Instituto de Matemática e Estatística – UERJ

O Último Teorema de Fermat

Autor: Daniel Cunha da Silva

Orientador: Rodrigo Salomão

Rio de Janeiro
Março de 2010

Agradecimentos

Conteúdo

Capítulo 1

Introdução

Um dos problemas mais famosos na matemática foi levantado por Pierre de Fermat (1601–1665), um dos maiores teórico dos números do século 17, e que constava na margem de sua cópia pessoal do livro chamado Diophantus. Traduziremos abaixo suas palavras que constavam nesta margem.

> É impossível resolver um cubo em (soma de) dois cubos, uma potência quarta em duas potências quartas, ou em geral, qualquer potência maior que a segunda em duas potências do mesmo tipo. Encontrei uma prova notável deste fato, mas a margem é muito pequena para contê-la.

Mais precisamente, Fermat afirmou que não existem números naturais x, y, z, todos não nulos, satisfazendo a seguinte equação Diophantina

$$x^n + y^n = z^n \tag{1.1}$$

onde n é um numero natural maior que 2.

Ao longo do século 19 todas as afirmações deixadas por Fermat foram sendo resolvidas, inclusive o surgimento de um contra-exemplo para uma conjectura falsa que afirmava que os números da forma $F_n = 2^{2^n} + 1$ são primos, onde n percorre os números naturais; de fato, F_5 é divisível por 641. A única afirmação remanescente e que desafiou a força de muitos matemáticos, foi a enunciada acima, que ficou conhecida como "*Último Teorema de Fermat*".

O primeiro a provar o caso $n = 3$ foi Leonhard Euler (1706–1783). Entretanto, em sua primeira tentativa de prova foi usado que o conjunto dos números da forma $x + y\sqrt{-3}$, com x, y inteiros, possuía propriedades parecidas com a dos números inteiros, como a unicidade da fatoração. Mas isto não era conhecido na época, o que o levou a fazer outra demonstração do caso $n = 3$.

A segunda pessoa a contribuir com novas idéias foi Sophie Germain (1776–1831). Tal contribuição se deu em duas partes. Primeiro ela trabalhou no caso em

que n e $2n + 1$ são primos, como por exemplo: 2, 3, 5, 11, 23, 29, 41, 43, 83, 89, 113, 131. Ela provou que se existe solução da equação (1.1), para um tal primo n, então x, y ou z deve ser um múltiplo de n. Sendo assim, ela dividiu o problema em dois casos:

1. Nenhum dos números x, y, z são divisíveis por n;

2. Somente um dos números x, y, z é divisível por n.

Ela provou o Último Teorema de Fermat para o caso (1) e Legendre (1752–1833) generalizou este caso para primos ímpares p tais que $kp + 1$ é primo, onde $k = 4, 8, 10, 14$ e 16. Desta forma, as atenções foram voltadas para o caso (2), que teve a primeira contribuição dada por Dirichlet (1805–1859) e Legendre, provando o caso $n = 5$. Dirichlet ainda conseguiu provar o caso $n = 14$, enquanto Lamé (1796–1870) provou o caso $n = 7$. Entretanto, este último caso requeria uma computação muito mais difícil que os outros casos, o que deixou a impressão que deveria ser mudado o foco na abordagem para obter mais sucesso na obtenção do caso geral. Foi quando Lamé, em 1847, anunciou que tinha provado o Último Teorema de Fermat. Sua idéia baseava-se em introduzir a raiz n-ésima da unidade $\zeta = e^{2\pi i/n}$, para fatorar a equação (1.1) em termos lineares:

$$x^n + y^n = (x + y)(x + \zeta y) \cdots (x + \zeta^{n-1} y).$$

Entretanto, Liouville (1809–1882) observou que esta idéia necessitava de uma fatoração única no conjunto dos números da forma $a_0 + a_1\zeta + \cdots + a_k\zeta^k$, com $a_1, \ldots, a_k$ números inteiros e k natural. Tão logo as atenções se voltaram para esta unicidade da fatoração. Apesar de alguns matemáticos terem obtido êxito nesta questão, foi Kummer (1810–1893), três anos antes, quem deu a maior contribuição. Ele provou que a unicidade da fatoração pode não ocorrer em certos casos, como por exemplo para $n = 23$, e ainda introduziu os "números ideais" que funcionavam para o estudo deste problema e que sempre podiam ser fatorados de maneira única. Em uma linguagem mais atual, estes números ideais correspondem aos ideais de um anel, como foi introduzido por Dedekind. Em 1850, Kummer provou o Último Teorema de Fermat para o que ele denominou por primos regulares, o que incluía todos os primos menores que 100, exceto 37, 59, 67. Ele até chegou a conjecturar a existência de infinitos destes primos, mas o máximo que se obteve foi a existência de infinitos primos irregulares, devido a Jensen em 1915. A partir 1920, a obtenção de métodos de aproximação computacional tornou possível abordar o Último Teorema de Fermat para inteiros muito grandes. Por exemplo, até 1993 o recorde estava em $n \leq 4.000.000$. Apesar desta abordagem não ter fornecido a prova do Último Teorema de Fermat em sua maior generalidade, ela deu um fabuloso passo inicial para a fundamentação de resultados, até então intuitivos, obtidos

na área da Geometria Algébrica. É importante destacar que a demonstração completa do Último Teorema de Fermat foi obtida por Andrew Wiles, após trezentos anos de pesquisas, e utiliza conceitos geométricos de curvas elípticas e funções modulares. Para uma breve visão sobre esta prova sugerimos [ST] seção 14.7.

O objetivo principal desta monografia será de demonstrar exatamente este caso particular do Último Teorema de Fermat, para primos regulares, devido a Kummer. Porém já iremos utilizar esta linguagem mais atual de ideais devido a Dedekind. No segundo capítulo iremos fazer a demonstração do Último Teorema de Fermat para $n = 4$, que utiliza apenas conceitos básicos de números inteiros, como por exemplo o conceito de divisibilidade. No terceiro capítulo introduziremos as definições e os resultados essenciais que são pré-requisitos para definirmos o conceito de primos regulares, como por exemplo a definição de números inteiros e o anel dos inteiros algébricos de um corpo de números, isto é, uma extensão finita do corpo dos números racionais. Já no quarto capítulo iremos fazer um estudo de algumas propriedades aritméticas, como o estudo dos elementos invertíveis do anel dos inteiros algébricos de um corpo de números ciclotômico, isto é, o corpo obtido pela adjunção de uma raiz primitiva p-ésima da unidade ao corpo dos números racionais, onde p é um número inteiro primo. O quinto e último capítulo é dedicado a demonstração do Último Teorema de Fermat no caso em que o expoente é um primo regular, que utiliza este estudo aritmético feito no capítulo anterior.

Capítulo 2

Considerações Elementares

Consideramos o que pode ser dito sobre a Equação de Fermat

$$x^n + y^n = z^n. \tag{2.1}$$

Se existir uma solução inteira não-nula da Equação (2.1), então deve existir uma solução na qual x, y, z sejam dois a dois primos entre si. Porque se um primo q divide x e y, então $x = qx'$, $y = qy'$,

$$q^n(x'^n + y'^n) = z^n$$

de modo que q divide z, digamos $z = qz'$, e então $x'^n + y'^n = z'^n$. De modo similar se q divide x, z ou y, z. Desta forma podemos eliminar todos os fatores em comum de x, y e z.

