Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

A Equação Diofantina $x^2 + C = y^n$

por

Jesús Fabian Muñoz Pomeo

sob orientação de

Prof. Dr. Hemar Teixeira Godinho

Brasília

2019

Jesús Fabian Muñoz Pomeo

A Equação Diofantina $x^2 + C = y^n$

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília como requisito parcial para obtenção do título de MESTRE EM MATEMÁTICA.

Área de Concentração: Teoria Dos Números

Brasília

2019

Universidade de Brasília
Instituto de Exatas
Departamento de Matemática

A Equação Diofantina $x^2 + C = y^n$

por

Jesús Fabian Muñoz Pomeo ♠

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília como requisito parcial para obtenção do título de

MESTRE EM MATEMÁTICA.

Área de Concentração: Teoria Dos Números

Aprovada por:

Prof. Dr. Hemar Teixeira Godinho (Orientador) – UnB

Prof. Dr. Matheus Bernardini de Souza - FGA/UnB

Prof. Dr. Victor Gonzalo Lopez Neumann - UFU

♠Este trabalho contou com apoio financeiro do CNPq.

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Me

Muñoz Pomeo, Jesús Fabian
A Equação Diofantina x^{2}+C=y^{n} / Jesús Fabian Muñoz Pomeo; orientador Hemar Teixeira Godinho . -- Brasília, 2019.
65 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2019.

1. . I. Teixeira Godinho , Hemar , orient. II. Título.

Agradecimentos

Agradeço a Deus por ter me acompanhado e me guiado durante toda a minha vida, por ser minha força naqueles momentos de dificuldade e fraqueza, por me dar uma vida cheia de aprendizado, experiências e também de felicidade.

À minha mãe María Teotiste Pomeo e minha família, que sempre me apoiaram em todas as decisões que tomei ao longo da minha vida e que, apesar de estarem longe, conseguem se fazer perto.

À Marta Calvache, foi quem me motivou vir a Brasília para conseguir esta nova conquista em minha vida. Agradeço também por seu carinho, apoio e compreensão durante esse período e por ser um excelente amiga.

Aos meus amigos Alan, Santiago, Marby, Carolina, Edwin, Andrés, Welinton, Filipe, Quintino, Alex, Wenison, Welber, Wilson, Edna, Elaine, Jean, Fábio, Christe, Guilherme, Jhon Freddy, Marcos, Mateus, Nathália, Paulo, Wállef, Letícia, Geraldo e Claudia, por confiarem e acreditarem em mim e terem feito do meu estágio universitário uma jornada de etapas e experiências que jamais esquecerei.

Por outro lado, gostaria de agradecer sinceramente meu orientador Prof. Dr. Hemar Teixeira Godinho, pelo seu esforço, dedicação, conhecimento, orientação, forma de trabalhar, paciência, motivação e confiança que foram fundamentais para minha formação como profissional.

Aos professores do Departamento de Matemática da UnB por terem contribuído na minha formação acadêmica.

Aos membros da banca, por aceitarem prontamente o convite para avaliação deste trabalho.

Ao CNPq pelo apoio financeiro.

Peço desculpas àqueles que injusta e involuntariamente tenham sido omitidos.

Meus sinceros agradecimentos a todos.

Dedicatória

Aos meus pais, María Teotiste Pomeo e Olegario Vargas. Aos meus irmãos, Sandra Katherine Pomeo, María Alejandra Pomeo e Alex Mauricio Pomeo. A minha Tia Luz Marina Pomeo. Por sempre estarem ao meu lado a pesar da distância.

"O sucesso não é um acidente. É trabalho árduo, perseverança, aprendizado, estudo, sacrifício, e acima de tudo, amor pelo que você está fazendo ou aprendendo a fazer. "

Pelé

Resumo

Neste trabalho estudaremos como as sequências de Lucas são aplicadas para obter soluções de algumas equações Diofantinas. Faremos um estudo dos trabalhos Pan Xioawei (2013) e Attila Bérczes (2012). Estudaremos as equações Diofantinas $x^2 + C = y^n$, para $C = d^{2l+1}$ ou $C = p^{2m}$ em que $l \geq 0$, $m > 1$, p é primo e $d > 0$ é um inteiro livre de quadrados. Verificaremos que as equações possuem o uso de sequências de Lucas para encontrar as soluções.

Palavras-chave: Sequências de Lucas, Equações Diofantinas, Estudo dos trabalhos Pan Xioawei e Attila Bérczes, Livre de quadrados.

Abstract

In this work we study how Lucas sequences is applied in order to obtain solutions of certain Diophantine equations. We study papers by Pan Xioawei (2013) and Attila Bérczes (2012) and we consider the Diophantine equations $x^2 + C = y^n$, for $C = d^{2l+1}$ or $C = p^{2m}$ where $l \geq 0$, $m > 1$, p is prime and $d > 0$ be a squarefree integer. We wil verify that Lucas sequences are used to find solutions of those equations.

Keywords: Lucas sequences, Diophantine equations, Study of the works Pan Xioawei and Attila Bérczes, Squarefree integer.

Conteúdo

Introdução

Suponha queremos encontrar as soluções da equação $25x + 10y = 20$. Se x pode assumir qualquer valor, então basta fazer $y = \frac{20-25x}{10}$. Se adicionarmos a condição de que x e y sejam inteiros, então o problema se torna mais difícil. Este tipo de equações, cujas soluções são obrigadas a ter valores inteiros, ou mais geralmente valores racionais, são conhecidas por equações Diofantinas, em homenagem ao matemático grego Diofanto de Alexandria, nascido em torno de 200/214 d. C. e falecido em torno de 284/298 d. C. Dados que não são conhecidos com precisão. Diofanto é conhecido por seu trabalho em aritmética relacionada com a solução de equações algébricas e na teoria dos números. Ele escreveu a obra "Aritmética" distribuída em treze livros dedicados à resolução de equações algébricas, buscando dar métodos para encontrar suas soluções inteiras ou racionais. É de salientar que dos 13 livros só os seis primeiros são conhecidos. O conteúdo desses livros é uma coleção de problemas e, em todos estes, o matemático grego apresenta uma solução única.

É indiscutível sua originalidade para resolver problemas, que chamaríamos hoje de Teoria dos Números elementar, e sua importância como inspiração grandes matemáticos ao longo da história. Um dos exemplos mais famosos dessa "inspiração" é, sem dúvida, o último teorema de Fermat.

Um dos problemas desta obra, o número 8 do livro II para ser exato, tem a seguinte declaração: escreva um dado quadrado como soma de dois quadrados. As afirmações de Diofanto descrevem sempre as equações (iguais) de maneira retórica. Hoje, escreveríamos assim: $x^2 + y^2 = a^2$.
Mas qual é a relação da equação descrita acima com último teorema de Fermat? Em 1621, Bachet publicou uma versão latina dos seis livros da Aritmética de Diofanto

com comentários próprios sobre cada problema. Fermat, que tinha uma cópia do livro de Bachet, acrescentou à margem desse problema a notação mais famosa da história da matemática. Na margem de sua cópia do Aritmética de Diofanto, Fermat tinha marcado o seu resultado: "você não pode escrever um cubo como uma soma de dois cubos ou uma quarta potência como uma soma de duas quartas potências". Em geral, uma potência maior que dois não pode ser escrita como a soma de duas potências do mesmo tipo. Ou seja, não há soluções racionais positivas para a seguinte equação: $x^n + y^n = z^n$ com $n > 2$. A qual, o mesmo Fermat acrescentou: "Eu tenho uma prova verdadeiramente notável deste fato, mas as margens do livro são demasiado estreitas para a conter". A prova deste resultado tão fácil de enunciar revelou-se extremamente evasiva e teria que esperar até 1995 para alcançá-la, usando técnicas bem sofisticadas. Essa provavelmente não era a prova que Fermat havia pensado para ao problema.

A demonstração do último teorema de Fermat (UTF) por Andrew Wiles, concluída em 1995, foi uma das realizações matemáticas mais proeminentes do final do século XX, e certamente um dos eventos científicos que recebeu mais atenção dos meios de comunicação e do público em geral. Não é todo dia que se resolve um problema que está aberto há mais de 350 anos. O trabalho de Wiles e o UTF ofereceram ao público não-matemático uma oportunidade sem precedentes para aprender mais sobre o mundo da pesquisa neste campo em geral e na teoria dos números em particular. A obra Aritmética serviu de inspiração para personalidades tão importantes para a matemática como Viète, Bachet, Fermat, Descartes, Euler, Dirichlet, Poincaré e muitas outras.

Os matemáticos devem frequentemente inventar ou desenvolver extensivamente ferramentas inteiramente novas para resolver os problemas teóricos, e estes, por sua vez, tornam-se ramos importantes da matemática, que muitas vezes têm aplicações em problemas completamente diferentes daqueles dos quais se originam.

A teoria das equações Diofantinas passou a ser citada entre as áreas mais belas e difíceis da matemática. O grande matemático Johann Carl Friedrich Gauss ($1777 - 1855$) chegou a dizer que a matemática é a rainha das ciências e a aritmética (chamada modernamente Teoria dos Números) é a rainha da matemática.

A equação $x^2 + C = y^n$ tem uma história interessante e atraiu a atenção de vários matemáticos. Vários artigos foram escritos sobre este tópico, especialmente

para valores particulares de C. O primeiro resultado não trivial é devido a Lebesgue e data de 1850. Ele provou que a equação acima não tem soluções para $C = 1$. Mais recentemente, outros valores de C foram considerados. O caso em que $C = p^k$, uma potência de um número primo, foi estudado em [3], [22] e [23] para $p = 2$, em [5], [27] e [35] para $p = 3$, em [37] e [34] para $p = 5$ e em [29] para $p = 7$. Alguns avanços para um p primo arbitrário aparecem em [4]. A equação $x^2 + C = y^n$ com $1 \leq C \leq 100$ foi completamente resolvida em [11]. Também, as soluções para os casos $C = 2^a \cdot 3^b$, $C = 2^a \cdot 5^b$ e $C = 5^a \cdot 13^b$, onde x e y são coprimos, podem ser encontrados em [28], [30] e [36], respectivamente. Progressos recentes sobre o assunto foram feitos nos casos $C = 5^a \cdot 11^b$, $C = 2^a \cdot 11^b$, $C = 2^a \cdot 3^b \cdot 11^c$, $C = 2^a \cdot 5^b \cdot 13^c$ e pode ser encontrado em [13], [12], [20] e [42].

Nosso interesse neste trabalho é estudar a equação $x^2 + C = y^n$, para os casos $C = d^{2l+1}$ e $C = p^{2m}$ que podem ser encontrados nos artigos de Xiowei [44] e Bérczes [9], nos quais são utilizadas as sequências de Lucas para encontrar as soluções das equações Diofantinas.

Na perspectiva de atingir o objetivo proposto, este trabalho foi organizado em duas partes, os quais apresentamos a seguir.

Nas preliminares, apresentamos os conceitos e resultados sobre sequência de recorrência, números de Lucas, números algébricos, corpos quadráticos, discriminante e base integral.

O capítulo 2 é dedicado ao estudo da equação Diofantina $x^2+C = y^n$ e apresentamos resultados para encontrar soluções de algumas equações Diofantinas que são similares em estrutura a equação mencionada. Em seguida, apresentamos as soluções das equações $x^2 + d^{2l+1} = y^n$ e $x^2 + p^{2m} = y^n$. Uma breve justificativa de como são empregadas as sequências de Lucas para ajudar a encontrar as soluções das duas equações Diofantinas é apresentada no final capítulo.

Capítulo 1

Preliminares

Neste capítulo, planejamos fixar as notações e estabelecer uma base para o texto, apresentando as definições e resultados que serão utilizados na construção do próximo capítulo e seções. Inicialmente apresentaremos a definição da sequência de Lucas, que é uma ferramenta muito útil para a solução de equações Diofantinas. Também apresentamos propriedades relacionadas a sequências recorrentes, números de Lucas e corpos quadráticos, que serão necessárias para entender os tópicos seguintes.

1.1 Sequências Recorrentes

Uma sequência numérica é uma função real com domínio $\mathbb{N}$ que a cada n, associa um número real Z_n. Vamos escrever as sequências na forma

$$Z_1, Z_2, Z_3, ..., Z_n, ... \tag{1.1}$$

ou vamos denotar por $(Z_n)_{n\geq 1}$.

Se existe um número natural k e números $a_1, a_2, ..., a_k$ (reais ou complexos), não todos nulos,

$$Z_n = a_1 Z_{n-1} + a_2 Z_{n-2} + \cdots + a_k Z_{n-k}, \quad n > k, \tag{1.2}$$

entao chamamos $(Z_n)_{n\geq k+1}$ de sequência recorrente linear homogênea de ordem k e (1.2) é chamada de equação recorrente de ordem k.

Um exemplo de sequências como (1.2), são as progressões aritméticas e as progressões geométricas. De fato, sejam Z e $d \in \mathbb{R}$, e (Z_n) a sequência tal que

$$Z_n = Z + (n-1)d, \text{para todo} n \in \mathbb{N},$$

isto é $Z_{n+1} = Z_n + d$ para todo $n \in \mathbb{N}$. Note que

$$Z_{n+2} = Z_{n+1} + d \quad e \quad Z_{n+1} = Z_n + d.$$

Subtraindo em cada membro e igualando os dois termos, obtém-se

$$Z_{n+2} - Z_{n+1} = Z_{n+1} - Z_n,$$

isto é $Z_{n+2} = 2Z_{n+1} - Z_n$. Isso implica que as progressões aritméticas são sequências recorrentes lineares de ordem 2. Por outro lado, se Z_n é uma sequência tal que

$$Z_n = Z \cdot d^{n-1}, \text{para todo} n \in \mathbb{N},$$

tem-se que $Z_{n+1} = d \cdot Z_n$, o que implica que as progressões geométricas são sequências recorrentes lineares de ordem 1.

Um dos exemplos mais famosos de sequência de recorrência linear, homogênea de ordem 2 é a sequência de Fibonacci dada por

$$F_n = F_{n-1} + F_{n-2}, \ com \ F_0 = 0 \ \ e \ \ F_1 = 1.$$

Assim obtemos a sequência

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ...$$

reescrevendo (1.2) para $n \geq 2$, obtemos

$$Z_n - A\,Z_{n-1} - B\,Z_{n-2} = 0. \tag{1.3}$$

Substituindo $Z_j = x^j$, assumindo $x \neq 0$, obtemos a equação polinomial

$$0 = x^n - Ax^{n-1} - Bx^{n-2} = x^{n-2}(x^2 - Ax - B).$$

O polinômio $P(x) = x^2 - Ax - B$ é chamado de polinômio característico da sequência (Z_n).

Vamos considerar somente sequências com $A^2 \neq -4B$, nesse caso o polinômio $P(x)$ tem duas raízes distintas

$$\alpha = \frac{A + \sqrt{A^2 + 4B}}{2} \quad e \quad \beta = \frac{A - \sqrt{A^2 + 4B}}{2}.$$

Consideremos agora a função geradora

$$F(x) = \sum_{n=0}^{\infty} Z_n x^n.$$

Retomando para (1.3) , com $n \geq 2$, obtemos

$$\begin{aligned} F(x) - Z_1 x - Z_0 &= \sum_{n\geq 2} Z_n x^n \\ &= A\sum_{n\geq 2} Z_{n-1}x^n + B\sum_{n\geq 2} Z_{n-2}x^n \\ &= xA\sum_{n=1}^{\infty} Z_n x^n + x^2 B\sum_{n=0}^{\infty} Z_n x^n. \end{aligned}$$

Logo,

$$F(x) - Z_1 x - Z_0 = xA(F(x) - Z_0) + x^2 BF(x),$$

e assim,

$$\begin{aligned} F(x)(1 - xA - x^2B) &= Z_0 + Z_1 x - xAZ_0 \\ F(x) &= \frac{Z_0 + x(Z_1 - AZ_0)}{1 - xA - x^2B}. \end{aligned}$$

Observe que $\frac{1}{\alpha}$ e $\frac{1}{\beta}$ são raízes de $1 - xA - x^2B$, logo

$$\begin{aligned} F(x) &= \frac{Z_0 + x\left(Z_1 - AZ_0\right)}{-B\left(x - \frac{1}{\alpha}\right)\left(x - \frac{1}{\beta}\right)} = \frac{Z_0 + x\left(Z_1 - AZ_0\right)}{\frac{-B}{\alpha\beta}\left(1 - x\alpha\right)\left(1 - x\beta\right)} \\ &= \frac{M}{1 - x\alpha} + \frac{N}{1 - x\beta} = \frac{M(1 - x\beta) + N(1 - x\alpha)}{(1 - x\alpha)(1 - x\beta)}. \end{aligned}$$

Então temos

$$\begin{aligned} M(1 - x\beta) + N(1 - x\alpha) &= -(Z_0 + x(Z_1 - AZ_0))\frac{\alpha\beta}{B} \\ M + N - x(M\beta + N\alpha) &= \frac{-Z_0\alpha\beta}{B} - \frac{x(Z_1 - AZ_0)\alpha\beta}{B}, \end{aligned}$$

logo

$$M\beta + N\alpha = \frac{(Z_1 - AZ_0)\alpha\beta}{B} = -Z_1 + AZ_0, \tag{1.4}$$

$$M + N = \frac{-Z_0\alpha\beta}{B} = Z_0, \ pois \ \alpha\beta = -B. \tag{1.5}$$

Das equações (1.4) e (1.5), concluímos que

$$\begin{aligned}(Z_0 - N)\beta + N\alpha &= AZ_0 - Z_1\\ N(\alpha - \beta) &= AZ_0 - Z_0\beta - Z_1\\ N &= \frac{Z_0(A - \beta - Z_1)}{\alpha - \beta}\end{aligned}$$

e

$$\begin{aligned}M = Z_0 - N &= \frac{Z_0(\alpha - \beta) - Z_0(A - \beta) + Z_1}{\alpha - \beta}\\ &= \frac{Z_0\alpha - Z_0\beta - Z_0A - Z_0\beta + Z_1}{\alpha - \beta}\\ &= \frac{Z_0(\alpha - A) + Z_1}{\alpha - \beta}.\end{aligned}$$

