \quad \text{grau} \quad g(X) \quad (\text{ ou } r_1(X) = 0) \\ \text{grau} \quad r_2(X) \quad < \quad \text{grau} \quad g(X) \quad (\text{ ou } r_2(X) = 0) \end{cases}$$

Colocando $g(X)$ em evidência em $(*)$, obtemos:

$$g(X)[t_1(X) - t_2(X)] = r_2(X) - r_1(X).$$

Suponhamos por absurdo que $[t_1(X) - t_2(X)] \neq 0$. Então, como o coeficiente do termo de maior grau de $g(X)$ é inversível, ou seja, não é um divisor de zero, vem que, $r_2(X) - r_1(X) \neq 0$. Desta maneira, pelo item a) do Lema 1.3 obtemos:

$$\begin{aligned} \text{grau } (r_2(X) - r_1(X)) &= \text{grau } (g(X)[t_1(X) - t_2(X)]) \\ &= \text{grau } g(X) + \text{grau } (t_1(X) - t_2(X)), \end{aligned}$$

Como a imagem da função grau está contida nos números naturais, vem que:

$$\text{grau } (r_2(X) - r_1(X)) \geq \text{ grau } g(X).$$

Mas isso é um absurdo, já que pelo item c) das propriedades de norma temos:

$$\text{grau } (r_2(X) - r_1(X)) \leq \max\{\text{grau } r_1(X), \text{ grau } r_2(X)\} < \text{ grau } g(X).$$

Portanto $[t_1(X) - t_2(X)] = 0$, ou seja, $t_1(X) = t_2(X)$.
Conseqüentemente, $r_2(X) - r_1(X) = 0$ e daí, $r_2(X) = r_1(X)$.

■

Corolário 1.1. *Seja $(K, +, \cdot)$ um corpo e seja $K[X]$ o anel de polinômios numa variável sobre K. Seja grau $: K[X]\backslash\{0\} \longrightarrow \mathbb{N}$ a função grau. Então:*

a) $(K[X], +, \cdot,$ grau$)$ é um domínio euclidiano, isto é:

$$\begin{cases} i)\ K[X] \text{ é um domínio.} \\ ii) \forall\ f(X),\ g(X) \in K[X], g(X) \neq 0, \text{ existem} \\ \qquad t(X),\ r(X) \in K[X] \text{ tais que :} \\ \qquad f(X) = g(X)t(X) + r(X) \text{ com} \begin{cases} \text{grau } r(X) \quad < \quad \text{grau } g(X) \\ \text{ou} \quad r(X) \quad = 0 \end{cases} \\ iii) \forall f(X),\ g(X) \in K[X]\backslash\{0\},\ \text{grau} f \leq \text{grau}(fg). \end{cases}$$

b) Tais $t(X)$ e $r(X)$ podem ser efetivamente calculados.

c) Tais $t(X)$ e $r(X)$ são unicamente determinados.

Demonstração. a) i) Já sabemos que $K[X]$ é um anel comutativo e com unidade, pois K é corpo e em particular é domínio. Logo, para mostrar que $K[X]$ é um domínio, basta verificar que não possui divisores de zero.
Sejam $p(X),\ q(X) \in K[X]\backslash\{0\}$.

$$p(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \text{ e}$$

$$q(X) = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0,$$

com $a_n \neq 0, b_m \neq 0, n \geq m$ e $\forall n_0 > n, a_{n_0} = 0$ e $\forall m_0 > m, b_{m_0} = 0$.

Então $p(X)q(X) = c_0 + c_1X + c_2X^2 + \cdots + c_{n+m}X^{m+n} + \cdots$,

onde $c_k = \sum_{i+j=k} a_ib_j$.
Note que c_{n+m}, o coeficiente de X^{m+n}, é distinto de zero pois,

$$c_{n+m} = \sum_{i+j=n+m} a_ib_j =$$

$$a_0b_{n+m} + a_1b_{n+m-1} + \cdots + a_nb_m + a_{n+1}b_{m-1} + \cdots + a_{n+m}b_0,$$

a parcela $a_nb_m \neq 0$ pois $a_n \neq 0, b_n \neq 0$, $a_n, b_m \in K$ e K é domínio e as demais parcelas são iguais a zero.
Logo $p(X)q(X) \neq 0 + 0X + 0X^2 + \cdots$, e portanto $K[X]$ é um domínio.

ii) Este item já foi provado no item a) do teorema anterior. Basta notar que $\forall g(X) \in K[X], g(X) \neq 0$, o coeficiente do termo de maior grau é invertível, visto que K é corpo.

iii) Dados $f(X), g(X) \in K[X]\backslash\{0\}$, como K é domínio, temos que:

$$\text{grau } (f(X)g(X)) = \text{grau } f(X) + \text{grau } g(X).$$

A imagem da função grau está contida no conjunto dos números naturais. Logo:

$$\text{grau } f(X) \leq \text{grau } f(X) + \text{grau } g(X) = \text{grau } (f(X)g(X)).$$

b) Já foi provado no teorema anterior.

c) Já foi provado no teorema anterior.

■

Vimos que $(\mathbb{Z}, +, \cdot, |\ |)$, $(\mathbb{Z}[i], +, \cdot, N)$, e $(K[X], +, \cdot, \text{grau}\ )$, K é corpo, são domínios euclidianos. Nosso próximo objetivo é mostrar que todo domínio euclidiano é domínio principal, e que todo domínio principal é um domínio fatorial no qual vale a Identidade de Bezout.

Iniciamos verificando que, em um domínio, quando existe mdc ele é único a menos de elementos associados.

Definição 1.13. Sejam A um anel e $a_1, a_2, \cdots, a_n \in A$. Um elemento $d \in A$ é um **máximo divisor comum** de $a_1, a_2, \cdots, a_n$ se d divide $a_1, a_2, \cdots, a_n$ e se todo elemento d' que divide $a_1, a_2, \cdots, a_n$, divide d também.

Notação: $d = mdc(a_1, a_2, \cdots, a_n)$.

Dizemos que o anel A satisfaz a Identidade de Bezout, se para quaisquer $a, b \in A$, existem $r, s \in A$ tais que $mdc(a, b) = ra + sb$.

Definição 1.14. Sejam A um anel com unidade e $a, b \in A$. Se existe $u \in \mathcal{U}(A)$ tal que $a = ub$ então a e b são denominados **elementos associados**. Notação: $a \sim b$.

Em geral, se A é um anel e $\alpha, \beta \in A$ então o $mdc(\alpha, \beta)$, quando existe, não é único. Por exemplo, 1 e -1 são máximos divisores comuns para 2 e 3 em $\mathbb{Z}$; $\overline{1}$ e $\overline{3}$ são máximos divisores comuns para $\overline{2}$ e $\overline{3}$ em $\mathbb{Z}_4$.

Se A for um domínio, então o mdc de elementos de A, quando existe, é único, a menos de elementos associados. Isso nos faz mostrar o resultado seguinte.

Proposição 1.3. Sejam $\alpha, \beta, x \in D$, onde D é domínio e $d = mdc(\alpha, \beta)$. Então $mdc(\alpha, \beta) = x$, se e somente se, $x \sim d$.

Demonstração. ($\Rightarrow$) Como $x = mdc(\alpha, \beta)$, $d|\alpha$ e $d|\beta$, temos, pela definição de máximo divisor comum, que $d|x$, ou seja, $\exists v \in D$ tal que $dv = x$ (*).
Como $d = mdc(\alpha, \beta)$, $x|\alpha$ e $x|\beta$, temos, pela definição de máximo divisor comum, que $x|d$, ou seja, $\exists u \in D$ tal que $xu = d$ (**).
Substituindo (**) em (*) vem que:

$$\begin{aligned} xu.v = x &\Longrightarrow x(uv - 1) = 0 \\ &\Longrightarrow x = 0 \text{ ou } (uv - 1) = 0 \text{ (pois } D \text{ não possui divisores de zero).} \end{aligned}$$

Se $x = 0$ então $\alpha = 0$ e $\beta = 0$, logo $d = 0$ e portanto $x = 1.d$.
Se $(uv - 1) = 0$ então $uv = 1$, e daí segue-se que $u, v \in \mathcal{U}(D)$. Portanto x e d são associados.

($\Leftarrow$) Se $x \sim d$ então existe $u \in \mathcal{U}(D)$ tal que $x = ud$.
Como $d|\alpha$ e $d|\beta$ temos que existem $t_1, t_2 \in D$ tais que:

$$dt_1 = \alpha \quad \text{e} \quad dt_2 = \beta.$$

Então multiplicando por uu^{-1} no lado esquerdo, de ambas as equações, obtemos:

$$(du)u^{-1}t_1 = \alpha \quad \text{e} \quad (du)u^{-1}t_2 = \beta.$$

Portanto $x = ud$ divide α e também divide β.
Seja $x^{'} \in D$ tal que $x^{'}|\alpha$ e $x^{'}|\beta$. Como $d = mdc(\alpha, \beta)$ vem que $x^{'}|d$, ou seja, $x^{'}t = d, t \in D$.
Multiplicando em ambos os lados de $x^{'}t = d$ por u temos:

$$x^{'}(tu) = du = x$$
$$\Longrightarrow x^{'}|x.$$

Logo $x = mdc(\alpha, \beta)$.

■

Definição 1.15. Seja A um anel comutativo. Um subconjunto não vazio $I \subseteq A$ é um **ideal** de A se satisfizer as duas condições a seguir:

$$\begin{cases} x, y \in I \Longrightarrow x - y \in I; \\ x \in I, r \in A \Longrightarrow rx \in I. \end{cases}$$

Definição 1.16. Seja A um anel. Um ideal I de A é dito ideal principal se existe $\alpha \in A$ tal que $I = \alpha.A$. Um domínio no qual todo ideal é principal é chamado **domínio principal**.

Proposição 1.4. Se A é um anel, então dado $a \in A$, temos que $aA = \{a.t; t \in A\}$ é um ideal de A.

Demonstração. Dados $x, y \in aA$ e $m \in A$ temos:

$$x = a.d, d \in A \text{ e } y = a.l, l \in A.$$

Logo $x - y = a.d - a.l$
$= a.(d - l) \in aA$ e

$x.m = a.d.m$
$= a.(d.m) \in aA.$

Portanto aA é ideal de A.

■

Observação 1.4. Chamamos aA de ideal principal gerado por a e também o denotaremos por (a).
Analogamente podemos mostrar que $(a_1, a_2, ..., a_n) = a_1A + a_2A + ... + a_nA = \{a_1x_1 + a_2x_2 + ... + a_nx_n; x_1, x_2, ..., x_n \in A\}$ é um ideal de A.

Proposição 1.5. Seja D um domínio.

a) Se $a_1, a_2, \cdots, a_n \in D$ são tais que $(a_1, a_2, \cdots, a_n)$ é um ideal principal, ou seja, $(a_1, a_2, \cdots, a_n) = (d)$, então $mdc(a_1, a_2, \cdots, a_n)$ existe, e é igual a d e também existem $\lambda_1, \lambda_2, \cdots, \lambda_n \in D$ tais que $mdc(a_1, a_2, \cdots, a_n) = \lambda_1 a_1 + \cdots + \lambda_n a_n$.

b) Sejam $a, b \in D\backslash\{0\}$ tais que $(a, c) = (1)$ e $(b, c) = (1)$ então $(ab, c) = (1)$.

Demonstração. a) Como $(a_1, a_2, \cdots, a_n) = (d)$, temos que, $\forall y_1, y_2, \cdots, y_n \in D, \exists l \in D$ tal que:

$$a_1.y_1 + a_2.y_2 + \cdots + a_n.y_n = dl.$$

Em particular, se $y_2 = y_3 = \cdots = y_n = 0$ e $y_1 = 1$ então existe $l_1 \in D$ tal que $a_1.1 = d.l_1$, e portanto, $d|a_1$.
Se $y_1 = y_3 = \cdots = y_n = 0$ e $y_2 = 1$ então existe $l_2 \in D$ tal que $a_2.1 = d.l_2$, e portanto, $d|a_2$.
Assim, podemos concluir que $d|a_i, \forall i = 1, 2, \cdots, n$.
Por outro lado, como $d \in (d) = (a_1, a_2, \cdots, a_n)$, existem $z_1, \cdots, z_n \in D$ tais que

$$d = a_1z_1 + a_2z_2 + \cdots + a_nz_n. \qquad (*)$$

Dessa maneira, se existir $d' \in D$ tal que $d'|a_1, d'|a_2, \cdots, d'|a_n$ então existem $x_1, x_2, \cdots, x_n$ tais que:

$$a_1 = d'.x_1,$$
$$a_2 = d'x_2,$$
$$\vdots$$
$$a_n = d'.x_n.$$

Substituindo as representações para $a_1, a_2, \cdots, a_n$ em (*) vem que:

$$d'(x_1 + x_2 + \cdots + x_n) = d$$

e portanto $d'|d$.
Logo, podemos concluir que, $d = mdc(a_1, a_2, \cdots, a_n)$.

b) (ab, c) é um ideal de $D = (1)$. Logo $(ab, c) \subseteq (1)$.
Falta mostrar que $(1) \subseteq (ab, c)$, ou seja, é preciso mostrar que existem $x, y \in D$ tais que $ab.x + cy = 1$.
Por hipótese, existem m_1, m_2, n_1 e n_2 tais que:

$$a.m_1 + c.m_2 = 1$$

$$b.n_1 + c.n_2 = 1$$

Multiplicando membro a membro as duas igualdades acima obtemos:

$$ab.(m_1.n_1) + c.(b.n_1.m_2 + a.m_1.n_2 + c.m_2.n_2) = 1.$$

Então $(1) \subseteq (ab, c)$ e portanto $(1) = (ab, c)$.

■

Podemos concluir a partir da Proposição 1.5 que em um domínio principal o mdc sempre existe, pois nele, todo ideal é principal.

Definição 1.17. Um domínio D é um domínio de fatoração única ou **domínio fatorial** se satisfaz as condições a seguir:

a) Todo elemento não-invertível e não nulo de D é um produto finito de fatores irredutíveis.

b) Se $\{p_i\}_{1 \leq i \leq s}$ e $\{q_j\}_{1 \leq j \leq t}$ são famílias finitas de elementos irredutíveis de D tais que $p_1 \cdots p_s = q_1 \cdots q_t$, então:

   i) $s = t$;

   ii) a menos da ordenação, p_i é associado a $q_i, \forall i = 1, 2, \ldots, s$.

Para provar que todo domínio principal é fatorial, usaremos os lemas abaixo:

Lema 1.4. Se D é um domínio principal então D não possui uma sequência infinita estritamente crescente de ideais $a_1D \subsetneqq a_2D \subsetneqq \cdots$.

Demonstração. Suponha por absurdo que D possui uma sequência infinita e estritamente crescente de ideais $a_1D \subsetneqq a_2D \subsetneqq \cdots$.
Considere $\bigcup_{i=1}^{\infty} a_iD = A$.

Afirmação: A é um ideal.
De fato, dados $x, y \in A$, temos que $x \in a_jD$ e $y \in a_iD; j, i \in \mathbb{N}^*$. Suponha sem perda de generalidade que $j < i$. Como $a_jD \subsetneq a_iD$, temos que $x, y \in a_iD$. Conseqüentemente $x - y \in a_iD \subseteq A$. Logo $x - y \in A$.
Dado $a \in A$ e $n \in D$, implica que $a \in a_iD$ para algum $i \in \mathbb{N}^*$, que é ideal. Logo $a.x \in a_iD \subseteq A$ e portanto $a.x \in A$.
Assim, pela Definição 1.14 podemos concluir que A é ideal de D.
Como A é um ideal de D, e D é um domínio principal, existe $\alpha \in D$ tal que $A = \alpha D$. Ainda por D ser um domínio temos que 1 (elemento neutro com relação a operação $\cdot$) $\in D$ e então $\alpha \in A$, ou seja, para algum $r \in \mathbb{N}^*, \alpha \in a_rD$.
Note que, $a_rD = \alpha D$.
De fato, como $\alpha \in a_rD$, existe $d \in D$ tal que $a_r.d = \alpha$. E então dado $x \in \alpha D$ temos que: $x = \alpha.l, l \in D$

$$= (a_r.d).l; l, d \in D$$
$$= a_r(d.l); d.l \in D, \text{ pois } D \text{ é domínio.}$$

Logo $x \in a_rD$ e então $\alpha D \subseteq a_rD$.
A inclusão $a_rD \subseteq \alpha D$ é óbvia, pois $\alpha D = \bigcup_{i=1}^{\infty} a_iD$.
Então $a_rD = \alpha D$, ou seja, $\bigcup_{i=1}^{\infty} a_iD = a_rD$ e isto implica que $a_jD = a_rD, \forall j \geq r$.
Absurdo, pois estamos supondo a sequência estritamente crescente.
Portanto, se D é um domínio então D não possui uma sequência infinita estritamente crescente de ideais.

■

Lema 1.5. Sejam D um domínio e $a \in D\backslash\{0\}, a$ não inversível. Se $a = a_1.x, a_1, x \notin \mathcal{U}(D)$, então $aD \subsetneq a_1D$.

Demonstração. Dado $y \in aD$, temos que $y = a.d = a_1.x.d, d \in D$. Logo $y = a_1(x.d)$, ou seja, $y \in a_1D$.
Agora vamos mostrar que existe $y' \in a_1D$ tal que $y' \notin aD$.
Tome $y' = a_1$.
Afirmação: $y' \notin aD$.
De fato, suponha por absurdo que $y' \in aD$. Então existe $l \in D$ tal que

$$a_1 = y' = a.l = a_1.x.l.$$

Assim, vem que $a_1(1 - xl) = 0$. Mas como $a_1 \neq 0$, pois $a \neq 0$, temos que $1 - x.l = 0$, ou seja, $x.l = 1$. E então $x \in \mathcal{U}(D)$. Absurdo!
Portanto $aD \subsetneq a_1D$.

■

Definição 1.18. Um elemento $a \in A\backslash\{0\}$ é um **elemento primo** se $a \notin \mathcal{U}(A)$ e $a|bc$ implica que $a|b$ ou $a|c$.

Lema 1.6. Sejam D um domínio principal e $p \in D$. São equivalentes:

(i) p é elemento primo.

(ii) p é elemento irredutível.