Em seguida, note que se a Equação (2.1) não tiver solução inteira para um expoente n, então não haverá solução para todos os múltiplos de n. De fato, se $x^m + y^{mn} = z^{mn}$, então $(x^m)^n + (y^m)^n = (z^m)^n$. Agora qualquer inteiro $n \geq 3$ é divisível por 4 ou por um primo ímpar. Daí para provar a conjectura é suficiente considerar os casos $n = 4$ e n um primo ímpar.

Começamos com a prova do Último Teorema de Fermat para $n = 4$. É com base da solução geral da conhecida Equação de Pitágoras $x^2 + y^2 = z^2$, dada por:

Lema 2.1. *AS soluções inteiras de $x^2 + y^2 = z^2$, com x, y, z dois a dois primos entre si, é dada parametricamente, a menos de permutação entre x e y, por*

$$\begin{aligned} \pm x &= 2rs \\ \pm y &= r^2 - s^2 \\ \pm z &= r^2 + s^2, \end{aligned}$$

onde r, s são primos entre si e exatamente um deles é ímpar.

Prova: É suficiente consideramos x, y, z positivos. Eles não podem ser todos ímpares, pois isso nos daria a contradição "ímpar + ímpar = ímpar". Uma vez que eles são dois a dois primos entre si, isso significa precisamente que um deles é par. Não pode ser z, pois então $z = 2k, x = 2a + 1, y = 2b + 1$ onde k, a, b são inteiros e

$$(2a + 1)^2 + (2b + 1)^2 = 4k^2.$$

Isso não pode ocorrer uma vez que o lado esquerdo é claramente não divisível por 4 enquanto o lado direito é. Portando, x ou y é par. Podemos supor que este é x. Então

$$x^2 = z^2 - y^2 = (z + y)(z - y).$$

Consequentemente x, $z + y$ e $z - y$ são todos pares e positivos, e logo, podemos escrever $x = 2u, z + y = 2v, z - y = 2w$, donde

$$(2u)^2 = 2v \cdot 2w$$

ou

$$u^2 = vw. \tag{2.2}$$

Agora v, w são primos entre si, pois um fator comum de v e w dividiria a sua soma $v + w = z$ e a sua diferença $v - w = y$, que não pode ocorrer, já que, y e z são primos entre si. Fatorando u, v, w em fatores primos, vemos que (2.2) implica que w, v são quadrados, digamos $v = r^2, w = s^2$. Além disso, r e s são primos entre si porque v e w são. Isto é

$$\begin{aligned} z &= v + w = r^2 + s^2 \\ y &= v - w = r^2 - s^2. \end{aligned}$$

Porque y, z são ambos ímpares, precisamente ou r é ímpar ou s é. Finalmente

$$x^2 = z^2 - y^2 = (r^2 + s^2)^2 - (r^2 - s^2)^2 = 4r^2s^2,$$

assim $x = 2rs$. □

Agora mostraremos um teorema mais forte do que a impossibilidade da Equação (2.1) para $n = 4$.

Teorema 2.1. *A equação $x^4 + y^4 = z^2$ não possui solução inteira com x, y, z não-nulos.*

Prova: Primeiro note que este resultado é mais forte, pois se $x^4 + y^4 = z^4$ então x, y, z^2 satisfazem a equação acima.

Suponha que exista solução da Equação

$$x^4 + y^4 = z^2. \tag{2.3}$$

Podemos assumir que x, y, z são positivos. Entre as soluções há uma na qual z é o menor dentre todas as soluções. Assumiremos que (2.3) seja esta. Então x, y, z são primos entre si, pois caso contrario poderíamos cancelar os fatores comuns deixando z ainda menor, o que contradiz a suposição. E pelo Lema (2.1) temos

$$x^2 = r^2 - s^2, \quad y^2 = 2rs \text{ e } z = r^2 + s^2$$

onde x e z são ímpares e y é par. A primeira delas implica

$$x^2 + s^2 = r^2$$

com x, s primos entre si. Novamente como x é ímpar temos pelo Lema (2.1) que

$$x = a^2 - b^2, s = 2ab, r = a^2 + b^2.$$

Agora observando que $y^2 = 2rs = 2 \cdot 2ab(a^2 + b^2)$ temos que y é par e podemos escrever que $y = 2k$, onde $k^2 = ab(a^2 + b^2)$. Uma vez que a, b e $a^2 + b^2$ são primos entre si temos $a = c^2, b = d^2$ e $a^2 + b^2 = e^2$ de modo que

$$c^4 + d^4 = e^2.$$

Esta é uma equação da forma de (2.3), mas $e \leq a^2 + b^2 = r < z$, contrariando a minimalidade de z. □

Capítulo 3

Noções Sobre Teoria Algébrica dos Números

Neste capítulo iremos estabelecer os conceitos e fatos mais importantes, da teoria de corpos e da teoria algébrica dos números, que servem como base para a demonstração do caso particular do último Teorema de Fermat. Entretanto, faremos poucas verificações neste capítulo, já que, o conteúdo presente aqui faz parte de cursos introdutórios em teoria de corpos e em teoria algébrica dos números. Para uma visão mais detalhada sobre teoria de corpos, o leitor pode consultar [E1] e [L]. Já para uma visão sobre teoria algébricas dos números, sugerimos [R], [E2] e [ST].

Sejam $R \subset S$ anéis e $\alpha \in S$. Dizemos que $\alpha \in S$ é um *inteiro algébrico* (ou simplesmente *inteiro*) sobre R quando α anula um polinômio mônico em $R[x]$, isto é, existem $a_1, \ldots, a_n \in R$ tais que

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0.$$

No caso em que R e S são corpos, também conhecemos, da teoria de corpos, um elemento inteiro por elemento algébrico.

Exemplo 3.1. Seja n um inteiro positivo. O número complexo $e^{\frac{2\pi i}{n}}$ é um inteiro algébrico sobre $\mathbb{Z}$. De fato, $e^{\frac{2\pi i}{n}}$ anula o polinômio $x^n - 1$. No caso em que $n \neq 1$ temos ainda que $e^{\frac{2\pi i}{n}}$ anula

$$x^{n-1} + x^{n-2} + \cdots + x + 1,$$

já que, $x^n - 1 = (x-1) \cdot (x^{n-1} + x^{n-2} + \cdots + x + 1)$. Quando $n = p$ é um primo ímpar e $\zeta = e^{\frac{2\pi i}{p}}$ temos que

$$P_{\zeta|\mathbb{Q}}(x) := x^{p-1} + x^{p-2} + \cdots + x + 1 = \prod_{i=1}^{p-1}(x - \zeta^i)$$

é o polinômio irredutível, mônico e de menor grau que anula ζ. Um tal polinômio é chamado de *polinômio mínimo* de ζ.

É possível provar que o conjunto dos elementos de S, inteiros sobre R, digamos

$$I_S(R) = \{\alpha \in S | \alpha \text{ é inteiro sobre } R\},$$

é um subanel anel de S (ver [E2] Corolário 1.3, pg. 11). Este subanel é denominado por *anel dos inteiros algébricos* de S sobre R.

Dizemos que o domínio R é *integralmente fechado* quando $I_S(R) = R$, onde S é o corpo quociente de R.

Exemplo 3.2. $\mathbb{Z}$ é integralmente fechado (ver [E2], Teorema 1.6 pg. 12).