Assim

$$F(x) = \frac{M}{1 - x\alpha} + \frac{N}{1 - x\beta},$$

com

$$M = \frac{Z_1 + Z_0(\alpha - A)}{\alpha - \beta} \quad e \quad N = \frac{Z_0(A - \beta) - Z_1}{\alpha - \beta}$$

e concluímos que

$$\begin{aligned}F(x) &= M\frac{1}{1 - x\alpha} + N\frac{1}{1 - x\beta}\\ &= M\sum_{n=0}^{\infty}\alpha^n x^n + N\sum_{n=0}^{\infty}\beta^n x^n.\end{aligned}$$

Como $F(x) = \sum_{n=0}^{\infty} Z_n x^n$, igualando os coeficientes obtemos

$$Z_n = M\alpha^n + N\beta^n.$$

Asim, podemos concluir que

$$Z_n = \frac{(Z_1 - Z_0\beta)\alpha^n - (Z_1 - Z_0\alpha)\beta^n}{\alpha - \beta}. \tag{1.6}$$

Tomando $n = 0$ e $n = 1$ recuperamos os valores de Z_0 e Z_1 fixados inicialmente. Assim dada a sequência de recorrência (Z_n) como em (1.3), com α e β sendo as raízes distintas do polinômio característico $P(x) = x^2 - Ax - B$, com $A = \alpha + \beta$ e $B = -\alpha\beta$, obtemos a fórmula explicita (1.6) para a determinação dos valores de Z_n, sem a necessidade de recorrer à relação de recorrência. Se considerarmos a sequência de Finonacci (F_n) e substituirmos os valores em (1.6) obtemos a famosa fórmula:

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Por outro lado, sendo $A = \alpha + \beta$ e $B = -\alpha\beta$, obtemos

$$\begin{aligned} AZ_{n-1} + BZ_{n-2} &= (\alpha+\beta)Z_{n-1} - \alpha\beta Z_{n-2} \\ &= \frac{(\alpha+\beta)}{\alpha-\beta}\left[(Z_1 - Z_0\beta)\alpha^{n-1} - (Z_1 - Z_0\alpha)\beta^{n-1}\right] \\ &\quad -\frac{\alpha\beta}{\alpha-\beta}\left[(Z_1 - Z_0\beta)\alpha^{n-2} - (Z_1 - Z_0\alpha)\beta^{n-2}\right] \\ &= \frac{(Z_1 - Z_0\beta)\alpha^n - (Z_1 - Z_0\alpha)\beta^n}{\alpha-\beta} \\ &= Z_n. \end{aligned}$$

1.2 Números De Lucas

Definição 1.2.1 *Definimos um* ***par de Lucas*** *como um par (α, β) de inteiros algébricos tal que $\alpha + \beta$ e $\alpha\beta$ são números inteiros coprimos diferentes de zero e $\frac{\alpha}{\beta}$ não é raiz da unidade.*

Assim, obtemos α, β como raízes de $x^2 - Ax - B$, ou seja,

$$\alpha = \frac{1}{2}(A + 1\sqrt{A^2+4B}), \;\; \beta = \frac{1}{2}(A - 1\sqrt{A^2+4B}) \quad .$$

Dado um par de Lucas (α, β), definimos os números de Lucas como

$$L_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \;\; n \in \mathbb{N}. \tag{1.7}$$

Logo temos $L_0 = 0$, $L_1 = 1$, $L_2 = \alpha+\beta$, etc. Como vimos na seção anterior, a expressão (1.7) determina uma sequência de recorrência (L_n), com

$$L_n = AL_{n-1} + BL_{n-2}, \;\; n \geq 2$$

com $A = \alpha + \beta$ e $B = -\alpha\beta$ e valores iniciais $L_0 = 0$ e $L_1 = 1$.

Um número primo p é chamado de **divisor primitivo** de L_n se p divide L_n, mas não divide $(\alpha - \beta)^2 L_1 \cdots L_{n-1}$.

Um par de Lucas (α, β) tal que $L_n(\alpha, \beta)$ não tem divisores primos, será chamado de par de **Lucas n-defeituoso**.

Chamamos (A, B) os parâmetros do par de Lucas (α, β). Dois pares de Lucas (α_1, β_1) e (α_2, β_2) são **equivalentes** se $\frac{\alpha_1}{\alpha_2} = \frac{\beta_1}{\beta_2} = \pm 1$. Para **pares equivalentes de Lucas** (α_1, β_1) e (α_2, β_2), temos $L_n(\alpha_1, \beta_1) = \pm L_n(\alpha_2, \beta_2)$ para qualquer $n \geq 0$. O resultado a seguir é uma compilação do Teorema 1.4 de [10] e do Teorema 1 de [43].

Teorema 1.2.2 *Se n satisfaz $4 < n \leq 30$ e $n \neq 6$. Então, a menos da equivalência definida acima, todos os parâmetros dos pares de Lucas defeituosos são dados na tabela 1.1. Para $n \geq 31$, todos os pares de Lucas são não defeituosos.*

n	(A,B)
5	(1, 5),(1,-7),(2,-40),(1,-11),(1,-15),(12,-76),(12,-1364)
7	(1, −7),(1,-19)
8	(2, −24),(1,-7)
10	(2, −8),(5-3),(5,-47)
12	(1, 5) , (1, −7),(2,-56),(1,-15),(1,-19)
13	(1, −7)
18	(1, −7)
30	(1, −7)

Tabela 1.1:

O próximo resultado também sera útil para nosso trabalho e pode ser encontrado em (*Lucas* [31]).

Lema 1.2.3 *Se p é um divisor primitivo de $L_k(\alpha, \beta)$ com $k > 2$, então $p \equiv \left(\frac{B}{p}\right) (mod\ k)$, donde $\left(\frac{B}{p}\right)$ é o simbolo de Legendre, e (A, B) são os parâmetros do Par de Lucas (α, β).*

1.3 Números Algébricos e Corpos Quadráticos

1.3.1 Corpo numérico algébrico

Nesta seção considera-se que L e K são corpos tais que $\mathbb{Q} \subset K \subset L \subset \mathbb{C}$.

Definição 1.3.1 *Seja K um corpo, uma extensão de K é um corpo L tal que $L \supset K$. Dizemos que $\alpha \in L$ é* ***algébrico sobre K*** *quando α é raiz de algum polinômio em $K[x]$. Caso contrario, dizemos que α é transcendente sobre K.*

Definição 1.3.2 *Seja K um corpo. Uma extensão $L \supset K$ é dita* ***extensão algébrica de K*** *quando todo $\alpha \in L$ é algébrico sobre K.*

Seja $\alpha \in L$ algébrico sobre K e seja $p(x)$ um polinômio em $K[x]$, mônico, de menor grau tal que $p(\alpha) = 0$. Pela minimalidade do grau de $p(x)$ segue claramente que $p(x)$ é o único polinômio mônico irredutível em $K[x]$ tal que $p(\alpha) = 0$ e denotamos por $p(x) = irr(\alpha, K)$.

Definição 1.3.3 *Um corpo numérico algébrico é um subcorpo de $\mathbb{C}$ da forma $\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$, onde $\alpha_1, \alpha_2, ..., \alpha_n$ são números algébricos.*

Exemplo 1.3.4 *$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{7})$, $\mathbb{Q}(\sqrt{1+i}, \theta)$, onde θ é uma raiz do polinômio $x^5 - x + 1$, e $\mathbb{Q}(\sqrt[3]{1+\sqrt{2}} + \sqrt{1-\sqrt{2}}, \sqrt{53} + \sqrt[3]{5})$ são todos exemplos de corpos numéricos algébricos.*

Definição 1.3.5 *Se $\alpha \in \mathbb{C}$ é uma raiz de um polinômio mônico integral de grau d, isso é uma raiz de um polinômio da forma*

$$f(x) = \sum_{j=0}^{d} a_j x^j = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} + a_d x^d \in \mathbb{Z}[x],$$

o qual é irredutível sobre $\mathbb{Q}$, então α é chamado um inteiro algébrico de grau d.

Exemplo 1.3.6 *$a + b\sqrt{-1} = a + bi$, $a, b \in \mathbb{Z}$, $b \neq 0$ é um inteiro algebrico de grau 2, raiz de $x^2 + 2ax + a^2 + b^2$.*

A seguir relembraremos vários resultados clássicos que podem ser encontrados por exemplo em [1].

Teorema 1.3.7 *Se K é um corpo numérico algébrico então existe um número algébrico θ tal que $K = \mathbb{Q}(\theta)$.*

O conjunto de todos os inteiros algébricos é um domínio de integridade e é denotado por Ω. O conjunto de todos os inteiros algébricos que se encontram no corpo numérico algébrico K é também um domínio de integridade. Esse conjunto será denotado por O_K; isso é, $O_K = \Omega \cap K$. Observe que K é o corpo de frações de O_K.

Definição 1.3.8 (Ideal fracionário) *Seja D um domínio de integridade. Seja K o corpo de frações de D. Um subconjunto não vazio A de K é chamado de ideal fracionário de D se satisfaz as seguintes três propriedades*

(i) $\alpha \in A$, $\beta \in A$ *então* $\alpha + \beta \in A$,

(ii) $\alpha \in A$, $\gamma \in D$ *então* $\gamma\alpha \in A$, *e*

(iii) existe $\gamma \in D$ *com* $\gamma \neq 0$ *tal que* $\gamma A \subseteq D$.

Teorema 1.3.9 *Seja K um corpo numérico algébrico. Seja O_K o anel de inteiros de K. Então o conjunto de todos os ideais fracionários de O_K formam um grupo abeliano $I(K)$ com respeito à multiplicação.*

Observe que os ideais principais em $I(K)$ são da forma $\langle\alpha\rangle = \{r\alpha | \, r \in O_K\}$ para algum $\alpha \in K^*$, e estes formam um subgrupo denotado por $P(K)$ de $I(K)$.

O Grupo $I(K)$ é um grupo abeliano, assim $P(K)$ é um subgrupo normal de $I(K)$ e o grupo de quociente $H(K) = I(K)/P(K)$ esta bem definido e é abeliano. Esse grupo é chamado Grupo de classes de K. A ordem do grupo de classes $H(K)$ é chamada de número de classes de K e é denotado por $h(K)$.

Se dois ideais diferentes de zero A e B de O_K estão na mesma classe de $H(K) = I(K)/P(K)$, dizemos que eles são equivalentes e escrevemos $A \sim B$. Claramente

$$\begin{aligned} A \sim B &\iff AP(K) = BP(K) \\ &\iff A^{-1}B \in P(K) \\ &\iff A^{-1}B = \langle\alpha\rangle \text{ para algum } \alpha \in K^* \\ &\iff B = A\langle\alpha\rangle \text{ para algum } \alpha \in K^* \\ &\iff \langle a\rangle A = \langle b\rangle B \text{ para alguns } a, b \in O_K. \end{aligned}$$

O principal resultado sobre o grupo de classes é que sua ordem $h(K)$ é sempre finito. Observe que

$$\begin{aligned} h(K) = 1 &\iff O_K \text{ é um domínio de ideias principais} \\ &\iff O_K \text{ é um domínio de fatoração única.} \end{aligned}$$

1.3.2 Corpos Quadráticos

Nesta seção vamos apresentar de forma mais detalhada o conceito de Corpos Quadráticos e suas principais propriedades.

Definição 1.3.10 *Um **corpo quadrático** é uma extensão finita de $\mathbb{Q}$ de grau 2.*

Seja $f(x) = x^2 + ax + b \in \mathbb{Q}[x]$ um polinômio irredutível e $\alpha \in \mathbb{C}$ uma raiz de $f(x)$, então o menor subcorpo de $\mathbb{C}$ contendo $\mathbb{Q}$ e α é denotado por $\mathbb{Q}(\alpha)$, então

$$\mathbb{Q}(\alpha) = \{x + y\alpha : x, y \in \mathbb{Q}\}.$$

Teorema 1.3.11 *Se K é um corpo quadrático, então existe um único inteiro livre de quadrados D tal que $K = \mathbb{Q}(\sqrt{D})$.*

Demonstração: Suponha que $K = \mathbb{Q}(\alpha)$, onde α é uma raiz do polinômio mônico irredutível $f(x) = x^2 + bx + c$.
Pela formula quadrática temos que $\alpha \in \{\alpha_1, \alpha_2\}$, onde

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4c}}{2} \quad e \quad \alpha_2 = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

Note que $\alpha_1 = -\alpha_2 - b$ com $b \in \mathbb{Q}$ então $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha)$. Logo

$$\mathbb{Q}(\alpha_1) = \mathbb{Q}\left(\frac{-b + \sqrt{b^2 - 4c}}{2}\right) = \mathbb{Q}(\sqrt{b^2 - 4c}).$$

Seja $a = b^2 - 4c = \dfrac{e}{f} \in \mathbb{Q}$, então $a \neq d^2$ para qualquer $d \in \mathbb{Q}$, pois $f(x)$ é irredutível em $\mathbb{Q}[x]$. Sem perda de generalidade, podemos supor que $mdc(e, f) = 1$ e f é positivo. Seja $ef = n^2 D$, em que D é a parte livre de quadrados de ef. Assim, $D \neq 1$ e

$$\mathbb{Q}\left(\sqrt{a}\right) = \mathbb{Q}\left(\sqrt{b^2 - 4c}\right) = \mathbb{Q}\left(\sqrt{\frac{ef}{f^2}}\right) = \mathbb{Q}\left(\sqrt{ef}\right) = \mathbb{Q}\left(\sqrt{n^2 D}\right) = \mathbb{Q}\left(\sqrt{D}\right),$$

logo $\mathbb{Q}\left(\dfrac{e}{f}\right) = \mathbb{Q}(ef)$, Isso mostra a existência.
Provemos agora a unicidade.
Seja D_1 é um inteiro livre de quadrados tal que $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}\left(\sqrt{D_1}\right)$. Então $\sqrt{D} = u + v\sqrt{D_1}$ com $u, v \in \mathbb{Q}$ e elevando ao quadrado temos

$$D = u^2 + 2uv\sqrt{D_1} + v^2 D_1.$$

Suponha, por absurdo, que $uv \neq 0$. Daí, temos que

$$\sqrt{D_1} = \frac{D - u^2 - Dv^2}{2uv}$$

logo $\sqrt{D_1} \in \mathbb{Q}$ o que é uma contradição já que D_1 é livre de quadrados, logo $uv = 0$. Se $v = 0$ então $\sqrt{D} = u \in \mathbb{Q}$, o que é, novamente, uma contradição com o fato de que D é livre de quadrados então $v^2 = 1$ e portanto $D = D_1$. ■

Agora vamos a determinar o conjunto O_K dos inteiros algébricos no corpo quadrático $K = \mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$, onde D é um inteiro livre de quadrados.

Teorema 1.3.12 (Anéis de inteiros em corpos Quadráticos) *Se K é um corpo quadrático e seja D o único inteiro livre de quadrados tal que $K = \mathbb{Q}(\sqrt{D})$ então*

$$O_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & , se\ D \equiv 1\ (mod\ 4) \\ \mathbb{Z}\left[\sqrt{D}\right] & , se\ D \not\equiv 1\ (mod\ 4). \end{cases}$$

A fim de demostrar o Teorema 1.3.12, vamos precisar do seguinte Teorema, que pode ser encontrado como Teorema 5.3.2, pag 92 [2].

Teorema 1.3.13 *Se α é um inteiro algébrico, então $irr_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$.*

Demonstração: (do Teorema 1.3.12)Seja

$$\sigma = \begin{cases} 2 & , \text{se } D \equiv 1\ (mod\ 4) \\ 1 & , \text{se } D \not\equiv 1\ (mod\ 4). \end{cases}$$

Então o número $\dfrac{1+\sqrt{D}}{\sigma}$ é uma raiz de $x^2 - \dfrac{2x}{\sigma} + \dfrac{1+D}{\sigma^2}$ então temos

$$\mathbb{Z} + \mathbb{Z}\left(\frac{\sigma - 1 + \sqrt{D}}{\sigma}\right) \subseteq O_K.$$

Provemos que

$$O_K \subseteq \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & , \text{se } D \equiv 1\ (mod\ 4) \\ \mathbb{Z}\left[\sqrt{D}\right] & , \text{se } D \not\equiv 1\ (mod\ 4). \end{cases}$$

Seja $\alpha \in O_K$ então $\alpha \in K$ e $\alpha = a + b\sqrt{D}$ para alguns $a, b \in \mathbb{Q}$. Então α é raiz do polinômio mônico

$$x^2 - 2ax + (a^2 - Db^2) \in \mathbb{Q}[x].$$

Temos que o discriminante deste polinômio é

$$(2a)^2 - 4(a^2 - Db^2) = 4Db^2,$$

deste modo temos que é redutível em $\mathbb{Q}[x]$ se $b = 0$ e irredutível em $\mathbb{Q}[x]$ se $b \neq 0$. Consequentemente temos que

$$irr_{\mathbb{Q}}(\alpha) = \begin{cases} x - a & , \text{se } b = 0 \\ x^2 - 2ax + (a^2 - Db^2) & , \text{se } b \neq 0, \end{cases}$$

em que $irr_{\mathbb{Q}}(\alpha)$ é o polinômio minimal de α sobre K.

Como α é um inteiro algebrico então $irr_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$ (Teorema 1.3.13), assim obtemos que

$$\begin{cases} a \in \mathbb{Z} & , \text{se } b = 0 \\ 2a,\ a^2 - Db^2 \in \mathbb{Z} & , \text{se } b \neq 0. \end{cases}$$

Se $b = 0$ então temos $\alpha = a \in \mathbb{Z} \subset \mathbb{Z}[x]$. Agora suponhamos que $b \neq 0$. Se $2a \in 2\mathbb{Z}$ então $a \in \mathbb{Z}$ e como $Db^2 \in \mathbb{Z}$ e dado que D é livre de quadrados temos que $b \in \mathbb{Z}$, nesse caso $\alpha = a + b\sqrt{D} \in \mathbb{Z}[D]$.