Demonstração. (i) $\Rightarrow$ (ii) Sejam $a, b \in D$ tais que $p = ab$. Como $p|ab$, segue de (i) que $p|a$ ou $p|b$.
• Se $p|a$ então $pt = a, t \in D$. Substituindo em $p = ab$ vem que $p = ptb$. Desde que $p \neq 0$ e D é domínio, temos que $tb = 1$, e portanto b é inversível.
• Analogamente, se $p|b$ concluímos que $a \in \mathcal{U}(D)$.
Portanto p é elemento irredutível.

(ii) $\Rightarrow$ (i) Sejam $a, b \in D$ tais que $p|ab$. Como D é domínio principal temos que $aD + pD = dD$, para algum $d \in \mathbb{Z}$.
Agora,

$$p \in aD + pD = dD \Longrightarrow p = dq, q \in D.$$

Desde que p é irredutível concluímos que $d \in \mathcal{U}(D)$ ou $q \in \mathcal{U}(D)$.

- $d \in \mathcal{U}(D) \Longrightarrow dD = D$
$\Longrightarrow 1 = ax + py; x, y \in D$
$\Longrightarrow b = abx + pby; x, y \in D.$

Como $p|ab$, temos que $p|b$.

- $q \in \mathcal{U}(D) \Longrightarrow d = pq^{-1}$
$\Longrightarrow p|d.$

Mas: $a \in aD + pD = dD \Longrightarrow d|a$.
Como $p|d$ e $d|a$, temos que $p|a$.
Logo, $p|a$ ou $p|b$. Portanto p é elemento primo.

■

Observação 1.5. Vimos na demonstração do Lema 1.6 que todo elemento primo é irredutível, pois para provar (i) $\Longrightarrow$ (ii), não usamos a hipótese de D ser domínio principal.

Teorema 1.4. *Seja $(D, +, \cdot)$ um domínio. Então as seguintes afirmações são equivalentes:*

(i) D *é um domínio principal.*

(ii) D *é um domínio fatorial que possui a seguinte propriedade:*
$\forall a, b \in D\backslash\{0\}, \exists e, f \in D$ *tais que* $mdc(a, b) = ea + fb$.

Demonstração. $(i) \Rightarrow (ii)$ Dado $a \in D\backslash\{0\}, a$ não inversível, vamos mostrar que a possui uma fatoração única em elementos irredutíveis.
Afirmamos que a possui um divisor irredutível.
De fato, suponhamos por absurdo que a não possua um divisor irredutível, então a não é irredutível.
Logo $a = a_1.a_1^{'}$, onde $a_1, a_1^{'} \notin \mathcal{U}(D)$ e $a_1, a_1^{'} \in D\backslash\{0\}$. Pelo Lema 1.5, $aD \subsetneq a_1D$.
Como a não possui nenhum divisor irredutível, temos que a_1 não é irredutível, ou seja, $a_1 = a_2.a_2^{'}$, com $a_2, a_2^{'} \notin \mathcal{U}(D)$.
Logo, pelo Lema 1.5, $a_1D \subsetneq a_2D$.
Note que $a = a_2a_2^{'}a_1^{'}$ e então a_2 não é irredutível. Desta forma $a_2 = a_3a_3^{'}$, $a_3, a_3^{'} \notin \mathcal{U}(D)$ e então $a_2D \subsetneq a_3D$.
Continuando desta maneira, teremos uma sequência infinita e crescente de ideais de A

$$aD \subsetneq a_1D \subsetneq a_2D \subsetneq \cdots .$$

No entanto, pelo Lema 1.4, isto é um absurdo, já que D é domínio principal.
Logo a possui um divisor irredutível p_1, ou seja, $a = p_1b_1, b_1 \in D$.
Se $b_1 \in \mathcal{U}(D)$ então acabou, a é irredutível, pois p_1b_1 é irredutível.
Se $b_1 \notin \mathcal{U}(D)$ então $aD \subsetneq b_1D$ e pelo mesmo raciocínio, obtemos que b_1 possui um divisor irredutível, ou seja, $b_1 = p_2.b_2$, com p_2 irredutível.
Se $b_2 \in \mathcal{U}(D)$, acabou, pois $a = p_1p_2b_2$.
Se $b_2 \notin \mathcal{U}(D)$ então $b_1D \subsetneq b_2D$ e b_2 possui um divisor irredutível, ou seja, $b_2 = p_3.b_3$.
Se $b_3 \in \mathcal{U}(D)$ então acabou.
Se $b_3 \notin \mathcal{U}(D)$ repetimos o mesmo processo de b_2 à b_3.
Note que este processo é finito, caso contrário, obteríamos uma sequência infinita estritamente crescente de ideais $aD \subsetneq b_1D \subsetneq b_2D \subsetneq \cdots$, mas, pelo Lema 1.4, isto é uma contradição com o fato de D ser domínio principal.
Logo a possui uma fatoração em elementos irredutíveis.
Agora, resta-nos mostrar a unicidade de tal fatoração.
Sejam $\{p_i\}_{1\leq i\leq s}$ e $\{q_j\}_{1\leq j\leq t}$ famílias de elementos irredutíveis de D, tais que

$$p_1 \cdots p_s = q_1 \cdots q_t. \quad (*)$$

Pelo Lema 1.6 os elementos $p_1, \cdots, p_s, q_1, \cdots, q_t$ são primos. Conseqüentemente, já que $p_1|q_1 \cdots q_t$, existe $j \in \{1, \cdots, t\}$ tal que $p_1|q_j$, isto é, $\alpha_1p_1 = q_j$.

Como q_j é irredutível e p_1 não é inversível, temos que $\alpha_1 \in \mathcal{U}(D)$. Logo $p_1 \sim q_j$. Reordenando, se necessário, o conjunto $\{q_j\}_{1\leq j\leq t}$, podemos considerar que $p_1 \sim q_1$, isto é $\alpha_1 p_1 = q_1, \alpha_1 \in \mathcal{U}(D)$.
Substituindo esta última igualdade em $(*)$ obtemos:

$$p_1 p_2 \cdots p_s = \alpha_1 p_1 q_2 \cdots q_t \Longrightarrow p_2 \cdots p_s = \alpha_1 q_2 \cdots q_t.$$

Como p_2 é primo e $p_2 | \alpha_1 q_2 \cdots q_s$, temos que $p_2 | \alpha_1$ ou $p_2 | q_j$ para algum $j \in \{2, \cdots, t\}$.
Afirmação: Elementos primos não dividem elementos inversíveis.
De fato, suponha que p é primo, u é inversível e $pv = u$.
Como u é inversível temos que $p(vu^{-1}) = 1$, implicando que p é inversível. Absurdo, pois, pela definição, um elemento primo não é inversível.
Segue da afirmação acima que $p_2 | q_j$, para algum $j \in \{2, \cdots, t\}$.
De forma análoga ao que fizemos com p_1, podemos considerar que $\alpha_2 p_2 = q_2, \alpha_2 \in \mathcal{U}(D)$. Logo $p_2 \sim q_2$.
Seguindo o processo, que é finito, concluímos que cada p_i é associado a algum q_j.
Resta provar que $s = t$.
• Se $s < t$ teremos, após as simplificações,

$$1 = \alpha_1 \alpha_2 \cdots \alpha_s q_{s+1} \cdots q_t.$$

Isto é um absurdo, pois afirma que $q_t \in \mathcal{U}(D)$.
• Se $s > t$ teremos, após as simplificações,

$$p_{t+1} p_{t+2} \cdots p_s = \alpha_1 \alpha_2 \cdots \alpha_t,$$

que equivale a $(\alpha_1 \cdots \alpha_t)^{-1}(p_{t+1} \cdots p_{s-1}) p_s = 1$. Isso é um absurdo, pois diz que $p_s \in \mathcal{U}(D)$.
Logo $s = t$.
Fica provada a unicidade, e portanto D é um domínio fatorial.
Dados $a, b \in D\backslash\{0\}$, como D é domínio principal, segue da Proposição 1.5 que existem $e, f \in D$ tais que $mdc(a, b) = ea + fb$.

$(ii) \Rightarrow (i)$ Primeiro vamos mostrar que todo ideal finitamente gerado de D é também um ideal principal. Desta forma, será suficiente mostrarmos que todo ideal de D é finitamente gerado.
Dado $(a_1, a_2, \cdots, a_n)$, por hipótese, existem $x_1, x_2, ..., x_n \in D$ tais que

$$a_1.x_1 + a_2.x_2 + ... + a_n.x_n = mdc(a_1, a_2, \cdots, a_n) = d.$$

E então podemos concluir que $d \in (a_1, a_2, \cdots, a_n)$, ou seja, $(d) \subseteq (a_1, a_2, \cdots, a_n)$.
Note que $d | a_1, d | a_2, \cdots, d | a_n$, ou seja, existem $l_1, l_2, \cdots, l_n$ tais que:

$$a_1 = d.l_1$$

$$a_2 = d.l_2$$
$$\vdots$$
$$a_n = d.l_n$$

pois $d = mdc(a_1, a_2, \cdots, a_n)$.
Desta forma, dado $l = a_1.y_1 + a_2.y_2 + ... + a_n.y_n \in (a_1, a_2, \cdots, a_n)$ temos que:

$$l = d.(l_1y_1 + l_2y_2 + \cdots + l_ny_n)$$

e então $l \in (d)$. Assim, vem que $(a_1, a_2, \cdots, a_n) \subseteq (d)$.
Portanto $(a_1, a_2, \cdots, a_n) = (d)$.
Agora suponhamos, por absurdo, que existe em D um ideal I que não seja finitamente gerado. Então existe uma sequência infinita de elementos de I, $a_1, a_2, \cdots, a_n, \cdots$ tal que:

$$(a_1) \subsetneqq (a_1, a_2) \subsetneqq \cdots \subsetneqq (a_1, a_2, \cdots, a_n) \subsetneqq \cdots$$

Para cada $n \in \{1, 2, 3, \cdots\}$, $(a_1, a_2, \cdots, a_n)$ é um ideal principal, ou seja,

$$(a_1, a_2, \cdots, a_n) = (b_n).$$

Logo, existe uma seqüência infinita estritamente crecente de ideais principais:

$$(b_1) \subsetneqq (b_2) \subsetneqq \cdots \subsetneqq (b_n) \cdots .$$

Dado n arbitrariamente grande, temos que $(b_{i-1}) \subsetneqq (b_i)$ e então, podemos fazer a seguinte afirmação:

$$\forall i \leq n,\ b_{i-1} \textit{ tem pelo menos um fator irredutível a mais que } b_i.$$

De fato, $b_{i-1} \in (b_i)$, $\forall i \leq n$, conseqüentemente $b_{i-1} = b_i.d, d \in D$, onde $d \notin \mathcal{U}(D)$, caso contrário, teríamos $(b_{i-1}) = (b_i)$, e $d \neq 0$, caso contrário, teríamos $(b_1) = (b_2) = \cdots = (b_{i-1})$.
Se d é irredutível, então b_{i-1} realmente tem um fator irredutível a mais que b_i.
Se d não é irredutível, tomemos sua fatoração em elementos irredutíveis:

$$d = p_1^{\alpha_1} \cdots p_n^{\alpha_n}.$$

Neste caso, $b_{i-1} = b_i p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ e então b_{i-1} também tem, pelo menos, um fator irredutível a mais que b_i.
Logo, $b_{i-1}, \forall i \leq n$, tem, pelo menos, um fator irredutível a mais que b_i.
Note também que $b_n, \forall n$, tem, pelo menos, um fator irredutível. Caso contrário, teríamos $b_n = 0$ ou $b_n \in \mathcal{U}(D)$ e, nestes dois casos obteríamos que:

$$(b_n) = (b_{n+1}) = (b_{n+2}) \cdots .$$

Absurdo!
Assim, podemos concluir que:
b_{n-1} tem pelo menos dois fatores irredutíveis;
b_{n-2} tem pelo menos três fatores irredutíveis;
$\vdots$
$b_1 = a_1$ tem pelo menos n fatores irredutíveis.
Infere-se daí um absurdo, pois, a quantidade de fatores irredutíveis de a_1 muda, dependendo da escolha de n, ou seja, não há unicidade na fatoração de a_1.
Portanto, todo ideal de D é finitamente gerado, e como neste caso, todo ideal finitamente gerado é principal, temos que D é um domínio principal.

■

Teorema 1.5. *Seja $(D, +, \cdot, \varphi)$ um domínio euclidiano. Então:*

a) D é um domínio principal.

b) $\forall a, b \in D\backslash\{0\}$, pode-se calcular efetivamente $e, f \in D$ tais que $mdc(a, b) = ea + fb$, se a divisão em D for efetiva.

Demonstração. a) Seja I um ideal de D, temos de mostrar que $I = aD$, onde $a \in D$, ou seja, dado $\varepsilon \in I$ precisamos mostrar que $\varepsilon = a.h, h \in D$.
Se $I = \{0\}$, onde 0 é o elemento neutro para a operação $+$, então $I = 0D$.
Se $I \neq \{0\}$, consideremos o seguinte conjunto:

$$\varphi(I) = \{\varphi(\alpha), \alpha \in I \text{ e } \alpha \neq 0\}$$

O conjunto dos números naturais é bem ordenado, e então todo subconjunto dele possui um menor elemento. Logo $\varphi(I)$ possui um menor elemento. Denotaremos tal elemento por $\varphi(a), a \in I$ e mostraremos que $I = aD$
Dado $\varepsilon \in I$, pela propriedade euclidiana existem $t, r \in D$ tais que:

$$\varepsilon = at + r \quad \text{com} \begin{cases} \varphi(r) & < & \varphi(a) \\ \text{ou} & r & = 0 \end{cases}$$

Note que, como I é ideal e $a \in I$ implica que $at \in I$. Assim temos que

$$r = (\varepsilon - at) \in I.$$

Suponha $r \neq 0$. Então $\varphi(r) < \varphi(a)$, mas, pela minimalidade de $\varphi(a)$ isso é um absurdo!
Em virtude disso, $r = 0$ e então $\varepsilon = at,\ t \in D$ e portanto $I \subseteq aD$.
Como $a \in I$ e I é ideal vem que $aD \subseteq I$. Logo $I = aD$.

b) Sejam $a, b \in D\backslash\{0\}$. Como D é um domínio euclidiano, existem $t_1, r_1 \in D$ tais que:

$$(1) \qquad a = bt_1 + r_1 \quad \text{com} \begin{cases} \varphi(r_1) < \varphi(b) \\ \text{ou} \quad r_1 = 0 \end{cases}$$

Se $r_1 = 0$ então $mdc(a, b) = b$ e portanto a partir da expressão (1) podemos escrever:

$$a.0 + b.1 = b.$$

Se $r_1 \neq 0$ temos que $mdc(a, b) = mdc(b, r_1)$.
De fato, seja $d = mdc(a, b)$. Como $d|b$ e $d|a$ então $d|r_1$, pois $r_1 = (a - bt_1)$. Logo $d|b$ e $d|r_1$. Seja $d' \in D$ tal que $d'|b$ e $d'|r_1$ então $d'|a$ pois $a = (bt_1 + r_1)$ e portanto, como $d = mdc(a, b)$, temos que $d'|d$. Assim $mdc(b, r_1) = d$.
Agora, novamente pela propriedade euclidiana, existem $t_2, r_2 \in D$ tais que:

$$(2) \qquad b = r_1t_2 + r_2 \quad \text{com} \begin{cases} \varphi(r_2) < \varphi(r_1) \\ \text{ou} \quad r_2 = 0 \end{cases}$$

Se $r_2 = 0$ então $mdc(a, b) = mdc(b, r_1) = r_1$. Logo, a partir de (1) podemos escrever:

$$a + b(-t_1) = r_1.$$

Se $r_2 \neq 0$, então por racicínio análogo ao acima, temos que $mdc(b, r_1) = mdc(r_1, r_2)$. Pela propriedade euclidiana existem t_3, r_3 tais que:

$$(3) \qquad r_1 = r_2t_3 + r_3 \quad \text{com} \begin{cases} \varphi(r_3) < \varphi(r_2) \\ \text{ou} \quad r_3 = 0 \end{cases}$$

Se $r_3 = 0$ então $mdc(a, b) = mdc(r_1, r_2) = r_2$. Substituindo (1) em (2) vem que:

$$(-t_2)a + (t_1t_2 + 1)b = r_2.$$

Se $r_3 \neq 0$ continuamos o processo, que é finito, pois a sequência

$$\varphi(r_1), \varphi(r_2), \varphi(r_3), \cdots, \varphi(r_i), \cdots$$

é estritamente decrescente e tem seus valores em $\mathbb{N}$.
Dessa maneira, existe algum $n \in \mathbb{N}$ tal que $\varphi(r_{n-1}) = 0$. Como $\varphi(r_n) < \varphi(r_{n-1})$ ou $r_n = 0$, e neste caso temos $\varphi(r_{n-1}) = 0$, vem que $r_n = 0$. Em virtude disso obtemos:

$$(n) \qquad r_{n-1} = r_nt_{n+1} + 0$$

Então $mdc(a, b) = mdc(r_{n-1}, r_n) = r_n$. Substituindo as equações (1), (2), (3),$\cdots$, (n-2), em ordem decrescente, na equação (n-1), obtemos r_n como combinação linear de a e b.

Note que atráves das divisões sucessivas em (1), (2), ...(n-1), no item i), calculamos efetivamente e e f.

■

Encerramos este capítulo com um resultado sobre raízes de polinômios, que também será necessário no próximo capítulo.