Se $R = \mathbb{Z}$ e L for um *corpo de números*, isto é, uma extensão finita de $\mathbb{Q}$, então denotaremos o conjunto dos inteiros algébricos de L sobre $\mathbb{Z}$ por

$$I_L = \{\alpha \in L | \alpha \text{ é inteiro algébrico}\},$$

que será chamado simplesmente por *anel dos inteiros algébricos* de L.

Antes de dar um exemplo de anel dos inteiros algébricos de um corpo de números vamos fazer uma breve revisão sobre algumas ferramentas importantes da teoria de corpos.

Consideremos K um corpo. Da teoria dos corpos podemos construir, a menos de isomorfismos, um corpo $\overline{K}$ contendo K, que é chamado de *fecho algébrico* de K e satisfaz:

1. Todo $P(x) \in K[x]$ pode ser fatorado, em $\overline{K}[x]$, em fatores de grau 1;
2. Todo elemento de $\overline{K}$ anula um polinômio em $K[x]$;
3. Os polinômios irredutíveis em $\overline{K}[x]$ têm grau 1.

Um polinômio $P(x)$ é dito *separável* quando todas as suas raízes são distintas. Equivalentemente, $P(x)$ e a sua derivada $D(P(x))$ são primos entre si (ver [E1], (3.2) pg. 53). Dizemos que $\alpha \in \overline{K}$ é *separável* sobre K quando seu polinômio mínimo $P_{\alpha|K}(x) \in K[x]$ é separável. Daí chegamos ao conceito de extensão separável. De fato, seja $L|K$ uma extensão algébrica de corpos, isto é, $L \subset \overline{K}$ a menos de isomorfismos. Dizemos que $L|K$ é *separável* quando todos os elementos de L são separáveis sobre K.

Exemplo 3.3. Toda extensão algébrica do corpo dos números racionais $\mathbb{Q}$ é separável (ver [E1], (3.6) pg. 55).

Além disso, certas extensões algébricas e separáveis satisfazem de uma propriedade muito particular, como podemos ver no teorema a seguir, cuja demonstração encontre-se em [E1], (3.17) pg. 63.

Teorema 3.1 (Teorema do elemento primitivo)**.** *Toda extensão finita e separável L de K é da forma $L = K(\alpha)$, para algum $\alpha \in L$.*

Seja $L = K(\alpha)$ uma extensão separável de K, de grau n. É possível verificar que existem exatamente n isomorfismos de $K(\alpha)$ em $\overline{K}$, que fixam K (cf. [E1], (3.11) pg. 58). Digamos $\sigma_1, \sigma_2, \ldots, \sigma_n$. Dado $\beta \in K(\alpha)$ definimos o *traço* de β, relativo a extensão $L|K$, por

$$Tr_{L|K}(\beta) = \sigma_1(\beta) + \cdots + \sigma_n(\beta) \in K$$

e definimos *norma* de β, relativo a extensão $L|K$, por

$$N_{L|K}(\beta) = \sigma_1(\beta) \cdots \sigma_n(\beta) \in K.$$

Segue direto da definição de homomorfismo que o traço e a norma satisfazem das seguinte propriedades:

$$Tr_{L|K}(\beta_1 + \beta_2) = Tr_{L|K}(\beta_1) + Tr_{L|K}(\beta_2) \text{ e } N_{L|K}(\beta_1 \cdot \beta_2) = N_{L|K}(\beta_1) \cdot N_{L|K}(\beta_2),$$

onde $\beta_1, \beta_2 \in L$.

Observamos que o cálculo do traço e da norma de α, relativo a extensão $L|K$, pode ser feito a partir de seu polinômio mínimo, digamos

$$P_{\alpha|K}(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1}x + a_n.$$

De fato,

$$Tr_{L|K}(\alpha) = -a_1 \text{ e } N_{L|K}(\alpha) = (-1)^n a_n,$$

já que, $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ são todas as raízes de $P_{\alpha|K}(x)$.

Além disso, o polinômio mínimo ainda pode ser útil para saber se um elemento de um corpo de números é inteiro sobre $\mathbb{Z}$.

Proposição 3.1. *O elemento β do corpo de números L é inteiro sobre $\mathbb{Z}$ se, e somente se, $P_{\beta|K}(x) \in \mathbb{Z}[x]$.*

Exemplo 3.4. No caso em que $\zeta = e^{\frac{2\pi i}{p}}$, onde p é um primo ímpar, e $L = \mathbb{Q}(\zeta)$ é o p-ésimo corpo ciclotômico, temos que os isomorfismos de $L|\mathbb{Q}$, digamos $\sigma_1, \sigma_2, \ldots, \sigma_{p-1}$, são definidos por

$$\sigma_i(\zeta) = \zeta^i \text{ e } \sigma_i(x) = x \text{ para todo } x \in \mathbb{Q}$$

onde $i = 1, \ldots, p-1$ (ver [E1], Teorema (7.15) pg. 116). Como o polinômio mínimo de ζ é $P_{\zeta|\mathbb{Q}}(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ obtemos que

$$Tr_{L|K}(\zeta) = -1 \text{ e } N_{L|K}(\zeta) = 1.$$

Antes de calcular o anel dos inteiros algébricos do corpo de números $\mathbb{Q}(\zeta)$ vamos fixar algumas notações.

Primeiramente consideraremos o anel

$$\mathbb{Z}[\zeta] := \{f(\zeta) \mid f(x) \in \mathbb{Z}[x]\}.$$

Como o polinômio $P_{\zeta|\mathbb{Q}}(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ anula ζ temos que

$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2} \mid a_0, \ldots, a_{p-2} \in \mathbb{Z}[x]\}.$$

O conjunto da direita, na igualdade acima, também é denotado por

$$\mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{p-2}.$$

É interessante observar que tal notação provém da teoria dos módulos finitamente gerados. Além disso, como $P_{\zeta|\mathbb{Q}}(x)$ é o polinômio mônico de menor grau que anula ζ, temos que a escrita de um elemento de $\mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{p-2}$ é unicamente determinada pelos coeficientes em $\mathbb{Z}$. Neste caso, para diferir a notação, denotamos o conjunto $\mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{p-2}$ por

$$Z \oplus \mathbb{Z}\zeta \oplus \cdots \oplus \mathbb{Z}\zeta^{p-2}.$$

É importante observar que a minimalidade do grau de $P_{\zeta|\mathbb{Q}}(x)$ ainda nos diz que $\{1, \zeta, \ldots, \zeta^{p-2}\}$ é uma base da extensão de corpos $\mathbb{Q}(\zeta)|\mathbb{Q}$, isto é, uma base do $\mathbb{Q}$-espaço vetorial $\mathbb{Q}(\zeta)$. Tal base é chamada de *base integral* pois todos os seus elementos são inteiros sobre $\mathbb{Z}$.

Agora estamos em condições de calcular o anel dos inteiros algébricos do corpo de números $\mathbb{Q}(\zeta)$.

Proposição 3.2. *O anel dos inteiros algébricos de $\mathbb{Q}(\zeta)$ é igual a $\mathbb{Z}[\zeta]$.*

Prova: Primeiramente afirmamos que $1 - \zeta$ e $1 - \zeta^j$ são associados em $I_{\mathbb{Q}(\zeta)}$. De fato, $1-\zeta$ divide $1-\zeta^j$ em $I_{\mathbb{Q}(\zeta)}$, já que, $1-\zeta^j = (1-\zeta)(\zeta^{j-1} + \cdots + \zeta + 1)$. Por outro lado, podemos escolher um inteiro positivo t tal que $jt \equiv 1 \pmod{p}$. Então, temos de forma análoga que $1 - \zeta^j$ divide $1 - \zeta^{jt} = 1 - \zeta$. Logo eles são associados.