Suponha agora $2a \in 2\mathbb{Z} + 1$. Como $4(a^2 - Db^2) \in \mathbb{Z}$ deduzimos que $4Db^2 \in \mathbb{Z}$ e como D é livre de quadrados temos que $2b \in \mathbb{Z}$. Se $2b \in 2\mathbb{Z}$ então $b \in \mathbb{Z}$ e assim $a^2 = (a^2 - Db^2) + Db^2 \in \mathbb{Z}$, contradizendo $2a \in 2\mathbb{Z} + 1$. Assim $2b \in 2\mathbb{Z} + 1$. Portanto $a = \dfrac{2u+1}{2}$ e $b = \dfrac{2v+1}{2}$ em que $u, v \in \mathbb{Z}$. Logo

$$\begin{aligned} a^2 - Db^2 &= \frac{(2u+1)^2}{4} + \frac{D(2v+1)^2}{4} \\ &= \frac{4u^2 + 4u + 1 - D(4v^2 + 4v + 1)}{4} \\ &= u^2 + u - D(v^2 - v) + \frac{1 - D}{4} \end{aligned}$$

que implica

$$\frac{1 - D}{4} = u^2 + u - D(v^2 - v) - a^2 + Db^2 \in \mathbb{Z}.$$

Assim, temos que $D \equiv 1 \ (mod\ 4)$ e

$$\begin{aligned}\alpha = a + b\sqrt{D} &= \frac{2u+1}{2} + \frac{2v+1}{2}\sqrt{D} \\ &= \frac{2u - 2v + 2v + 2v\sqrt{D} + 1 + \sqrt{D}}{2} \\ &= \frac{2u - 2v + (2u+1)(1+\sqrt{D})}{2} \\ &= (u-v) + (2v+1)\left(\frac{1+\sqrt{D}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right].\end{aligned}$$

Isso completa a prova do teorema. ■

1.3.3 Discriminante e Base Integral

Dado um corpo numérico K, seja α um inteiro algébrico tal que $K = \mathbb{Q}(\alpha)$. Dado $\beta \in K$, podemos escrevê-lo como ser escrito como

$$\beta = q_0 + q_1\alpha + \cdots + q_{d-1}\alpha^{d-1} \in \mathbb{Q}$$

em que $|K : \mathbb{Q}| = d$. Em outras palavras, $\{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$ é uma base para K.

Definição 1.3.14 (Base integral) *Se O_K é um anel de inteiros de um corpo numérico K, então uma base de O_K sobre $\mathbb{Z}$ é chamada uma base integral de K.*

Corolário 1.3.15 *A base integral de $K = \mathbb{Q}(\sqrt{D})$ é igual a*

$$\begin{cases} \{1, \frac{1+\sqrt{D}}{2}\} & , se\ D \equiv 1\,(mod\ 4), \\ \{1, \sqrt{D}\} & , se\ D \not\equiv 1\,(mod\ 4). \end{cases}$$

Demonstração: Segue do Teorema 1.3.12. ■

Exemplo 1.3.16 *Se $K = \mathbb{Q}(\sqrt{2})$, então $O_K = \mathbb{Z}[\sqrt{2}]$ pelo Teorema 1.3.12. Logo $B = \{1, \sqrt{2}\}$ é uma base integral para K.*

Exemplo 1.3.17 *Se $K = \mathbb{Q}(\sqrt{13})$, então pelo teorema 1.3.12 temos*

$$O_K = \mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right] \neq \mathbb{Z}[\sqrt{13}]$$

em que $\alpha = \frac{1+\sqrt{13}}{2}$ é uma raiz do polinômio minimal $P(x) = x^2 - x - 3$, enquanto que $\beta = \sqrt{13}$ é uma raiz de $H(X) = x^2 - 13$. Assim, embora $\{1, \beta\}$ seja uma base para K consistindo de inteiros algébricos, não é uma base integral para K. Uma base integral para K é $\{1, \alpha\}$.

Lembre-se que o discriminante de un corpo numérico algébrico K é o discriminante de uma base integral de K.

Definição 1.3.18 (Discriminante de uma Base) *Seja $K = \mathbb{Q}(\alpha)$ um corpo numérico algébrico com $|K : \mathbb{Q}| = d$. Se $B = \{\alpha_1, \alpha_2, ..., \alpha_d\}$ é uma base de K e θ_j $(1 \leq j \leq d)$ são todas as imersões de K em $\mathbb{C}$, então o discriminante da base é dada por*

$$disc(B) = det(\theta_j(\alpha_i))^2,$$

onde det denota o determinante da matriz com entrada $\theta_j(\alpha_i)$ na i-ésima linha e j-ésima coluna.
Em particular, se $B = \{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$, então o determinante da matriz $(\theta_j(\alpha^{i-1}))$ é chamado o determinante de Vandermonte e tem valor

$$det(\theta_j(\alpha^{i-1})) = \prod_{1 \leq i < j \leq d} (\alpha_j - \alpha_i)$$

onde $\alpha_K = \theta_K(\alpha)$ é o K-ésimo conjugado de α para $K = 1, 2, ..., d$.

Teorema 1.3.19 (Discriminante de corpo quadrático) *Se D é o único inteiro livre de quadrados tal que $K = \mathbb{Q}(\sqrt{D}\,)$ é um corpo quadrático, então o discriminante de K é dado por*

$$\Delta_K = \begin{cases} D & , se\ D \equiv 1\,(mod\ 4), \\ 4D & , se\ D \not\equiv 1\,(mod\ 4). \end{cases}$$

Demonstração: Seja $K = \mathbb{Q}(\sqrt{D})$ um corpo quadrático, onde $D \not\equiv 1(mod\ 4)$. Então pelo Teorema 1.3.12, temos que $O_K = \mathbb{Z}[\sqrt{D}]$. Assim, $B = \{1, \sqrt{D}\}$ é uma base integral de K e

$$\theta_1 : \sqrt{D} \mapsto \sqrt{D} \quad e \quad \theta_2 : \sqrt{D} \mapsto -\sqrt{D}$$

são imersões de K em $\mathbb{C}$, então

$$\begin{aligned} disc(B) = det(\theta_j(\alpha^{i-1}))^2 &= det \begin{pmatrix} \theta_1(1) & \theta_2(1) \\ \theta_1(\sqrt{D}) & \theta_2(\sqrt{D}) \end{pmatrix}^2 \\ &= det \begin{pmatrix} 1 & 1 \\ \sqrt{D} & -\sqrt{D} \end{pmatrix}^2 = (-2\sqrt{D})^2 = 4D. \end{aligned}$$

Vamos considerar $D \equiv 1(mod\ 4)$. Então pelo Teorema 1.3.12, temos que $O_K = \mathbb{Z}[\sqrt{D}]$. Assim, $B = \{1, \frac{1+\sqrt{D}}{2}\}$ é uma base integral de K e

$$\theta_1 : \frac{1+\sqrt{D}}{2} \mapsto \frac{1+\sqrt{D}}{2} \quad e \quad \theta_2 : \frac{1+\sqrt{D}}{2} \mapsto \frac{1-\sqrt{D}}{2}$$

são imersões de K em $\mathbb{C}$. Então

$$\begin{aligned} disc(B) = det(\theta_j(\alpha^{i-1}))^2 &= det\begin{pmatrix} \theta_1(1) & \theta_2(1) \\ \theta_1\left(\frac{1+\sqrt{D}}{2}\right) & \theta_2\left(\frac{1+\sqrt{D}}{2}\right) \end{pmatrix}^2 \\ &= det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{D}}{2} & \frac{1-\sqrt{D}}{2} \end{pmatrix}^2 \\ &= \left(\frac{1-\sqrt{D}}{2} - \frac{1+\sqrt{D}}{2}\right)^2 = \left(-\sqrt{D}\right)^2 = D. \end{aligned}$$

■

Teorema 1.3.20 (Unidades em corpos quadráticos imaginário) *Se $K = \mathbb{Q}(\sqrt{D})$ é um corpo quadrático imaginário, isto é $D < 0$, então*

$$U_K = U_{O_K} = \begin{cases} \langle\zeta_6\rangle = \langle\frac{1+\sqrt{-3}}{2}\rangle & , se\ K = \mathbb{Q}(\sqrt{-3}), \\ \langle\zeta_4\rangle = \langle\sqrt{-1}\rangle & , se\ K = \mathbb{Q}(\sqrt{-1}), \\ \langle\zeta_2\rangle = \langle -1\rangle & , caso\ contrário. \end{cases}$$

Demonstração: Pelo Teorema 1.3.12 podemos escrever $u = a + b\sqrt{D} \in U_{O_K}$ com $\sigma a, \sigma b \in \mathbb{Z}$ onde σ é definido como no Teorema 1.3.12. Daqui, se $D \not\equiv 1\,(mod\ 4)$ então $a^2 - b^2D = 1$ para alguns $a, b \in \mathbb{Z}$. Se $D < -1$, então $a^2 - b^2D > 1$ para $b \neq 0$. Então, $b = 0$ para $D \not\equiv 1\,(mod\ 4)$ com $D < -1$. Em outras palavras

$$U_{O_K} = \langle -1\rangle = \langle\zeta_2\rangle \ \ se\ \ D \equiv 2, 3\,(mod\ 4)\ \ e\ \ D < -1.$$

Agora assumimos que $D \equiv 1(mod\ 4)$, então $a^2 - b^2D = 4$ para $a, b \in \mathbb{Z}$. Se $D < -4$, então para $b \neq 0$, $a^2 - Db^2 > 4$, uma contradição. Daqui, para $D \equiv 1(mod\ 4)$ e $D < -4$, $U_{O_K} = \langle\zeta_2\rangle$. Resta considerar os casos $D = -1, -3$. Se $D = -1$ então pelo Teorema 1.3.12 $O_K = \mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ com $a + bi$ uma unidade de O_K se, e somente se $a^2 + b^2 = 1$. As soluções são $(a, b) \in \{(0\pm, 1), (\pm 1, 0)\}$.

Em outras palavras

$$U_{\mathbb{Q}[i]} = \{\pm 1, \pm i\}$$

Se $D = -3$ então $a^2 + 3b^2 = 4$, então temos $a = b = \pm 1$ ou $b = 0$ e $a = \pm 2$. Portanto

as unidades são $\pm 1, \frac{-1+\sqrt{-3}}{2}$. No entanto, $1 = \zeta_6^6$ e temos:

$$\begin{aligned} -1 &= \zeta_6^3 \\ \frac{1-\sqrt{-3}}{2} &= \zeta_6^5 \\ \frac{1+\sqrt{-3}}{2} &= \zeta_6^2 \end{aligned}$$

e

$$\frac{-1-\sqrt{-3}}{2} = \zeta_6^5,$$

assim, $U_{O_K} = \langle \zeta_6 \rangle$, como se queria provar. ■

Capítulo 2

A Equação Diofantina $x^2 + C = y^n$

Neste capítulo apresentamos os conceitos e propriedades relacionados à equação $x^2 + C = y^n$. Iniciamos, com um breve *survey* sobre resultados relacionados com essa equação e apresentamos alguns resultados sobre soluções de equações Diofantinas semelhantes em estrutura à equação que queremos desenvolver neste trabalho.

Na seção 2.2, apresentamos o resultado de Attila Bérczeso, o qual estende o resultado de Saradha e Srinivasan [41] e Le e Zhu [45], que resolvem completamente a equação $x^2 + d^{2l+1} = y^n$ sob a hipótese de $h(-d) = 1$.

Finalmente apresentamos, na seção 2.3, o resultado de Pan Xioawei, que faz uma classificação completa de todas as soluções positivas (x, y, m, n) da equação $x^2 + p^{2m} = y^n$, $mdc(x, y) = 1$, com $n > 2$.

Muitos casos especiais da equação $x^2 + C = y^n$, onde x e y são inteiros positivos e $n \geq 3$, foram considerados ao longo dos anos, mas a maioria dos resultados para n geral é de origem bastante recente. A referência mais antiga parece ser uma afirmação de Fermat de que ele havia mostrado que, quando $C = 2$, $n = 3$, a única solução é dada por $x = 5$, $y = 3$; uma prova foi publicada por Euler [18]. O primeiro resultado para n geral é devido a V. A. Lebesgue [25] que provou que quando $C = 1$ não há soluções. Nagell [38] provou que não há soluções para $C = 3$ e $C = 5$, mas não completou uma prova para $C = 2$. Ljunggren [26] generalizou o resultado de Fermat e provou que para $C = 2$ a equação não tem outra solução senão $x = 5$, um resultado redescoberto por Nagell [39], que também mostrou em [40] que quando $C = 4$ as únicas soluções são

$x = 2$ e $x = 11$. Chao Ko [21] provou que $x = 3$ é a única solução para $C = -1$.

Nesta capítulo, vamos olhar soluções inteiras da equação $x^2 + C = y^n$, onde C e n são inteiros dados para $n \geq 3$ (de outra maneira a equação é trivial).

Comentários sobre o caso n par

Vamos escrever $n = 2m$, e nossa equação pode ser reescrita como $C = (y^m + x)(y^m - x)$. Observe que podemos considerar somente soluções com $x, y \geq 0$, pois obtemos imediatamente que $(x, -y), (-x, y)$ e $(-x, -y)$ também serão soluções. Assim vamos assumir $y^m + x \geq y^m - x$. Vamos considerar dois casos simples.

Se $C = 1$, teremos $1 = y^m + x = y^m - x$, logo $x = 0$ e $y = 1$ são soluções.

Se $C = 4$ temos duas possibilidades:

(i) $y^m + x = 4$, $y^m - x = 1$

e

(ii) $y^m + x = y^m - x = 2$

No caso (i), obtemos $2x = 3$, logo $x \notin \mathbb{Z}$ ou seja, não existem soluções. No caso (ii) obtemos $x = 0$ e $y^m = 2$. Logo existem soluções para a equação $x^2 + 4 = y^{2m}$, somente se $m = 1$ e as soluções para esse caso serão $x = 0$ e $y = \pm 2$.

Podemos prosseguir um pouco mais e considerar C um primo. Nesse caso, $y^m + x = C$ e $y^m - x = 1$. Logo $x = \dfrac{C-1}{2}$ e $y^m = \dfrac{C+1}{2}$. Considerando C primo e $C < 100$, é fácil verificar a equação $x^2 + C = y^{2m}$ tem solução somente para $C \in \{7, 17, 31, 53, 71, 97\}$ e as soluções são facilmente obtidas pelas fórmulas acima. Outra consequência imediata desas formulas é que se $C = 2^{m+1} + 1$ então a equação $x^2 + C = y^{2m}$ tem solução.

Teorema 2.0.1 *Seja $n \geq 4$ par e seja C um inteiro positivo com $1 \leq C \leq 100$ livre de quadrados não congruente a -1 módulo 8. Os únicos valores de n e C para os quais a equação Diofantina $x^2 + C = y^n$ tem solução são para $(n, C = 1)$ com soluções $(x, y) = (0, \pm 1)$ ou $(n, C) \in \{(4, 17), (6, 53), (4, 65), (4, 77), (4, 97)\}$ com as respectivas soluções $(x, y) = (\pm 8, \pm 3)$, $(\pm 26, \pm 3)$,$(\pm 4, \pm 3)$,$(\pm 2, \pm 3)$ e $(\pm 48, \pm 7)$.*

Demonstração: Seja $n \geq 4$ um inteiro e C um inteiro positivo com $1 \leq C \leq 100$ livre de quadrados tal que $C \not\equiv -1 (mod\ 8)$. Vamos a considerar dois casos, o primeiro caso quando C é par e o segundo quando C é ímpar.

(i) Suponhamos C par, então $C = 2r$, com $r \in \mathbb{N}$, então a equação $x^2 + C = y^{2m}$, pode ser escrita como $(y^m + x)(y^m - x) = C$. Fatore $r = p_1 \cdots p_k$ como produto de primos, com $k \in \mathbb{N}$, temos os seguintes sub-casos:

1. $y^m + x = 2r$, $y^m - x = 1$. Neste caso, $2x = 2r + 1$, o que implica que $x \notin \mathbb{Z}$. Logo não existem soluções.
2. $y^m + x = r$, $y^m - x = 2$. Como C é livre de quadrados temos que $C = 2r = 2(p_1 \cdot p_2 \cdot ... \cdot p_k)$, $k \in \mathbb{N}$, com p_i primos diferentes e $p_i \neq 2$. Temos que $2x = r - 2 = 2l + 1 - 2 = 2l - 1$, $l \in \mathbb{N}$, logo $x \notin \mathbb{Z}$. Assim temos que não existem soluções.
3. $y^m + x = p_1 \cdot ... \cdot p_j$ e $y^m - x = 2 \cdot p_{j+1} \cdot ... \cdot p_k$, com $1 \leq j < k$, segue análogo ao caso 2. Assim temos que não existem soluções.
4. $y^m + x = 2 \cdot p_1 \cdot ... \cdot p_i$ e $y^m - x = p_{i+1} \cdot ... \cdot p_k$, com $1 \leq i < k$, segue análogo ao caso 2. Assim temos que não existem soluções.

Portanto para C par não existem soluções para a equação $x^2 + C = y^{2m}$.

(ii) Suponhamos C ímpar, como C é livre de quadrados e não congruente a -1 modulo 8 com $1 \leq C \leq 100$, temos que C pertence ao conjunto $E = \{1, 3, 5, 11, 13, 17, 19, 21, 29, 33, 35, 37, 41, 43, 51, 53, 57, 59, 61, 65, 67, 69, 73, 77, 83, 85, 89, 91, 93, 97\}$.

