UNIVERSIDADE FEDERAL DA PARAÍBA
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática em Rede Nacional

Resolução de algumas equações em números inteiros

por

Ambrósio Elias de Araújo Pontes

2013

UNIVERSIDADE FEDERAL DA PARAÍBA
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática em Rede Nacional

Resolução de algumas equações em números inteiros [†]

por

Ambrósio Elias de Araújo Pontes

sob orientação do

Prof. Dr. Napoleón Caro Tuesta

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Curso de Pós-Graduação em Matemática em Rede Nacional - PROFMAT - DM - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto/2013

João Pessoa - PB

[†] O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

Resolução de algumas equações em números inteiros

por

Ambrósio Elias de Araújo Pontes

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Curso de Pós-Graduação em Matemática em Rede Nacional - PROFMAT - DM - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Teoria dos Números.

Aprovado por:

Prof. Dr. Napoleón Caro Tuesta - UFPB (Orientador)

Prof. Dr. Antônio de Andrade e Silva - UFPB

Prof. Dr. Washington César de Almeida Costa - IFPB

Agosto/2013

Agradecimentos

Inicialmente quero agradecer a Deus por ter me dado saúde e coragem para que pudesse enfrentar e superar todos os problemas e não desistir.

A minha esposa, que em todos os momentos sempre me apoiou e me deu forças nesse desafio.

As minhas filhas Jéssica e Raissa, que tanto torceram pela realização desse trabalho.

Aos meus pais, Maria do Socorro de Araújo Pontes e Luis Mendes de Pontes (*In Memoriam*) por terem me ensinado a importância dos valores e respeito pelo ser humano.

Aos meus irmãos e irmãs, companheiros de todos os momentos, principalmente Luiz Renato (In Memoriam) que sempre incentivou o meu crescimento profissional e pessoal.

Aos meus sogros, que sempre me ajudaram com palavras de incentivo.

Ao professor Napoleón, pela orientação e paciência.

Aos amigos Sheldon e Martinho pelas palavras de estímulo.

A todos os professores do PROFMAT, que com muita paciência e dedicação, me ajudaram na conclusão desse mestrado.

Enfim, a todos aqueles que contribuíram de alguma forma para realização deste trabalho.

Dedicatória

Dedico este trabalho à minha família que sempre esteve ao meu lado suportando os momentos de dificuldades, me dando amor e palavras de carinho. Sem eles, nada teria conseguido. Minha eterna gratidão.

Resumo

Neste trabalho apresentamos algumas técnicas de resolução de equações com coeficientes inteiros. Tais equações, apesar de serem bastante semelhantes, apresentam técnicas muito distintas umas das outras. Mostraremos quais são as soluções inteiras de equações do tipo $x^2+y^2=z^2$ e $x^{-2}+y^{-2}=z^{-2}$, que são conhecidas como equações de Pitágoras. Também apresentamos um breve histórico sobre o Último Teorema de Fermat e mostraremos que a equação $x^4+y^4=z^4$ não possui solução inteira.

Abstract

In this work we present some resolution techniques of equations with integers coefficients. Such equations although they're very similar, presents quite different techniques from each other. We show which are the integer solutions of the equations like $x^2 + y^2 = z^2$ and $x^{-2} + y^{-2} = z^{-2}$, as they are known as the Pythagorean equations. We also present a brief history about the Fermat's Last Theorem and we show that the equation $x^4 + y^4 = z^4$ has no integer solution.

Sumário

Introdução

A Teoria dos Números é um ramo da Matemática que estuda, com mais ênfase, as propriedades aritméticas dos números inteiros. Um dos principais problemas dessa teoria é encontrar soluções inteiras para determinadas equações, que foram estudadas por grandes matemáticos da antiguidade como Pitágoras, Diofanto de Alexandria, Fermat, Langrange e Euler.

Tais equações podem ser de diferentes tipos, como por exemplo, equações com duas ou três incógnitas com coeficientes inteiros. Para determinar soluções para esse tipo de equação, nos deparamos com três perguntas cruciais:

(a) A equação em questão possui solução?

(b) Se a equação é solúvel, então o número de soluções é finito ou infinito?

(c) Se a equação é solúvel, então como determinar todas as soluções?