Portanto,

$$p = P_{\zeta|\mathbb{Q}}(1) = \prod_{i=1}^{p-1}(1 - \zeta^i) = u(1 - \zeta)^{p-1},$$

com u invertível em $I_{\mathbb{Q}(\zeta)}$. Desta forma o elemento $1 - \zeta$ não é invertível em $I_{\mathbb{Q}(\zeta)}$, pois caso contrário p teria inverso, que pertenceria a $I_{\mathbb{Q}(\zeta)} \cap \mathbb{Q} = \mathbb{Z}$, já que, $\mathbb{Z}$ é integralmente fechado.

Dado $x \in I_{\mathbb{Q}(\zeta)}$, existem números racionais $a_0, \ldots, a_{p-2}$ unicamente determinados de modo que:

$$x = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}.$$

Mostraremos que cada $a_i \in \mathbb{Z}$. Para isso, multiplicamos a igualdade anterior por ζ e obtemos:

$$x\zeta = a_0\zeta + a_1\zeta^2 + \cdots + a_{p-2}\zeta^{p-1}.$$

Subtraindo as igualdades anteriores, obtemos

$$x(1-\zeta) = a_0(1-\zeta) + a_1(\zeta - \zeta^2) + \cdots + a_{p-2}(\zeta^{p-2} - \zeta^{p-1}).$$

Notemos que o traço relativo extensão $\mathbb{Q}(\zeta)|\mathbb{Q}$, que denotaremos simplesmente por Tr, de $\zeta, \zeta^2, \cdots, \zeta^{p-1}$ são todos iguais, uma vez que esses elementos são dois a dois conjugados, isto é, ambos possuem o mesmo polinômio mínimo $P_{\zeta,\mathbb{Q}}$. Por isso

$$Tr(x(1-\zeta)) = Tr(a_0(1-\zeta)) = a_0 Tr(1-\zeta) = a_0[(p-1)+1] = a_0 p. \qquad (3.1)$$

Para mostrar que $a_0 \in \mathbb{Z}$, calcularemos $Tr(x(1-\zeta))$. Denotaremos x por x_1 e $x_2, \cdots, x_{p-1} \in I_{\mathbb{Q}(\zeta)}$ seus conjugados. Assim

$$\begin{aligned} Tr(x(1-\zeta)) &= x_1(1-\zeta) + x_2(1-\zeta^2) + \cdots + x_{p-1}(1-\zeta^{p-1}) \\ &= (1-\zeta)x' \in <1-\zeta> \end{aligned}$$

onde $<1-\zeta>$ é o ideal de $I_{\mathbb{Q}(\zeta)}$ gerado por $1-\zeta$. Mas $Tr(x(1-\zeta)) \in I_{\mathbb{Q}(\zeta)} \cap \mathbb{Q} = \mathbb{Z}$. Segue então que $Tr(x(1-\zeta)) \in <1-\zeta> \cap \mathbb{Z} = \mathbb{Z}p$, e logo, por (3.1), temos que $a_0 \in \mathbb{Z}$.

Agora mostraremos por indução que qualquer $a_1, \cdots, a_{p-2} \in \mathbb{Z}$. Para provar que $a_j \in \mathbb{Z}$ multiplicamos x por ζ^{p-j}, obtendo

$$x\zeta^{p-j} = a_0\zeta^{p-j} + a_1\zeta^{p-j+1} + \cdots + a_{j-1}\zeta^{p-1} + a_j + a_{j+1}\zeta + \cdots + a_{p-2}\zeta^{p-j-2}. \quad \square$$

Agora vamos prosseguir com as definições e os fatos que necessitamos no decorrer do trabalho.

Dizemos que um anel A é *Noetheriano* quando todo ideal de A é finitamente gerado.

Exemplo 3.5. O anel $\mathbb{Z}[\zeta]$ é Noetheriano, como consequência de [E2], Corolário 7.12 pg. 68.

Observação 3.1.

1. $\mathbb{Z}[\zeta]$ é subanel do corpo $\mathbb{Q}(\zeta)$ e portanto é um domínio;
2. $\mathbb{Z}[\zeta]$ é integralmente fechado, pois $I_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$;
3. Todo ideal primo não-nulo em $\mathbb{Z}[\zeta]$ é maximal. Isto segue como consequência imediata de [E2], Corolário 1.13 pg. 16.

Segue da observação acima e do exemplo anterior que $\mathbb{Z}[\zeta]$ satisfaz a definição abaixo.

Um domínio A é dito domínio de *Dedekind* quando ele satisfaz uma das seguintes condições equivalentes:

1. A é Noetheriano, integralmente fechado e todo ideal primo não-nulo de A é maximal;

2. Todo ideal não-nulo de A é escrito como produto de ideais primos, de forma única;

3. O conjunto dos ideais fracionários de A forma um grupo multiplicativo.

Observação 3.2. 1. Primeiramente vamos definir o conceito de ideal fracionário e a estrutura de grupo do conjunto formado por estes objetos. Um grupo abeliano M, escrito aditivamente e munido de uma operação externa (usualmente denotada pela multiplicação), é dito um A-*módulo* quando ele satisfaz das seguintes propriedades:

$$\begin{aligned} a \cdot (x + y) &= a \cdot x + a \cdot y \\ (a + b) \cdot x &= a \cdot x + b \cdot x \\ (a \cdot b) \cdot x &= a \cdot (b \cdot x) \\ 1 \cdot x &= x \end{aligned}$$

Seja K o corpo de frações do domínio A. Um A-módulo $M \subset K$ é dito *ideal fracionário* de A quando existe $d \in A$, não-nulo, tal que $d \cdot M \subset A$. Já o produto de dois ideais fracionários M e N é definido por

$$M \cdot N := \left\{ \sum_{i=1}^{s} m_i \cdot n_i \mid m_i \in M, n_i \in N \text{ e } s \in \mathbb{N} \right\}.$$

2. Para ver que as três condições acima são equivalentes sugerimos como referência [R], Teorema 1 pg. 125.

3. Ainda pode ser verificado que o anel dos inteiros algébricos I_L de um corpo de números L também é um domínio de Dedekind (ver [E2], Corolário 8.2 pg. 70).