Agora a equação $x^2 + C = y^n$ pode ser escrita como $y^m + x = p_1$ e $y^m - x = p_2$, onde p_1 e p_2 são números primos (se C não for primo), podendo ocorrer $p_1 = 1$ ou $p_2 = 1$ (se C for primo). Logo $x = \dfrac{p_1 - p_2}{2}$ e $y^m = \dfrac{p_1 + p_2}{2}$. Logo podemos verificar que os elementos do conjunto E para os quais a equação $x^2 + C = y^n$ tem solução são $(n, C, x, y) \in \{(n, 1, 0, \pm 1), (4, 17, \pm 8, \pm 3), (6, 53, \pm 26, \pm 3), (4, 65, \pm 4, \pm 3), (4, 77, \pm 2, \pm 3), (4, 97, \pm 48, \pm 7)\}$.

■

2.1 O caso C livre de quadrados

Nesta seção seguimos a apresentação dada em [16]. Inicialmente observe que é suficiente resolver a equação $x^2 + C = y^p$, com p primo. Pois se $n = p \cdot Q$ então a

equação $x^2 + C = y^n$ pode ser escrita como $x^2 + C = (y^Q)^p$ que, em principio sabemos resolver. Por razões que logo se tornarão claras, fazemos as seguintes definições.

Definição 2.1.1 *Diremos que a condição $H(p, C)$ é satisfeita por p e C, se p for um primo ímpar, C é inteiro positivo livre de quadrados não congruente a -1 módulo 8, e p não divide o número de classes do corpo quadrático imaginário $\mathbb{Q}(\sqrt{-C})$. Por abuso de notação, vamos dizer que $H(C)$ está satisfeito se C é um inteiro positivo livre de quadrados não congruente a -1 módulo 8.*

Proposição 2.1.2 *Assuma que $H(p, C)$ é satisfeita e defina $A_p(C)$ para ser o (possivelmente vazio) conjunto de inteiros não-negativos que satisfazem*

$$\sum_{k=0}^{(p-1)/2} \binom{p}{2k} a^{2k}(-C)^{[(p-1)/2]-k} = \pm 1.$$

O conjunto de soluções $(x, y) \in \mathbb{Z}^2$ da equação Diofantina $x^2 + C = y^n$ é dada pelo par

$$(x, y) = \left(\pm \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} a^{2k+1}(-C)^{[(p-1)/2]-k},\ a^2 + C \right)$$

para cada $a \in A_p(C)$, além dos chamados pares especiais

$$(x, y) = (\pm(a^3 + 3\varepsilon a), a^2 + 2\varepsilon)$$

se p=3 e $C = 3a^2 + 8\varepsilon$ para $\varepsilon = \pm 1$ e a impar tal que $a \geq 1$ se $\varepsilon = 1$ ou $a \geq 3$ se $\varepsilon = -1$.

Demonstração: Seja (x, y) uma solução da equação $x^2 + C = y^p$. No corpo quadrático $K = \mathbb{Q}(\sqrt{-C})$ podemos escrever $(x - \sqrt{-C})(x + \sqrt{-C}) = y^p$. Notemos que os ideais formados pelos dois fatores a esquerda são coprimos. De fato, assuma o contrário, então seja I um ideal primo de O_K dividindo esses fatores. Assim, divide sua soma e diferença, então se q é o menor número primo em I temos que $q \,|\, 2x$ e $q \,|\, 2C$. Se y é par, então x é ímpar (caso contrário $4 \,|\, C$, o que contradiz o fato de C ser livre de quadrados), então $C = y^p - x^2 \equiv -1 (mod\ 8)$, contradiz nossa suposição sobre C. Assim y é ímpar, portanto, I não pode conter 2. Como $q \,|\, mdc(x, C)$ então $q \,|\, y$, logo $q^2 \,|\, C$, novamente contradizendo o fato de que C é livre de quadrados e provando a afirmação. Já que o produto dos dois ideais coprimos $(x - \sqrt{-C})O_K$ e $(x + \sqrt{-C})O_K$ é uma p - ésima potência, segue-se que $(x + \sqrt{-C})O_K = \mathfrak{a}^p$ para algum ideal $\mathfrak{a}$ de O_K. Por outro

lado, se h denota o número de classes de K, então, o ideal $\mathfrak{a}^h$ é um ideal principal. Já que por suposição p e h são coprimos, existem inteiros v e w tal que $vp + wh = 1$, de modo que $\mathfrak{a} = (\mathfrak{a}^p)^v(\mathfrak{a}^h)^w$ é um ideal principal, digamos $\mathfrak{a} = \alpha O_K$ para algum $\alpha \in O_K$. Deduzimos assim que existe uma unidade $\varepsilon \in K$ tal que $x + \sqrt{-C} = \varepsilon\alpha^p$. No entanto, como K é um corpo quadrático imaginário, então o grupo de unidades é $\{\pm 1\}$ exceto para $C = 1$ e $C = 3$. Nesses casos, os grupos tem ordem 4 e 6 respetivamente. Segue-se que além do caso especial $(p, C) = (3, 3)$ a ordem do grupo de unidades é coprima com p, daí qualquer unidade é uma p-ésima potência, então, nesses casos, a equação fica reduzida a $x + \sqrt{-C} = \alpha^p$ com $\alpha \in O_K$. Veremos na Proposição 2.1.5 abaixo que não há solução para $(p, C) = (3, 3)$. De outra forma, escrevemos $\alpha = \dfrac{(a + b\sqrt{-C})}{d}$ com a e b inteiros, em que $d = 1$ ou quando $C \equiv -5\,(mod\ 8)$, além $d = 2$ e a e b ímpares.
Expandindo a relação $x + \sqrt{-C} = \alpha^p$ obtemos as duas equações

$$\begin{aligned} d^p x &= \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} a^{2k+1} b^{p-2k-1} (-C)^{[(p-1)/2]-k} \\ &\quad e \\ d^p &= \sum_{k=0}^{(p-1)/2} \binom{p}{2k} a^{2k} b^{p-2k} (-C)^{[(p-1)/2]-k}, \end{aligned}$$

pois, temos que $d^p x + d^p\sqrt{-C} = (a + b\sqrt{-C})^p$, logo

$$\begin{aligned} (a + b\sqrt{-C})^p &= \sum_{k=0}^{p} \binom{p}{k} a^k (b\sqrt{-C})^{p-k} \\ &= \left[\binom{p}{0} a^0 (b\sqrt{-C})^p + \binom{p}{1} a^1 (b\sqrt{-C})^{p-1} + \cdots + \binom{p}{p} a^p (b\sqrt{-C})^0\right] \\ &= \left[\binom{p}{0} a^0 (b\sqrt{-C})^p + \binom{p}{2} a^2 (b\sqrt{-C})^{p-2} + \cdots + \binom{p}{p-1} a^{p-1} (b\sqrt{-C})\right] \\ &\quad + \left[\binom{p}{1} a (b\sqrt{-C})^{p-1} + \binom{p}{3} a^3 (b\sqrt{-C})^{p-3} + \cdots + \binom{p}{p} a^p (b\sqrt{-C})^0\right], \end{aligned}$$

da equação de acima denotaremos por

$$\begin{aligned} I &= \left[\binom{p}{0} a^0 (b\sqrt{-C})^p + \binom{p}{2} a^2 (b\sqrt{-C})^{p-2} + \cdots + \binom{p}{p-1} a^{p-1} (b\sqrt{-C})\right] \\ &\quad e \\ II &= \left[\binom{p}{1} a (b\sqrt{-C})^{p-1} + \binom{p}{3} a^3 (b\sqrt{-C})^{p-3} + \cdots + \binom{p}{p} a^p (b\sqrt{-C})^0\right], \end{aligned}$$

logo

$$\begin{aligned} I &= b\sqrt{-C}\sum_{k=0}^{(p-1)/2}\binom{p}{2k}a^{2k}(b\sqrt{-C})^{p-(2k+1)} \\ &= \sqrt{-C}\sum_{k=0}^{(p-1)/2}\binom{p}{2k}a^{2k}(b)^{p-2k}(-C)^{[(p-1)/2]-k} \end{aligned}$$

e

$$\begin{aligned} II &= \sum_{k=0}^{(p-1)/2}\binom{p}{2k+1}a^{2k+1}(b\sqrt{-C})^{p-(2k+1)} \\ &= \sum_{k=0}^{(p-1)/2}\binom{p}{2k+1}a^{2k+1}(b)^{p-2k-1}(-C)^{[(p-1)/2]-k}, \end{aligned}$$

logo, igualando as partes real e imaginaria obtemos:

$$\begin{aligned} d^p x &= \sum_{k=0}^{(p-1)/2}\binom{p}{2k+1}a^{2k+1}b^{p-2k-1}(-C)^{[(p-1)/2]-k} \\ &\quad e \\ d^p &= \sum_{k=0}^{(p-1)/2}\binom{p}{2k}a^{2k}b^{p-2k}(-C)^{[(p-1)/2]-k}. \end{aligned}$$

Notemos que podemos supor $a \geq 0$ pois mudar a para $-a$ não altera a segunda equação e mudar x para $-x$ não altera a primeira equação. Pela segunda equação concluí-se que $b \mid d^p$ e logo $b = \pm 1$. Segue que

$$d^p = \pm\sum_{k=0}^{(p-1)/2}\binom{p}{2k}a^{2k}(-C)^{[(p-1)/2]-k}$$

Se $d = 1$, obtemos a formula para x substituindo na primeira equação e temos $y = a^2 + b^2C$. Se $d = 2$, então já que p é um primo ímpar temos

$$2 \equiv 2^p \equiv \pm C^{(p-1)/2} \equiv \pm\left(\frac{-C}{p}\right) \equiv 0,\ \pm 1 (mod\ p),$$

o qual é possível para $p = 3$, dados $C = (3a^2 \mp 8)$, $x = -a^3 \pm 3a$, $y = a^2 \mp 2$, obtendo os casos dados na proposição. ■

Observação 2.1.3 *(i) Para dados C e p, em principio é possível encontrar todos os valores possíveis de $a \in A_p(C)$. O que é consideravelmente mais difícil em geral é encontrar os conjuntos $A_p(C)$ quando só p é fixo. Graças a um Teorema notavél de Bilu, Hanrot, e Voutier, esse problema esta parcialmente resolvido; ver abaixo.*

(ii) Considerando a fórmula módulo p, note que o sinal $\pm$ no lado direito da definição da fórmula $A_p(C)$ é igual a $\left(\frac{-C}{p}\right)$ (O Símbolo de Legendre).

Corolário 2.1.4 *Seja $p \geq 3$ um primo, seja x e y inteiros, e assuma que $C = y^p - x^2$ satisfazendo $H(C)$ (de modo que, em particular, x e y são coprimos e y é ímpar). Suponha também que $y - C$ é não quadrado, e além disso quando $p = 3$ temos que $(y, C) \neq (a^2 + 2\varepsilon, 3a^2 + 8\varepsilon)$ para algum ímpar a e algum $\varepsilon = \pm 1$. Então, o número de classes do corpo quadrático imaginário $\mathbb{Q}(\sqrt{-C})$ é divisível por p.*

2.1.1 O caso $p = 3$ e C livre de quadrados

Para aplicar a proposição 2.1.2 (*assumindo que $H(p, C)$* é satisfeita), resta encontrar os conjuntos $A_p(C)$. Como já mencionado, podemos conseguir, se p e C forem fixados. A dificuldade é dar resultados gerais quando apenas uma dessas duas variáveis é fixa. Vamos dar resultados detalhados abaixo e, em particular, resultados completos para alguns valores fixos de C. Nas próximas subseções, nós damos os resultados completos para p fixo.

Proposição 2.1.5 *Suponha que $H(3, C)$ é satisfeita.*

(i) Seja $C \equiv -2 \,(mod\ 4)$ ou $C \equiv -3 \,(mod\ 4)$. Então :

- *Se C não é da forma $3a^2 \pm 1$, com $\varepsilon \in \{\pm 1\}$, a equação $x^2 = y^3 - C$ não tem soluções inteiras.*
- *Se C é da forma $3a^2 + \varepsilon$, com $\varepsilon = \pm 1$, as soluções inteiras são $y = 4a^2 + \varepsilon$, $x = \pm 8a^3 + 3a\varepsilon$.*

(ii) Quando $C \equiv -5 \,(mod\ 8)$. Então :

- *Se C não é da forma $12a^2 - 1$ ou $3a^2 \pm 8$, ambos com a ímpar, a equação $x^2 + C = y^3$ não tem soluções inteiras.*
- *Se C é da forma $12a^2 - 1$, com a ímpar, as soluções inteiras são $y = 16a^2 - 1$, $x = \pm(64a^3 - 6a)$.*
- *Se C é da forma $3a^2 + 8\varepsilon$, com $\varepsilon = \pm 1$ e a ímpar, as soluções inteiras são $y = a^2 + 2\varepsilon$, $x = \pm(a^3 + 3a\varepsilon)$.*

Demonstração: Mostraremos apenas o caso (i). Neste caso, podemos ver que as equações que definem os conjuntos $A_3(C)$ são lineares em C. Obtemos também pela Proposição 2.1.2 que $C = 3a^2 \pm 1$, $y = a^2 + C$, e $x = \pm(a^3 - 3aC)$, para o qual devemos

adicionar as soluções para o caso especial $C = 3a^2 \pm 8$.

Agora consideremos o caso $C = 3$, que foi adiado em resultados anteriores. Na prova da Proposição 2.1.2, temos que $x + \sqrt{-C} = u\alpha^3$ para alguma unidade u. Então voltamos à equação da proposição, se $u = \pm 1$; ou existe $\varepsilon \in \{\pm 1\}$ tal que $x + \sqrt{-C} = ((a + b\sqrt{-C})/2)^3(-1 + \varepsilon\sqrt{-C})/2)$. Igualando os coeficientes de $\sqrt{-C}$ obtemos

$$16 = \varepsilon(a^3 - 9b^2a) - 3b(a^2 - b^2). \tag{2.1}$$

Se $a \equiv 0\,(mod\ 3)$, então $3 \mid 16$, oque é uma absurdo. Logo $3 \nmid a$. Se $b \equiv 0\,(mod\ 3)$, obtemos que $16 \equiv \varepsilon a^3\,(mod\ 9)$. Como $\varepsilon a^3\,(mod\ 9) \in \{\pm 1\}$, temos novamente uma contradição. Assim, nem a nem b são divisíveis por 3. Consequentemente $a^2 \equiv b^2 \equiv 1\,(mod\ 3)$, desta última congruência obtemos que 16 é congruente a $\varepsilon(a^3 - 9a)$. Note que o lado direito de (2.1) ainda é congruente a ± 1 módulo 9, o que é mais uma vez uma contradição, portanto não há soluções para $C = 3$. ■

Notemos que o caso $C = 2$ da equação $x^2 + C = y^3$ já foi resolvido por Fermat, que o colocou como um problema desafiador para seus contemporâneos ingleses.

2.1.2 Comentários sobre o caso $C < 0$ e $p = 3$.

Proposição 2.1.6 *Seja a um inteiro ímpar e seja b um inteiro tal que $3 \nmid b$. Suponha que $C = b^2 - 8a^3$, com b ímpar, ou que $C = 4b^2 - a^3$, com $C \not\equiv -1\,(mod\ 8)$. Então, se C é livre de quadrados, podendo ser positivo ou negativo, a equação $x^2 + C = y^3$ não tem solução inteira.*

Demonstração: Notemos que em ambos casos C é ímpar. Podemos comprovar que y deve ser impar e x par. De fato, se y é par, então $x^2 = y^3 - C$ é ímpar o que implica em $C \equiv y^3 - x^2 \equiv -1\,(mod\ 8)$, o que contradiz a suposição do segundo caso e contradiz a congruência $C \equiv b^2 \equiv 1\,(mod\ 8)$ do primeiro caso.

Agora separamos os casos e reescrevemos a primeira equação $x^2 = y^3 + (8a^3 - b^2)$ como

$$x^2 + b^2 = (y + 2a)((y - a)^2 + 3a^2).$$

Como y e a são ímpares, segue que $(y - a)^2 + 3a^2 \equiv 3(mod\ 4)$ e como esse é um número positivo, isso implica que existe um primo $p \equiv 3(mod\ 4)$ dividindo $(y-a)^2+3a^2$

com uma potência ímpar. Portanto, $x^2 + b^2 \equiv 0\,(mod\ p)$ e como $\left(\frac{-1}{p}\right) = -1$, então p divide b e x. Podemos afirmar que $p \nmid (y + 2a)$. De fato, dado

$$(y - a)^2 + 3a^2 = (y + 2a)(y - 4a) + 12a^2$$

se $p|(y + 2a)$ temos então que $p \mid 12a^2$, ou seja, temos que ou $p \mid a$ ou $p = 3$ ($p = 2$ é impossível já que $p \equiv 3(mod\ 4)$). Mas $p \mid a$ implica $p^2 \mid -C = 8a^3 - b^2$, o que é uma contradição, já que C é livre de quadrados. Enquanto que $p = 3$, implica $3 \mid b$, contraria uma hipótese, provando a afirmação. Assim, a avaliação p-ádica de $x^2 + b^2$ é igual à avaliação p-ádica de $(y - a)^2 + 3a^2$, o que é uma contradição, já que $(y - a)^2 + 3a^2$ é ímpar, portanto $\left(\frac{-1}{p}\right) = -1$.
Para o segundo caso, já que x é par escrevemos $x = 2x_1$, onde $x_1 \in \mathbb{Z}$, então reescrevemos a equação $x^2 = y^3 + (a^3 - 4b^2)$ como

$$4(x_1^2 + b^2) = y^3 + a^3 = (y + a)(y(y - a) + a^2).$$

Como $y - a$ é par e a é ímpar, segue-se que $4 \mid (y + a)$. Fazendo $y + a = 4y_1$, onde $y_1 \in \mathbb{Z}$ obtemos

$$x_1^2 + b^2 = y_1((4y_1 - a)(4y_1 - 2a) + a^2) = y_1(16y_1^2 - 12ay_1 + 3a^2).$$

Já que a é ímpar temos $16y_1^2 - 12ay_1 + 3a^2 \equiv 3\,(mod\ 4)$. Assim como na prova anterior existe um primo $p \equiv 3(mod\ 4)$ dividindo essa expressão com uma potência ímpar. Como acima, isso implica que p divide x_1 e b. Pode-se afirmar que $p \nmid y_1$. De fato, caso contrário $p \mid 3a^2$, então $p \mid a$ ou $p = 3$. Como acima, $p \mid a$ é impossível, uma vez que implica $p^2 \mid C$, uma contradição desde que C é livre de quadrados, se $p = 3$, então $3 \mid b$, que foi excluído. Assim, a avaliação p-ádica de $x^2 + b^2$ é ímpar, uma contradição, isso implicaria $\left(\frac{-1}{p}\right) = -1$. ■

A Proposição 2.1.5 aplica-se a C livre de quadrado, negativo, não congruente a -1 módulo 8, de modo que o número da classe de $\mathbb{Q}(\sqrt{-C})$ não é divisível por 3. A Proposição 2.1.6 acima resolve a equação $x^2 + C = y^3$ para os seguintes valores adicionais de C com $|C| < 250$: $C = 241, 129$ (número de classe divisível por 3), -7, -11, -13, -23, -39, -47, -53, -61, -67, -83, -87, -95, -109, -139, -155, -159, -167, -191, -215, -239 ($C < 0$).