Teorema 1.6. *Se A é um domínio de integridade, então todo polinômio não nulo, de grau n, $f(X) \in A[X]$ tem, no máximo, n raízes.*

Demonstração. Usaremos indução sobre o grau n de $f(X)$.
Se $n = 0$ então $f(X) = a, a \neq 0$ e então $f(X)$ não tem raízes.
Se $n > 0$, suponha que o teorema seja válido para todo polinômio não nulo de $A[X]$ e de grau menor que n.
Queremos mostrar que, se $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X^1 + a_0$ é um polinômio de grau n de $A[X]$ então $f(X)$ tem no máximo n raízes.
Suponhamos por absurdo, que $f(X)$ tenha $n+1$ raízes distintas $x_0, x_1, ..., x_n$ em A. Então podemos escrever $f(X)$ da seguinte forma:

$$f(X) = a_n(X - x_0)(X - x_1)\cdots(X - x_n).$$

Considere o seguinte polinômio em $A[X]$.

$$\begin{aligned} g(X) &= f(X) - a_n(X - x_1)(X - x_2)\cdots(X - x_n) \\ &= a_n(X - x_1)(X - x_2)\cdots(X - x_n).((X - x_0) - 1) \end{aligned}$$

Quando subtraímos $a_n(X - x_1)(X - x_2)\cdots(X - x_n)$ de $f(X)$ eliminamos o termo a_nX^n de $f(X)$. Assim podemos concluir que

$$m \leq \text{ grau } g(X) < \text{ grau } f(X) = n.$$

Note que

$$g(x_0) = -a_n(x_0 - x_1)(x_0 - x_2)\cdots(x_0 - x_n),$$

onde $a_n \neq 0$ e $(x_0 - x_i) \neq 0 \, \forall i = 1, 2 \ldots, n$.
Desta maneira $g(x_0) \neq 0$ e então $g(X)$ é diferente da função identicamente nula.
Pela hipótese de indução, $g(X)$ tem no máximo m raízes em A, mas, supondo que $f(X)$ tem $n+1$ raízes vem que $g(X)$ tem $n > m$ raízes. Absurdo!
Portanto $f(X)$ tem no máximo n raízes em A.

■

Capítulo 2

Números que são somas de dois quadrados

O principal objetivo deste capítulo é provar que um número natural n é soma de dois quadrados se, e somente se, os números primos da forma $4k + 3$ que aparecem na decomposição de n têm expoente par. Em particular, isso responde afirmativamente ao problema 8 da Aritmética, citado na Introdução.

Iniciaremos com alguns lemas e resultados, que serão úteis neste e também no capítulo seguinte.

Lema 2.1. a) Sejam $a, b \in \mathbb{Z}$ primos relativos.
Se $ab = \pm c^2$ então existem $u, v \in \mathbb{Z}$ tais que $a = \pm u^2$ e $b = \pm v^2$.

b) Sejam $a, b \in \mathbb{Z}[i]$ primos relativos, ou seja, $mdc(a, b) \in \{\pm 1, \pm i\}$.
Se $ab = \varepsilon_1 c^2$ com $c \in \mathbb{Z}[i]$ e $\varepsilon_1 \in \mathcal{U}(\mathbb{Z}[i])$ então existem $u, v \in \mathbb{Z}[i]$ tais que $a = \varepsilon_2 u^2$ e $b = \varepsilon_3 v^2$ com ε_2 e $\varepsilon_3 \in \mathcal{U}(\mathbb{Z}[i])$.

Demonstração:

a) Vamos considerar primeiro os casos triviais.
Caso 1: $a = 0$ ou $b = 0$.
Se $a = 0$, então $mdc(a, b) = mdc(0, b) = b$, mas $mdc(a, b) = \pm 1$. Logo $b = \pm 1$. Então tome $u = 0$ e $v = \pm 1$.
O caso onde $b = 0$ é análogo.
Caso 2: $a = \pm 1$ ou $b = \pm 1$.
Se $a = \pm 1$, podemos substituir o valor de a em $ab = \pm c^2$, isto implica que $b = \pm c^2$. Então tome $u = \pm 1$ e $v = \pm c$.
Se $b = \pm 1$ é análogo.

Caso 3: $a \neq 0, \pm 1$ e $b \neq 0, \pm 1$.
Note que $c \neq 0, \pm 1$.
Se tivéssemos $c = 0$ teríamos $a = 0$ ou $b = 0$. Absurdo!
Se $c = \pm 1$ teríamos:
$ab = \pm 1 \Rightarrow a = \pm 1$ e $b = \pm 1$. Absurdo!
Como $\mathbb{Z}$ é domínio fatorial podemos fatorar a, b e c em elementos irredutíveis de forma única:

$$\begin{aligned} a &= \pm p_1^{e_1} ... p_t^{e_t}, \text{ onde } p_i \text{ não é associado a } p_j; \\ b &= \pm q_1^{a_1} ... q_s^{a_s}, \text{ onde } q_i \text{ não é associado a } q_j; \\ c &= \pm l_1^{g_1} ... l_r^{g_r}, \text{ onde } l_i \text{ não é associado a } l_j. \end{aligned}$$

Mostraremos que q_i não é associado à p_j.
Suponha que q_i seja associado à algum p_j, então como $\mathcal{U}(\mathbb{Z}) = \{\pm 1\}$, temos que $p_j = \pm q_i$. Desta maneira $\pm q_i$ está na decomposição em elementos irredutíveis de a e b. Isto implica que $mdc(a, b) \neq \pm 1$. Absurdo!
Portanto q_i não é associado à p_j.
Como $ab = \pm c^2$, temos

$$ab = \pm p_1^{e_1} ... p_t^{e_t} q_1^{a_1} ... q_s^{a_s} = \pm l_1^{2g_1} ... l_r^{2g_r}.$$

Note que, $r = t + s$, pois $\mathbb{Z}$ é domínio fatorial. E reordenando, se necessário, o conjunto $\{l_1, ..., l_r\}$ temos, pela unicidade da decomposição, que:

$$\begin{aligned} p_j^{e_j} = l_j^{2g_j} &\Longrightarrow a = \pm (l_1^{g_1} ... l_t^{g_t})^2 \Longrightarrow a = \pm u^2 \\ q_j^{a_j} = l_j^{2g_j} &\Longrightarrow b = \pm (l_{t+1}^{g_{t+1}} ... l_r^{g_r})^2 \Longrightarrow b = \pm v^2 \end{aligned}$$

b) Vamos resolver primeiro os casos triviais:
Caso 1: $a = 0$ ou $b = 0$.
Se $a = 0$ então $mdc(a, b) = mdc(0, b) = b$, mas $mdc(a, b) \in \{\pm 1, \pm i\}$ e portanto, segue que $b = \pm 1$ ou $b = \pm i$.
Logo, tome $b = \pm 1^2$ ou $b = \pm i 1^2$ e $a = 0^2$.
Se $b = 0$ é análogo.
Caso 2: $a \in \mathcal{U}(\mathbb{Z}[i])$ ou $b \in \mathcal{U}(\mathbb{Z}[i])$.
Se $a \in \mathcal{U}(\mathbb{Z}[i])$ então multiplicando-se $ab = \varepsilon_1 c^2$ pelo inverso de a temos $b = \varepsilon_1 a^{-1} c^2$.
Então $a = a1^2$ e $b = \varepsilon_1 a^{-1} c^2$.
Se $b \in \mathcal{U}(\mathbb{Z}[i])$ é análogo.

Caso 3: $a, b \notin \mathcal{U}(\mathbb{Z}[i])$ e $a, b \neq 0$.
Neste caso, necessariamente $c \neq 0$ e $c \notin \mathcal{U}(\mathbb{Z}[i])$.
De fato, se $c = 0$ temos que a ou $b = 0$ pois $\mathbb{Z}[i]$ é domínio. Absurdo, pois $a, b \neq 0$.
Se $c \in \mathcal{U}(\mathbb{Z}[i])$ então $a, b \in \mathcal{U}(\mathbb{Z}[i])$. Absurdo, pois $a, b \notin \mathcal{U}(\mathbb{Z}[i])$.
Como $\mathbb{Z}[i]$ é domínio fatorial, vamos fatorar a, b, c em elementos irredutíveis de $\mathbb{Z}[i]$:

$$a = \mu_1 p_1^{\gamma_1} ... p_t^{\gamma_t};$$
$$b = \mu_2 q_1^{\beta_1} ... q_s^{\beta_s};$$
$$c = \mu_3 l_1^{\alpha_1} ... l_r^{\alpha_r};$$

onde $\mu_1, \mu_2, \mu_3 \in \mathcal{U}(\mathbb{Z}[i])$ e $p_i \nsim p_j, q_i \nsim q_j$ e $l_i \nsim l_j$.
Note que $p_i \nsim q_j$.
De fato, suponha que $p_i \sim q_j$, então $p_i = wq_j$, onde $w \in \mathcal{U}(\mathbb{Z}[i])$.
Assim $q_j | p_i$ e então $q_j | a$ e $q_j | b$. Logo $q_j | d$, $d = mdc(a, b)$, mas $d \in \mathcal{U}(\mathbb{Z}[i])$ e então $q_j \in \mathcal{U}(\mathbb{Z}[i])$. Absurdo!
Portanto $p_i \nsim q_j$.
Como $ab = \varepsilon_1 c^2$, juntando as decomposições em fatores irredutíveis de a e b, temos:

$$ab = \mu_1 \mu_2 p_1^{\gamma_1} ... p_t^{\gamma_t} q_1^{\beta_1} ... q_s^{\beta_s} = (\mu_3)^2 l_1^{2\alpha_1} ... l_r^{2\alpha_r}$$

Como $\mathbb{Z}[i]$ é domínio fatorial, a fatoração de ab é única e então reordenando, se necessário, o conjunto $l_1^{2\alpha_1} ... l_r^{2\alpha_r}$ temos que $r = t + s$ e :

$$p_j^{e_j} = l_j^{2g_j} \Longrightarrow a = \varepsilon_2 (l_1^{g_1} ... l_t^{g_t})^2 \Longrightarrow a = \varepsilon_2 u^2$$
$$q_j^{a_j} = l_j^{2g_j} \Longrightarrow b = \varepsilon_3 (l_{t+1}^{g_{t+1}} ... l_r^{g_r})^2 \Longrightarrow b = \varepsilon_3 v^2$$

■

Lema 2.2. Sejam $x, y \in \mathbb{Z}$.

a) x é par $\Longleftrightarrow x^2$ é par.

b) $x + y$ é par $\Longleftrightarrow x$ e y são pares ou x e y são ímpares.

c) $x + y$ é ímpar $\Longleftrightarrow x$ é par e y é ímpar ou x é ímpar e y é par.

d) $x^2 + y^2$ é ímpar $\Longleftrightarrow x + y$ é ímpar.

Demonstração. a) ($\Rightarrow$) Se x é par, $x = 2t$, $t \in \mathbb{Z}$. Então $x^2 = (2t)^2$
$= 4t^2$
$= 2(2t^2)$ é par.

($\Leftarrow$) Se x^2 é par temos $x^2 = 2t$, $t \in \mathbb{Z}$.
Como 2 é irredutível, ele está na fatoração de x. Portanto $x = 2h, h \in \mathbb{Z}$.

b) ($\Rightarrow$)
$x + y$ é par $\Longrightarrow x + y = 2k$ $(k \in \mathbb{Z})$
$\Longrightarrow x = 2k - y$.
Se y for par então $y = 2t$ e portanto $x = 2k - 2t = 2(k - t)$. Logo x é par.
Se y for ímpar então $y = 2t + 1$ e portanto $x = 2k - 2t - 1 = 2(k - t) - 1$.
Logo x é ímpar.
Portanto, se $x + y$ é par então x, y são ambos pares ou ambos ímpares.

($\Leftarrow$)
x e y pares $\Longrightarrow x = 2t$ e $y = 2h$, com $h, t \in \mathbb{Z}$
$\Longrightarrow x + y = 2(t + h)$
$\Longrightarrow x + y$ é par.
x e y ímpares $\Longrightarrow x = 2t + 1$ e $y = 2h + 1$, com $t, h \in \mathbb{Z}$
$\Longrightarrow x + y = 2(t + h + 1)$
$\Longrightarrow x + y$ é par.

c) ($\Rightarrow$)
$x + y = 2k + 1, k \in \mathbb{Z} \Longrightarrow y = 2k + 1 - x$.
Se $x = 2t, t \in \mathbb{Z}$, temos que $y = 2k + 1 - 2t = 2(k - t) + 1$ é ímpar.
Se $x = 2t + 1, t \in \mathbb{Z}$, temos que $y = 2k + 1 - 2t - 1 = 2(k - t)$ é par.

($\Leftarrow$) Se $x = 2k$ e $y = 2t + 1, k, t \in \mathbb{Z}$, temos que $x + y = 2(k + t) + 1$ e então $x + y$ é ímpar.
Se $x = 2k + 1$ e $y = 2t; k, t \in \mathbb{Z}$, temos que $x + y = 2(k + t) + 1$ e então $x + y$ é ímpar.

d) ($\Rightarrow$) $x^2 + y^2 = 2k + 1, k \in \mathbb{Z}$.
Caso 1: y é par.
Se $y = 2h, h \in \mathbb{Z}$ então pelo item (a) vem que $y^2 = 2t, t \in \mathbb{Z}$. Dessa forma temos:
$x^2 = 2k + 1 - y^2 \Longrightarrow x^2 = 2k + 1 - 2t$

$\Longrightarrow x^2$ é ímpar

$\Longrightarrow x$ é ímpar (pelo item (a))

$\Longrightarrow x + y$ é ímpar.

Caso 2: y é ímpar.
Se $y = 2h + 1, h \in \mathbb{Z}$ então pelo item (a) vem que $y^2 = 2t + 1, t \in \mathbb{Z}$. Dessa maneira temos: $x^2 = 2k + 1 - y^2 \Longrightarrow x^2 = 2k + 1 - 2t - 1$

$\Longrightarrow x^2$ é par

$\Longrightarrow x$ é par (pelo item (a))

$\Longrightarrow x + y$ é ímpar.

($\Leftarrow$) Se $x + y = 2k + 1$ temos dois casos à analisar:
Caso 1: $x = 2k$ e $y = 2t + 1; k, t \in \mathbb{Z}$.
Temos $x^2 = (2k)^2 = 2(2k^2)$ e $y^2 = 4t^2 + 4t + 1$.
Então $x^2 + y^2 = 2(2k^2 + 2t^2 + 2t) + 1$ e portanto $x^2 + y^2$ é ímpar.
Caso 2: $x = 2k + 1$ e $y = 2t$, $k, t \in \mathbb{Z}$.
Temos $y^2 = (2t)^2 = 2(2t^2)$ e $x^2 = 4k^2 + 4k + 1$.
Então $x^2 + y^2 = 2(2t^2 + 2k^2 + 2k) + 1$ e portanto $x^2 + y^2$ é ímpar.

■

A definição, o teorema e a demonstração a seguir, propostos por Euler em aproximadamente 1760, mostram uma generalização de um resultado proposto por Fermat cerca de um século antes. Este resultado é conhecido como *"o Pequeno Teorema de Fermat"*, e será provado como um corolário do teorema de Euler.

Definição 2.1. A função $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ que associa a cada $m \in \mathbb{N}^*$ a quantidade de elementos do conjunto $\{k \in \mathbb{N}^*; 1 \leq k \leq m$ e $mdc(k, m) = 1\}$, é chamada função de Euler.

Teorema 2.1. *Para todo inteiro $m > 1$ e para todo $a \in \mathbb{Z}$, primo com m, vale a congruência $a^{\varphi(m)} \equiv 1 (mod\, m)$.*

Demonstração. Sejam $s_1, s_2, ..., s_k$ os inteiros de 1 a m que são primos relativos com m. Então $\varphi(m) = k$. Ao dividir cada as_i por m obtemos:

$$as_i = mq_i + r_i, \quad (0 \leq r_i < m)$$

Afirmação: m e r_i são primos relativos, ou seja $mdc(m, r_i) = 1$.
Suponha por absurdo que exista um número primo p tal que $p|m$ e $p|r_i$.

Se $p|m$ então $p|mq_i$ e assim $p|(mq_i + r_i)$, ou seja, $p|as_i$.
Como $mdc(a, m) = 1$ temos que $p|s_i$, mas então $p|s_i$ e $p|m$. Absurdo, pois $mdc(s_i, m) = 1$. Logo $mdc(m, r_i) = 1$.
Note que na sequência dos restos $r_1, r_2, ..., r_k$ não há elementos repetidos. De fato, suponha por absurdo que $r_i = r_j$, onde $1 \leq i, j \leq k$ e $i \neq j$.

$$\text{Então de } \begin{cases} as_i = mq_i + r_i \\ as_j = mq_j + r_j \end{cases} \text{ vem que :}$$

$$as_i - mq_i = as_j - mq_j \Longrightarrow a(s_i - s_j) = m(q_i - q_j).$$

Como $mdc(m, a) = 1$ vem que $m|(s_i - s_j)$.
Mas $1 \leq s_i, s_j \leq m \Longrightarrow s_i - s_j < m$

$$\Longrightarrow s_i - s_j = 0$$

$$\Longrightarrow s_i = s_j. \text{ Absurdo!}$$

Afirmação: $r_i \neq 0, \forall i \in \{1, 2, ..., k\}$.
Se $r_i = 0$ temos $as_i = mq_i$ e então $m|as_i$, mas $mdc(a, m) = 1$, logo $m|s_i$. Absurdo!
Portanto $r_i \neq 0, \forall i \in \{1, 2, ..., k\}$.
Então temos:

$(a) 1 \leq r_i < m$ e $r_i \neq r_j$.
$(b)\{s_1, ..., s_k\}$ é o conjunto de todos os primos relativos com m no intervalo explicitado acima.
$(c)\{r_1, ..., r_k\}$ é o conjunto de todos os restos da divisão de as_i por m. Então, como vimos, $r_1, .., r_k$ são k elementos primos com m no intervalo acima explicitado.

Em (b) vimos que há exatamente k primos relativos com m no intervalo $1 \leq s_i < m$. Portanto como $\{r_1, ..., r_k\}$ é um conjunto de k elementos distintos e primos relativos com m no intervalo $1 \leq r_i < m$, temos que:

$$\{r_1, r_2, ..., r_k\} = \{s_1, s_2, ..., s_k\}$$

Denote: $r_1 r_2 ... r_k = s_1 s_2 ... s_k = \alpha \quad (*)$.
Ao multiplicarmos todas as congruências $as_i \equiv r_i (mod\, m)$, que decorrem de todas as divisões $as_i = mq_i + r_i,\ (1 \leq i \leq k)$ obtemos:

$$a^k s_1 s_2 ... s_k \equiv r_1 r_2 ... r_k (mod\ m) \Longrightarrow a^k s_1 s_2 ... s_k - r_1 r_2 ... r_k = mf, f \in \mathbb{Z}.$$

Por $(*)$ temos: $a^k \alpha - \alpha = mf \Longrightarrow \alpha(a^k - 1) = mf$

$$\Longrightarrow m|\alpha(a^k - 1).$$

Mas $m \nmid \alpha$, pois α é o produto de elementos primos com m, ou seja m e α são primos relativos, então:

$$\begin{aligned} & m\,|(a^k - 1) \\ \Longrightarrow\ & a^k \equiv 1(mod\, m) \\ \Longrightarrow\ & a^{\varphi(m)} \equiv 1(mod\, m). \end{aligned}$$

■

Corolário 2.1. ***(Pequeno Teorema de Fermat)***
Se $p > 1$ é um número primo que não divide o inteiro a, então: $a^{p-1} \equiv 1(mod\, p)$.