Seja J um ideal de um domínio de Dedekind A, bem como sua fatoração em ideais primos

$$J = P_1^{r_1} \cdots P_n^{r_n}.$$

Pelo Teorema Chinês dos Restos (ver [R], Teorema 3 pg. 131) temos um isomorfismo entre anéis quociente

$$\frac{A}{J} \simeq \prod_{i=1}^{n} \frac{A}{P_i^{r_i}}.$$

Como podemos ver em [E2], (9.4) pg. 84, temos que os quocientes $A/P_i^{r_i}$ são finitos. Logo a cardinalidade de A/J é a soma das cardinalidades dos quocientes $A/P_i^{r_i}$. Desta forma, definimos a *norma* $N(J)$ de um ideal J de A, pela seguinte cardinalidade.

$$N(J) := \sharp\,(A/J)$$

No caso em que $J =< y >$ é um ideal principal do anel dos inteiros algébricos I_L de um corpo de números L temos a seguinte igualdade (ver [E2], Teorema 9.7 pg. 85).

$$N(J) = |N_{L|\mathbb{Q}}(y)|.$$

Consideremos agora A um domínio de Dedekind e K seu corpo de frações. Denotemos por $\mathscr{F}$ o grupo dos ideais fracionários de A. Um ideal fracionário M é dito *principal* quando existe $y \in K$ tal que $M = yA$. Claramente, o subconjunto $\mathscr{P}$ de $\mathscr{F}$, formado pelos ideais fracionários e principais de A é um subgrupo de $\mathscr{F}$. O subgrupo quociente

$$\mathscr{C} := \mathscr{F}/\mathscr{P}$$

é denominado por *grupo de classes de ideais* de A. Sua ordem, denotada por

$$h_A$$

e denominada por *número de classes* de A, desempenha um papel importante na obtenção de propriedades aritméticas do anel A. Como um exemplo simples, observamos que A é um domínio principal se, e somente se, $h_A = 1$. É importante ressaltar que o número de classes de um domínio de Dedekind pode não ser finito. Porém, no caso em que lidamos com o anel dos inteiros algébricos de um corpo de números, a finitude do números de classes pode ser obtida (ver [E2], Teorema 10.3 pg.90).

Um primo p é dito *regular* quando ele não divide o número de classes de $I_{\mathbb{Q}(\zeta)}$, onde $\zeta = e^{\frac{2\pi i}{p}}$.

Como exemplo de primos regulares citamos, sem demonstração, $p = 3, 5$ e 7. Decidimos não verificar estes exemplos, pois precisaríamos nos alongar com o desenvolvimento de técnicas como, por exemplo, o método analítico de redes em $\mathbb{R}^n$, que fugiria do nosso objetivo. Uma discussão sobre alguns cálculos de números de classes pode ser encontrada na seção 10.3 de [ST]. É interessante ressaltar que Kummer conjecturou que existem infinitos primos regulares. Porém o que se sabe, até então, é que existem infinitos primos que não são regulares.

Por fim mencionaremos os dois últimos resultados que serão necessários para nós no decorrer do trabalho e cujas demonstrações encontram-se em [ST], respectivamente nas página 17, Teorema 1.5 e na página 170, Teorema 10.1.

Teorema 3.2. *Seja K um corpo de característica zero. Um polinômio não-nulo $f(x)$ sobre K é divisível pelo quadrado de um polinômio de grau maior que zero se, e somente se, $f(x)$ e $D(f(x))$ possuem um fator comum de grau maior que zero.*

Observação 3.3. Em corpos de característica positiva somente a ida deste teorema é válida.

Teorema 3.3. *Sejam L um corpo de números, $n = [L : \mathbb{Q}]$ o grau da extensão de corpos $L|\mathbb{Q}$ e p um número primo positivo. Suponhamos que $I_L = \mathbb{Z}[\theta]$, com $\theta \in I_L$, e que a imagem do polinômio mínimo $P_{\theta,\mathbb{Q}}$ sobre que $\mathbb{Q}$, via o homomorfismo $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$, possua a seguinte fatoração em polinômios irredutíveis*

$$\overline{P}_{\theta,\mathbb{Q}}(x) = \overline{f}_1^{e_1} \cdots \overline{f}_r^{e_r}$$

onde $f_1, \ldots, f_r \in \mathbb{Z}[x]$. Então o ideal de I_L

$$\mathfrak{p}_i :=< p > + < f_i(\theta) >$$

é primo e a fatoração do ideal principal $< p >$ é dada por

$$< p >= \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Capítulo 4

Aritmética no Anel dos Inteiros Algébricos de Corpos Ciclotômicos

Este capítulo tem o objetivo de introduzir as ferramentas necessárias para a prova do Teorema de Kummer, que demonstra o Último Teorema de Fermat no caso em que o expoente n da equação $x^n + y^n = z^n$ é um primo regular. Para tal, será necessário estudar algumas propriedades do corpo ciclotômico $\mathbb{Q}(\zeta)$, onde $\zeta = e^{\frac{2\pi i}{p}}$ é o gerador do grupo das raízes p-ésimas da unidade, com p primo ímpar. Mais precisamente, estudaremos a caracterização dos elementos invertíveis do anel de inteiros algébricos $\mathbb{Z}[\zeta]$, bem como as unidades em $\mathbb{Q}(\zeta)$.

Lema 4.1. *Considere I o ideal de $\mathbb{Z}[\zeta]$ gerado por $1-\zeta$. Então $I^{p-1} =< p >$ e conseqüentemente $N(I) = p$.*

Prova: Avaliando o polinômio mínimo de ζ, à saber,

$$P_{\zeta|\mathbb{Q}(\zeta)}(t) = t^{p-1} + \cdots + t + 1 = \prod_{j=1}^{p-1}(t - \zeta^j)$$

em $t = 1$, obtemos $p = P_{\zeta|\mathbb{Q}(\zeta)}(1) = \prod_{j=1}^{p-1}(1 - \zeta^j)$. Portanto

$$< p >= \prod_{j=1}^{p-1} < 1 - \zeta^j > .$$

A demonstração da Preposição (3.2) mostra que $1-\zeta$ e $1-\zeta^j$ são associados, portanto $< 1-\zeta >=< 1-\zeta^j >$, provando esta parte do lema. Para a segunda parte observamos que

$$N(I^{p-1}) = (p-1)N(I).$$

Por outro lado,

$$N(< p >) = |N(p)| = \underbrace{[\mathbb{Q}(\zeta) : \mathbb{Q}]}_{p-1} p.$$

Portanto, $N(I) = p$. □

Lema 4.2. *Para cada $\alpha \in \mathbb{Z}[\zeta]$ existe $a \in \mathbb{Z}$ tal que $\alpha^p \equiv a \ (mod p)$.*

Prova: Dado $\alpha \in \mathbb{Z}[\zeta]$ podemos escrevê-lo como combinação dos elementos da base integral, à saber, $\alpha = a_0 + a_1\zeta + ... + a_{p-1}\zeta^{p-1}$ com $a_j \in \mathbb{Z}$, $j = 0, \cdots, p-1$. Deste modo, considerando o polinômio $p(x) = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1}$ em $\mathbb{Z}[x]$ temos, pelo algoritmo da divisão, que $p(x) = (1-x)q(x) + r$, com $q(x), r \in \mathbb{Z}[x]$ e $gr(r) = 0$. Portanto, fazendo $x = \zeta$ temos que

$$\alpha = p(\zeta) = (1-\zeta)q(\zeta) + r,$$

ou seja,

$$\alpha \equiv r \ (modI),$$

com $r \in \mathbb{Z}$. Além disso, temos que

$$\alpha^p - r^p = \prod_{j=0}^{p-1}(\alpha - r\zeta^j).$$

Desta forma, como $\zeta \equiv 1 \ (modI)$ temos que os fatores da direita são congruentes a zero módulo I, pois $\alpha - r\zeta^j \equiv r(1-\zeta^j) \equiv 0 \ (modI)$. Deste modo, aplicando o módulo no produto obtemos que

$$\alpha^p - r^p \equiv 0 \, (modI^{p-1}),$$

que prova o lema. □

Proposição 4.1. *As únicas raízes da unidade em $\mathbb{Q}(\zeta)$ são da forma $\pm\zeta^s$, com s inteiro.*

Prova: A raízes da unidade são zeros de polinômios da forma $p(x) = x^m - 1$. E, deste modo, podemos escrevê-las da forma $e^{\frac{2\pi i}{m}}$, onde m é um número natural. Agora veremos as condições sobre o que fazem $e^{\frac{2\pi i}{m}}$ pertencer a $\mathbb{Q}(\zeta)$.