Finalmente, note que já se resolveu o caso $C = -1$ (Corolário 6.4.32), página 386, [15], como uma aplicação do teorema de Skolem.

2.1.3 O caso $p = 5$ e C livre de quadrados

Neste caso, podemos também dar uma resposta completa da seguinte forma.

Proposição 2.1.7 *Suponha que $H(5, C)$ é satisfeita. Os únicos valores de C para os quais a equação $x^2 + C = y^5$ tem uma solução são $C = 1$ (com única solução $(x, y) = (0, 1)$), $C = 19$ (com únicas soluções $(x, y) = (\pm 22434, 55)$), e $C = 341$ (com únicas soluções $(x, y) = (\pm 2759646, 377)$).*

A fim de demostrar a Proposição 2.1.7, vamos precisar do seguinte lema, que pode ser encontrado como Corolário 6.8.4, pag 423, [15], consequência do estudo de quadrados nas sequências de Lucas e Fibonacci.

Lema 2.1.8 *Considere a equação Diofantina*

$$y^2 = 5x^4 + a.$$

(i) Para $a = 1$, as únicas soluções inteiras são $(x, y) = (0, \pm 1)$ e $(\pm 2, \pm 9)$.

(ii) Para $a = -1$, as únicas soluções inteiras são $(x, y) = (\pm 1, \pm 2)$.

(iii) Para $a = 4$, as únicas soluções inteiras são $(x, y) = (0, \pm 2)$,$(\pm 1, \pm 3)$ e $(\pm 12, \pm 322)$.

(iv) Para $a = -4$, as únicas soluções inteiras são $(x, y) = (\pm 1, \pm 1)$.

Demonstração: (**da Proposição** 2.1.7) A equação que define o conjunto $A_5(C)$ (via Proposição 2.1.2) é $C^2 - 10a^2C + 5a^4 \pm 1 = 0$. Isto tem uma solução racional em C se, e somente se, o discriminante é um quadrado, consequentemente, se, e somente se, $20a^4 \mp 1 = b^2$, para algum inteiro b. Olhando módulo 4 concluímos que $b^2 = 20a^4 + 1$, já que $b^2 \equiv -1 \, (mod\ 4)$ não tem solução em $\mathbb{Z}$ e portanto $(2b)^2 = 5(2a)^4 + 4$. Essa é uma das equações que são resolvidas no Lema 2.1.7. Concluímos que $a = 0$ ou $a = \pm 6$. O valor $a = 0$ leva a $C = 1$ (dando a solução $(x, y) = (0, 1)$) e $a = \pm 6$ leva a $C = 19$, $(x, y) = (\pm 22434, 55)$ e $C = 341$, $(x, y) = (\pm 2758646, 377)$. ■

O seguinte Corolário é um fortalecimento do Corolário 2.1.4, no caso $p = 5$.

Corolário 2.1.9 *Sejam x e y inteiros tais que o par ordenado (x, y) não é igual a $(0, 1), (\pm 22434, 55)$, ou $(\pm 2758646, 377)$. Suponha que $C = y^5 - x^2$ satisfaz $H(C)$ (de modo que, em particular, x e x são coprimos e y é ímpar). Então o número de classes do corpo quadrático imaginário $\mathbb{Q}(\sqrt{-C})$ é divisível por 5.*

Notemos que é necessário impor algumas condições em x e y. Por exemplo, se $(x, y) = (5, 2)$ temos que $C = 7 \equiv -1 \, (mod\ 8)$, mas o número de classes de $\mathbb{Q}(\sqrt{-7})$ é 1. No entanto, pode-se mostrar que, se assumirmos que apenas x e y são coprimos, mas C não necessariamente livres de quadrados, então o número da classe da ordem quadrática do discriminante C (*ou* $-4C$ *se* $C \equiv -2$ *ou* -3 módulo 4) é divisível por 5.

2.1.4 Aplicação do Teorema de Bilu-Hanrot-Voutier

Para tratar o caso $p \geq 7$, usamos um teorema notável dos autores acima, mencionado no Capítulo 1. O teorema a seguir apresenta um caso especial do Teorema 1.2.2 no Capítulo 1.

Teorema 2.1.10 *Seja $L_n = L_n(\alpha, \beta)$ uma sequência de Lucas como na Definição* 1.2.1 *. Então*

(i) Se $n > 30$, L_n sempre tem um divisor primitivo.

(ii) Se $5 < n < 30$ é primo e $L_n = L_n(\alpha, \beta)$ não tem divisor primitivo, então
ou $n = 7$ e $(\alpha, \beta) = ((1 + \sqrt{-7})/2, (1 - \sqrt{-7})/2)$,
ou $n = 7$ e $(\alpha, \beta) = ((1 + \sqrt{-19})/2, (1 - \sqrt{-19})/2)$,
ou $n = 13$ e $(\alpha, \beta) = ((1 + \sqrt{-7})/2, (1 - \sqrt{-7})/2)$.

Este teorema resolve um problema secular, e sua prova envolve estimativas muito delicadas sobre formas lineares em logaritmos e novos algoritmos para resolver equações de Thue. É, portanto, uma bela combinação de matemática com uma extensa computação rigorosa. Uma aplicação imediata do teorema acima para nosso problema é a seguinte.

Teorema 2.1.11 *Seja $p \geq 7$ um primo, e suponha que $H(p, C)$ é satisfeita. O único valor de C livre de quadrados para o qual a equação $x^2 + C = y^p$ tem uma solução é $C = 1$ com única solução $(x, y) = (0, 1)$.*

Demonstração: A equação que define o conjunto $A_p(C)$ é $(\alpha^p - \beta^p)/(\alpha - \beta) = \pm 1$ com $\alpha = a + \sqrt{-C}$ e $\beta = a - \sqrt{-C}$. De fato, note que

$$\frac{\alpha^p - \beta^p}{\alpha - \beta} = \frac{1}{2\sqrt{-C}} \left[(a + \sqrt{-C})^n - (a - \sqrt{-C})^n) \right]$$

$$
\begin{aligned}
&= \frac{1}{2\sqrt{-C}}\left[\sum_{k=0}^{p}\binom{p}{k}a^k(\sqrt{-C})^{p-k} - \sum_{k=0}^{p}\binom{p}{k}a^k(\sqrt{-C})^{p-k}(-1)^{p-k}\right]\\
&= \frac{1}{\sqrt{-C}}\left[\binom{p}{0}a^0(\sqrt{-C})^{p-0} + \binom{p}{2}a^2(\sqrt{-C})^{p-2} + \cdots + \binom{p}{p-1}a^{p-1}(\sqrt{-C})\right]\\
&= \left[\binom{p}{0}a^0(\sqrt{-C})^{p-1} + \binom{p}{2}a^2(\sqrt{-C})^{p-3} + \cdots + \binom{p}{p-1}a^{p-1}\right]\\
&= \sum_{k=0}^{(p-1)/2}\binom{p}{2k}a^{2k}(\sqrt{-C})^{p-(2k+1)}\\
&= \sum_{k=0}^{(p-1)/2}\binom{p}{2k}a^{2k}(-C)^{[p-(2k+1)]/2}\\
&= \sum_{k=0}^{(p-1)/2}\binom{p}{2k}a^{2k}(-C)^{\frac{p-1}{2}-k}.
\end{aligned}
$$

Com a notação da definição acima $L_p(\alpha,\beta) = \pm 1$. Temos $0 \in A_p(C)$ se e só se $C = \pm 1$, de modo que $C = 1$ já que assumimos $C > 0$. Caso contrário, temos que $\alpha+\beta$ e $\alpha\beta$ são inteiros, e α/β pertence ao corpo quadrático imaginário $\mathbb{Q}(\sqrt{-C})$. Já que $\alpha/\beta \neq \pm 1$ para $a \neq 0$ pode ser uma raiz de unidade somente quando $C = 1$ ou $C = 3$. No entanto, é verificado que para $C = 1$ os únicos valores não nulos de a tal que α/β é uma raiz da unidade são $a = \pm 1$, e para $C = 3$ são $a = \pm 1$ e $a = \pm 3$. Em todos esses casos, se mostra que para $p \geq 7$ se tem $|L_p(\alpha,\beta)| > 1$. Assim, esses casos não fornecem nenhum elemento de $A_p(C)$, portanto, podemos aplicar o teorema acima. Assim, para $p > 30$, $A_p(C)$ deve ter um divisor primitivo, e em particular, não pode ser igual a ± 1, enquanto para $7 \leq p < 30$ todas as possibilidades listadas no teorema dão $\alpha = (u + \sqrt{v})/2$ com u e v ímpares, que assim não podem ser da forma $a + \sqrt{-C}$.

■

Observação 2.1.12 *Se pode generalizar o raciocínio acima para outros valores de C, mas, graças ao teorema de Bilu-Hanrot-Voutier, não precisamos fazê-lo. De fato, para valores pequenos de C satisfazendo $H(C)$ temos o seguinte resultado definitivo, provado em [15] e [32].*

Teorema 2.1.13 *Suponha que ocorre $H(C)$. Para $n \geq 3$ e $1 \leq C \leq 100$ a equação Diofantina $x^2 + C = y^n$ não tem nenhuma solução inteira, exceto para as soluções com $x = 0$, quando $C = 1$, e para os pares (C, n) dados na tabela abaixo, para os quais as únicas soluções (x, y) são as indicadas.*

(C, n)	(x, y)	(C, n)	(x, y)
$(2, 3)$	$(\pm 5, 3)$	$(11, 3)$	$(\pm 4, 3)$ e $(\pm 58, 15)$
$(13, 3)$	$(\pm 70, 17)$	$(17, 4)$	$(\pm 8, \pm 3)$
$(19, 3)$	$(\pm 18, 7)$	$(19, 5)$	$(\pm 22434, 5)$
$(26, 3)$	$(\pm 1, 3)$ e $(\pm 207, 35)$	$(35, 3)$	$(\pm 36, 11)$
$(53, 3)$	$(\pm 26, 9)$ e $(\pm 156, 29)$	$(53, 6)$	$(\pm 26, 3)$
$(61, 3)$	$(\pm 8, 5)$	$(65, 4)$	$(\pm 4, \pm 3)$
$(67, 3)$	$(\pm 110, 23)$	$(74, 3)$	$(\pm 985, 99)$
$(74, 5)$	$(\pm 13, 3)$	$(77, 4)$	$(\pm 2, \pm 3)$
$(83, 3)$	$(\pm 140, 27)$	$(83, 9)$	$(\pm 140, 3)$
$(89, 3)$	$(\pm 6, 5)$	$(97, 4)$	$(\pm 48, \pm 7)$

Soluções de $x^2 + C = y^n$ para (C, n) como no Teorema.

2.2 A Equação Diofantina $x^2 + d^{2l+1} = y^n$

Nesta seção e na próxima apresentamos alguns resultados que servirão de ilustração dos métodos desenvolvidos até o momento. Inicialmente vamos revisar os resultados anteriores, agora considerando $C = dc^2$, com $d > 0$ e livre de quadrados. Vamos assumir n ímpar e $n \geq 5$ e usaremos a notação $K = \mathbb{Q}(\sqrt{-d})$. Continuamos interessados em encontrar soluções inteiras para a equação

$$y^n = x^2 + dc^2$$

assumindo que $mdc(x, y) = 1$. Sobre o corpo K podemos reescrever essa equação como

$$y^n = (x + c\sqrt{-d})(x - c\sqrt{-d}).$$

Aqui observaremos alguns lemas como apresentados em [19]. Nos lemas abaixo assumiremos $y^n = x^2 + dc^2$.

Lema 2.2.1 *Suponha que $d \not\equiv 7 \, (mod\ 8)$ ou y ímpar. Então os ideais*

$$(x + c\sqrt{-d}) \quad e \quad (x - c\sqrt{-d}) \tag{2.2}$$

são coprimos em O_K.

Demonstração: Inicialmente suponha que y é par, logo x deve ser ímpar, pois $mdc(x, y) = 1$. Então

$$0 \equiv y^n = x^2 + dc^2 = 1 + d\,(mod\ 8)$$

um absurdo pois $d \not\equiv 7\,(mod\ 8)$. Portanto vamos assumir que y é ímpar. Seja $\mathfrak{P}$ um ideal primo divisor comum dos ideais em (2.2). Nesse caso y e $2x \in \mathfrak{P}$. Como y é ímpar, isso implica que $1 \in \mathfrak{P}$, um absurdo. ■

Lema 2.2.2 *Se os ideais em* (2.2) *são coprimos e* $mdc(h(-d), n) = 1$ *então existe* $\alpha \in O_K$ *tal que* $x + c\sqrt{-d} = \alpha^n$.

Demonstração: Como $y^n = (x+c\sqrt{-d})(x-c\sqrt{-d})$ e esses ideais são coprimos, então existem um ideal J tal que $(x + c\sqrt{-d}) = J^n$. Como $mdc(h(-d), n) = 1$, esse ideal J tem que ser principal. Logo existem $\beta \in O_K$ e μ uma unidade em O_K tal que

$$x + c\sqrt{-d} = \mu\beta^n.$$

Como K é um corpo quadrático imaginário, temos que $\mu^{12} = 1$. Como n é ímpar, $n \geq 5$, então $mdc(12, n) = 1$. Logo existe uma unidade $\omega \in O_K$ tal que $\omega^n = \mu$. Portanto temos que $x + c\sqrt{-d} = \alpha^n$. ■

Lema 2.2.3 *Se* $\alpha \in O_K$ *é tal que* $\alpha^n = x + c\sqrt{-d}$, *então existem* $u, v \in \mathbb{Z}$ *tais que* $\alpha = u + v\sqrt{-d}$.

Demonstração: Sem perda de geralidade, escreva

$$\alpha = \frac{a + b\sqrt{-d}}{2}$$

com $a, b \in \mathbb{Z}$ e $a \equiv b\,(mod\ 2)$. Vamos assumir que a, b são ímpares. Neste caso devemos ter

$$O_K \in \mathbb{Z}[\theta],\ com\ \theta = \frac{1 + \sqrt{-d}}{2} \quad e \quad d \equiv 3\,(mod\ 4).$$

Como estamos assumindo que a, b são ímpares nós temos que

$$\alpha^n = \left(\frac{a + b\sqrt{-d}}{2}\right)^n = \left(\frac{a-b}{2} + b\theta\right)^n \equiv \theta^n \quad ou \quad (1+\theta)^n (mod\ 2) \qquad (2.3)$$

Agora, $\theta^2 \equiv \theta \quad$ ou $\quad 1+\theta\,(mod\ 2)$, e se $\quad \theta^2 \equiv 1+\theta\,(mod\ 2) \quad$ então $\quad \theta^3 \equiv 1\,(mod\ 2)$. Em qualquer caso, como n é ímpar e $n \geq 5$, nós temos que

$$\theta^n \equiv \theta \quad ou \quad 1+\theta\,(mod\ 2).$$

Um raciocínio similar nos dá que $(1+\theta)^n \equiv \theta$ ou $1+\theta\,(mod\ 2)$. Portanto segue de (2.3) e dos ideais acima que

$$\alpha^n \equiv \theta \quad ou \quad 1+\theta\,(mod\ 2).$$

Por outro lado, $\alpha^n = x + c\sqrt{-d} = (x-c) + 2\,c\,\theta \equiv 0$ ou $1\,(mod\ 2)$, um absurdo. Portanto a, b devem ser pares e temos que $\alpha = u + v\sqrt{-d}$. ■

Teorema 2.2.4 *Suponha que $x, y \in \mathbb{Z}$ com $mdc(x,y) = 1$, se são soluções da equação $x^2 + dc^2 = y^n$, com n ímpar e $n \geq 5$. Se $d \not\equiv 7\,(mod\ 8)$ ou y é ímpar, e $mdc(h(-d), n) = 1$, então podemos escrever $x + c\sqrt{-d} = \alpha^n$, com $\alpha = u + v\sqrt{-d}$, e $u, v \in \mathbb{Z}$. Além disso, temos que*

$$\begin{aligned} x &= u\left(\sum_{j=0}^{(n-1)/2} \binom{n}{2j} u^{n-2j} v^{2j} (-1)^j d^j\right) \\ c &= v\left(\sum_{j=0}^{(n-1)/2} \binom{n}{2j+1} u^{n-2j-1} v^{2j+1} (-1)^j d^j\right) \end{aligned}$$

$y = \alpha\bar{\alpha} = u^2 + v^2 d$.