Demonstração. Basta aplicar o teorema anterior. Note que $\varphi(p) = p - 1$, pois p é número primo.

■

O teorema a seguir foi proposto por Fermat em 1637 e provado por Euler em 1749, após 7 anos de trabalho. Após provado este teorema, dado um número primo p qualquer, teremos condições de afirmar se p pode ou não ser escrito como a soma de dois quadrados. Esta verificação será feita olhando para o resto da divisão de p por 4.

Teorema 2.2. *As condições abaixo são equivalentes para um número p primo:*

(i) $p = 2$ *ou* $p = 4k + 1, k \in \mathbb{N}^*$.

(ii) $\exists\, a \in \mathbb{Z}; a^2 \equiv -1(mod\, p)$.

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

(iv) p *é a soma de dois quadrados.*

Demonstração. $(i) \Rightarrow (ii)$ Se $p = 2$ tome $a = 1$.
Sejam $p = 4k + 1$ e $\overline{x} \in \mathbb{Z}_p^*$.
Note que, se $\overline{x} \in \mathbb{Z}_p^*$ então $x \in \mathbb{Z} - p\mathbb{Z}$. Portanto $p \nmid x$.
Como $p \nmid x$, segue do Pequeno Teorema de Fermat que $x^{p-1} \equiv 1(mod\, p)$.
Como $p = 4k + 1$ obtemos:

$$\begin{aligned} x^{(4k+1)-1} \equiv 1(mod\, p) &\Longrightarrow x^{4k} \equiv 1(mod\, p) \\ &\Longrightarrow (x^{2k})^2 - 1 = np, n \in \mathbb{Z}. \end{aligned}$$

Analisando em $\mathbb{Z}_p$ temos:

$$(\overline{x}^{2k})^2 - \overline{1} = \overline{np} \Longrightarrow (\overline{x}^{2k})^2 - \overline{1} = \overline{0}$$
$$\Longrightarrow \overline{x}^{2k} \text{ é raiz de } X^2 - \overline{1} \in \mathbb{Z}_p[X].$$

Desde que $\mathbb{Z}_p$ é domínio, pelo Teorema 1.6, $X^2 - \overline{1}$ tem no máximo duas raízes em $\mathbb{Z}_p$. Como $\overline{1}$ e $\overline{p-1}$ são raízes de $X^2 - \overline{1}$ em $\mathbb{Z}_p$, temos $\overline{x}^{2k} = \overline{1}$ ou $\overline{x}^{2k} = \overline{p-1}$, para todo $\overline{x} \in \mathbb{Z}_p^*$.
Note que $\mathbb{Z}_p - \{\overline{0}\} = \mathbb{Z}_{4k+1} - \{\overline{0}\}$ tem exatamente $4k$ elementos.
Se $\overline{x}^{2k} = \overline{1}$, então $\overline{x}$ é raiz de $X^{2k} - \overline{1} \in \mathbb{Z}_p[X]$. Mas este polinômio tem no máximo 2k raízes em $\mathbb{Z}_p$, pois $\mathbb{Z}_p$ é domínio.
Então, como todos os $4k$ elementos de $\mathbb{Z}_p - \{\overline{0}\}$ satisfazem $\overline{x}^{2k} = \overline{1}$ ou $\overline{x}^{2k} = \overline{p-1}$, e como apenas no máximo 2k elementos satisfazem $\overline{x}^{2k} = \overline{1}$, temos que existe $\overline{x}_0 \in \mathbb{Z}_p - \{\overline{0}\}$ que satisfaz $\overline{x}_0^{2k} = \overline{p-1}$.
Tome $a = x_0^k$.
Assim temos: $\overline{a}^2 = \overline{x}_0^{2k} = \overline{p-1} \Longrightarrow a^2 \equiv p - 1 (mod\, p)$.
Como $p - 1 \equiv -1 (mod\, p)$ vem que

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

$(ii) \Rightarrow (iii)$

$$a^2 + 1 = pn, n \in \mathbb{Z} \Longrightarrow p|(a^2+1)$$
$$\Longrightarrow p|(a+i)(a-i).$$

Queremos mostrar que p não é irredutível em $\mathbb{Z}[i]$. Como $\mathbb{Z}[i]$ é domínio fatorial, provar que p não é irredutível é equivalente a provar que p não é elemento primo em $\mathbb{Z}[i]$. Então basta mostrar que $p \nmid (a+i)$ e $p \nmid (a-i)$.

- $p|(a-i) \Longrightarrow \exists\, e + fi \in \mathbb{Z}[i]$ tal que $p(e+fi) = a - i$
  $\Longrightarrow pf = -1$
  $\Longrightarrow p$ é inversível. Absurdo!
- $p|(a+i) \Longrightarrow \exists\, c + di \in \mathbb{Z}[i]$ tal que $p(c+di) = a + i$
  $\Longrightarrow pd = 1$
  $\Longrightarrow p$ é inversível. Absurdo!

Portanto p não é primo em $\mathbb{Z}[i]$, logo não é irredutível em $\mathbb{Z}[i]$.

$(iii) \Rightarrow (iv)$
Por hipótese p não é irredutível em $\mathbb{Z}[i]$. Então $p = (a+bi)(c+di)$, $a+bi$, $c+di \in \mathbb{Z}[i] \setminus \mathcal{U}(\mathbb{Z}[i])$.
Ao aplicarmos a função norma em p obtemos:

$$p^2 = N(p) = N((a+bi)(c+di))$$

$$
\begin{aligned}
&= N(a+bi)N(c+di) \\
&\Longrightarrow p^2 = (a^2+b^2)(c^2+d^2) \\
&\Longrightarrow a^2+b^2 = p \text{ e } c^2+d^2 = p \\
&\qquad \text{ou } a^2+b^2 = p^2 \text{ e } c^2+d^2 = 1 \\
&\qquad \text{ou } a^2+b^2 = 1 \text{ e } c^2+d^2 = p^2.
\end{aligned}
$$

Se $c^2+d^2 = 1$ então $c+di \in \mathcal{U}(\mathbb{Z}[i])$. Absurdo!
Analogamente não podemos ter $a^2+b^2 = 1$.
Portanto $p = a^2+b^2$.

$(iv) \Rightarrow (i)$
Queremos mostrar que se p é soma de dois quadrados então $p = 2$ ou $p = 4k+1$.
Dado $n \in \mathbb{N}$ temos as seguintes possibilidades de resto na divisão de n por 4:

$$n = 4k,\ n = 4k+1,\ n = 4k+2,\ n = 4k+3$$

Se n é um número primo, a possibilidade $n = 4k$ está descartadada pois n é um múltiplo de quatro e a possibilidade $n = 4k+2$ fica restrita apenas ao número dois. Deste modo, se p é primo, então:

$$p = 2 \text{ ou } p = 4k+1 \text{ ou } 4k+3.$$

Por hipótese $p = a^2+b^2$, onde $a, b \in \mathbb{Z}$. Então temos:

$$a = 4v, 4v+1, 4v+2 \text{ ou } 4v+3 \Longrightarrow a^2 = 4v \text{ ou } a^2 = 4v+1.$$

$$b = 4l, 4l+1, 4l+2 \text{ ou } 4l+3 \Longrightarrow b^2 = 4l \text{ ou } b^2 = 4l+1.$$

Portanto $p = a^2+b^2 = 4v+4l = 4(v+l)$, é múltiplo de quatro. Absurdo!
$p = a^2+b^2 = 4v+4l+1 = 4(v+l)+1 \Longrightarrow p = 4k+1$;
$p = a^2+b^2 = 4v+1+4l+1 = 4(v+l)+2 \Longrightarrow p = 2$;
$p = a^2+b^2 = 4v+1+4l = 4(v+l)+1 \Longrightarrow p = 4k+1$.
Logo, se $p = a^2+b^2$ então $p = 4k+1$ ou $p = 2$.

■

Observação 2.1. Um número inteiro positivo pode ser a soma de dois quadrados de maneiras distintas. Por exemplo $125 = 10^2+5^2 = 11^2+2^2$.

Observação 2.2. Se um número primo positivo é soma de dois quadrados, então só existe um par de números positivos a, b tal que $a^2+b^2 = p$.
De fato, suponha que existem dois pares de números positivos a, b e c, d tais que:

$$p = a^2 + b^2 = c^2 + d^2$$
$$\Longrightarrow p = (a + bi)(a - bi) = (c + di)(c - di).$$

Denote $a + bi = \alpha$ e $c + di = \beta$. Desta forma $p = \alpha\overline{\alpha} = \beta\overline{\beta} \quad (*)$.
Aplicando a função norma obtemos:

$$p^2 = N(\alpha)N(\overline{\alpha}) \text{ e } p^2 = N(\beta)N(\overline{\beta}).$$

Como $N(\alpha) = N(\overline{\alpha})$ e $= N(\beta) = N(\overline{\beta})$, segue que:

$$p = N(\alpha) = N(\overline{\alpha}) = N(\beta) = N(\overline{\beta}).$$

Assim α, β são irredutíveis em $\mathbb{Z}[i]$ e portanto, também são primos em $\mathbb{Z}[i]$.
De $(*)$ vem que:

$$\begin{aligned} \alpha|\beta\overline{\beta} &\Longrightarrow \alpha|\beta \text{ ou } \alpha|\overline{\beta} \\ &\Longrightarrow \alpha u = \beta \text{ ou } \alpha v = \overline{\beta} \\ &\Longrightarrow u, v \in \mathcal{U}(\mathbb{Z}[i]) = \{\pm 1, \pm i\} \\ &\Longrightarrow \alpha \sim \beta \text{ ou } \alpha \sim \overline{\beta}. \end{aligned}$$

Trataremos o caso $\alpha \sim \beta$. O caso $\alpha \sim \overline{\beta}$ é análogo.
$\alpha \sim \beta \Longrightarrow (a + bi) = u(c + di)$, $u \in \mathcal{U}(\mathbb{Z}[i])$.
Se $u = 1$ então $a + bi = c + di$. Portanto $a = c$ e $b = d$.
Se $u = -1$ então $a + bi = -c - di$. Portanto $a = -c$ e $b = -d$. Absurdo, pois $a, b, c, d \in \mathbb{N}^*$.
Se $u = i$ então $a + bi = ci - d$. Portanto $a = -d$ e $b = c$. Absurdo!
Se $u = -i$ então $a + bi = -ci + d$. Portanto $a = d$ e $b = -c$. Absurdo!
Portanto, se existem dois pares de números positivos a, b e c, d tais que $p = a^2 + b^2 = c^2 + d^2$ então $a = c$ e $d = b$.

■

O resultado do Teorema 2.2 pode ser generalizado, isto é, podemos caracterizar os inteiros que são somas de dois quadrados. Para tanto será necessário provar o seguinte lema:

Lema 2.3. Se f e g são inteiros que são somas de dois quadrados então fg é soma de dois quadrados.

Demonstração. $f = a^2 + b^2,\ g = c^2 + d^2$.

$$\begin{aligned} fg = (a^2+b^2)(c^2+d^2) &= N(a+bi)N(c+di) \\ &= N[(a+bi)(c+di)] \\ &= N[(ac-db)+(ad+cb)i] \\ &= (ac-db)^2+(ad+cb)^2. \end{aligned}$$

■

Teorema 2.3. *Seja n um inteiro positivo e $n = 2^r p_1^{u_1}...p_t^{u_t} q_1^{v_1}...q_s^{v_s}$ sua decomposição em $\mathbb{Z}$, onde $p_1, ..., p_t$ são primos da forma $4k+1$ e $q_1, ..., q_s$ são primos da forma $4k+3$. Então, n é soma de dois quadrados se e somente se $v_1, ..., v_s$ são pares.*

Demonstração. ($\Rightarrow$) Por hipótese $n = a^2 + b^2$. Seja p primo, $p \neq 2$. Então $p = 4k+1$ ou $p = 4k+3$.
Suponha que a maior potência de p que divide n é ímpar. Então basta provar que p é da forma 4k+1. Se provarmos este fato, por sua contra positiva teremos provado a ida do teorema.
Seja $d = mdc(a, b)$ então $a = da_1, b = db_1$, onde $mdc(a_1, b_1) = 1$. Conseqüentemente $n = d^2(a_1^2 + b_1^2)$.
Seja m ímpar a maior potência de p tal que $p^m | n$. Então existe $\alpha \in \mathbb{Z}$ tal que

$$p^m \alpha = d^2(a_1^2 + b_1^2).$$

Note que as potências máximas dos primos que dividem d^2 são pares. Em particular, a maior potência de p que divide d^2 é par. Portanto, da igualdade $p^m\alpha = d^2(a_1^2 + b_1^2)$ com m ímpar, concluimos que $p|(a_1^2 + b_1^2)$.
Afirmação: $p \nmid b_1$.
Suponha por absurdo que $p|b_1$. Segue desta hipótese que $p|b_1^2$ e $p|(a_1^2 + b_1^2)$, ou seja, $p|a_1$. Absurdo, pois $mdc(a_1, b_1) = 1$.
Temos:

$$\begin{aligned} p \nmid b_1 &\Longrightarrow mdc(p, b_1) = 1 \\ &\Longrightarrow \exists\, e, f \in \mathbb{Z} \text{ tal que } ep + fb_1 = 1 \\ &\Longrightarrow a_1 = ea_1p + fa_1b_1. \end{aligned}$$

Escreva $c = a_1 f$.
Então $a_1 = ea_1p + cb_1$.
Tomando classes módulo p vem que $\overline{a_1 ep} = \overline{0}$ e portanto $\overline{a_1} = \overline{b_1 c}$.
Como $p|(a_1^2 + b_1^2)$, em $\mathbb{Z}_p$ temos:

$$\begin{aligned} \overline{0} = \overline{a_1^2 + b_1^2} = \overline{b_1^2 c^2 + b_1^2} = \overline{b}_1^2(\overline{c}^2 + \overline{1}) &\Longrightarrow \overline{c}^2 = -\overline{1} \;\; (p \nmid b_1 \Longrightarrow \overline{b_1} \neq \overline{0} \Longrightarrow \overline{b_1}^2 \neq \overline{0}) \\ &\Longrightarrow c^2 \equiv -1 (mod\, p) \\ &\Longrightarrow p = 2 \text{ ou } p = 4k+1 \\ &\text{(Pelas equivalências (i) e (ii) do Teorema 2.2).} \end{aligned}$$

Mas estamos supondo $p \neq 2$, portanto se $p^m | n$ então $p = 4k + 1$.

($\Leftarrow$) Já provamos que todo primo da forma $p = 4k + 1$ ou $p = 2$ é soma de dois quadrados. Pelo lema anterior, $2^r p_1^{u_1} ... p_t^{u_t}$ é soma de dois quadrados.
Como $v_1, ..., v_2$ são pares, temos que, $q_1^{v_1}, ..., q_s^{v_s}$ são quadrados. Logo $q_1^{v_1}, ..., q_s^{v_s}$ são somas de dois quadrados. Assim $q_1^{v_1} ... q_s^{v_s}$ é soma de dois quadrados. Portanto $2^r p_1^{u_1} ... p_t^{u_t} q_1^{v_1} ... q_s^{v_s}$é soma de dois quadrados.

■

Este teorema resolve o "Problema 8 generalizado" do livro de Diophantus: Quando um número inteiro positivo, qualquer, pode ser ecrito como a soma de dois quadrados de inteiros?

Um número inteiro positivo, qualquer, poderá ser escrito como a soma de dois quadrados quando os primos da forma $4k + 3$ que o dividem têm expoentes pares. Desta maneira, para indenticar tais números, basta analisar sua fatoração em elementos primos.

Em particular, se n é um quadrado, então sua decomposição em fatores primos admite apenas expoentes pares. Logo os expoentes dos primos da forma $4k + 3$ são pares. Portanto n é soma de dois quadrados.

Capítulo 3

Redução do Último Teorema de Fermat para n primo

Neste capítulo nosso maior objetivo é reduzir o Último Teorema de Fermat

" A equação $X^m+Y^m = Z^m$ não tem solução não trivial em $\mathbb{Q}^*$, para $m \geq 3$."

ao caso onde m é um número primo, ou seja, mostraremos que não é necessário verificá-lo para todo número inteiro $m \geq 3$, basta verificá-lo para os números primos maiores ou iguais a 3. Para tanto, será suficiente provarmos o seguinte teorema:

Teorema 3.1. Se $X^p + Y^p = Z^p$ não tem solução não trivial em $\mathbb{Z}$ para $p \geq 3, p$ primo, então $X^m + Y^m = Z^m$ não tem solução não trivial em $\mathbb{Z}$ para $m \geq 3$.

No entanto para demonstrarmos este teorema é preciso desenvolver alguns resultados, dentre eles está o próprio Último Teorema de Fermat para o caso $n = 4$. A prova para este caso foi feita sem detalhamento por Fermat.

Lema 3.1. Se $a^m|b^m$, com $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}^*$ então $a|b$.