A primeira restrição é que $4 \nmid m$. Caso contrario, teríamos que $e^{\frac{2\pi i}{4}} = i \in \mathbb{Q}(\zeta)$. Portanto $i \in \mathbb{Z}[\zeta]$, pois i é inteiro sobre $\mathbb{Z}$. Logo,

$$< 2 >= < 1 - i >^2,$$

já que, $2 = i(1-i)^2$. Assim obtemos uma decomposição em fatores primos em $\mathbb{Z}[\zeta]$ para $< 2 >$, com fatores repetidos.

Conseqüentemente , pelo Teorema (3.3) temos que o polinômio

$$P_{\zeta|\mathbb{Q}(\zeta)}(x) = \frac{x^p - 1}{x - 1} \tag{4.1}$$

possui fatores irredutíveis repetidos visto como polinômio em $\mathbb{Z}_2[x]$, logo $t^p - 1$ também possui fatores irredutíveis repetidos visto como polinômio em $\mathbb{Z}_2[x]$. Pela Observação (3.3) temos que $x^p - 1$ e $D(x^p - 1) = px^{p-1}$ não são primos entre si. Mas como p é ímpar temos que estes polinômios vistos como polinômios em $\mathbb{Z}_2[x]$ assumem a forma $x^p - 1$, x^{p-1}, que são obviamente primos entre si, chegando a uma contradição.

A segunda restrição é que se q é um primo ímpar diferente de p, então $q \nmid p$. Caso contrário, teríamos $e^{\frac{2\pi i}{q}} \in \mathbb{Q}(\zeta)$ e como $e^{\frac{2\pi i}{q}}$ é inteiro sobre $\mathbb{Z}$, também teríamos que $e^{\frac{2\pi i}{q}} \in \mathbb{Z}[\zeta]$. Portanto pelo Lema (4.1) temos

$$< q >=< 1 - e^{\frac{2\pi i}{q}} >^{q-1},$$

ou seja, obtemos uma fatoração em fatores primos de $< q >$ em $\mathbb{Z}[\zeta]$, com fatores repetidos. E novamente pelo Teorema (3.3) temos que o polinômio descrito em (4.1) possui fatores irredutíveis repetidos visto como um polinômio em $\mathbb{Z}_q[x]$. Logo $x^p - 1$ também possui fatores irredutíveis repetidos visto como polinômio em $\mathbb{Z}_q[x]$. Pela Observação (3.3) temos que $x^p - 1$ e $D(txp - 1) = px^{p-1}$ não são primos entre si. Mas como p é primo diferente de q temos que estes polinômios vistos como polinômios em $\mathbb{Z}_q[x]$ assumem a forma $x^p - 1$, x^{p-1} que são primos entre si, chegando a uma contradição.

A terceira condição é $p^k \nmid m$, para $k > 1$. De fato

$$[\mathbb{Q}(e^{\frac{2\pi i}{p^k}}) : \mathbb{Q}] = \phi(p^k) = p^{k-1}(p - 1) > p - 1 = [\mathbb{Q}(\zeta) : \mathbb{Q}],$$

nos diz que $e^{\frac{2\pi i}{p^k}} \notin \mathbb{Q}(\zeta)$ e logo, $m \neq p^k$.

Portanto só nos resta a opção que $m \mid 2p$, ou seja, temos que $e^{\frac{2\pi i}{2p}} \in \mathbb{Q}(\zeta)$. Podemos observar que

$$e^{\frac{2\pi i}{2p}} = e^{(\pi i + \frac{1-p}{2}\frac{2\pi i}{p})} = e^{\pi i}(e^{\frac{2\pi i}{p}})^{\frac{1-p}{2}} = -\zeta^{\frac{1-p}{2}},$$

provando a proposição. □

Lema 4.3. *Se $p(x) \in \mathbb{Z}[x]$ é um polinômio mônico e todos as suas raízes tem valor absoluto 1, então cada raiz é uma raiz da unidade.*

Prova: Sejam $\alpha_1, \cdots, \alpha_k$ raízes de $p(x) \in \mathbb{Z}[x]$. Logo $p(x) = (x-\alpha_1)\cdots(x-\alpha_k) = x^k + A_{k-1}x^{k-1} + \cdots + A_0$, onde $A_0, A_1, \cdots, A_{k-1}$ são as funções simétricas elementares nas raízes de $p(x)$. Para cada inteiro $l > 0$ temos que

$$p_l(x) = (x - \alpha_1^l)...(x - \alpha_k^l) = x^k + a_{k-1}x^{k-1} + ... + a_0,$$

onde $a_0, \cdots, a_{k-1}$ são funções elementares em $\alpha_1^l, \cdots, \alpha_r^l$. Logo são funções simétricas em $\alpha_1, \alpha_2, \cdots, \alpha_k$. Pela proposição III.4.8, página 92 [GL], temos que $a_0, \cdots, a_{k-1} \in \mathbb{Z}$, isto é, $p_l(x) \in \mathbb{Z}[x]$. Além disso

$$|a_j| \leq \begin{pmatrix} k \\ j \end{pmatrix} \qquad (j = 0, ..., k-1).$$

, pois cada a_j possui $\begin{pmatrix} k \\ j \end{pmatrix}$ parcelas de produtos dos zeros de $p_l(x)$ somadas pelas relações de Girad e α_j tem valor absoluto igual a um. Por outro lado somente finitos polinômios sobre $\mathbb{Z}$ podem satisfazer este sistema de desigualdades. Assim, para algum m diferente de l temos que ter:

$$p_l(x) = p_m(x).$$

Dai existe uma permutação π de $\{1, ..., k\}$ tal que

$$\alpha_j^l = \alpha_{\pi(j)}^m$$

para $j = 1, ..., k$. Assim

$$\alpha_j^{l^2} = (\alpha_j^l)^2 = (\alpha_{\pi(j)^m})^l = (\alpha_{\pi(j)^l})^m = (\alpha_{\pi(\pi(j))^m})^m = \alpha_{\pi^2(j)}^{m^2}$$

e, indutivamente achamos que

$$\alpha_j^{l^r} = \alpha_{\pi^r(j)}^{m^r}.$$

Por outro lado $\pi^{k!}(j) = j$, nos diz que $\alpha_j^{l^{k!}} = \alpha_j^{m^{k!}}$ isto é

$$\alpha_j^{(l^{k!} - m^{k!})} = 1$$

. Como $l^{k!} \neq m^{k!}$, temos que α_j é uma raiz da unidade. □

Proposição 4.2. *Todo invertível em $\mathbb{Z}[\zeta]$ é da forma $r\zeta^g$, onde r é um número real e g é um numero inteiro.*

Prova: Seja ϵ um invertível em $\mathbb{Z}[\zeta]$. Existe um polinômio $e(t) \in \mathbb{Z}[t]$ tal que $\epsilon = e(\zeta)$. Para cada $s = 1, ..., p-1$ temos

$$\epsilon_s = e(\zeta^s)$$

é conjugados a ϵ. Deste modo, $\pm 1 = N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\epsilon) = \epsilon_1 \cdots \epsilon_{p-1}$, e, consequentemente, cada ϵ_s é uma unidade de $\mathbb{Z}[\zeta]$. Além disso, o conjugado complexo de ϵ_s é

$$\overline{\epsilon_s} = \overline{e(\zeta^s)} = e\left(\overline{\zeta^s}\right) = e\left(\overline{\zeta}^s\right) = e(\zeta^{p-s}) = \epsilon_{p-s}.$$

Assim, como $\epsilon_s\epsilon_{p-s} = |\epsilon_s|^2 > 0$, temos que $(\epsilon_1\epsilon - 1_p)(\epsilon_2\epsilon_{p-2})... > 0$. Portanto, $N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\epsilon) = 1$.