Demonstração: Segue dos lemas anteriores e de seguinte expansão de

$$\begin{aligned} x + c\sqrt{-d} &= (u + v\sqrt{-d})^n \\ &= \sum_{j=0}^{n} \binom{n}{j} u^{n-j} (v\sqrt{-d})^j \\ &= \sum_{j=0}^{(n-1)/2} \binom{n}{2j} u^{n-2j} (v\sqrt{-d})^{2j} + \sum_{j=0}^{(n-1)/2} \binom{n}{2j} u^{n-2j-1} (v\sqrt{-d})^{2j+1} \\ &= \sum_{j=0}^{(n-1)/2} \binom{n}{2j} u^{n-2j} v^{2j} (-1)^j d^j + \sqrt{-d}\left(\sum_{j=0}^{(n-1)/2} \binom{n}{2j} u^{n-2j-1} v^{2j+1} (-1)^j d^j\right) \end{aligned}$$

de onde obtemos o resultado desejado. Já que $(y)^n = (\alpha\bar{\alpha})^n$, logo $y = \alpha\bar{\alpha} = u^2 + v^2 d$.

■

Nossa primeira ilustração desses métodos é o seguinte teorema devido a Bérzes e Pink [9].

Teorema 2.2.5 *Considere $n, d, l \in \mathbb{N} \cup \{0\}$, com n, d ímpares, $n \geq 5$, com $mdc(n, 6) = 1$ e d livre de quadrados. Suponha que d não seja primo e que $h(-d) \in \{1, 2, 3\}$.*
Nesse caso a equação

$$x^2 + d^{2l+1} = y^n \tag{2.4}$$

não tem solução inteira, se $d \not\equiv 7\,(mod\ 8)$ ou se $d \equiv 7\,(mod\ 8)$ e y é ímpar.

Demonstração: Como estamos assumindo que $h(-d) \in \{1, 2, 3\}$ e n é ímpar e maior ou igual a 5, temos que $mdc(h(-d), n) = 1$. Assim todas as hipóteses do Teorema 2.2.4 acima estão satisfeitas. Se existem soluções inteiras x, y, com $mdc(x, y) = 1$, então existem $\alpha \in O_K$, $u, v \in \mathbb{Z}$ tais que $x + d^l\sqrt{-d} = \alpha^n = (u + v\sqrt{-d})^n$. Além disso temos que $u \mid x$, $v \mid d^l$, $y = u^2 + v^2 d$, e y é ímpar. Logo x é par pois d é ímpar. Como $mdc(x, y) = 1$ e $u \mid x$ temos que $mdc(u, y) = 1$. Denote $\alpha = u + v\sqrt{-d}$ e $\beta = u - v\sqrt{-d} = \bar{\alpha}$.
Nesse caso temos que

$$\alpha + \beta = 2u \in \mathbb{Z} \quad e \quad \alpha \cdot \beta = y = u^2 + v^2 d \in \mathbb{Z}.$$

Além disso temos que $mdc(\alpha + \beta, \alpha\beta) = mdc(2u, y) = 1$.
Para o corpo quadrático imaginário as únicas possibilidades satisfazendo as condições de d ser ímpar livre de quadrados e $h(-d) \in \{1, 2, 3\}$ são

$$d \in T = \{15, 35, 51, 91, 115, 123, 187, 235, 267, 403, 427\} \tag{2.5}$$

(ver por exemplo Cohn [14]), cujas fatorações são:

$$\begin{array}{lllll} 15 = 3 \cdot 5, & 35 = 7 \cdot 5, & 51 = 3 \cdot 17, & 91 = 7 \cdot 13, & 115 = 5 \cdot 23, \\ 123 = 3 \cdot 41, & 117 = 11 \cdot 17, & 235 = 5 \cdot 47, & 267 = 3 \cdot 89, & 403 = 13 \cdot 31, \\ 427 = 7 \cdot 61. & & & & \end{array} \tag{2.6}$$

Nesses casos temos que o conjunto das unidades de O_K é igual a $\{\pm 1\}$, logo se $\dfrac{\alpha}{\beta}$ é uma unidade então $\dfrac{\alpha}{\beta} = \pm 1$. Mas

$$\frac{\alpha}{\beta} = \frac{u^2 - v^2 d}{u^2 + v^2 d} + \frac{2uvi\sqrt{d}}{u^2 + v^2 d} = \pm 1$$

logo isso implica que $u = 0$ *ou* $v = 0$, se $v = 0$ então $d = 0$ absurdo, se $u = 0$ então $x = 0$ implicaria que $y^n = dd^{2l}$ não é possível.

Portanto (α, β) é um par de Lucas e temos a sequência de Lucas

$$\begin{aligned} L_n &= \frac{\alpha^n - \beta^n}{\alpha - \beta} \\ &= \frac{(u + v\sqrt{-d})^n - (u - v\sqrt{-d})^n}{(u + v\sqrt{-d}) - (u - v\sqrt{-d})} \\ &= \frac{(x + d^l\sqrt{-d}) - (x - d^l\sqrt{-d})}{2v\sqrt{-d}} \\ &= \frac{2d^l\sqrt{-d}}{2v\sqrt{-d}} \\ &= \frac{d^l}{v}. \end{aligned}$$

Os possíveis divisores primitivos de L_n, são os divisores primos de d, mas estes não podem dividir

$$(\alpha - \beta)^2 L_1 \cdots L_{n-1} = (2v\sqrt{-d})^2 L_1 \cdots L_{n-1} = -4dv^2 L_1 \cdots L_{n-1}.$$

o que é impossuível pois d é divisor desse número. Logo L_n não tem divisores primitivos. Segue do Teorema 1.2.2 que se $n \geq 31$, L_n tem divisores primitivos, portanto concluímos que a equação (2.4) não tem soluções se $n \geq 31$. Para valores de n ímpares e menores que 31, as únicas possibilidades estão descrita na tabela 1.2 (pág. 20). Assim a equação (2.4) não tem solução para n ímpar, $n \geq 5$, com as possíveis exceções de $n \in \{5, 7, 13\}$ com os parâmetros $A = \alpha + \beta$ e $B = -\alpha\beta$ descritos na tabela 1.2. Inicialmente temos que

$$A = \alpha + \beta = 2u, \ par \quad e \quad B = -\alpha\beta = -\left(u^2 + v^2 d\right) = -y \ \text{ e } y \text{ é ímpar}$$

com isso excluímos os casos $n = 7$ e $n = 13$, pois nesses casos temos $A = 1$. Para $n = 5$, também não temos um par (A, B), pois precisamos de A par e $|B|$ ímpar. Portanto concluímos que a equação (2.4) não possui soluções inteiras x, y com $mdc(x, y) = 1$. ■

Observação 2.2.6 *Claramente podemos estender esses resultados considerando a inclusão de outros valores de d em nosso conjunto T mencionado nessa demostração.*

Gostaríamos de mencionar que Arif e Murifach [4], provaram o seguinte Teorema.

Teorema 2.2.7 *Considere a equação $x^2 + q^{2l+1} = y^n$, com q um primo ímpar, tal que $q \not\equiv 7 \,(mod\, 8)$, $n \geq 5$ e ímpar e suponha que n não é múltiplo de 3 e que $mdc(n, h(-q)) = 1$. Então essa equação não tem soluções a menos que $q = 19$ e $n = 5$. Nesse caso temos a seguinte família de soluções*

$$l = 5M, \quad x = 22434 \cdot 19^{5M}, \quad y = 55 \cdot 19^{2M}.$$

Vamos concluir essa seção considerando a equação

$$x^2 + d^{2l+1} = y^4 \tag{2.7}$$

e como anteriormente fizemos, vamos considerar $d > 0$ livre de quadrados, ímpar, $h(-d) \in \{1, 2, 3\}$ e $mdc(x, y) = 1$ com y ímpar e x par.
Podemos escrever (2.7) como

$$(y^2 + x)(y^2 - x) = d^{2l+1},$$

logo $mdc(y^2 + x, y^2 - x) = 1$, pois $mdc(x, y) = 1$. Assim temos que

$$y^2 + x = d_1^{2l+1} \quad e \quad y^2 - x = d_2^{2l+1},$$

com $d_1, d_2 \in \mathbb{N}$, $d_1 d_2 = d$, $mdc(d_1, d_2) = 1$ e d_1, d_2 livres de quadrados. Consequentemente temos

$$d_1^{2l+1} + d_2^{2l+1} = 2y^2. \tag{2.8}$$

Para completar a demostração do caso $n = 4$, vamos recorrer ao seguinte resultado provado em Bennett e Skinner [7].

Teorema 2.2.8 *Suponha que $x, y, z \in \mathbb{Z}$ são diferentes de zero e dois a dois coprimos. Se $m \geq 5$ um inteiro, então a equação*

$$x^m + y^m = 2z^2$$

tem únicas soluções $(m, x, y, z) \in \{(5, 3, -1, \pm 11), (5, -1, 3, \pm 11)\}$.

Retomando a equação (2.8), temos que como $d_1 \cdot d_2 = d > 0$, então não existem soluções para (2.7) para $2l+1 \geq 5$, ou seja, para $l \geq 2$. Vamos considerar $l \in \{0, 1\}$. Lembremos que estamos considerando $d \in T$. Temos em (2.6), todas as possíveis fatorações de d. Precisamos determinar quando $d_1 d_2 = d$ e (ver (2.8))

$$\frac{d_1 + d_2}{2} \quad \text{é um quadrado} \quad ou \quad \frac{d_1^3 + d_2^3}{2} \quad \text{é um quadrado.}$$

Percorrendo o conjunto T dado em (2.5), verificamos que $15 = 3 \cdot 5$ e $\frac{3+5}{2} = 4$, um quadrado. Nesse caso temos $y = 2$, ou seja, par e $d = 15 \equiv 7\,(mod\ 8)$, uma impossibilidade. Portanto a equação (2.7) também não tem soluções inteiras, com as condições impostas.

2.3 A Equação Diofantina $x^2 + p^{2m} = y^n$, p primo ímpar

Outro tópico central deste trabalho é o Teorema de Pan Xiaowei [44], que apresenta soluções para essa equação.Vamos iniciar considerando a equação $x^2 + p^2 = y^n$, para entendermos mais sobre a equação do título desta seção.
Observe que, podemos fatorar $x^2 + p^2 = y^n$ em $K = \mathbb{Q}(\sqrt{-1})$ e obter

$$y^n = (x + p\sqrt{-1})(x - p\sqrt{-1}).$$

É conhecido que $h(-1) = 1$, ou seja, O_K é domínio de fatoração única. Como $d = 1 \not\equiv 7\,(mod\ 8)$ podemos aplicar o Teorema 2.2.4 da seção anterior e obter

$$x + p\sqrt{-1} = \alpha^n = (u + v\sqrt{-1})^n, \text{com } u, v \in \mathbb{Z},.$$

Além disso

$$\begin{aligned} x = u \cdot M_0 &\implies u \,|\, x \\ p = v \cdot M_1 &\implies v = 1 \text{ ou } p \\ y = u^2 + v^2. & \end{aligned}$$

Temos também que y é ímpar e como p primo ímpar, segue que x é par. Como visto anteriormente, tomando $\alpha = u + v\sqrt{-1}$ e $\beta = u - v\sqrt{-1}$, obtemos

$$\alpha + \beta = 2u \in \mathbb{Z} \quad e \quad \alpha\beta = u^2 + v^2 = y \in \mathbb{Z}$$

como $u \,|\, x$ e $mdc(x, y) = 1$, tem que $mdc(\alpha + \beta, \alpha\beta) = 1$. As unidades de O_K são $\{\pm 1, \pm i\}$ que são raízes da unidade, assim devemos consideramos as possibilidades de

$$\frac{\alpha}{\beta} \in \{\pm 1, \pm i\}.$$

Agora $\frac{\alpha}{\beta} = \frac{u^2 - v^2}{u^2 + v^2} + \frac{2uv}{u^2 + v^2}\sqrt{-1}$, como vimos na seção anterior $\frac{\alpha}{\beta} \notin \{\pm 1\}$. Vamos supor que

$$u^2 - v^2 = 0 \quad e \quad \frac{2uv}{u^2 + v^2} = \pm 1$$

Isso implica que $u^2 = v^2$ e

$$\frac{2uv}{u^2 + v^2} = \frac{2uv}{2v^2} = \frac{u}{v} = \pm 1$$

logo $u = \pm v$. Mas então $y = u^2 + v^2 = 2u^2$, par, um absurdo.
Logo $\frac{\alpha}{\beta}$ não é raiz da unidade e, portanto (α, β) é um par de Lucas. Assim temos

$$L_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{p}{v}.$$

Se $v = p$ temos que L_n não tem divisores primitivos $\forall\ n \geq 31$, contrariando o Teorema 1.2.2. Vamos assumir $v = 1$. Então p é o único possível divisor primitivo de L_n. Como

$$(\alpha - \beta)^2 L_1 \cdots L_{n-1} = (2\sqrt{-1})^2 L_1 \cdots L_{n-1} = -4L_1 \cdots L_{n-1}.$$

O que mantém a possibilidade de p ser divisor primitivo de L_n. Neste ponto o método é inconclusivo. Assim precisamos de uma abordagem mais eficiente.
Vamos começar apresentando alguns resultados e notações que serão úteis para a demostração de nossos resultados. Para qualquer inteiro não negativo k definimos:

$$\begin{aligned} U_k &= \frac{(1+\sqrt{2})^k + (1-\sqrt{2})^k}{2}, \qquad V_k = \frac{(1+\sqrt{2})^k - (1-\sqrt{2})^k}{2\sqrt{2}}, \\ u_k &= \frac{(2+\sqrt{3})^k + (2-\sqrt{3})^k}{2}, \qquad v_k = \frac{(2+\sqrt{3})^k - (2-\sqrt{3})^k}{2\sqrt{3}}, \end{aligned} \tag{2.9}$$

e

$$\bar{L}_k(a) = \frac{1}{2}(\theta^k + \bar{\theta}^k), \qquad L_k(a) = \frac{1}{2\sqrt{-1}}(\theta^k - \bar{\theta}^k), \tag{2.10}$$

em que $a \in \mathbb{Z}^+$,

$$\theta = a + \sqrt{-1}, \qquad \bar{\theta} = a - \sqrt{-1}, \tag{2.11}$$

também enunciaremos agora três Lemas e dois Teoremas os quais ajudarão na demonstração de nosso Teorema principal e corolários.

O livro de L. J. Mordell [33] é uma mina de ouro de resultados especiais em análise de equações Diofantinas. O livro esta dividido em 30 capítulos, mas só vamos precisar de um lema do capítulo 15, o qual está enunciado abaixo. O conteúdo deste capítulo é formado por aplicações da teoria algébrica dos números.

Lema 2.3.1 *Seja n um inteiro positivo ímpar. Toda solução (X, Y, Z) da equação*

$$X^2 + Y^2 = Z^n, \quad X, Y, Z \in \mathbb{N}, \ mdc(X, Y) = 1,$$

pode ser expresso como

$$\begin{aligned} X + Y\sqrt{-1} &= \lambda_1(a + \lambda_2 b\sqrt{-1})^n, & \lambda_1, \lambda_2 \in \{\pm 1\}. \\ Z &= a^2 + b^2, & a, b \in \mathbb{N}, \ mdc(a, b) = 1, \ 2 \,|\, a. \end{aligned}$$

No artigo [17] foi mostrado que a equação $A^4 + B^2 = C^p$, não tem soluções inteiras para os primos maiores que 211 e $mdc(A, B, C) = 1$. Os artigos de Ellenberg [17]; Bennett, Ellenberg e Ng [6] conseguiram estender esse resultado para expoentes menores. E para a equação relacionada $A^4 + 2B^2 = C^p$. Desses resultados temos o seguente lema:

Lema 2.3.2 *Seja q um primo ímpar com $q \geq 5$. A equação*

$$X^2 + Y^4 = Z^q, \qquad X, Y, Z \in \mathbb{N}, \ mdc(X, Y) = 1,$$

não tem solução (X, Y, Z).

Agora vamos enunciar alguns resultados que serão usados nesta seção para a demonstração dos dois corolários que seguem do Teorema de Pan Xiaowei [44].

Teorema 2.3.3 *Se (x, y, m, n) é solução de $x^2 + p^{2m} = y^n$ com $2 \,|\, n$, então $m = 1$.*

Teorema 2.3.4 *Se (x, y, m, n) é solução de $x^2 + p^{2m} = y^n$ com $3 \,|\, n$, então $m = 1$, exceto para $(p, x, y, m, n) = (3, 46, 13, 2, 3)$.*

Nesta seção vamos apresentar uma classificação completa de todos os inteiros positivos (x, y, m, n) soluções da equação $x^2 + p^{2m} = y^n$ onde $mdc(x, y) = 1$, $n > 2$ e p primo, conhecida como a equação exponencial de Lebesgue-Nagell.

Alguns matemáticos trabalharam na equação $x^2 + p^{2m} = y^n$ para certos valores pequenos de p. Um deles é o trabalho de Bérczes e Pink [8] resolvendo a equação $x^2 + p^{2m} = y^n$ para todos os valores de $1 < p < 100$. Nesta seção, também trabalharemos tal

equação para certos casos interessantes, utilizando resultados recentes sobre a existência de números de Lucas e a solubilidade da equação exponencial Diofantina.

O resultado abaixo é um Teorema devido a M. H. Le [24].