Demonstração. Se $a = 0$ então $0 = b^m$ e portanto $b = 0$. Logo $a|b$.
Se $a = \pm 1$ então é claro que $a|b$.
Se $b = \pm 1$ temos que $a^m h = \pm 1$, $h \in \mathbb{Z}$. Então $a^m \in \mathcal{U}(\mathbb{Z}) = \{\pm 1\}$ e portanto $a|b$.
Consideremos então $a, b \neq 0$ e $a, b \neq \pm 1$.
Seja

$$a = (\pm 1)p_1^{\alpha_1}...p_t^{\alpha_t}$$

e

$$b = (\pm 1)q_1^{\beta_1}...q_s^{\beta_s}$$

a decomposição de a e b em elementos irredutíveis de $\mathbb{Z}$.
Para provar que $a|b$, basta verificar que para cada $i \in \{1, ..., t\}$, existe $j \in \{1, ..., s\}$ tal que $p_i^{\alpha_i} = q_j^{\lambda_j}$ com $0 \leq \lambda_j \leq \beta_j$.
Note que isso prova que $a|b$ e o quociente é $q = (\pm 1)q_1^{\beta_1 - \lambda_1}...q_s^{\beta_s - \lambda_s}$.
Tome então $i \in \{1, ..., t\}$. Como $p_i^{\alpha_i}|a$ temos que $p_i^{m\alpha_i}|a^m$. Por hipótese $a^m|b^m$, e segue que $p_i^{m\alpha_i}|b^m$. Assim existe $r \in \mathbb{Z}$ tal que

$$p_i^{m\alpha_i} r = b^m = (\pm 1)q_1^{m\beta_1}...q_s^{m\beta_s}.$$

Pela unicidade da decomposição de números inteiros em primos positivos, vem que $p_i = q_j$ para algum $j \in \{1, ..., t\}$ e além disso, $m\alpha_i \leq m\beta_j$. Reordenando, se necessário, o conjunto $\{1, ..., t\}$, podemos considerar $p_i = q_i$ e $m\alpha_i \leq m\beta_i$.
Como $m \neq 0$, vem que $\alpha_i \leq \beta_i$. Tome $\lambda_i = \alpha_i$.

■

Lema 3.2. a) Se (x_o, y_o, z_o) é uma solução de $X^m + Y^m = Z^m$ então, para $\alpha \in \mathbb{Z}^*$, $(\alpha x_o, \alpha y_o, \alpha z_o)$ também é solução.

b) Se $X^m + Y^m = Z^m$ não tem solução em $\mathbb{Z}$ então também não tem solução em $\mathbb{Q}$.

c) Se (x_0, y_0, z_0) é solução não trivial de $X^m + Y^m = Z^m$ em $\mathbb{Z}$ então existe uma solução (x_1, y_1, z_1) em $\mathbb{Z}$ com $mdc(x_1, y_1) = 1$.

Demonstração. a) Se (x_o, y_o, z_o) é uma solução então

$$x_o^m + y_o^m = z_o^m \quad (*)$$

Logo: $(\alpha x_o)^m + (\alpha y_o)^m = \alpha^m(x_o^m + y_o^m)$

$$= \alpha^m z_o^m, \textit{ por } (*).$$

$$\Longrightarrow (\alpha x_o)^m + (\alpha y_o)^m = (\alpha z_o)^m.$$

b) Suponha que existe solução em $\mathbb{Q}$.
Seja $x_o = \frac{x_1}{x_2}, y_o = \frac{y_1}{y_2}, z_o = \frac{z_1}{z_2}$ uma solução de $X^m + Y^m = Z^m$ em $\mathbb{Q}$. Considere $\alpha = x_2 y_2 z_2$. Mostraremos que $(\alpha x_0, \alpha y_0, \alpha z_0,)$ é solução em $\mathbb{Z}$.
É obvio que $\alpha x_o, \alpha y_o, \alpha z_o \in \mathbb{Z}$, pois α é o produto dos denominadores. Além disso,

$$(\alpha x_o)^m + (\alpha y_o)^m = \alpha^m(x_o^m + y_o^m)$$

$$= \alpha^m z_o^m$$

$$= (\alpha z_o)^m.$$

Então $(\alpha x_o, \alpha y_o, \alpha z_o)$ é solução. Absurdo, pois por hipótese não há solução em $\mathbb{Z}$.

c) Seja $d = mdc(x_o, y_o)$.
Se $d = 1$ nada temos a fazer. Assim assumimos $d \neq 1$.
É claro que $d \neq 0$, pois $(x_0, y_0) \neq (0, 0)$.
Como $d|x_0$ e $d|y_0$ existem $x_1,\ y_1 \in \mathbb{Z}$ tais que $x_0 = dx_1$, $y_0 = dy_1$ e $mdc(x_1, y_1) = 1$. Substituindo $x_0 = dx_1$ e $y_0 = dy_1$ em $z_0^m = x_0^m + y_0^m$ obtemos:

$$\begin{aligned} z_0^m &= x_0^m + y_0^m \\ &= (dx_1)^m + (dy_1)^m \\ &\Longrightarrow d^m(x_1^m + y_1^m) = z_0^m \\ &\Longrightarrow d^m | z_0^m. \end{aligned}$$

Pelo Lema 3.1, $d|z_0$ e assim existe $z_1 \in \mathbb{Z}$ tal que $z_0 = dz_1$. Desta forma temos:

$$\begin{aligned} &(dx_1)^m + (dy_1)^m = (dz_1)^m \\ &\Longrightarrow d^m(x_1^m + y_1^m) = d^m z_1^m. \\ &\Longrightarrow x_1^m + y_1^m = z_1^m, \text{ pois } d \neq 0 \text{ e } \mathbb{Z} \text{ é domínio.} \end{aligned}$$

■

Observação 3.1. 1) A solução (x_1, y_1, z_1) obtida em (c) é denominada **solução primitiva**.

2) O item (a), nos diz que, se existe uma solução para o Último Teorema de Fermat então existem infinitas.

3) O item (b), mostra que a equação diofantina $X^m + Y^m = Z^m$ tem solução em $\mathbb{Z}$ se, e somente se, tem solução em $\mathbb{Q}$. Portanto, basta estudar em $\mathbb{Z}$ e também estaremos estudando em $\mathbb{Q}$.

Lema 3.3. Sejam $x, y \in \mathbb{Z} - \{0\}$ com $mdc(x, y) = 1$.

a) O único possível fator comum irredutível em $\mathbb{Z}[i]$ para $\alpha = x + yi$ e $\overline{\alpha} = x - yi$ é $1 + i$ (ou associado a $1 + i$).

b) $\alpha = x + yi$ e $\overline{\alpha} = x - yi$ são primos relativos em $\mathbb{Z}[i]$ se e somente se $x^2 + y^2$ é ímpar, ou seja, x e y não têm a mesma paridade.

Demonstração. a) Seja $\lambda \in \mathbb{Z}[i]$, λ irredutível, tal que $\lambda|\alpha$ e $\lambda|\overline{\alpha}$.
Se assim for, obtemos que $\lambda|(\alpha+\overline{\alpha})$ e $\lambda|(\alpha-\overline{\alpha})$ e então $\lambda|2x$ e $\lambda|2iy$.
Se $\lambda|2iy$ então $\lambda|(-i)2iy$ e portanto $\lambda|2y$.
Como $mdc(x,y)=1$, existem $a,b \in \mathbb{Z}$ tais que $ax+by=1$. Então temos:

$$\begin{aligned} ax+by=1 &\Longrightarrow 2ax+2by=2 \\ &\Longrightarrow \lambda|2 \\ &\Longrightarrow \lambda|(1+i)(1-i) \\ &\Longrightarrow \lambda|(1+i)(1+i)(-i) \\ &\Longrightarrow \lambda|(1+i)^2(-i)(i) \\ &\Longrightarrow \lambda|(1+i)^2. \end{aligned}$$

Como $\mathbb{Z}[i]$ é domínio eucidiano, vem que $\mathbb{Z}[i]$ é domínio fatorial. Então como λ é irredutível, segue que λ é primo.
Logo se $\lambda|(1+i)^2$ então $\lambda|(1+i)$ e portanto $\lambda h=(1+i)$.
Mas $(1+i)$ é irredutível pois sua norma é dois. Em vista disso, $\lambda \in \mathcal{U}(\mathbb{Z}[i])$ ou $h \in \mathcal{U}(\mathbb{Z}[i])$. Por hipótese λ é irredutível então $h \in \mathcal{U}(\mathbb{Z}[i])$.
Portanto $\lambda \sim (1+i)$.

b) ($\Rightarrow$) Suponha por absurdo que x^2+y^2 é par. Assim x e y devem ter a mesma paridade, ou seja,

$$x=2h \text{ e } y=2t$$

ou

$$x=2h+1 \text{ e } y=2t+1;\ h,t \in \mathbb{Z}.$$

Caso 1: $x=2h$ e $y=2t$.
Como $\alpha=x+yi$ e $\overline{\alpha}=x-yi$ temos:

$$\begin{aligned} \alpha=2h+2ti \text{ e } \overline{\alpha}=2h-2ti &\Longrightarrow \alpha=2(h+it) \text{ e } \overline{\alpha}=2(h-it) \\ &\Longrightarrow 2|\alpha \text{ e } 2|\overline{\alpha} \\ &\Longrightarrow mdc(\alpha,\overline{\alpha})=2. \end{aligned}$$

Absurdo, pois $2 \notin \mathcal{U}(\mathbb{Z}[i])$.

Caso 2: $x=2h+1$ e $y=2t+1$.

• $\alpha = 2h + 1 + 2ti + i$

$= 2(h + ti) + (i + 1)$

$\Longrightarrow \alpha^2 = (2(h + ti) + (i + 1))^2$

$= 4(h^2 + 2hti - t^2) + (-1 + 2i + 1) + 2(2(h + ti)(1 + i))$

$= 2r, r \in \mathbb{Z}[i]$.

Desta forma conseguimos mostrar que $2|\alpha^2$.
Note que $(1+i)|2$, pois $(1+i)(1-i) = 2$. Então, por transitividade, $(1+i)|\alpha^2$, ou seja, $(1 + i)|\alpha\alpha$. Como a norma de $(1 + i)$ é um número primo, temos que $(1 + i)$ é irredutível e portanto é primo em $\mathbb{Z}[i]$. Então $(1 + i)|\alpha$.

• $\overline{\alpha} = 2h + 1 - 2ti - i$

$= 2(h - ti) + (1 - i)$

$\Longrightarrow \overline{\alpha}^2 = (2(h - ti) + (1 - i))^2$

$= 4(h^2 - 2hti + t^2) + (1 - 2i - 1) + 2(2(h - ti)(1 - i))$

$= 2s, s \in \mathbb{Z}[i]$.

Então $(1 + i)|\overline{\alpha}$.
Encontramos um primo em comum na decomposição de α e $\overline{\alpha}$. Absurdo, pois α e $\overline{\alpha}$ são primos relativos. Portanto $x^2 + y^2$ é ímpar.

($\Leftarrow$) Suponha que α e $\overline{\alpha}$ não são primos relativos. Conseqüentemente existe $\gamma \in \mathbb{Z}[i], \gamma$ irredutível, tal que $\gamma|\alpha$ e $\gamma|\overline{\alpha}$. Por (a) $\gamma = 1 + i$. Então temos:

$(1 + i)^2|\alpha\overline{\alpha} \Longrightarrow (1 + i)^2|(x^2 + y^2)$

$\Longrightarrow -i(1 + i)^2|(x^2 + y^2)$

$\Longrightarrow 2|(x^2 + y^2)$ em $\mathbb{Z}[i]$

$\Longrightarrow 2(a + bi) = x^2 + y^2$

$\Longrightarrow x^2 + y^2 = 2a$ e $2b = 0$

$\Longrightarrow 2|(x^2 + y^2)$ em $\mathbb{Z}$

$\Longrightarrow x^2 + y^2$ é par. Absurdo!

■

A proposição a seguir, além de ser um resultado auxiliar para provarmos o Teorema 3.1, mostra como obter triplas pitagóricas primitivas.

Proposição 3.1. Sejam $x, y \in \mathbb{Z}\backslash\{0\}$ com $mdc(x, y) = 1$. São equivalentes:

(i) Existe $z \in \mathbb{Z}\backslash\{0\}$ tal que $x^2 + y^2 = z^2$.

(ii) $x + yi = \varepsilon(a + bi)^2$ com $\varepsilon \in \mathcal{U}(\mathbb{Z}[i])$.

(iii) $x = \pm(a^2 - b^2)$ e $y = \pm 2ab$ ou $x = \pm 2ab$ e $y = \pm(a^2 - b^2)$, com $a, b \in \mathbb{Z} - \{0\}, mdc(a, b) = 1$ e a, b não têm a mesma paridade.

Demonstração. $(i) \Rightarrow (ii)$ Inicialmente vamos provar que x, y não têm a mesma paridade.
Como $mdc(x, y) = 1$, então x e y não são ambos pares.
Suponha que x e y são ambos ímpares.
Em $\mathbb{Z}_4$, temos que, $\overline{x} = \overline{1}$ ou $\overline{x} = \overline{3}$ e $\overline{y} = \overline{1}$ ou $\overline{y} = \overline{3}$.
Logo $\overline{x}^2 = \overline{1}$ e $\overline{y}^2 = \overline{1}$ e portanto $\overline{x}^2 + \overline{y}^2 = \overline{2}$. Mas isso é um absurdo, pois os valores que $\overline{z}$ pode assumir em $\mathbb{Z}_4$ são: $\overline{0}, \overline{1}, \overline{2}, \overline{3}$. Portanto $\overline{z}^2 = \overline{0}$ ou $\overline{z}^2 = \overline{1}$.
Segue que x é par e y é ímpar (ou vice-versa).
Então, pelo Lema 2.2, $x^2 + y^2$ é ímpar, e, pelo lema anterior, $\alpha = x + yi$ e $\overline{\alpha} = x - yi$ são primos relativos em $\mathbb{Z}[i]$.
Como $x^2 + y^2 = z^2$, segue que, $\alpha\overline{\alpha} = z^2$. Então como α e $\overline{\alpha}$ são primos relativos em $\mathbb{Z}[i]$, pelo item (b) do Lema 2.1 temos que $\alpha = \varepsilon u^2$, onde $\varepsilon \in \{\pm 1, \pm i\}$ e $u = a + bi \in \mathbb{Z}[i]$.
Logo $x + yi = \varepsilon(a + bi)^2$.

$(ii) \Rightarrow (iii)$ $x + yi = \varepsilon(a + bi)^2$ com $\varepsilon \in \{\pm 1, \pm i\}$.
Se $\varepsilon = \pm 1$ então $x + yi = \pm(a + bi)^2$

$$= \pm(a^2 - b^2 + 2abi)$$

e portanto $x = \pm(a^2 - b^2)$ e $y = \pm 2ab$.
Se $\varepsilon = \pm i$ então $x + yi = \pm i(a + bi)^2$

$$= \pm i(a^2 - b^2 + 2abi)$$

e portanto $x = \pm 2ab$ e $y = \pm(a^2 - b^2)$.
Se $a = 0$ ou $b = 0$ então $x = 0$ ou $y = 0$. Absurdo!
Se a e b forem pares então $\pm(a^2 - b^2)$ e $\pm 2ab$ são ambos pares e portanto x e y são pares. Absurdo!
Se a e b forem ímpares então $\pm(a^2 - b^2)$ e $\pm 2ab$ são ambos pares e portanto x e

y são pares. Absurdo!
Segue que a e b não têm a mesma paridade.
Agora vamos mostrar que $mdc(a,b) = 1$.
Seja $d = mdc(a,b)$. Suponha $d \neq 1$. Então existe $p \in \mathbb{Z}, p$ primo, tal que $p|a$ e $p|b$. Conseqüentemente $p| \pm (a^2 - b^2)$ e $p| \pm 2ab$, ou seja, $p|x$ e $p|y$. Deste modo $mdc(x,y) \neq 1$. Absurdo! Logo $d = mdc(a,b) = 1$.

$(iii) \Rightarrow (i)$ Das hipóteses de (iii), temos:

$$\begin{aligned} x^2 + y^2 &= (a^2 - b^2)^2 + (2ab)^2 \\ &= a^4 + b^4 + 2b^2a^2 \\ &= (a^2)^2 + 2b^2a^2 + (b^2)^2 \\ &= (a^2 + b^2)^2. \end{aligned}$$

Denote $a^2 + b^2 = z, z \in \mathbb{Z}$. Então $x^2 + y^2 = z^2$.

■

Teorema 3.2. A equação $X^4 + Y^4 = Z^2$ não tem solução não trivial em $\mathbb{Z}$.

Demonstração. Suponha que $x, y, z \in \mathbb{Z}\backslash\{0\}$ seja solução de $X^4 + Y^4 = Z^2$. Vamos mostrar que mantendo esta hipótese chegaremos a um absurdo.
Podemos assumir que x, y, z são maiores do que zero, pois em $X^4 + Y^4 = Z^2$ temos apenas expoentes pares, ou seja, se $-x$ é solução então x também é solução já que $(-x)^2 = x^2$.
Podemos assumir que $mdc(x,y) = 1$, pois, se existe uma solução (x,y,z) então existe uma solução (x_1, y_1, z_1) tal que $mdc(x_1, y_1) = 1$.
De fato, suponha que existe um primo p tal que $p|x$ e $p|y$. Então existe $x_1, y_1 \in \mathbb{Z}$ tal que $px_1 = x$ e $py_1 = y$.
Como (x,y,z) é solução, obtemos:

$$\begin{aligned} (px_1)^4 + (py_1)^4 = z^2 &\Longrightarrow p^4(x_1^4 + y_1^4) = z^2 \qquad (*) \\ &\Longrightarrow p(p^3(x_1^4 + y_1^4)) = z^2 \\ &\Longrightarrow p|z^2 \\ &\Longrightarrow p|z \\ &\Longrightarrow \exists\, \alpha \in \mathbb{Z} \text{ tal que } \alpha p = z. \end{aligned}$$

Por outro lado temos:

$$\begin{aligned} p^4(x_1^4 + y_1^4) = z^2 &\Longrightarrow p^4|z^2 \\ &\Longrightarrow \exists\, \beta \in \mathbb{Z} \text{ tal que } \beta p^4 = z^2 = \alpha^2 p^2 \end{aligned}$$

$$\begin{aligned}
&\Longrightarrow \beta p^2 = \alpha^2 \\
&\Longrightarrow p|\alpha \\
&\Longrightarrow \exists\, z_1 \in \mathbb{Z} \text{ tal que } pz_1 = \alpha.
\end{aligned}$$

Então como $\alpha p = z$ e $pz_1 = \alpha$ obtemos:

$$\begin{aligned}
p^2 z_1 = z &\Longrightarrow p^4 z_1^2 = z^2 = p^4(x_1^4 + y_1^4) \text{ por } (*). \\
&\Longrightarrow x_1^4 + y_1^4 = z_1^2.
\end{aligned}$$

Obtemos uma nova solução a partir de x, y. Note que, se $mdc(x_1, y_1) = 1$, conseguimos uma solução da maneira desejada. Se $mdc(x_1, y_1) \neq 1$ então basta repetir o processo até termos $mdc(x_n, y_n) = 1$. O processo é finito, pois em cada etapa eliminamos um número primo que é divisor de x e y .
Portanto, dada uma solução para $X^4 + Y^4 = Z^2$, existe uma outra solução (x_1, y_1, z_1) tal que $mdc(x_1, y_1) = 1$. Em virtude disto, vamos assumir a partir de agora que $mdc(x, y) = 1$.
Por hipótese (x, y, z) é solução de $X^4 + Y^4 = Z^2$. Então (x^2, y^2, z) é solução primitiva de $X^2 + Y^2 = Z^2$, pois $(x^2)^2 + (y^2)^2 = x^4 + y^4 = z^2$ e $mdc(x^2, y^2) = 1$, já que $mdc(x, y) = 1$.
Dessa maneira, pela proposição anterior, existem $a, b \in \mathbb{Z}\backslash\{0\}$, tais que:

- $mdc(a, b) = 1$.
- a e b não tem a mesma paridade.
- $(a^2 - b^2 = \pm x^2$ e $2ab = \pm y^2)$ ou $(a^2 - b^2 = \pm y^2$ e $2ab = \pm x^2)$.