Agora, $\dfrac{\epsilon_s}{\epsilon_{p-s}}$ é uma unidade de valor absoluto 1. Por outro lado, como as raízes do polinômio

$$\prod_{s=1}^{p-1}\left(t - \frac{\epsilon_s}{\epsilon_{p-s}}\right)$$

são todos os conjugados de $\dfrac{\epsilon_1}{\epsilon_{p-1}}$ em $\mathbb{Q}(\zeta)|\mathbb{Q}$ temos que este é o seu polinômio característico. Logo possui todos os seus coeficientes em $\mathbb{Z}$, já que, este polinômio é uma potência do polinômio minimal de $\dfrac{\epsilon_1}{\epsilon_{p-1}}$, que por sua vez pertence a $\mathbb{Z}[t]$, pois $\dfrac{\epsilon_1}{\epsilon_{p-1}}$ é inteiro sobre $\mathbb{Z}$. Do Lema (4.1), segue que os zeros deste polinômio são raízes da unidade. Logo, pela Proposição (4.1) temos que $\dfrac{\epsilon}{\epsilon_{p-1}} = \pm\zeta^u$ para algum inteiro u. Como p é ímpar, temos que u ou $u + p$ é par, e assim podemos escrever

$$\frac{\epsilon}{\epsilon_{p-1}} = \pm\zeta^{2g} \tag{4.2}$$

para algum inteiro $g > 0$.

O passo fundamental agora é determinar o sinal da igualdade acima. Para tal, observamos que

$$t^g e(t^{p-1}) = (1 - t)q(t) + v,$$

pelo Algoritmo da Divisão de Euclides, com $v \in \mathbb{Z}$. Aplicando ζ nesta igualdade obtemos $\zeta^g e(\zeta^{p-1}) - v = q(\zeta)(1 - \zeta)$, isto é,

$$\zeta^g\epsilon_{p-1} \equiv v \ (mod\, I).$$

Agora usando o fato que $1 - \zeta$ e $1 - \zeta^{p-1} = \overline{1 - \zeta}$ são associados também obtemos que

$$\zeta^{-g}\epsilon \equiv v \ (mod\, I).$$

Subtraindo as congruências acima obtemos

$$\zeta^{-g}\epsilon \equiv \zeta^g\epsilon_{p-1} \ (mod\, I).$$

Como o $\epsilon_p - 1$é invertível concluímos que

$$\frac{\epsilon}{\epsilon_{p-1}} \equiv \zeta^{2g} \ (mod\, I).$$

Agora estamos em condições de avaliar o sinal da equação (4.2). Supondo

$$\frac{\epsilon}{\epsilon_{p-1}} = -\zeta^{2g}$$

temos, $\zeta^{2g} \equiv -\zeta^{2g}$ $(mod\, I)$, isto é, $2\zeta^{2g} \equiv 0$ $(mod\, I)$. Assim, $I \subset < 2\zeta^{2g} >$, e logo,

$$p = N(I) | N(< 2\zeta^{2g} >) = 2^{p-1}$$

o que é uma contradição, pois p é ímpar. Então só nos resta a opção positiva

$$\frac{\epsilon}{\epsilon_{p-1}} = \zeta^{2g},$$

o que equivale a $\zeta^{-g}\epsilon = \zeta^{g}\epsilon_{p-1} = r \in \mathbb{R}$, já que, $\zeta^{-g}\epsilon$ e $\zeta^{g}\epsilon_{p-1}$ são conjugados complexos. Portanto,$\epsilon = r\zeta^{g}$. $\square$

Capítulo 5

Teorema de Kummer

Teorema 5.1. *Seja p primo ímpar e regular. Então a equação*

$$x^p + y^p = z^p$$

não possui soluções inteiras x, y e z satisfazendo

$$p \nmid x, p \nmid y, p \nmid z.$$

Prova: Como p é ímpar temos uma bijeção entre as soluções da equação de Fermat $x^p + y^p = z^p$ e da equação

$$x^p + y^p + z^p = 0. \tag{5.1}$$

O polinômio associado a esta equação, à saber $f(x, y, z) = x^p + y^p + z^p$, é simétrico. Isto nos permite permutar as suas variáveis sem perda de generalidade. Por este motivo usaremos a equação (5.1) como alternativa a equação de Fermat.

Agora assumindo a contra positiva do Teorema de Krummer, existem x, y, z em $\mathbb{Z}$ satisfazendo (5.1) para algum primo ímpar p. Dividindo pelos fatores em comum na equação (5.1) podemos assumir que x, y, z são dois a dois primos entre si. Portanto isolando o membro da variável z temos que $x^p + y^p = -z^p$ e fatorando o lado esquerdo em $\mathbb{Q}(\zeta)$, obtemos:

$$\prod_{j=0}^{p-1}(x + \zeta^j y) = -z^p,$$

o que implica na seguinte igualdade de ideais:

$$\prod_{j=0}^{p-1} < x + \zeta^j y > = < z >^p . \tag{5.2}$$

Os fatores da esquerda são dois a dois primos entre si. De fato, suponha que exista um ideal primo P dividindo $< x + \zeta^k y >$ e $< x + \zeta^l y >$, com $0 \leq k < l \leq p - 1$. Então P contém $(x+\zeta^k y)-(x+\zeta^l y) = y\zeta^k(1-\zeta^{l-k})$. Além disso, $1-\zeta^{l-k}$ é associado de $1 - \zeta$ e ζ^k é invertível. Assim P contém $y(1 - \zeta)$. Como P é ideal primo $y \in P$ ou $(1 - \zeta) \in P$. Observe que (5.2) nos diz que P divide $< z >^p$, e logo Pdivide $< z >$, pois p é ideal primo. Consequentemente temos que $z \in P$. Agora, sendo z e y primos entre si, existem $a, b \in \mathbb{Z}$ tais que $az + by = 1$. Sendo assim, se $y \in P$, então $1 \in P$, o que é uma contradição. No caso em que $1 - \zeta \in P$ temos que P divide o ideal $I =< 1 - \zeta >$. Por outro lado, $N(I) = p$ nos diz que I é ideal primo e portanto $P = I$. Então $I| < z >$. Assim,

$$p = N(I)|N(< z >) = z^{p-1}$$

e como p é ímpar temos que $p|z$ contrariando a hipótese.

A unicidade da fatoração em ideais primos nos garante que cada fator no lado esquerdo da equação (5.2) é uma p potência de algum ideal, desde que do lado direito seja uma p potência e os fatores sejam dois a dois primos entre si. Em particular, existe um ideal a tal que $< x + \zeta y >= a^p$. Portanto a^p é principal.