As soluções dessas equações não têm interesse apenas teórico, mas sim em outras áreas do conhecimento, como a Física. O interesse teórico é constante já que serve para resolver diversos problemas dentro da própria Teoria dos Números. Enfatizamos também que o conhecimento das técnicas de resolução são extremamente atraentes para quem estuda Matemática. Neste trabalho procuramos abordar de maneira didática a resolução de problemas como esses.

No Capítulo 1, apresentamos diversos resultados básicos da Teoria dos Números que servirão de suporte para o decorrer do trabalho. Todos os resultados lá

encontrados serão usados nos capítulos posteriores.

O Capítulo 2 é dedicado ao estudo inicial de equações com coeficientes inteiros. Começamos a estudar uma simples equação do primeiro grau e com apenas uma incógnita. Esta equação servirá de motivação para estudar equação com coeficientes inteiros de graus maiores. Obtemos todas as soluções inteiras de uma equação polinomial de grau n. Nesse mesmo capítulo, estudamos as equações de primeiro grau com duas incógnitas e, para tanto, faremos uso das *frações contínuas* e através de um exemplo, construiremos passo a passo o método de resolução para esse tipo de equação.

Alguns exemplos de equações do segundo grau com três incógnitas são dados no Capítulo 3. Em cada seção desse capítulo, mostramos como resolver um tipo de equação dessa forma. Destacamos a diversidade de técnicas utilizadas em cada exemplo. Em uma das seções, mostramos que a equação $x^4 + y^4 = z^4$ não possui soluções inteiras. No final desse capítulo, damos uma abordagem histórica do Último Teorema de Fermat, uma equação bastante famosa dentro da Matemática.

Finalmente, no Capítulo 4 determinamos todas as soluções inteiras da equação $x^2 - Ay^2 = 1$, conhecida como equação de Pell. Para resolver esse problema utilizamos o método das frações contínuas para representação de números irracionais. Para a obtenção das soluções, usamos ideias semelhantes as do Capítulo 1.

Esse trabalho foi inspirado principalmente nas referências [2, 3].

Capítulo 1

Preliminares

Neste capítulo são apresentados vários resultados básicos de teoria dos números que darão suporte para a compreensão geral dos próximos capítulos. Cada resultado aqui mencionado ou provado é utilizado de alguma maneira no decorrer do trabalho sem que, necessariamente, se faça menção dos mesmos quando utilizados. O leitor interessado em mais detalhes pode consultar [7].

1.1 Princípio da Boa Ordem

O *Princípio da Boa Ordem* ou *Princípio da Boa Ordenação* afirma que todo subconjunto do conjunto dos números naturais possui um menor elemento. Mais precisamente, isso quer dizer que se A é um subconjunto não vazio de $\mathbb{N}$, então existe $n_0 \in A$ tal que $n_0 \leq n$ para todo $n \in A$.

1.2 Indução Matemática

Uma ferramenta fundamental na demonstração das propriedades referentes aos números naturais é o *Princípio da Indução Matemática* que é descrito a seguir. Seja A um subconjunto dos números naturais que goza das seguintes propriedades:

(1) $1 \in A$;

(2) $n+1 \in A$, sempre que $n \in A$,

então $A = \mathbb{N}$.

Exemplo 1. Dados a e b números reais, e $n \in \mathbb{N}$, tem-se que

$$(a+b)^n = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) a^{n-i} b^i,$$

em que

$$\left(\begin{array}{c} n \\ i \end{array} \right) = \frac{n!}{i!(n-i)!}.$$

A igualdade acima é conhecida como o *binômio de Newton*. Para provar esta igualdade, vamos utilizar indução sobre o número natural n. Primeiramente, note que se $n = 1$, então

$$\begin{aligned} (a+b)^1 &= a+b \\ &= \left(\begin{array}{c} 1 \\ 0 \end{array} \right) a^{1-0} b^0 + \left(\begin{array}{c} 1 \\ 1 \end{array} \right) a^{1-1} b^1, \end{aligned}$$

ou seja, a igualdade é válida para $n = 1$. Suponha agora que a afirmação é verdadeira para $n \in \mathbb{N}$ e provemos que é válida para $n+1$. Note que

$$\begin{aligned} (a+b)^{n+1} &= (a+b) \cdot (a+b)^n \\ &= a \cdot (a+b)^n + b \cdot (a+b)^n \\ &= a \cdot \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) a^{n-i} b^i + b \cdot \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) a^{n-i} b^i \\ &= \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) a^{n+1-i} b^i + \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) a^{n-i} b^{i+1}. \end{aligned}$$