Note que se a ou b é negativo, podemos trocar este elemento negativo pelo seu simétrico, e as condições acima continuam sendo verificadas. Desta forma, podemos considerar que $a > 0$ e $b > 0$.
Como $a > 0$ e $b > 0$, as equações

$$(a^2 - b^2 = \pm x^2 \text{ e } 2ab = \pm y^2) \text{ ou } (a^2 - b^2 = \pm y^2 \text{ e } 2ab = \pm x^2),$$

podem ser escritas, trocando a por b, se necessário, como:

$$(a^2 - b^2 = x^2 \text{ e } 2ab = y^2) \text{ ou } (a^2 - b^2 = y^2 \text{ e } 2ab = x^2).$$

Note ainda que b é par e a é ímpar.
De fato, suponha que b seja ímpar. Como a e b não têm a mesma paridade, segue que a é par.

- b^2 é ímpar $\Longrightarrow b^2 \equiv 1 (mod\, 4)$
  $\Longrightarrow -b^2 \equiv -1 (mod\, 4)$.

Mas $-1 \equiv 3(mod\ 4)$, então por transitividade $-b^2 \equiv 3(mod\ 4)$.

- a é par $\Longrightarrow a^2 = 4t, t \in \mathbb{N}$
  $\Longrightarrow a^2 \equiv 0(mod\ 4)$.

Como $x^2 = a^2 - b^2$, temos que $x^2 \equiv 3(mod\ 4)$. Logo $\overline{x}^2 = \overline{3}$. Absurdo, pois se $\overline{x} \in \mathbb{Z}_4$, então $\overline{x} = \overline{0}, \overline{1}, \overline{2}, \overline{3}$ e portanto $\overline{x}^2 = \overline{0}, \overline{1}$.
Mostramos que $b = 2v, v \in \mathbb{N}$ e $a = 2h + 1, h \in \mathbb{N}$.
A partir de agora vamos assumir $x^2 = a^2 - b^2$ e $y^2 = 2ab$ (o caso $x^2 = 2ab$ e $y^2 = a^2 - b^2$ é análogo). Assim, de

$$\begin{aligned} z^2 &= x^4 + y^4 \\ &= (x^2)^2 + (y^2)^2 \\ &= (a^2 - b^2)^2 + (2ab)^2 \\ &= (a^2 + b^2)^2 \end{aligned}$$

temos $z = a^2 + b^2$. (2)
Se $y^2 = 2ab = 4av$ então $(\frac{y}{2})^2 = av$. Como $b = 2v$ e $mdc(a, b) = 1$ obtemos que $mdc(a, v) = 1$. Logo, pelo Lema 2.1, temos que $a = \pm c^2$ e $v = \pm d^2$. No entanto como estamos considerando $a, b > 0$, temos que $a = c^2$ e $v = d^2$.
De $x^2 = a^2 - b^2$, vem que $a^2 = x^2 + b^2$.
Como $mdc(x^2, y^2) = 1$ e $y^2 = 2ab$, inferimos que $mdc(x, b) = 1$.
Pela proposição anterior, as soluções de $x^2 + b^2 = a^2$ são dadas por:

$$x = e^2 - f^2 \text{ e } b = 2ef$$

$$ou$$

$$x = 2ef \text{ e } b = e^2 - f^2$$

onde $mdc(e, f) = 1$ e e, f não têm a mesma paridade, $e, f > 0$.
Mas b é par e então $x = e^2 - f^2$ e $b = 2ef$. A outra opção leva a um absurdo.
Conseguimos as seguintes igualdades: $b = 2v = 2ef$. Elas implicam que $v = ef = d^2$. Pelo item a) do Lema 2.1 temos $e = k^2$ e $f = s^2$.
Segue que:

$$\begin{aligned} a^2 &= x^2 + b^2 \\ &= (e^2 - f^2)^2 + (2ef)^2 \\ &= e^4 + f^4 - 2e^2f^2 + 4e^2f^2 \\ &= e^4 + 2e^2f^2 + f^2 \\ &= (e^2 + f^2)^2. \end{aligned}$$

Logo $a = e^2 + f^2$, pois $a > 0$.
Então temos:

$$\begin{aligned} c^2 &= a \\ &= e^2 + f^2 \\ &= (k^2)^2 + (s^2)^2 \\ &= k^4 + s^4 \\ &\Longrightarrow c^2 = k^4 + s^4. \end{aligned}$$

Logo (k, s, c) é outra solução de $X^4 + Y^4 = Z^2$.
Pela equação (2), temos que $z = a^2 + b^2$ e então vemos que $z = a^2 + b^2 > a$. Por outro lado $a = c^2$ e $c^2 \geq c$. Por transitividade $z > c$.
Portanto o c obtido na solução é estritamente menor que z, ou seja, se (x, y, z) é solução da equação $X^4 + Y^4 = Z^2$, então existe outra solução (k, s, c) tal que $c < z$.
Repetindo o processo, um número finito, de vezes obteremos uma solução (k_n, s_n, c_n) para $X^4 + Y^4 = Z^2$ com $c_n = 1$. Mas isto é um absurdo, pois

$$1 = c_n^2 = k_n^4 + s_n^4 \geq 2.$$

Portanto não existe solução para $X^4 + Y^4 = Z^2$.

■

Corolário 3.1. *$X^4 + Y^4 = Z^4$ não tem solução não trivial em $\mathbb{Z}$.*

Demonstração. Suponha por absurdo que (x_0, y_0, z_0) é uma solução não trivial em $\mathbb{Z}$. Então temos:

$$x_0^4 + y_0^4 = z_0^4 = (z_0^2)^2.$$

Conseqüentemente (x_0, y_0, z_0^2) é uma solução para $X^4 + Y^4 = Z^2$. Absurdo, pois $X^4 + Y^4 = Z^2$ não possui solução não trivial em $\mathbb{Z}$.
Logo não existe solução não trivial para $X^4 + Y^4 = Z^4$.

■

Corolário 3.2. *$X^{4k} + Y^{4k} = Z^{4k}$ não tem solução não trivial em $\mathbb{Z}$.*

Demonstração. Seja (x_0, y_0, z_0) uma solução não trivial em $\mathbb{Z}$ para $X^{4k} + Y^{4k} = Z^{4k}$. Então (x_0^k, y_0^k, z_0^k) é uma solução para $X^4 + Y^4 = Z^4$. Absurdo!
Portanto, $X^{4k} + Y^{4k} = Z^{4k}$ não possui solução não trivial em $\mathbb{Z}$.

■

Corolário 3.3. *Sejam p primo e $m \in \mathbb{N}$.*
Se $X^{pm} + Y^{pm} = Z^{pm}$ tem solução não trivial em $\mathbb{Z}$ então $X^p + Y^p = Z^p$ tem solução não trivial em $\mathbb{Z}$.

Demonstração. Seja (x_0, y_0, z_0) uma solução não trivial, em $\mathbb{Z}$, para $X^{pm} + Y^{pm} = Z^{pm}$.
Então temos: $x_0^{pm} + y_0^{pm} = z_0^{pm} \Longrightarrow (x_0^m)^p + (y_0^m)^p = (z_0^m)^p$.
Logo (x_0^m, y_0^m, z_0^m) é solução não trivial para $X^p + Y^p = Z^p$.

■

Logo, se não existe solução para $X^p + Y^p = Z^p$ então não existe solução para nenhum múltiplo de p.

Agora podemos provar o Teorema 3.1 enunciado no início do capítulo.

Teorema 3.1. Se $X^p + Y^p = Z^p$ não tem solução não trivial para $p \geq 3, p$ primo, então $X^m + Y^m = Z^m$ não tem solução não trivial para $m \geq 3, m \in \mathbb{Z}$.

Demonstração. Considere $m \in \mathbb{Z}, m \geq 3$. Na decomposição de m há pelo menos um número primo $p \geq 3$ ou há apenas o número primo 2. Neste último caso o primo 2 deve ter uma potência maior ou igual a dois, ou seja, m deve ser um múltiplo de 4, caso contrário seria igual a dois; um absurdo com nossa hipótese.
Vamos considerar estes dois casos separadamente:
Caso 1: Existe p primo, $p \geq 3$, tal que $p|m$. Conseqüentemente existe $k \in \mathbb{Z}$ tal que $pk = m$.
Por hipótese, não existe solução não trivial em $\mathbb{Z}$ para $X^p + Y^p = Z^p$. Pelo Corolário 3.3, não existe solução para $X^{pk} + Y^{pk} = Z^{pk}$.
Logo, como $m = pk$, não existe solução não trivial para $X^m + Y^m = Z^m$ em $\mathbb{Z}$.
Caso 2: O único primo que divide m é o 2. Neste caso $m = 2^r, r \in \mathbb{Z}$.
Por hipótese, $m > 3$, então $r \geq 2$. Assim sendo, $r = 2 + l, l \in \mathbb{N}$ e $m = 2^{2+l} = 4k$. Pelo Corolário 3.2 a equação $X^{4k} + Y^{4k} = Z^{4k}$ não tem solução não trivial em $\mathbb{Z}$.
Logo $X^m + Y^m = Z^m$ não tem solução não trivial em $\mathbb{Z}$.

■

Capítulo 4

Todo inteiro positivo é uma soma de 4 quadrados

Neste capítulo, vamos mostrar que todo número inteiro positivo pode ser escrito como a soma de quatro quadrados de inteiros.

Para tanto, faremos um desenvolvimento análogo ao feito no Capítulo 2. No entanto, ao invés de trabalhar com o domínio euclidiano $\mathbb{Z}[i]$ e com a função norma N, iremos trabalhar com um anel principal, que é um subanel de $\mathbb{C}X\mathbb{C}$, e com a função φ, que será definida no decorrer do capítulo.

Consideremos então o conjunto $\mathbb{C}X\mathbb{C}$, que denotaremos por Q, com as operações $\oplus$ e $\otimes$ definidas da seguinte maneira:

$$(\alpha, \beta) \oplus (\gamma, \delta) = (\alpha + \gamma, \beta + \delta)$$

$$(\alpha, \beta) \otimes (\gamma, \delta) = (\alpha\gamma - \beta\overline{\delta}, \alpha\delta + \beta\overline{\gamma})$$

Proposição 4.1. $(Q, \oplus, \otimes)$ é um anel não comutativo e com unidade.

Demonstração. Vamos mostrar que $(Q, \oplus, \otimes)$ satisfaz as seis condições de anel, S_1, S_2, S_3, S_4, S_5 e S_6, satisfaz também S_7 e não satisfaz S_8:

S_1) Sejam (α_1, β_1), (α_2, β_2), $(\alpha_3, \beta_3) \in Q$, temos:

$$\begin{aligned}((\alpha_1, \beta_1) \oplus (\alpha_2, \beta_2)) \oplus (\alpha_3, \beta_3) &= (\alpha_1 + \alpha_2, \beta_1 + \beta_2) \oplus (\alpha_3, \beta_3) \\ &= ((\alpha_1 + \alpha_2) + \alpha_3, (\beta_1 + \beta_2) + \beta_3) \\ &= (\alpha_1 + (\alpha_2 + \alpha_3), \beta_1 + (\beta_2 + \beta_3)), \\ &\quad \text{(pois } + \text{ é associativa em } \mathbb{C}).\end{aligned}$$

$$= (\alpha_1, \beta_1) \oplus ((\alpha_2, \beta_2) \oplus (\alpha_3, \beta_3))$$

Portanto a operação $\oplus$ é associativa.

S_2) Considere o elemento $(0, 0) \in \mathbb{C}X\mathbb{C}$.
Dados $(\alpha, \beta) \in Q$ temos:

$$(\alpha, \beta) \oplus (0, 0) = (\alpha + 0, \beta + 0) = (\alpha, \beta)$$

$$(0, 0) \oplus (\alpha, \beta) = (0 + \alpha, 0 + \beta) = (\alpha, \beta)$$

Logo $(0, 0)$ é o elemento neutro para $\oplus$ em Q.

S_3) Dado $(\alpha, \beta) \in Q$, considere o elemento $(-\alpha, -\beta) \in Q$, onde $-\alpha$ e $-\beta$ são, respectivamente, os inversos aditivos de α e β em $\mathbb{C}$.

$$(\alpha, \beta) \oplus (-\alpha, -\beta) = (\alpha + (-\alpha), \beta + (-\beta)) = (0, 0)$$

$$(-\alpha, -\beta) \oplus (\alpha, \beta) = (-\alpha + \alpha, -\beta + \beta) = (0, 0)$$

Logo $(-\alpha, -\beta)$ é o inverso aditivo de (α, β) em Q.

S_4) A operação $\oplus$ é comutativa em Q.
De fato, dados $(\alpha, \beta), (\gamma, \delta) \in Q$ temos que:

$$\begin{aligned}(\alpha, \beta) \oplus (\gamma, \delta) &= (\alpha + \gamma, \beta + \delta) \\ &= (\gamma + \alpha, \delta + \beta), \text{ pois } + \text{ é comutativa em } \mathbb{C}. \\ &= (\gamma, \delta) \oplus (\alpha, \beta).\end{aligned}$$

S_5) A operação $\otimes$ é associativa.
De fato, se (α_1, β_1), (α_2, β_2), $(\alpha_3, \beta_3) \in Q$, temos:

- $((\alpha_1, \beta_1) \otimes (\alpha_2, \beta_2)) \otimes (\alpha_3, \beta_3) =$

$$= (\alpha_1\alpha_2 - \beta_1\overline{\beta_2}, \alpha_1\beta_2 + \beta_1\overline{\alpha_2}) \otimes (\alpha_3, \beta_3)$$

$$= ((\alpha_1\alpha_2)\alpha_3 - (\beta_1\overline{\beta_2})\alpha_3 - (\alpha_1\beta_2)\overline{\beta_3} - (\beta_1\overline{\alpha_2})\overline{\beta_3},$$
$$(\alpha_1\alpha_2)\beta_3 - (\beta_1\overline{\beta_2})\beta_3 + (\alpha_1\beta_2)\overline{\alpha_3} + (\beta_1\overline{\alpha_2})\overline{\alpha_3}) \quad (*)$$

- $(\alpha_1, \beta_1) \otimes ((\alpha_2, \beta_2) \otimes (\alpha_3, \beta_3)) =$

$$= (\alpha_1, \beta_1) \otimes (\alpha_2\alpha_3 - \beta_2\overline{\beta_3}, \alpha_2\beta_3 + \beta_2\overline{\alpha_3})$$

$$= (\alpha_1(\alpha_2\alpha_3) - \alpha_1(\beta_2\overline{\beta_3}) - \beta_1(\overline{\alpha_2\beta_3 + \beta_2\overline{\alpha_3}}), \alpha_1(\alpha_2\beta_3) + \alpha_1(\beta_2\overline{\alpha_3}) + \beta_1(\overline{\alpha_2\alpha_3 - \beta_2\overline{\beta_3}}))$$

$$= (\alpha_1(\alpha_2\alpha_3) - \alpha_1(\beta_2\overline{\beta_3}) - \beta_1(\overline{\alpha_2}\,\overline{\beta_3}) - \beta_1(\overline{\beta_2}\alpha_3),$$
$$\alpha_1(\alpha_2\beta_3) + \alpha_1(\beta_2\overline{\alpha_3}) + \beta_1(\overline{\alpha}_2\overline{\alpha}_3) - \beta_1(\overline{\beta_2}\beta_3))$$

$$= ((\alpha_1\alpha_2)\alpha_3 - (\beta_1\overline{\beta_2})\alpha_3 - (\alpha_1\beta_2)\overline{\beta_3} - (\beta_1\overline{\alpha_2})\overline{\beta_3},$$
$$(\alpha_1\alpha_2)\beta_3 - (\beta_1\overline{\beta_2})\beta_3 + (\alpha_1\beta_2)\overline{\alpha_3} + (\beta_1\overline{\alpha_2})\overline{\alpha_3}) \quad (**)$$

Portanto, como $(*) = (**)$, temos que a operação $\otimes$ é associativa.