Pela definição do $\mathscr{C}$, o grupo das classes dos ideais de $\mathbb{Z}[\zeta]$, temos que a^p pertence a classe $1_{\mathscr{C}}$, o elemento neutro de $\mathscr{C}$, ou seja $[a^p] = 1_{\mathscr{C}}$. Por outro lado, a regularidade p significa que $p \nmid h_{\mathbb{Z}[\zeta]}$. Logo p e $h_{\mathbb{Z}[\zeta]}$ são primos entre si, isto é, existem $r, s \in \mathbb{Z}$ tais que $rp + sh_{\mathbb{Z}[\zeta]} = 1$. Portanto

$$[a] = [a^{rp+sh_{\mathbb{Z}[\zeta]}}] = [a^{rp}][a^{sh_{\mathbb{Z}[\zeta]}}] = [a^p]^r[a^{h_{\mathbb{Z}[\zeta]}}]^s = 1^r_{\mathscr{C}}1^s_{\mathscr{C}} = 1_{\mathscr{C}}$$

e assim temos que a é principal, ou seja, $a =< \delta >$. Resultando que

$$x + \zeta y = \epsilon\delta^p,$$

onde ϵ é um invertível.

Pela Proposição (4.2) segue que $x + \zeta y = r\zeta^g\delta^p$, com $r \in \mathbb{R}$ e $g \in \mathbb{Z}$. Além disso, pelo Lema (4.2) existe $t \in \mathbb{Z}$ tal que $\delta^p \equiv t\ (modI^p)$ e portanto

$$x + \zeta y \equiv rt\zeta^g\ (modI^p).$$

O Lema (4.1) mostra que $< p > |I^p$ e assim $x + \zeta y \equiv rt\zeta^g(mod < p >)$. Como ζ^g é invertível temos que

$$\zeta^{-g}(x + \zeta y) \equiv rt\ (mod < p >)$$

e passando o conjugado complexo obtemos que

$$\zeta^g(x + \zeta^{-1}y) \equiv rt\ (mod < p >).$$

Fazendo a diferença das duas congruências acima, obtemos a equação

$$x\zeta^{-g} + y\zeta^{1-g} - x\zeta^{g} - y\zeta^{g-1} \equiv 0 \ (mod < p >). \tag{5.3}$$

Agora podemos analisar os possíveis valores de g em (5.3).

Suponhamos $g \equiv 0 \ (modp)$. Então $\zeta^g = 1$. Assim os termos com x em (5.3) são cancelados, obtendo $y(\zeta - \zeta^{-1}) \equiv 0 \ (mod < p >)$. Passando o conjugado complexo temos que $y(\zeta^{-1} - \zeta) \equiv 0 \ (mod < p >)$ e multiplicando por ζ chegamos a

$$y(1 - \zeta^2) \equiv 0 \ (mod < p >),$$

isto é,

$$y(1 + \zeta)(1 - \zeta) \equiv 0 \ (mod < p >).$$

Aplicando $x = -1$ no polinômio mínimo de ζ

$$P_{\zeta|\mathbb{Q}}(x) = \frac{x^p - 1}{x - 1} = (x - \zeta)(x - \zeta^2)...(x - \zeta^{p-1}),$$

temos que

$$1 = (1 + \zeta)(1 + \zeta^2)...(1 + \zeta^{p-1}),$$

logo $1 + \zeta$ é invertível. Portanto,

$$y(1 - \zeta) \equiv 0 \ (mod < p >).$$

Como $< p >=< 1 - \zeta >^{p-1}$ e $p - 1 \geq 2$, temos que $(1 - \zeta)|y$. Logo $p = N(1 - \zeta)|N(y) = y^{p-1}$, e portanto $p|y$ contrariando a hipótese. Portanto $g \not\equiv 0 \ (mod < p >)$.

Um argumento semelhante mostra que $g \not\equiv 1(modp)$. Reescrevemos (5.3) da seguinte maneira.

$$\alpha p = x\zeta^{-g} + y\zeta^{1-g} - x\zeta^{g} - y\zeta^{g-1},$$

para algum $\alpha \in \mathbb{Z}[\zeta]$. Note que, sendo $g \not\equiv 0 \ (modp)$ e $g \not\equiv 1 \ (modp)$, temos que $-g, g, 1 - g, g - 1$ não são divisíveis por p. Temos que

$$\alpha = \frac{x}{p}\zeta^{-g} + \frac{y}{p}\zeta^{1-g} - \frac{x}{p}\zeta^{g} - \frac{y}{p}\zeta^{g-1}. \tag{5.4}$$

Agora $\alpha \in \mathbb{Z}[\zeta]$ e $\{1, \zeta, ..., \zeta^{p-2}\}$ é base integral de $\mathbb{Q}(\zeta)$. Desde que todos os expoentes de (5.4) sejam incongruentes modulo p, temos $\frac{x}{p}, \frac{y}{p} \in \mathbb{Z}$, contrariando a hipótese.

Assim algum par de expoentes em (5.4) devem ser congruentes modulo p. Como $g \not\equiv 0, 1 \ (modp)$, só nos resta que $g - 1 \equiv -g \ (modp)$, ou equivalentemente $1 - g \equiv g \ (modp)$. Assim temos que $2g \equiv 1(modp)$ e logo podemos escrever

$$\begin{aligned} \alpha p\zeta^g &= x + y\zeta - x\zeta^{2g} - y\zeta^{2g-1} \\ &= x(1 - \zeta^{2g}) + y(\zeta - \zeta^{2g-1}) \\ &= x(1 - \zeta) + y(\zeta - 1) \\ &= (x - y)(1 - \zeta). \end{aligned}$$

Portanto, aplicando a norma obtemos que $N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\alpha p\zeta^g) = N_{\mathbb{Q}(\zeta)|\mathbb{Q}}((x-y)(1-\zeta))$, isto é, $N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\alpha)p^{p-1} = (x-y)^{p-1}p$. Logo $p|(x-y)$. Portanto

$$x \equiv y \ (mod p)$$

e pela simetria de (5.1) concluirmos que

$$y \equiv z \ (mod p).$$

Portanto

$$0 \equiv x^p + y^p + z^p \equiv 3x^p \ (mod p).$$

Desde que $p \nmid x$ devemos ter $p = 3$. Note que em módulo 9, os cubos dos números relativamente primos a 3, à saber $1, 2, 4, 5, 7, 8$, são congruentes a ± 1. Assim em módulo 9 a solução de (3.1) em inteiros primos com 3 assume a forma:

$$\pm 1 \pm 1 \pm 1 \equiv 0 \ (mod 9),$$

que é um absurdo. □

Bibliografia

[GL] A. Garcia e Y. Lequain, *Elementos de Álgebra,* Impa, Rio de Janeiro, (2002).

[E1] O. Endler, *Teoria dos Corpos,* Publicações Matemáticas, Impa, Rio de Janeiro, (2007).

[E2] O. Endler, *Teoria dos Números Algébricos,* Projeto Euclides, Impa, Rio de Janeiro, (2006).

[L] S. Lang, *Algebra,* Springer US, (2005).

[R] P. Ribenboim, *Classical Theory of Algebraic Numbers,* Springer US, (2001).

[ST] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem,* A K Peters, Massachusetts, (2002).