Mas a primeira soma pode ser escrita da seguinte maneira:

$$\sum_{i=0}^{n} \begin{pmatrix} n \\ i \end{pmatrix} a^{n+1-i}b^i = a^{n+1} + \sum_{i=1}^{n} \begin{pmatrix} n \\ i \end{pmatrix} a^{n+1-i}b^i$$

e a segunda:

$$\begin{aligned} \sum_{i=0}^{n} \begin{pmatrix} n \\ i \end{pmatrix} a^{n-i}b^{i+1} &= b^{n+1} + \sum_{i=0}^{n-1} \begin{pmatrix} n \\ i \end{pmatrix} a^{n-i}b^{i+1} \\ &= b^{n+1} + \sum_{i=1}^{n} \begin{pmatrix} n \\ i-1 \end{pmatrix} a^{n+1-i}b^i. \end{aligned}$$

Portanto,

$$\begin{aligned} (a+b)^{n+1} &= a^{n+1} + b^{n+1} + \sum_{i=1}^{n} \left[\begin{pmatrix} n \\ i \end{pmatrix} + \begin{pmatrix} n \\ i-1 \end{pmatrix} \right] a^{n+1-i}b^i \\ &= a^{n+1} + b^{n+1} + \sum_{i=1}^{n} \begin{pmatrix} n+1 \\ i \end{pmatrix} a^{n+1-i}b^i \\ &= \sum_{i=0}^{n+1} \begin{pmatrix} n+1 \\ i \end{pmatrix} a^{n+1-i}b^i \end{aligned}$$

que é a fórmula para $n+1$.

1.3 Divisibilidade em $\mathbb{Z}$

Sejam a e b dois números inteiros. Dizemos que a *divide* b se existe $c \in \mathbb{Z}$ tal que $b = ac$. Neste caso, escrevemos $a \mid b$.

Proposição 1. Sejam a, b e c números inteiros. Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração. De fato, como $a \mid b$ e $b|c$, existem $k_1 \in \mathbb{Z}$ e $k_2 \in \mathbb{Z}$ tais que $b = k_1 a$

e $c = k_2 b$. Portanto,

$$c = k_2 b = k_2 \cdot k_1 a.$$

Sendo $k_2 \cdot k_1 \in \mathbb{Z}$, segue que $a \mid c$. □

Proposição 2. Sejam a, b, c, m e n números inteiros. Se c divide a e c divide b, então c divide $(ma + nb)$.

Demonstração. Temos que existe $k_1, k_2 \in \mathbb{Z}$ tais que

$$a = k_1 c \quad \text{e} \quad b = k_2 c.$$

Multiplicando ambos os membros de $a = k_1 c$ por m e ambos os membros de $b = k_2 c$ por n, obtemos

$$ma = m \cdot k_1 c \quad \text{e} \quad bn = n \cdot k_2 c.$$

Logo,

$$\begin{aligned} ma + nb &= m \cdot k_1 c + n \cdot k_2 c \\ &= (mk_1 + nk_2) \cdot c. \end{aligned}$$

Sendo $mk_1 + nk_2 \in \mathbb{Z}$, temos que $c \mid (ma + nb)$, como queríamos. □

São listadas abaixo algumas das propriedades mais importantes de divisibilidade entre números inteiros.

(1) $n \mid n$, para todo $n \in \mathbb{Z}$;

(2) se $d, n \in \mathbb{Z}$ e $d \mid n$, então $ad \mid an$ para qualquer $a \in \mathbb{Z}$;

(3) se $ad \mid an$ e $a \neq 0$, então $d \mid n$;

(4) $1 \mid n$ para cada $n \in \mathbb{Z}$;

(5) $n \mid 0$, para cada $n \in \mathbb{Z}$.