S_6) Vale a propriedade distributiva em Q.
De fato,

$$(\alpha_1, \beta_1) \otimes ((\alpha_2, \beta_2) \oplus (\alpha_3, \beta_3)) =$$
$$= (\alpha_1, \beta_1) \otimes (\alpha_2 + \alpha_3, \beta_2 + \beta_3)$$
$$= (\alpha_1(\alpha_2 + \alpha_3) - \beta_1(\overline{\beta_2 + \beta_3}), \alpha_1(\beta_2 + \beta_3) + \beta_1(\overline{\alpha_2 + \alpha_3}))$$
$$= (\alpha_1\alpha_2 + \alpha_1\alpha_3 - \beta_1\overline{\beta_2} - \beta_1\overline{\beta_3}, \alpha_1\beta_2 + \alpha_1\beta_3 + \beta_1\overline{\alpha_2} + \beta_1\overline{\alpha_3}),$$
(pois vale a propriedade distributiva em $\mathbb{C}$.)
$$= (\alpha_1\alpha_2 - \beta_1\overline{\beta_2}, \alpha_1\beta_2 + \beta_1\overline{\alpha_2}) \oplus (\alpha_1\alpha_3 - \beta_1\overline{\beta_3}, \alpha_1\beta_3 + \beta_1\overline{\alpha_3})$$
$$= (\alpha_1, \beta_1) \otimes (\alpha_2, \beta_2) \oplus (\alpha_1, \beta_1) \otimes (\alpha_3, \beta_3).$$

Analogamente temos que:

$$((\alpha_1, \beta_1) \oplus (\alpha_2, \beta_2)) \otimes (\alpha_3, \beta_3) = (\alpha_1, \beta_1) \otimes (\alpha_3, \beta_3) \oplus (\alpha_2, \beta_2) \otimes (\alpha_3, \beta_3).$$

S_7) O elemento $(1, 0) \in \mathbb{C}X\mathbb{C}$ é o elemento neutro da operação $\otimes$ em Q.
De fato, dado $(\alpha, \beta) \in Q$, temos que:

$$\begin{aligned}(\alpha, \beta) \otimes (1, 0) &= (\alpha.1 - \beta.\overline{0}, \alpha.0 + \beta.\overline{1}) \\ &= (\alpha - 0, 0 + \beta) \\ &= (\alpha, \beta)\end{aligned}$$
$$\begin{aligned}(1, 0) \otimes (\alpha, \beta) &= (1.\alpha - 0.\overline{\beta}, 1.\beta + 0.\overline{\alpha}) \\ &= (\alpha - 0, \beta + 0) \\ &= (\alpha, \beta)\end{aligned}$$

S_8) Q não é comutativo. Considere o seguinte contra- exemplo:

$$\begin{aligned}(i, 1 + i) \otimes (1, -i) &= (i - (1 + i)i, 1 + (1 + i)) \\ &= (1, 2 + i)\end{aligned}$$
$$\begin{aligned}(1, -i) \otimes (i, 1 + i) &= (i + i(1 - i), 1 + i - i(-i)) \\ &= (2i + 1, i)\end{aligned}$$

Portanto Q é um anel com unidade e não comutativo.

■

Consideremos agora, em Q, a seguinte função:

$$\varphi : Q \longrightarrow \mathbb{R}_+$$

$$(\alpha, \beta) \longmapsto \alpha\overline{\alpha} + \beta\overline{\beta}$$

Note que, se $\alpha = a_1 + a_2 i$ e $\beta = a_3 + a_4 i$, então $\varphi((\alpha, \beta)) = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Também é fácil ver que $\varphi((\alpha, \beta)) = 0$ se, e somente se, $(\alpha, \beta) = (0, 0)$.

Proposição 4.2. A função φ é multiplicativa, ou seja, φ satisfaz a seguinte condição:

$$\varphi(x \otimes y) = \varphi(x)\varphi(y), \forall x, y \in Q.$$

Demonstração. Dado $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in Q$ temos:

- $\varphi((\alpha_1, \beta_1) \otimes (\alpha_2, \beta_2)) =$

$= \varphi((\alpha_1\alpha_2 - \beta_1\overline{\beta_2}, \alpha_1\beta_2 + \beta_1\overline{\alpha_2}))$

$= (\alpha_1\alpha_2 - \beta_1\overline{\beta_2})(\overline{\alpha_1\alpha_2 - \beta_1\overline{\beta_2}}) + (\alpha_1\beta_2 + \beta_1\overline{\alpha_2})(\overline{\alpha_1\beta_2 + \beta_1\overline{\alpha_2}})$

$= \alpha_1\overline{\alpha_1}\alpha_2\overline{\alpha_2} + \beta_1\overline{\beta_1}\beta_2\overline{\beta_2} + \alpha_1\overline{\alpha_1}\beta_2\overline{\beta_2} + \beta_1\overline{\beta_1}\alpha_2\overline{\alpha_2} \quad (*).$

- $\varphi((\alpha_1, \beta_1))\varphi((\alpha_2, \beta_2)) =$

$= (\alpha_1\overline{\alpha_1} + \beta_1\overline{\beta_1})(\alpha_2\overline{\alpha_2} + \beta_2\overline{\beta_2})$

$= \alpha_1\overline{\alpha_1}\alpha_2\overline{\alpha_2} + \beta_1\overline{\beta_1}\beta_2\overline{\beta_2} + \alpha_1\overline{\alpha_1}\beta_2\overline{\beta_2} + \beta_1\overline{\beta_1}\alpha_2\overline{\alpha_2} \quad (**).$

Como $(*) = (**)$ temos que φ é multiplicativa.

■

Proposição 4.3. Todo elemento não nulo de Q tem inverso multiplicativo com relação a operação $\otimes$.

Demonstração. Seja $(\alpha, \beta) \in Q$, não nulo. Então seu inverso, com relação a operação $\otimes$, é:

$$(\alpha, \beta)^{-1} = \left(\frac{\overline{\alpha}}{\varphi((\alpha, \beta))}, \frac{-\beta}{\varphi((\alpha, \beta))}\right).$$

De fato,

$$(\alpha,\beta)\otimes\left(\frac{\overline{\alpha}}{\varphi((\alpha,\beta))},\frac{-\beta}{\varphi((\alpha,\beta))}\right)=$$

$$=\left(\alpha.\frac{\overline{\alpha}}{\varphi((\alpha,\beta))}-\beta\left(\overline{\frac{-\beta}{\varphi((\alpha,\beta))}}\right),\alpha.\frac{-\beta}{\varphi((\alpha,\beta))}+\beta.\left(\overline{\frac{\overline{\alpha}}{\varphi((\alpha,\beta))}}\right)\right)$$

$$=\left(\frac{\alpha.\overline{\alpha}}{\varphi((\alpha,\beta))}-\frac{\beta.(-\overline{\beta})}{\varphi((\alpha,\beta))},\frac{-\alpha.\beta}{\varphi((\alpha,\beta))}+\frac{\beta\alpha}{\varphi((\alpha,\beta))}\right)$$

$$=\left(\frac{\alpha.\overline{\alpha}+\beta\overline{\beta}}{\alpha.\overline{\alpha}+\beta\overline{\beta}},\frac{-\alpha\beta+\beta\alpha}{\alpha.\overline{\alpha}+\beta\overline{\beta}}\right)$$

$$=(1,0).$$

Analogamente, verifica-se que:

$$\left(\frac{\overline{\alpha}}{\varphi((\alpha,\beta))},\frac{-\beta}{\varphi((\alpha,\beta))}\right)\otimes(\alpha,\beta)=(1,0).$$

■

Observação 4.1. Vimos que o anel $(Q,\oplus,\otimes)$ satisfaz os axiomas de corpo, com exceção da comutatividade. Por isso dizemos que $(Q,\oplus,\otimes)$ é um **anel de divisão**.

Proposição 4.4. O subconjunto

$$H=\left\{\left(\left(\frac{a}{2}+\frac{ib}{2}\right),\left(\frac{c}{2}+\frac{id}{2}\right)\right);a,b,c,d\in\mathbb{Z}\text{ com }a\equiv b\equiv c\equiv d(\text{mod }2)\right\}$$

é um subanel de Q, tal que $\varphi(x)\in\mathbb{Z},\forall x\in H$.

Demonstração. Note que $H\neq\emptyset$, pois $(0,0)\in H$.
Dados $x,y\in H$ temos:

$$x=\left(\left(\frac{a_1}{2}+\frac{ib_1}{2}\right),\left(\frac{c_1}{2}+\frac{id_1}{2}\right)\right);a_1\equiv b_1\equiv c_1\equiv d_1(\text{mod }2).$$
$$y=\left(\left(\frac{a_2}{2}+\frac{ib_2}{2}\right),\left(\frac{c_2}{2}+\frac{id_2}{2}\right)\right);a_2\equiv b_2\equiv c_2\equiv d_2(\text{mod }2).$$

E então,

$$x \oplus (-y) = \left(\left(\frac{a_1}{2} + \frac{ib_1}{2}\right), \left(\frac{c_1}{2} + \frac{id_1}{2}\right)\right) \oplus \left(\left(\frac{-a_2}{2} + \frac{-ib_2}{2}\right), \left(\frac{-c_2}{2} + \frac{-id_2}{2}\right)\right)$$

$$= \left(\frac{a_1 - a_2}{2} + \frac{(b_1 - b_2)i}{2}, \frac{c_1 - c_2}{2} + \frac{(d_1 - d_2)i}{2}\right) \in H.$$

De fato, por hipótese temos:

$$a_1 \equiv b_1 \equiv c_1 \equiv d_1 (\text{mod } 2) \text{ e } a_2 \equiv b_2 \equiv c_2 \equiv d_2 (\text{mod } 2),$$

e então

$$a_1 - a_2 \equiv b_1 - b_2 \equiv c_1 - c_2 \equiv d_1 - d_2 (\text{mod } 2),$$

ou seja, $(a_1 - a_2), (b_1 - b_2), (c_1 - c_2), (d_1 - d_2)$ têm a mesma paridade.

$$x \otimes y = \left(\left(\frac{a_1}{2} + \frac{ib_1}{2}\right), \left(\frac{c_1}{2} + \frac{id_1}{2}\right)\right) \otimes \left(\left(\frac{a_2}{2} + \frac{ib_2}{2}\right), \left(\frac{c_2}{2} + \frac{id_2}{2}\right)\right)$$

$$= \frac{1}{4}(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 + (a_1b_2 + b_1a_2 - d_1c_2 + c_1d_2)i,$$
$$a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2 + (a_1d_2 + b_1c_2 + d_1a_2 - c_1b_2)i)$$

Denote:

$$\frac{a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2}{2} = h$$
$$\frac{a_1b_2 + b_1a_2 - d_1c_2 + c_1d_2}{2} = l$$
$$\frac{a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2}{2} = m$$
$$\frac{a_1d_2 + b_1c_2 + d_1a_2 - c_1b_2}{2} = n$$

Precisamos mostrar que h, l, m, n têm a mesma paridade.

Sabemos que $a_1 \equiv b_1 \equiv c_1 \equiv d_1 (\text{mod } 2)$ e $a_2 \equiv b_2 \equiv c_2 \equiv d_2 (\text{mod } 2)$ e então:

$$a_1 = 2k_1, b_1 = 2k_2, c_1 = 2k_3, d_1 = 2k_4 \quad (1) \text{ ou}$$
$$a_1 = 2f_1 + 1, b_1 = 2f_2 + 1, c_1 = 2f_3 + 1, d_1 = 2f_4 + 1 \quad (2)$$
e
$$a_2 = 2r_1, b_2 = 2r_2, c_2 = 2r_3, d_2 = 2r_4 \quad (3) \text{ ou}$$

$$a_2 = 2s_1 + 1, b_2 = 2s_2 + 1, c_2 = 2s_3 + 1, d_2 = 2s_4 + 1 \quad (4)$$

Se ocorrer (1) e (3) temos claramente que h, l, m, n são pares.
Se ocorrer (1) e (4) temos que h, l, m, n possuem a paridade de $k_1 + k_2 + k_3 + k_4$.
Se ocorrer (2) e (3) então h, l, m, n possuem a paridade de $r_1 + r_2 + r_3 + r_4$.
Se ocorrer (2) e (4) então h, l, m, n possuem a paridade de $f_1 + f_2 + f_3 + f_4 + s_1 + s_2 + s_3 + s_4$.

Portanto h, l, m, n possuem a mesma paridade e então $x \otimes y \in H$.
Isso mostra que que H é subanel de Q.
Agora vamos provar que $\varphi(x) \in \mathbb{Z}, \forall x \in H$.
Seja $x \in H, x = \left(\frac{a}{2} + \frac{b}{2}i, \frac{c}{2} + \frac{d}{2}i\right)$ onde $a, b, c, d \in \mathbb{Z}$ são todos pares ou todos ímpares. Então

$$\varphi(x) = \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2 + \left(\frac{d}{2}\right)^2 = \frac{a^2 + b^2 + c^2 + d^2}{4}.$$

• Se a, b, c, d são pares, então $a = 2k_1, b = 2k_2, c = 2k_3$ e $d = 2k_4$. Assim

$$\varphi(x) = \frac{4(k_1^2 + k_2^2 + k_3^2 + k_4^2)}{4} \in \mathbb{Z}.$$

• Se a, b, c, d são ímpares, então $a = 2k_1 + 1, b = 2k_2 + 1, c = 2k_3 + 1$ e $d = 2k_4 + 1$. Assim

$$\varphi(x) = \frac{4(k_1^2 + k_1 + k_2^2 + k_2 + k_3^2 + k_3 + k_4^2 + k_4 + 1)}{4} \in \mathbb{Z}.$$

■

Proposição 4.5. $(H, \oplus, \otimes, \varphi)$ tem a seguinte propriedade euclidiana:
Dados dois elementos x e y não nulos de H, existem elementos $t, r \in H$ tais que

$$y = t \otimes x \oplus r \text{ com } \varphi(r) < \varphi(x).$$

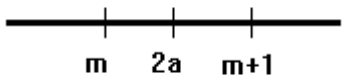
Demonstração. Seja $x \in H, x \neq 0$. Como $H \subseteq Q$ temos, em particular, que $x \in Q$. Pela Proposição 4.3 sabemos que $x^{-1} \in Q$. Logo $y \otimes x^{-1} \in Q$, ou seja,

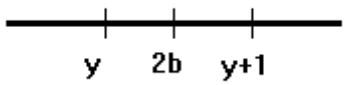
$$y \otimes x^{-1} = ((a + bi), (c + di)); a, b, c, d \in \mathbb{R}.$$

Escolha então $m, n \in \mathbb{Z}$ tais que:

- m e n tem sempre a mesma paridade $(m \equiv n (\text{mod } 2))$.
- $|2a - m| \leq \frac{1}{2}$ e $|2b - n| \leq 1$.

Note que esta escolha sempre é possível.
De fato, $2a, 2b \in \mathbb{R}$ e assim $2a$ está sempre entre dois inteiros consecutivos e $2b$ está sempre entre dois inteiros consecutivos.





Seja m o inteiro mais próximo de $2a$. Então $|2a - m| \leq \frac{1}{2}$.
Escolha $n \in \{y, y+1\} \subseteq \mathbb{Z}$ tal que $n \equiv m (\text{mod } 2)$. Então $|2b - n| \leq 1$.
Analogamente, escolha $u, v \in \mathbb{Z}$ tais que:

- $u \equiv v \equiv n (\text{mod } 2)$.
- $|2c - u| \leq 1$ e $|2d - v| \leq 1$.

Reescrevendo $y \otimes x^{-1}$ temos:

$$y \otimes x^{-1} = \left(\left(\frac{m}{2} + \frac{n}{2}i\right), \left(\frac{u}{2} + \frac{v}{2}i\right)\right) \oplus \left(\left(\frac{2a-m}{2} + \frac{2b-n}{2}i\right), \left(\frac{2c-u}{2} + \frac{2d-v}{2}i\right)\right) \quad (*)$$

Denotando $\left(\left(\frac{m}{2} + \frac{n}{2}i\right), \left(\frac{u}{2} + \frac{v}{2}i\right)\right)$ por t, $\left(\left(\frac{2a-m}{2} + \frac{2b-n}{2}i\right), \left(\frac{2c-u}{2} + \frac{2d-v}{2}i\right)\right)$ por $r^{'}$ e multiplicando em ambos os lados de $(*)$ por x, obtemos:

$$y = t \otimes x \oplus (r^{'} \otimes x).$$

Note que $t \in H$ e deste modo, como H é anel,

$$y \oplus (-t \otimes x) = r^{'} \otimes x \in H.$$

Denote $r^{'} \otimes x = r$. Então obtemos $y = t \otimes x \oplus r$.
Falta apenas mostrar que $\varphi(r) < \varphi(x)$.

$$\begin{aligned}
\varphi(r) &= \varphi(r^{'} \otimes x) \\
&= \varphi(r^{'}).\varphi(x) \\
&= \varphi(x)\left(\frac{(2a-m)^2 + (2b-n)^2 + (2c-u)^2 + (2d-v)^2}{4}\right) \\
&= \varphi(x)\left(\frac{|2a-m|^2 + |2b-n|^2 + |2c-u|^2 + |2d-v|^2}{4}\right) \\
&\leq \varphi(x)\frac{1}{4}\left(\frac{1}{4} + 1 + 1 + 1\right)
\end{aligned}$$

$$= \varphi(x)\frac{13}{16}$$
$$< \varphi(x).$$

■

Observação 4.2. $(H, \oplus, \otimes, \varphi)$ não é um domínio euclidiano, pois seus elementos não gozam da propriedade comutativa. Nas próximas proposições veremos que todo ideal à esquerda de H é um ideal à esquerda principal, e que H não possui divisores de zero.

Proposição 4.6. Todo ideal à esquerda de H é um ideal à esquerda principal.

Demonstração. Seja I um ideal à esquerda de H, $I \neq \emptyset$, temos de mostrar que $I = H \otimes a$, onde $a \in H$, ou seja, dado $\varepsilon \in I$ precisamos mostrar que $\varepsilon = h \otimes a, h \in H$.
Se $I = \{(0,0)\}$, onde $(0,0)$ é o elemento neutro para a operação $\oplus$, então

$$I = H \otimes (0,0).$$

Se $I \neq \{(0,0)\}$, consideremos o seguinte conjunto:

$$\varphi(I) = \{\varphi(\alpha), \alpha \in I \text{ e } \alpha \neq 0\} \subseteq \mathbb{N}.$$

O conjunto dos números naturais é bem ordenado, e então todo subconjunto não vazio possui um menor elemento. Logo $\varphi(I)$ possui um menor elemento. Denotaremos tal elemento por $\varphi(a), a \in I$ e mostraremos que $I = H \otimes a$.
Dado $\varepsilon \in I$, pela propriedade euclidiana existem $t, r \in H$ tais que:

$$\varepsilon = t \otimes a \oplus r \quad \text{com } \varphi(r) < \varphi(a).$$

Note que, como I é ideal à esquerda e $a \in I$ então $t \otimes a \in I$. Assim temos que

$$r = \varepsilon \oplus t \otimes (-a) \in I.$$

Como $r \in I$ e $\varphi(r) < \varphi(a)$, a minimalidade de $\varphi(a)$ assegura que $r = 0$. Em virtude disso,

$$\varepsilon = t \otimes a \in H \otimes a.$$

Portanto $I \subseteq H \otimes a$.
Como $a \in I$ e I é ideal à esquerda vem que $H \otimes a \subseteq I$. Logo $I = H \otimes a$.