Teorema 2.3.5 *Se (x,y,m,n) é uma solução de $x^2 + p^{2m} = y^n$ com $m = 1$, então é obrigado a cumprir um dos quatro tipos seguintes:*

(i) $p = 239$, $(x, y, m, n) = (28560, 13, 1, 8)$;

(ii) $p = U_q$,$(x, y, m, n) = \left(\frac{(U_q^2-1)}{2}, V_q, 1, 4\right)$, *em que q é um primo ímpar;*

(iii) $p = u_{2^r}$, $(x, y, m, n) = (8v_{2^r}^3 + 3v_{2^r}, 4v_{2^r} + 1, 1, 3)$, *em que r é um inteiro positivo;*

(iv) $p = (-1)^{(p-1)/2+(q-1)/2} L_q(a)$, $(x, y, m, n) = (|\bar{L}_q(a)|, a^2 + 1, 1, q)$, *em que q é um primo ímpar, a é um inteiro par positivo.*

Nosso objetivo nesta seção é apresentar a demostração completa da seguinte generalização do teorema acima provado por Pan Xiaowei [44]

Teorema 2.3.6 *Se (x, y, m, n) é uma solução de $x^2 + p^{2m} = y^n$ com $m > 1$ e $mdc(6, n) = 1$, então temos*

(v) $p^{2l+1} = (-1)^{(p-1)/2\,+\,(q-1)/2}\, L_q(a), (x, y, m, n) = (|\bar{L}_q(a)|, a_2 + 1, 2l + 1, q)$,

onde q é um primo impar com $q \geq 5$, a e l são inteiros positivos com $2 \mid a$.

Demonstração: Seja (x, y, m, n) uma solução de $x^2 + p^{2m} = y^n$ com $m > 1$ e $mdc(6, n) = 1$. Considere q um primo ímpar com $q \geq 5$ e suponha que $2 \mid m$. Note que $x^2 + p^{2m} = y^n$ pode ser visto como $x^2 + (p^{m/2})^4 = (y^{n/q})^q$, logo temos que $(X, Y, Z) = (x, p^{m/2}, n/q)$, então dado $q \geq 5$ e pelo Lema 2.3.2 temos uma contradição, já que a equação $X^2 + Y^4 = Z^q$, com $mdc(X, Y) = 1$ não tem solução. Assim temos que que $2 \nmid m$ e $m = 2l + 1$, $l \in \mathbb{N}$.

Além disso, temos que $x^2 + p^{2m} = y^n$ pode ser visto como $x^2 + (p^m)^2 = (y^{n/q})^q$, logo pelo Lema 2.3.1 temos

$$\begin{aligned} x + p^m\sqrt{-1} &= \lambda_1(a + \lambda_2 b\sqrt{-1})^q, & \lambda_1, \lambda_2 \in \{\pm 1\}. \\ y^{n/q} &= a^2 + b^2, & a, b \in \mathbb{N},\ mdc(a, b) = 1,\ 2 \mid a. \end{aligned}$$

Assim,

$$\begin{aligned}
(x + p^m\sqrt{-1}) &= \lambda_1(a + b\lambda_2\sqrt{-1})^q \\
&= \lambda_1 \sum_{k=0}^{q} \binom{q}{k} a^{q-k}(\lambda_2 b\sqrt{-1})^k \\
&= \lambda_1 \left[\binom{q}{0} a^{q-0} + \binom{q}{1} a^{q-1}(\lambda_2 bi)^1 + \cdots + \binom{q}{q} a^0(\lambda_2 bi)^q \right] \\
&= \lambda_1 \left[\binom{q}{0} a^{q-0}(\lambda_2 b\sqrt{-1})^0 + \cdots + \binom{q}{q-1} a(b\sqrt{-1})^{q-1} \right] \\
&\quad + \lambda_1 \left[\binom{q}{1} a^{q-1}(\lambda_2 b\sqrt{-1}) + \cdots + \binom{q}{q} a^0(\lambda_2 b\sqrt{-1})^q \right].
\end{aligned}$$

Da ultima igualdade vamos denotar

$$\begin{aligned}
I &= \lambda_1 \left[\binom{q}{0} a^{q-0}(\lambda_2 b\sqrt{-1})^0 + \cdots + \binom{q}{q-1} a(b\sqrt{-1})^{q-1} \right] \\
&\quad e \\
II &= \lambda_1 \left[\binom{q}{1} a^{q-1}(\lambda_2 b\sqrt{-1}) + \cdots + \binom{q}{q} a^0(\lambda_2 b\sqrt{-1})^q \right],
\end{aligned}$$

logo

$$\begin{aligned}
I &= \lambda_1 a \left[\binom{q}{0} a^{q-1}(\lambda_2 bi)^0 + \binom{q}{0} a^{q-1}(\lambda_2 bi)^0 + \cdots + \binom{q}{q-1} a^0(bi)^{q-1} \right] \\
&= \lambda_1 a \sum_{j=0}^{(q-1)/2} \binom{q}{2j} a^{q-1-2j}(\lambda_2 bi)^{2j} \\
&= \lambda_1 a \sum_{j=0}^{(q-1)/2} \binom{q}{2j} a^{q-1-2j}(-b^2)^j
\end{aligned}$$

e

$$\begin{aligned}
II &= \lambda_1\lambda_2 b \left[\binom{q}{1} a^{q-1}(i) + \binom{q}{3} a^{q-3}(\lambda_2 b)^2(i)^3 + \cdots + \binom{q}{q} a^0(\lambda_2 b)^{q-1}(i)^q \right] \\
&= \lambda_1\lambda_2 b \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(\lambda_2 b)^{2j}(i)^{2j+1} \\
&= \lambda_1\lambda_2 b \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(\lambda_2 b)^{2j}(i)^{2j}\, i \\
&= \lambda_1\lambda_2 b \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(-b^2)^j\, i.
\end{aligned}$$

Desta maneira temos

$$x = \lambda_1 a \sum_{j=0}^{(q-1)/2} \binom{q}{2j} a^{q-1-2j}(-b^2)^j \tag{2.12}$$

e

$$p^m = \lambda_1\lambda_2 b \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(-b^2)^j. \tag{2.13}$$

Dado que p é um número primo ímpar, temos por (2.13) que

$$b = p^r, \ \ r \in \mathbb{Z}, \ 0 \leq r \leq m.$$

Fazendo $b = p^r$ em (2.13) temos

$$p^{m-r} = \left| \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(-p^{2r})^j \right|. \tag{2.14}$$

Sejam

$$\alpha = a + p^r\sqrt{-1}, \ \ \beta = a - p^r\sqrt{-1}. \tag{2.15}$$

note que $\alpha + \beta = 2a$ e $\alpha\beta = a^2 + p^{2r} = y^{n/q}$ são inteiros coprimos positivos, α/β satisfaz

$$y^{n/q}(\alpha/\beta)^2 - 2(a^2 - p^{2r})(\alpha/\beta) + y^{n/q} = 0,$$

De fato, seja $P(x) = y^{n/q}x^2 - 2(a^2 - p^{2r})x + y^{n/q}$. Logo

$$\begin{aligned} \Delta &= 4(a^2 - b^2)^2 - 4(a^2 + b^2)^2 \\ &= -16a^2b^2. \end{aligned}$$

Assim, temos que as raízes do polinômio $P(x)$ são:

$$\begin{aligned} x &= \frac{2(a^2 - b^2) \pm 4ab\sqrt{-1}}{2(a^2 + b^2)} \\ &= \frac{a^2 - b^2}{a^2 + b^2} \pm \frac{2ab}{a^2 + b^2}\sqrt{-1}. \end{aligned} \tag{2.16}$$

Como

$$\frac{\alpha}{\beta} = \frac{a + b\sqrt{-1}}{a - b\sqrt{-1}} = \frac{(a^2 - b^2) + 2ab\sqrt{-1}}{a^2 + b^2},$$

por (2.16) temos que $\dfrac{\alpha}{\beta}$ é raiz de $P(x)$. Logo $\dfrac{\alpha}{\beta}$ não é raiz da unidade. Portanto temos que (α, β) é um par de Lucas com parâmetros $(A, B) = (\alpha + \beta, (\alpha + \beta)^2 - 4\alpha\beta) =$

$(2a, 4a^2 - 4(a^2 + b^2)) = (2a, -p^{2r})$.

Notemos que por (2.14) e (2.15) temos

$$p^{m-r} = |L_q(\alpha, \beta)|. \tag{2.17}$$

De fato, por (2.15) temos

$$\begin{aligned}
\alpha^q - \beta^q &= \sum_{k=0}^{q} \binom{q}{k} a^{q-k}(p^r i)^k - \sum_{k=0}^{q} \binom{q}{k} a^{q-k}(p^r i)^k(-1)^k \\
&= \left[\binom{q}{0} a^q(p^r i)^0 + \binom{q}{1} a^{q-1}(p^r i) + \cdots + \binom{q}{q} a^0(p^r i)^q\right] \\
&\quad - \left[\binom{q}{0} a^q(p^r i)^0 - \binom{q}{1} a^{q-1}(p^r i) + \cdots - \binom{q}{q} a^0(p^r i)^q\right] \\
&= 2\left[\binom{q}{1} a^{q-1}(p^r i) + \binom{q}{3} a^{q-3}(p^r i)^3 + \cdots + \binom{q}{q} a^0(p^r i)^q\right] \\
&= 2p^r\left[\binom{q}{1} a^{q-1}(i) + \binom{q}{3} a^{q-3}(p^r)^2(i)^3 + \cdots + \binom{q}{q} (p^r)^{q-1}(i)^q\right] \\
&= 2p^r \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(p^{2r})^j (i)^{2j+1} \\
&= 2p^r i \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(p^{2r})^j (i)^{2j} \\
&= 2p^r i \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(-p^{2r})^j.
\end{aligned}$$

Logo,

$$\frac{\alpha^q - \beta^q}{\alpha - \beta} = \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(-p^{2r})^j.$$

Assim,

$$L_q(\alpha, \beta) = \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(-p^{2r})^j \tag{2.18}$$

logo por (2.14) e por (2.18) temos

$$p^{m-r} = |L_q(\alpha, \beta)|.$$

Se $r > 0$, temos que $L_q(\alpha, \beta)$ não tem divisor primitivo, já que

$$(\alpha - \beta)^2 L_1 \cdots L_{n-1} = -p^{2r} L_1 \cdots L_{n-1},$$

é divisível por p primo. Logo, como $q \geq 5$ e $(A, B) = (2a, -4p^{2r})$, pelo Teorema 1.2.2 temos que L_q tem um divisor primitivo, o que é uma contradição.
Logo $r = 0$, como $b = p^r$ então $b = 1$. Substituindo $b = 1$ em $y^{n/q} = a^2 + b^2$ temos

$$y^{n/q} = a^2 + 1. \tag{2.19}$$

Aplicando o Teorema (2.1.11) da seção 2.1.4 em (2.19) temos que $n/q = 1$ então $n = q$. Logo

$$y = a^2 + 1.$$

Agora por (2.10) e (2.11) temos $\theta = \alpha$, $\bar{\theta} = \beta$ e $L_q(a) = L_q(\alpha, \beta)$. De fato

$$\begin{aligned} L_q(a) &= \frac{1}{2\sqrt{-1}}(\theta^q - \bar{\theta}^q) \\ &= \frac{1}{2\sqrt{-1}}(\alpha^q - \beta^q) \\ &= \frac{1}{2\sqrt{-1}}\left[(a + p^r i)^q - (a - p^r i)^q)\right] \\ &= \frac{1}{2i}\ 2p^r i \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(-p^{2r})^j. \end{aligned}$$

Como $b = p^r = 1$, então

$$L_q(a) = \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} a^{q-1-2j}(-p^{2r})^j.$$

Por (2.18)

$$L_q(a) = L_q(\alpha, \beta).$$

Além disso, por (2.10), (2.12) e (2.17), temos

$$x = |\bar{L}_q(a)|$$

e

$$p^m = |L_q(a)|. \tag{2.20}$$

De fato, com $p^r = 1$ temos

$$\begin{aligned}
\bar{L}(a) &= \frac{1}{2}(\theta^q + \bar{\theta}^q) \\
&= \frac{1}{2}\left[(a+i)^q + (a-i)^q)\right] \\
&= \frac{1}{2}\left[\sum_{k=0}^{q}\binom{q}{k}a^{q-k}(i)^k + \sum_{k=0}^{q}\binom{q}{k}a^{q-k}(i)^k(-1)^k\right] \\
&= \left[\binom{q}{0}a^q(i)^0 + \binom{q}{2}a^{q-2}(i)^2 + \cdots + \binom{q}{q-1}a(i)^{q-1}\right] \\
&= a\left[\binom{q}{0}a^{q-1}(i)^0 + \binom{q}{2}a^{q-3}(i)^2 + \cdots + \binom{q}{q-1}(i)^{q-1}\right] \\
&= a\sum_{j=0}^{(q-1)/2}\binom{q}{2j}a^{q-1-2j}(i)^{q-1-2j}(i)^{2j} \\
&= a\sum_{j=0}^{(q-1)/2}\binom{q}{2j}a^{q-1-2j}(-1)^{2j}.
\end{aligned}$$

Por (2.12), $b = p^r = 1$ e $\lambda_1, \lambda_2 \in \{\pm 1\}$ temos

$$x = |\bar{L}_q(a)|,$$

e por outro lado

$$\begin{aligned}
L_q(a) &= \frac{1}{2\sqrt{-1}}(\theta^q - \bar{\theta}^q) \\
&= \frac{1}{2i}\left[(a+i)^q - (a-i)^q)\right] \\
&= \frac{1}{2i}\left[\sum_{k=0}^{q}\binom{q}{k}a^{q-k}(i)^k - \sum_{k=0}^{q}\binom{q}{k}a^{q-k}(i)^k(-1)^k\right] \\
&= \frac{1}{i}\left[\binom{q}{1}a^{q-1}(i)^1 + \binom{q}{3}a^{q-3}(i)^3 + \cdots + \binom{q}{q}a(i)^q\right] \\
&= \frac{1}{i}\sum_{j=0}^{(q-1)/2}\binom{q}{2j+1}a^{q-(2j+1)}(i)^{2j+1} \\
&= \sum_{j=0}^{(q-1)/2}\binom{q}{2j+1}a^{q-1-2j}(-1)^j.
\end{aligned}$$

Como $r = 0$, temos

$$p^m = |L_q(a)|.$$

Por (2.10) e (2.11) temos

$$L_q(a) = (-1)^{(q-1)/2}\sum_{j=0}^{(q-1)/2}(-1)^j\binom{q}{2j}a^{2j}. \tag{2.21}$$

De fato,

$$\begin{aligned}
L_q(a) &= \frac{1}{2\sqrt{-1}}(\theta^q - \bar{\theta}^q) \\
&= \frac{1}{2i}\left[(a+i)^q - (a-i)^q)\right] \\
&= \frac{1}{2i}\left[\sum_{k=0}^{q}\binom{q}{k}a^k(i)^{q-k} - \sum_{k=0}^{q}\binom{q}{k}a^k(i)^{q-k}(-1)^k\right] \\
&= \frac{1}{i}\left[\binom{q}{0}a^0(i)^{q-0} + \binom{q}{2}a^2(i)^{q-2} + \cdots + \binom{q}{q-1}a^{q-1}(i)\right] \\
&= \left[\binom{q}{0}a^0(i)^{q-1} + \binom{q}{2}a^2(i)^{q-3} + \cdots + \binom{q}{q-1}a^{q-1}\right] \\
&= \sum_{j=0}^{(q-1)/2}\binom{q}{2j}a^{2j}(i)^{q-(2j+1)} \\
&= \sum_{j=0}^{(q-1)/2}\binom{q}{2j}a^{2j}(-1)^{(q-(2j+1))/2} \\
&= (-1)^{(q-1)/2}\sum_{j=0}^{(q-1)/2}\binom{q}{2j+1}a^{2j}(-1)^j.
\end{aligned}$$

Como $2 \,|\, a$, e por (2.21) temos

$$L_q(a) \equiv (-1)^{(q-1)/2}(mod\ 4). \tag{2.22}$$

De fato, como $2 \,|\, a$ então $a^2 \equiv 0\,(mod\ 4)$. Além disso, por (2.21) temos que

$$L_q(a) - (-1)^{(q-1)/2} = \sum_{j=1}^{(q-1)/2}\binom{q}{2j}a^{2j}(-1)^j.$$

Logo

$$\sum_{j=1}^{(q-1)/2}\binom{q}{2j}a^{2j}(-1)^j \equiv 0(mod\ 4).$$

Por outro lado, dado que $2 \nmid m$ e $p^m \equiv p \equiv (-1)^{(p-1)/2}(mod\ 4)$, da equação (2.20), temos $p^m = -L_q(a)$ ou $p^m = L_q(a)$.

Se $p^m = -L_q(a)$ então , por (2.22) obtemos

$$\begin{aligned}
p^m &\equiv -L_q(a)\,(mod\ 4) \\
(-1)^{(p-1)/2} &\equiv (-1)^{(q-1)/2}(-1)(mod\ 4) \\
(-1)^{(p-1)/2+(q-1)/2} &\equiv (-1)(mod\ 4).
\end{aligned}$$

Desse modo,

$$p^m = (-1)^{(p-1)/2+(q-1)/2} L_q(a).$$

De maneira análoga, quando $p^m = L_q(a)$, temos por (2.22) que

$$\begin{aligned} (-1)^{(p-1)/2} &\equiv (-1)^{(q-1)/2} (mod\ 4) \\ (-1)^{(p-1)/2+(q-1)/2} &\equiv 1 (mod\ 4). \end{aligned}$$

Dai,

$$p^m = (-1)^{(p-1)/2+(q-1)/2} L_q(a).$$

Dessa maneira concluímos que

$$p^m = p^{2l+1} = (-1)^{(p-1)/2+(q-1)/2} L_q(a). \tag{2.23}$$

Portanto, vemos que $m = 2l+1$, $n = q$, $y = a^2+1$ e $x = |\bar{L}_q(a)|$, se a equação $x^2 + p^{2m} = y^n$ tem solução (x, y, m, n) com $m > 1$ e $mdc(6, n) = 1$, então p satisfaz (2.23). Além disso, se (2.23) é satisfeita, então a equação $x^2 + p^{2m} = y^n$ tem solução $(x, y, m, n) = (|\bar{L}_q(a)|, a^2+1, 2l+1, q)$.