1.4 O Algoritmo de Euclides

Euclides de Alexandria, como era conhecido, nasceu na Síria e viveu entre 330 e 290 a.c.. Foi um dos maiores matemáticos da antiguidade. Trabalhou em Alexandria onde foi o primeiro diretor da famosa Biblioteca de Alexandria. A sua principal obra - Os Elementos - é onde se encontra o que hoje conhecemos como o *algoritmo de Euclides* que é de fundamental importância para várias áreas da matemática até os dias atuais.

Antes de introduzirmos este algoritmo, que também é conhecido como o *algoritmo da divisão*, enunciamos o

Teorema 1. (Teorema de Eudóxius) Sejam a e b dois números inteiros, com $b \neq 0$. Então, existe $q \in \mathbb{Z}$ tal que

$$qb \leq a < (q+1)b, \text{ se } b > 0$$

e

$$qb \leq a < (q-1)b, \text{ se } b < 0.$$

Demonstração. Suponha que $b > 0$. A prova para quando $b < 0$ é inteiramente análoga. Definamos o conjunto

$$A := \{h \in \mathbb{N} : hb > a\}.$$

Note que o número natural $|a| + 1$ é tal que

$$(|a| + 1)b = |a|b + b.$$

Como $|a| = \max\{-a, a\}$ e estamos supondo que $b > 0$, segue que $(|a| + 1)b > a$ e, portanto, $|a| + 1 \in A$, o que mostra que $A \subset \mathbb{N}$ é um subconjunto não vazio. Agora,

pelo Princípio da Boa Ordenação, A possui um menor elemento, digamos h_0. Logo, $h_0 b > a$. Usando a minimalidade do número natural h_0, segue que $h_0 - 1 \notin A$, isto é, $(h_0 - 1)b \leq a$. Assim, tomando $q = h_0 - 1$, segue que

$$qb = (h_0 - 1)b \leq a$$

e

$$(q + 1)b = (h_0 - 1 + 1)b = h_0 b > a,$$

ou seja, $qb \leq a < (q + 1)b$, como queríamos. □

Teorema 2. (Algoritmo de Euclides) Dados dois números inteiros a e b, com $b > 0$, existe um único par de inteiros q e r tais que

$$a = qb + r, \text{ onde } 0 \leq r < b.$$

Dizemos que q é o *quociente* e r é o *resto* da divisão de a por b.

Demonstração. Pelo Teorema de Eudóxius, existe $q \in \mathbb{Z}$ satisfazendo a seguinte relação

$$qb \leq a < (q + 1)b,$$

o que acarreta que $0 \leq a - qb$ e $a - qb < b$. Sendo assim, podemos definir $r = a - qb$ para mostrar que existem números inteiros q e r que satisfazem o algoritmo. Falta mostrar que eles são únicos. Com efeito, suponha que existe um outro par q_1 e r_1 de números inteiros verificando a seguinte igualdade

$$a = q_1 b + r_1, \text{ com } 0 \leq r_1 < b.$$

Portanto, temos que $qb + r = q_1 b + r_1$. Logo,

$$b(q - q_1) = r_1 - r.$$

Isto quer dizer que b divide $r_1 - r$. Mas como r_1 e r são ambos estritamente menores do que b, segue que $|r_1 - r| < b$ e, portanto, $r_1 - r = 0$, ou seja, $r_1 = r$. Logo, $q_1 b = qb$, donde $q_1 = q$. □

1.5 Máximo Divisor Comum

Dizemos que d é o *máximo divisor comum* entre dois números inteiros a e b se é o maior inteiro positivo que divide a e b. Neste caso, escrevemos $d = \text{mdc}(a, b)$.

Uma das propriedades que vamos usar do máximo divisor comum, provada em qualquer livro de Teoria dos Números, é a seguinte: se d é o máximo divisor comum entre a e b, então existem números inteiros x e y tais que

$$d = xa + yb.$$

Observe que o máximo divisor comum d de a e b é o divisor positivo de a e b o qual é divisível por todo divisor comum. Além disso, valem as seguintes igualdades:

$$\text{mdc}(ta, tb) = |t| \cdot \text{mdc}(a, b)$$

e, se $c > 0$ e a e b são divisíveis por c, então

$$\text{mdc}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} \cdot \text{mdc}(a, b).$$

Uma última propriedade que usaremos é descrita a seguir: se a e b são números

inteiros, então vale a seguinte igualdade

$$\text{mdc}(a, b) = \text{mdc}(a, b - ax),$$

em que x é qualquer número inteiro.