■

Proposição 4.7. Q não possui divisores de zero.

Demonstração. Sejam $(\alpha, \beta), (\gamma, \delta) \in Q$ tais que $(\alpha, \beta) \otimes (\gamma, \delta) = (0, 0) \quad (*)$. Suponha que $(\alpha, \beta) \neq 0$ então $(\alpha, \beta)^{-1} \in Q$. Multiplicando $(*)$ por $(\alpha, \beta)^{-1}$ à esquerda temos:

$$\begin{aligned}
&(\alpha, \beta)^{-1} \otimes ((\alpha, \beta) \otimes (\gamma, \delta)) = (\alpha, \beta)^{-1} \otimes (0, 0) \\
&\quad \Longrightarrow ((\alpha, \beta)^{-1} \otimes (\alpha, \beta)) \otimes (\gamma, \delta) = (0, 0) \\
&\quad \Longrightarrow (1, 0) \otimes (\gamma, \delta) = (0, 0) \\
&\quad \Longrightarrow (\gamma, \delta) = (0, 0).
\end{aligned}$$

Suponha agora que $(\gamma, \delta) \neq 0$, então $(\gamma, \delta)^{-1} \in Q$. Multiplicando $(*)$ por $(\gamma, \delta)^{-1}$ à direita temos:

$$\begin{aligned}
&((\alpha, \beta) \otimes (\gamma, \delta)) \otimes (\gamma, \delta)^{-1} = (0, 0) \otimes (\gamma, \delta)^{-1} \\
&\quad \Longrightarrow (\alpha, \beta) \otimes ((\gamma, \delta) \otimes (\gamma, \delta)^{-1}) = (0, 0) \\
&\quad \Longrightarrow (\alpha, \beta) \otimes (1, 0) = (0, 0) \\
&\quad \Longrightarrow (\alpha, \beta) = (0, 0).
\end{aligned}$$

Portanto Q não possui divisores zero.

■

Proposição 4.8. Seja $x \in H, x \neq (0, 0)$. Então $x \in \mathcal{U}(H)$ se, e somente se, $\varphi(x) = 1$.

Demonstração. $(\Rightarrow)$ Se $x \in \mathcal{U}(H)$ então existe $y \in H$ tal que $x \otimes y = (1, 0)$. Conseqüentemente $\varphi(x) \otimes \varphi(y) = \varphi((1, 0)) = 1$.
Pela Proposição 4.4, vem que $\varphi(x) \in \mathbb{Z}_+$ e $\varphi(y) \in \mathbb{Z}_+$. Logo $\varphi(x) \in \mathcal{U}(\mathbb{Z})$ e portanto $\varphi(x) = 1$.

$(\Leftarrow)$ Seja $x \in H, x = \left(\frac{a}{2} + \frac{b}{2}i, \frac{c}{2} + \frac{d}{2}i\right)$, tal que $\varphi(x) = 1$.
Pela Proposição 4.3, x possui um elemento inverso em Q e ele é dado por:

$$x^{-1} = \left(\frac{\frac{a - bi}{2}}{\frac{a^2 + b^2 + c^2 + d^2}{4}}, \frac{\frac{-(c + di)}{2}}{\frac{a^2 + b^2 + c^2 + d^2}{4}} \right) \quad (*).$$

Então, para mostrar que x é inversível em H, basta mostrar que, se $\varphi(x) = 1$ então $x^{-1} \in H$.
De fato, se $\varphi(x) = 1$ temos que:

$$\frac{a^2 + b^2 + c^2 + d^2}{4} = 1 \ (**).$$

Substituindo $(**)$ em $(*)$ obtemos que:

$$x^{-1} = \left(\frac{a - bi}{2}, \frac{-(c + di)}{2} \right),$$

ou seja, $x^{-1} \in H$, e portanto $x \in \mathcal{U}(H)$.

■

Definição 4.1. Um elemento $x \in H$ é denominado **central** se $x \otimes y = y \otimes x, \forall y \in H$.

Observação 4.3. Na próxima proposição, a hipótese de x ser elemento central é usada apenas para que a relação de divisibilidade $x|y$, independa do lado que multipicamos x para obter y.

Proposição 4.9. Se $x \in H$ é um elemento central e irredutível então x é um elemento primo.

Demonstração. Seja $x \in H$ um elemento central e irredutível.
Sejam $y, z \in H$ tais que $x|y \otimes z$.
É fácil ver que $H \otimes x \oplus H \otimes y = \{h_1 \otimes x \oplus h_2 \otimes y; h_1, h_2 \in H\}$ é ideal à esquerda de H. Segue da Proposição 4.6, que existe $w \in H$ tal que $H \otimes x \oplus H \otimes y = H \otimes w$.
Como

$$\begin{aligned} x &= (1,0) \otimes x \oplus (0,0) \otimes y \\ &\in H \otimes x \oplus H \otimes y \\ &= H \otimes w, \end{aligned}$$

existe $h \in H$ tal que $x = h \otimes w$.
Por hipótese, x é irredutível e então $h \in \mathcal{U}(H)$ ou $w \in \mathcal{U}(H)$.

• $h \in \mathcal{U}(H)$.
$x = h \otimes w \Longrightarrow h^{-1} \otimes x = w \quad (*)$.
Por outro lado,

$$\begin{aligned} y &= (0,0) \otimes x \oplus (1,0) \otimes y \\ &\in H \otimes x \oplus H \otimes y \\ &= H \otimes w, \end{aligned}$$

e então existe $h_1 \in H$ tal que $y = h_1 \otimes w$.
Assim, multiplicando $(*)$ por h_1 à esquerda temos:

$$h_1 \otimes h^{-1} \otimes x = h_1 \otimes w = y \Longrightarrow x|y.$$

• $w \in \mathcal{U}(H)$.
Da igualdade $H \otimes w = H \otimes x \oplus H \otimes y$ e do fato de $w \in H \otimes w$, tiramos que

$w = \alpha \otimes x \oplus \beta \otimes y$, para α e β escolhidos em H.
Como $w \in \mathcal{U}(H)$ temos:

$$1 = w^{-1} \otimes \alpha \otimes x \oplus w^{-1} \otimes \beta \otimes y$$

$z = w^{-1} \otimes \alpha \otimes x \otimes z \oplus w^{-1} \otimes \beta \otimes y \otimes z$, (multiplicando por z à direita). $(**)$

Agora:

$$x|x \Longrightarrow x|(w^{-1} \otimes \alpha \otimes x \otimes z).$$
$$x|y \otimes z \Longrightarrow x|(w^{-1} \otimes \beta \otimes y \otimes z).$$

Conseqüentemente, como p divide as duas parcelas de $(**)$, temos $x|z$ e portanto x é primo.

■

Proposição 4.10. Seja $p \in \mathbb{Z}$ um número primo. Então o elemento $(p, 0)$ não é irredutível em H.

Demonstração. Inicialmente note que $(p, 0) \in H$, pois

$$(p, 0) = \left(\frac{2p}{2} + 0i, 0 + 0i\right) \in H, \text{ e } 2p \equiv 0 (\text{mod } 2).$$

Afirmação: $(p, 0)$ é um elemento central de H.
De fato, seja $(a + bi, c + di) \in H$ então:

$$\begin{aligned}(p, 0) \otimes (a + bi, c + di) &= (pa + pbi, pc + pdi) \\ &= (ap + bpi, cp + dpi), \text{ pois } \cdot \text{ é comutativo em } \mathbb{Z}. \\ &= (a + bi, c + di) \otimes (p, 0).\end{aligned}$$

A contra- positiva da Proposição 4.9 nos garante que: " Se $(p, 0)$ não é um elemento primo em H, então $(p, 0)$ não é um elemento central ou $(p, 0)$ não é um elemento irredutível em H."
Note que já demonstramos que $(p, 0)$ é um elemento central de H, logo se $(p, 0)$ não é primo, então $(p, 0)$ não é irredutível em H.
Vamos mostrar então que $(p, 0)$ não é um elemento primo em H.
Como p é um número primo, por ([7], Teorema $5.1.3$, pg 108) existem $a, b \in \mathbb{Z}$ tais que $p|(a^2 + b^2 + 1)$. Desse modo, existe $x \in \mathbb{Z}$ tal que $px = a^2 + b^2 + 1$. Em conseqüência temos:

$$\begin{aligned}(p, 0) \otimes (x, 0) &= (a^2 + b^2 + 1, 0) \\ &= (a + bi, 1) \otimes (a - bi, -1), \\ &\Longrightarrow (p, 0)|(a + bi, 1) \otimes (a - bi, -1).\end{aligned}$$

Suponha que exista $(c+di, f+gi) \in H$ tal que

$$(p,0) \otimes (c+di, f+gi) = (a+bi, 1).$$

Então temos:

$$(pc+pdi, pf+pgi) = (a+bi, 1).$$

Logo, $pf+pgi = 1$, ou seja, $pf = 1$ e $pg = 0$. Mas isto implica que $p \in \mathcal{U}(\mathbb{Z})$. Absurdo. Portanto $(p,0) \nmid (a+bi, 1)$.
Suponha agora, que exista $(m+li, n+hi) \in H$ tal que

$$(p,0) \otimes (m+li, n+hi) = (a-bi, -1).$$

Analogamente, isto infere que $p \in \mathcal{U}(\mathbb{Z})$. Então, $(p,0) \nmid (a-bi, -1)$ e portanto $(p,0)$ não é primo.

■

Teorema 4.1. *Se $p \in \mathbb{N}$ é um número primo então existem inteiros $a, b, c, d \in \mathbb{Z}$ tais que $4p = a^2 + b^2 + c^2 + d^2$.*

Demonstração. Como $(p,0)$ não é irredutível em H, existem $(\alpha, \beta), (\gamma, \delta) \in H$ tais que:

$$(p,0) = (\alpha,\beta) \otimes (\gamma,\delta) \text{ e } (\alpha,\beta), (\gamma,\delta) \notin \mathcal{U}(H).$$

Conseqüentemente,

$$p^2 = \varphi((p,0)) = \varphi((\alpha,\beta)).\varphi((\gamma,\delta)).$$

E então, como p é irredutível em $\mathbb{Z}$, temos as seguintes possibilidades:

$$p = \varphi((\alpha,\beta)) \text{ e } p = \varphi((\gamma,\delta)) \ (*) \text{ ou}$$

$$p^2 = \varphi((\alpha,\beta)) \text{ e } 1 = \varphi((\gamma,\delta)) \quad (**).$$

Note que $(**)$ leva a um absurdo, pois infere que (γ, δ) é um elemento inversível, como vimos na Proposição 4.8. Logo, temos que $p = \varphi((\alpha,\beta))$.
Como $(\alpha,\beta) \in H$ temos que $(\alpha,\beta) = \left(\frac{a}{2} + \frac{b}{2}i, \frac{c}{2} + \frac{d}{2}i\right)$ e então:

$$p = \varphi((\alpha,\beta)) = \frac{a^2+b^2+c^2+d^2}{4}$$

$$\Longrightarrow 4p = a^2 + b^2 + c^2 + d^2.$$

■

Teorema 4.2. *Seja $n \in \mathbb{N}$ tal que $2n$ é uma soma de quatro quadrados de inteiros positivos. Então n também é uma soma de quatro quadrados de inteiros.*

Demonstração. Se $n \in \mathbb{N}$ é tal que $2n = a^2 + b^2 + c^2 + d^2$, $a, b, c, d, \in \mathbb{Z}$ então:

$$n = \frac{a^2 + b^2 + c^2 + d^2}{2}$$

$$= \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2.$$

Note que, para mostrarmos que $\left(\frac{a+b}{2}\right), \left(\frac{a-b}{2}\right), \left(\frac{c+d}{2}\right), \left(\frac{c-d}{2}\right) \in \mathbb{Z}$,

basta mostrarmos que $a \equiv b (\text{mod } 2)$ e $c \equiv d (\text{mod } 2)$.
Por hipótese, $2n = a^2 + b^2 + c^2 + d^2$. Conseqüentemente temos as seguintes possibilidades de paridade para a, b, c e d.

	a	b	c	d
Caso 1	par	par	par	par
Caso 2	par	par	ímpar	ímpar
Caso 3	par	ímpar	par	ímpar
Caso 4	par	ímpar	ímpar	par
Caso 5	ímpar	ímpar	par	par
Caso 6	ímpar	ímpar	ímpar	ímpar
Caso 7	ímpar	par	par	ímpar
Caso 8	ímpar	par	ímpar	par

Nos casos $1, 2, 5$ e 6 temos $a \equiv b (\text{mod } 2)$ e $c \equiv d (\text{mod } 2)$. Nos outros casos, sempre temos 2 elementos pares e dois ímpares. Logo, basta denotar os dois elementos pares como sendo a e b e os dois ímpares como sendo c e d. Deste modo, também teremos $a \equiv b (\text{mod } 2)$ e $c \equiv d (\text{mod } 2)$.
Portanto, n é soma de quatro quadrados de inteiros.

■

Teorema 4.3. *Se $p \in \mathbb{N}$ é um número primo, então p é uma soma de quatro quadrados de inteiros.*

Demonstração. Se $p \in \mathbb{N}$ é um número primo, então pelo Teorema 4.1 temos:

$$4p = a_1^2 + b_1^2 + c_1^2 + d_1^2;\ a_1, b_1, c_1, d_1 \in \mathbb{Z}.$$

Mas então, pelo Teorema 4.2, obtemos:

$$2p = a_2^2 + b_2^2 + c_2^2 + d_2^2;\ a_2, b_2, c_2, d_2 \in \mathbb{Z}.$$

E portanto, novamente pelo Teorema 4.2, temos:

$$p = a^2 + b^2 + c^2 + d^2;\ a, b, c, d \in \mathbb{Z}.$$

■

Teorema 4.4. *Se $m, n \in \mathbb{N}$ são somas de quatro quadrados de inteiros, então $m.n$ é soma de quatro quadrados de inteiros.*

Demonstração. Se $m, n \in \mathbb{N}$ são tais que

$$n = a_1^2 + b_1^2 + c_1^2 + d_1^2 \text{ e}$$

$$m = a_2^2 + b_2^2 + c_2^2 + d_2^2$$

então

$$\begin{aligned} n.m &= (a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) \\ &= \varphi((a_1 + ib_1, c_1 + id_1))\varphi((a_2 + ib_2, c_2 + id_2)) \\ &= \varphi((a_1 + ib_1, c_1 + id_1)(a_2 + ib_2, c_2 + id_2)) \\ &= \varphi(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i, \\ &\qquad a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2 + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)i) \\ &= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)^2 + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)^2 + \\ &\qquad + (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)^2 + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)^2. \end{aligned}$$

Portanto $n.m$ é uma soma de quatro quadrados de inteiros.

■

Teorema 4.5. *Todo inteiro positivo é uma soma de quatro quadrados de inteiros.*

Demonstração. Seja $x \in \mathbb{Z}_+^*$.
Se $x \in \mathcal{U}(\mathbb{Z})$ então $x = 1$ e neste caso $1 = 1^2 + 0^2 + 0^2 + 0^2$.
Se $x \notin \mathcal{U}(\mathbb{Z})$ então, como $\mathbb{Z}$ é domínio fatorial, podemos tomar a fatoração em elementos primos de x:

$$x = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Pelo Teorema 4.3, $p_1, p_2, \cdots, p_r$, são somas de quatro quadrados de inteiros. Logo, aplicando-se sucessivamente o Teorema 4.4 obtemos que x é uma soma de quatro quadrados de inteiros.

■

Considerações Finais

No primeiro capítulo, além de mostrarmos que todo domínio euclidiano é principal e que todo domínio principal é fatorial, mostramos como a existência e unicidade do mdc se comportam nestas estruturas: Em um anel, o mdc, quando existir, pode não ser único. Em um domínio, quando existir, o mdc é único a menos de elementos associados. Em um domínio principal o $mdc(a, b)$ sempre existe e existem também e e f tais que $ae + bf = mdc(a, b)$. Em um domínio euclidiano, além do $mdc(a, b)$, e e f sempre existirem, podemos calculá-los efetivamente, graças a propriedade euclidiana.

No segundo, respondemos ao problema 8 da "Aritmética" e como conseqüência, caracterizamos todos os inteiros que podem ser escritos como a soma de dois quadrados.

No terceiro capítulo, reduzimos o Último Teorema de Fermat ao caso onde m é um número primo.

No quarto, mostramos que todo número inteiro positivo pode ser escrito como a soma de quatro quadrados. Pelos resultados do Capítulo 2, todo quadrado pode ser escrito como a soma de dois quadrados. Logo todo número inteiro positivo pode ser escrito como a soma de 4 ou 5 ou 6 ou 7 ou 8.... quadrados, onde claramente alguns dos quadrados serão nulos.

Para finalizar, salientamos a importância da transferência de problemas de uma estrutura para outra, onde o problema torna-se, de certa forma, mais simples.

Referências Bibliográficas

[1] GARCIA, Arnaldo; LEQUAIN, Yves - *Elementos de Álgebra*. 2ª edição, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2003.

[2] HERSTEIN, L. H. - *Tópicos de Álgebra*. Ed. Polígono, 1970.

[3] MONTEIRO, L.H. Jacy - *Elementos de Álgebra*. 2ª edição, LTC, Rio de Janeiro, 1978.

[4] DOMINGUES, Hygino H. - *Fundamentos de ARITMÉTICA*. Ed. Record, São Paulo, 1991.

[5] SINGH, Simon - *O Último Teorema de Fermat*. 7ª edição, Ed. Record, 2000.

[6] BOYER, Carl B. - *História da Matemática*. Ed. Edgar Blücher, São Paulo, 1974.

[7] SANTOS, José Plínio de Oliveira - *Introdução à Teoria dos Números*. Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1988.

[8] EVES, Howard - *Introdução à História da Matemática*. 2ª edição, Ed. da UNICAMP, São Paulo, 1995.