■

Corolário 2.3.7 *Se (x, y, m, n) é uma solução da equação de $x^2 + p^{2m} = y^n$, então*

$$p - (-1)^{(p-1)/2} \equiv \begin{cases} 0\ (mod\ 2n), & se\ 2 \mid n, \\ 0\ (mod\ 4n), & se\ 2 \nmid n. \end{cases} \tag{2.24}$$

exceto para $(p, x, y, m, n) = (3, 46, 13, 2, 3)$ e $(7, 524, 65, 1, 3)$.

Demonstração: Usaremos os Teoremas 2.3.5, 2.3.4 e 2.3.6, se $p > 3$, toda solução (p, x, y, m, n) de $x^2 + p^{2m} = y^n$ deve ser de um dos tipos *(i)*, *(ii)*, *(iii)*, *(iv)* e *(v)*, (o caso *(v)* é o Teorema 2.3.6).

Para tipo *(i)*, temos $p = 239$, $n = 8$, $p - (-1)^{(p-1)/2} = 240 = 2 \cdot 8 \cdot 15$ e (2.24) ocorre.

Para tipo (*ii*), temos $p = U_p$ e $n = 4$. Dado $U_q^2 - 2V_q^2 = -1$, de fato

$$\begin{aligned} U_q^2 - 2V_q^2 &= \left[\frac{(1+\sqrt{2})^q - (1-\sqrt{2})^q}{2}\right] - \left[\frac{(1+\sqrt{2})^q - (1-\sqrt{2})^q}{2\sqrt{2}}\right] \\ &= \frac{4(1+\sqrt{2})(1-\sqrt{2})}{4} \\ &= -1. \end{aligned}$$

Aplicando módulo p, temos

$$\begin{aligned} 2V_q^2 &\equiv 1(mod\ p) \\ 4V_q^2 &\equiv 2(mod\ p) \\ (2V_q)^2 &\equiv 2(mod\ p). \end{aligned}$$

Logo temos que $\left(\frac{2}{p}\right) = 1$, já que $2V_q$ é solução de $x^2 \equiv 2\ (mod\ p)$. Como

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

Isso implica que $p \equiv \pm 1\ (mod\ 8)$, e temos que $p - (-1)^{(p-1)/2} \equiv 0\,(mod\ 8)$. De fato:

(i) Se $p \equiv -1\ (mod\ 8)$ então $p = 8k - 1,\ onde\ k \in \mathbb{Z}$, logo

$$\frac{p-1}{2} = \frac{8k-2}{2} = 4k - 1,\ \text{é ímpar}$$

então

$$p \equiv (-1)^{(p-1)/2}\ (mod\ 8),$$

(ii) Se $p \equiv 1\ (mod\ 8)$ então $p = 8k + 1,\ onde\ k \in \mathbb{Z}$, logo

$$\frac{p-1}{2} = \frac{8k}{2} = 4k, \text{é par}$$

então

$$p \equiv (-1)^{(p-1)/2}\ (mod\ 8).$$

Portanto, temos $p - (-1)^{(p-1)/2} \equiv 0\,(mod\ 8)$ e (2.24) ocorre.

Para o caso *(iii)*, temos $p = u_{2^r}$ e $n = 3$. Por (2.9), obtemos

$$p = u_{2^r} = u_{2^{r-1}}^2 + 3v_{2^{r-1}}^2 = \begin{cases} 7 & ,\text{se } r = 1, \\ 2 \cdot 3v_{2^{r-1}}^2 + 1 & ,\text{se } r > 1. \end{cases} \tag{2.25}$$

De fato, seja

$$u_{2^r} = \frac{(2+\sqrt{3})^{2^r} + (2-\sqrt{3})^{2^r}}{2}.$$

Se $r = 1$, então $u_{2^r} = 7$. Além disso, para qualquer inteiro positivo k , obtemos

$$u_k^2 - 3v_k^2 = 1,\ u_k, v_k \in \mathbb{N}. \tag{2.26}$$

De fato, sejam $\alpha = (2 + \sqrt{3})$ e $\beta = (2 - \sqrt{3})$.Logo

$$\begin{aligned} u_k^2 - 3v_k^2 &= \frac{(\alpha^k + \beta^k)^2}{4} - \frac{(\alpha^k - \beta^k)^2}{4} \\ &= \alpha^k\beta^k \\ &= ((2+\sqrt{3})(2-\sqrt{3}))^k \\ &= 1. \end{aligned}$$

Assim por (2.26) temos

$$\begin{aligned} u_{2^r} &= u_{2^{r-1}}^2 + 3v_{2^{r-1}}^2 \\ &= 3v_{2^{r-1}}^2 + 1 + 3v_{2^{r-1}}^2 \\ &= 2 \cdot 3v_{2^{r-1}}^2 + 1\ . \end{aligned}$$

Note que $2 \,|\, v_{2^{r-1}}$ se $r > 1$. De fato,

$$\begin{aligned} v_{2^{r-1}} &= \frac{(2+\sqrt{3})^{2^{r-1}} - (2-\sqrt{3})^{2^{r-1}}}{2\sqrt{3}} \\ &= \binom{2^{2^{r-1}}}{1} 2^{2^{r-1}-1}(\sqrt{3}) + \binom{2^{2^{r-1}}}{3} 2^{2^{r-1}-3}(\sqrt{3})^3 + \cdots + \binom{2^{2^{r-1}}}{2^{2^{r-1}}} 2^0(\sqrt{3})^{2^{r-1}-1} \\ &= \sum_{j=1}^{2^{r-2}} \binom{2^{r-1}}{2j-1} 2^{2^{r-1}-(2i-1)}(3)^i. \end{aligned}$$

Alem disso, temos

$$\begin{aligned} p - (-1)^{(p-1)/2} &\equiv 0\,(mod\ 4n) \\ 2 \cdot 3v_{2^{r-1}}^2 + 1 - (-1)^{\frac{2\cdot 3v_{2^{r-1}}^2 + 1 - 1}{2}} &\equiv 0\,(mod\ 12) \\ 2 \cdot 3v_{2^{r-1}}^2 + 1 - (-1)^{3v_{2^{r-1}}^2} &\equiv 0\,(mod\ 12) \\ 6v_{2^{r-1}}^2 &\equiv 0\,(mod\ 12) \end{aligned}$$

Portanto, vemos por (2.25) que (2.24) ocorre, exceto para $(p, x, y, m, n) = (7, 524, 65, 1, 3)$.

Para os tipos (iv) e (v), no Teorema 2.3.6 foi provado que p é um divisor primitivo dos números de Lucas $L_n(\alpha, \beta)$, com $n = q$ um primo ímpar, $b = p^{2r} = 1$, (α, β)

é um par de Lucas com parâmetros $(A, B) = (2a, -4)$ e $p \equiv (-1)^{(p-1)/2} (mod\ 4)$. Portanto, temos $4 \mid p - (-1)^{(p-1)/2}$. Então, pelo Lema 1.2.3 e propriedades do simbolo de Legendre obtemos

$$p - \left(\frac{-4}{p}\right) \equiv p - \left(\frac{-1}{p}\right) \equiv p - (-1)^{(p-1)/2} \equiv 0(mod\ 4n).$$

Assim, o corolário está provado. ■

Corolário 2.3.8 *Se $p > 3$, $p \equiv \pm 3\,(mod\ 8)$ e todo divisor primo ímpar q de $p-(-1)^{(p-1)/2}$ satisfaz $q \equiv 1\,(mod\ 4)$, então $x^2+p^{2m} = y^n$ não tem solução (x, y, m, n).*

Demonstração: Suponha que (x, y, m, n) é uma solução da equação $x^2 + p^{2m} = y^n$ sob as hipóteses do Corolário 2.3.8 .
Seja $p \equiv \pm 3(mod\ 8)$. Pela demostração do Corolário 2.3.7 temos que a solução deve pertencer aos tipos (iv) ou (v).

Como $2 \nmid m$ e pelo Corolário 2.3.7 temos que $n = q$ é um primo e $p - (-1)^{(p-1)/2} \equiv 0(mod\ 4)$. Então n é um divisor primo ímpar de $p - (-1)^{(p-1)/2}$. Isso implica que $n \equiv 1(mod\ 4)$. Entretanto, já que $p - (-1)^{(p-1)/2} \equiv 0(mod\ 4)$ e $2 \mid \binom{n}{2i}$ para $i \geq 1$, pelos Teoremas 2.3.5 e 2.3.6, temos que

$$\begin{aligned} p^m &\equiv p \equiv (-1)^{(p-1)/2+(n-1)/2} L_n(a) \\ &\equiv (-1)^{(p-1)/2} \left(1 - \binom{n}{2} a^2 + \cdots + \binom{n}{n-1} a^{n-1}\right) \\ &\equiv (-1)^{(p-1)/2} (mod\ 8) \\ p - (-1)^{(p-1)/2} &\equiv 0(mod\ 8), \end{aligned}$$

o que é uma contradição. Assim, o corolário está provado. ■

Pelo Corolário 2.3.8, pode-se concluir que a equação $x^2 + p^{2m} = y^n$ não tem solução para $p = 19$, 53, 67, 101, 149, 163, 211, 269, 293, 389, 499, 47, 677, 739, 773, 787, 821, 883.

Finalmente, vejamos como os resultados relacionados aos divisores primitivos dos números de Lucas e Lehmer são úteis na resolução de certos problemas às equações Diofantinas.

Vimos para $n \geq 5$ como empregar os números de Lucas, em que relacionados α e β são inteiros algébricos tais que $\alpha + \beta$ e $\alpha\beta$ são inteiros coprimos diferentes de zero.

Também temos que $\frac{\alpha}{\beta}$ não é raiz da unidade e denotamos (α, β) como um par de Lucas, assim conseguimos uma sequência de Lucas $L_n(\alpha, \beta)$.

Pela escolha de α e β em nas demonstrações do estudo de nosso trabalho, temos que $L_n(\alpha, \beta) = L_n$ não tem divisores primitivos. Mas pelo Teorema 1.2.2 temos que se L_n é uma sequência de Lucas com $n \geq 5$, n primo, então L_n tem um divisor primitivo. O qual é uma contradição. Isto mostra que a equação Diofantina tratada não tem solução para valores $n \geq 5$.

Assim, as sequências de Lucas e Lehmer são ferramentas importantes para a solução de equações Diofantinas que foram estudadas neste trabalho.

Bibliografia

[1] S. Alaca and K. S. Williams, *Introductory algebraic number theory*, The Mathematical Gazette **89** (2005), no. 514, 145–147.

[2] S. Alaca and Kenneth S Williams, *Introductory algebraic number theory.*, Cambridge University Press, 2004.

[3] S. A.. Arif and Fadwa S Abu Muriefah, *On the diophantine equation* $x^2+2^k = y^n$., International Journal of Mathematics and Mathematical Sciences **20** (1997), no. 2, 299–304.

[4] S. A. Arif. and F. S A. Muriefah, *On the diophantine equation* $x^2 + q^{2k+1} = y^n$, Journal of Number Theory **95** (2002), no. 1, 95–100.

[5] S. Akhtar Arif and Fadwa S Abu Muriefah, *The diophantine equation* $x^2+3^m = y^n$, International Journal of Mathematics and Mathematical Sciences **21** (1998), no. 3, 619–620.

[6] M. A. Bennett, Jordan S Ellenberg, and Nathan C Ng, *The diophantine equation* $a^4 + 2^\delta b^2 = c^n$, International Journal of Number Theory **6** (2010), no. 02, 311–338.

[7] M. A. Bennett and Chris M Skinner, *Ternary diophantine equations via galois representations and modular forms*, Canadian Journal of Mathematics **56** (2004), no. 1, 23–54.

[8] A. Bérczes and István Pink, *On the diophantine equation* $x^2 + p^{2k} = y^n$, Archiv der Mathematik **91** (2008), no. 6, 505–517.

[9] A. Berczes and Istvan Pink, *On the diophantine equation* $x^2+d^{2l+1}=y^n$, Glasgow Mathematical Journal **54** (2012), no. 2, 415–428.

[10] Y. Bilu, Guillaume Hanrot, Paul M Voutier, et al., *Existence of primitive divisors of lucas and lehmer numbers*, Journal fur die Reine und Angewandte Mathematik **539** (2001), 75–122.

[11] Y. Bugeaud, Maurice Mignotte, and Samir Siksek, *Classical and modular approaches to exponential diophantine equations ii. the lebesgue–nagell equation*, Compositio Mathematica **142** (2006), no. 1, 31–62.

[12] I. N. Cangül, Musa Demirci, Gökhan Soydan, Nikos Tzanakis, et al., *On the diophantine equation* $x^2 + 5^a 3^b 11^c = y^n$, Functiones et Approximatio Commentarii Mathematici **43** (2010), no. 2, 209–225.

[13] I.N. Cangül, Musa Demirci, Florian Luca, A Pintér, and GOKHAN Soydan, *On the diophantine equation* $x^2 + 2^a 11^b = y^n$, Fibonacci Quart **48** (2010), no. 1, 39–46.

[14] H. Cohen., *A course in computational algebraic number theory*, Graduate texts in Math. **138** (1993), 88.

[15] H. Cohen, *Number theory; volume i: Tools and diophantine equations.*, 2007.

[16] J. Cohn., *The diophantine equation* $x^2 + c = y^n$, *ii*, Acta Arithmetica **109** (2003), 205–206.

[17] J. S. Ellenberg, *Galois representations attached to q-curves and the generalized fermat equation* $a^4 + b^2 = c^p$, Amer. J. Math, Citeseer.

[18] L. Euler, *Algebra*, vol. 2.

[19] H. Godinho and V. Neumann, *The diophantine equation* $x^2 + p^a q^b = y^q$, Mathematics Subject Classification. (2010).

[20] E. Goins, Florian Luca, and Alain Togbé, *On the diophantine equation* $x^2 + 2^a 5^b 13^c = y^n$, International Algorithmic Number Theory Symposium, Springer, 2008, pp. 430–442.

[21] C. Ko, *On the d1ophantine equation* $x^2 = y^n + 1$,$xy \neq 0$., Journal of Sichuan University (Natural Science Edition) **1** (1962), 000.

[22] M. Le., *An exponential diophantine equation*, Bulletin of the Australian Mathematical Society **64** (2001), no. 1, 99–105.

[23] M. Le, *On cohn's conjecture concerning the diophantine equation* $x^2 + 2^m = y^n$, Archiv der Mathematik **78** (2002), no. 1, 26–35.

[24] M.-H. Le, *On the diophantine equation* $x^2 + p^2 = y^n$, Publ. Math. Debrecen **63** (2003), 67–78.

[25] Victor A Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation* $x^m = y^2 + 1$, *nouv*, Ann. Math **9** (1850), no. 9, 178–181.

[26] W. Ljunggren, *Über einige arcustangensgleichungen, die auf interessante unbestimmte gleichungen führen*, Natura, 1943.

[27] F. Luca, *On an diophantine equation*, Bulletin of the Australian Mathematical Society **61** (2000), no. 2, 241–246.

[28] F. Luca., *On the equation* $x^2 + 2^a 3^b = y^n$, International Journal of Mathematics and Mathematical Sciences **29** (2002), no. 4, 239–244.

[29] F. Luca and Alain Togbé, *On the diophantine equation* $x^2 + 7^{2k} = y^n$, Fibonacci Quart **45** (2007), no. 4, 322–326.

[30] F. Luca. and Alain Togbé, *On the diophantine equation* $x^2 + 2^a 5^b = y^n$, International Journal of Number Theory **4** (2008), no. 06, 973–979.

[31] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, American Journal of Mathematics (1878), 289–321.

[32] M. Mignotte and Benjamin MM de Weger, *On the diophantine equations* $x^2+74 = y^5$ *and* $x^2 + 86 = y^5$, Glasgow Mathematical Journal **38** (1996), no. 1, 77–85.

[33] L. J. Mordell, *Diophantine equations*, vol. 30, Academic Press, 1969.

[34] F. S A. Muriefah, *On the diophantine equation* $x^2 + 5^{2k} = y^n$, Demonstratio Mathematica **39** (2006), no. 2, 285–290.

[35] F. S. A. Muriefah and S Akhtar Arif, *On a diophantine equation*, Bulletin of the Australian Mathematical Society **57** (1998), no. 2, 189–198.

[36] F. S. A. Muriefah, Florian Luca, and Alain Togbé, *On the diophantine equation* $x^2 + 5^a 13^b = y^n$, Glasgow Mathematical Journal **50** (2008), no. 1, 175–181.

[37] F.S.A. Muriefah and S Akhtar Arif, *The diophantine equation* $x^2 + 5^{2k+1} = y^n$, INDIAN JOURNAL OF PURE & APPLIED MATHEMATICS **30** (1999), no. 3, 229–231.

[38] T. Nagell, *Sur l'impossibilité de quelques équations a deux indeterminées*, Norsk. Mat. Forensings Sknifter **13** (1923), 65–82.

[39] T. Nagell., *Verallgemeinerung eines fermat schen satzes*, Archiv der Mathematik **5** (1954), no. 1-3, 153–159.

[40] T. Nagell.., *Contributions to the theory of a category of diophantine equations of the second degree with two unknowns*, Almqvist & Wiksells boktr., 1955.

[41] N. Saradha and Anitha Srinivasan, *Solutions of some generalized ramanujan-nagell equations*, Indagationes Mathematicae **17** (2006), no. 1, 103–114.

[42] G. Soydan and N Tzanakis, *Complete solution of the diophantine equation* $x^2 + 5^a 11^b = y^n$, Bull. of the Hellenic Math. Soc **60** (2016), 125–151.

[43] P. M. Voutier, *Primitive divisors of lucas and lehmer sequences*, mathematics of computation **64** (1995), no. 210, 869–888.

[44] P. Xiaowei, *The exponential lebesgue-nagell equation* $x^2 + p^{2m} = y^n$, Periodica Mathematica Hungarica **67** (2013), no. 2, 231–242.

[45] H. L. Zhu, *A note on the diophantine equation* $x^2 + q^m = y^3$, Acta Arith **146** (2011), no. 2, 195–202.