Capítulo 2

Equações do Primeiro Grau com Coeficientes Inteiros

Vamos estudar primeiramente equações do primeiro grau com uma incógnita que correspondem a equações do seguinte tipo:

$$a_1 x + a_0 = 0, \tag{2.1}$$

em que a_0 e a_1 são números inteiros. Evidentemente, a solução desta equação é dada por

$$x = -\frac{a_0}{a_1},$$

com $a_1 \neq 0$, e tal solução será um número inteiro quando a_0 for divisível por a_1, isto é, quando o resto da divisão de a_0 por a_1 for zero. Nem sempre a solução de uma equação desta natureza é inteira. Este é o caso da equação $9x + 11 = 0$. Por outro lado, a solução da equação $5x - 25 = 0$ é $x = 5$, que é um número inteiro.

Uma situação similar aparece em equações que possuem grau superior a 1. Note

que a equação de segundo grau

$$x^2 + 3x - 10 = 0$$

possui duas soluções e ambas são inteiras, $x_1 = 2$ e $x_2 = -5$. No entanto, a equação $x^2 - 2x - 2 = 0$ não possui soluções inteiras, já que os dois números que satisfazem tal equação são irracionais, dadas por $1 + \sqrt{3}$ e $1 - \sqrt{3}$.

Mais geralmente, podemos considerar o problema de encontrar raízes de equações de grau n com coeficientes inteiros. De fato, sejam $n \geq 1$ e $a_0, a_1, \ldots, a_n$ números inteiros, e considere a equação

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0. \tag{2.2}$$

Estamos interessados em obter um valor inteiro de x tal que (2.2) seja satisfeita. Com efeito, se $x = a$ é uma solução inteira de (2.2), então

$$a_n a^n + a_{n-1} a^{n-1} + \cdots + a_1 a + a_0 = 0$$

e, portanto, isolando a_0, temos que

$$\begin{aligned} a_0 &= -a_n a^n - a_{n-1} a^{n-1} - \cdots - a_1 a \\ &= (-a)(a_n a^{n-1} + a_{n-1} a^{n-2} + \cdots + a_1). \end{aligned}$$

Sendo assim, concluímos que a raiz inteira a divide o número inteiro a_0, donde cada raiz inteira da equação considerada, caso exista, é divisor do termo independente a_0. Por isso, para encontrar as soluções de (2.2) é necessário encontrar os divisores de a_0 que satisfaçam tal equação.

Exemplo 2. Considere a equação

$$x^{10} + x^7 + 2x^3 + 2 = 0.$$

Então, pelo que fizemos acima, as possíveis soluções inteiras para a equação dada são $2, -2, 1$ e -1. Entretanto,

$$2^{10} + 2^7 + 2 \cdot 2^3 + 2 \neq 0,$$

o mesmo acontecendo com -2 e 1 quando substituimos estes na equação acima. Por outro lado, $x = -1$ é a única solução inteira deste equação, visto que

$$(-1)^{10} + (-1)^7 + 2 \cdot (-1)^3 + 2 = 1 - 1 + 2 - 2 = 0.$$

Utilizando este mesmo raciocínio, não é difícil ver que a equação

$$x^6 - x^5 + 3x^4 + x^2 - x + 3 = 0$$

não possui soluções inteiras, já que $1^6 - 1^5 + 3 \cdot 1^4 + 1^2 - 1 + 3 = 6 \neq 0$, $(-1)^6 - (-1)^5 + 3 \cdot (-1)^4 + (-1)^2 - (-1) + 3 = 10 \neq 0$, $3^6 - 3^5 + 3 \cdot 3^4 + 3^2 - 3 + 3 = 3^6 + 3^2 \neq 0$ e $(-3)^6 - (-3)^5 + 3 \cdot (-3)^4 + (-3)^2 - (-3) + 3 = 3^6 + 3^5 + 3^5 + 3^2 + 3 + 3 \neq 0$.

Passemos agora a analisar equações de primeiro grau com duas incógnitas, que são equações da seguinte forma:

$$ax + by + c = 0, \tag{2.3}$$

em que a e b são números inteiros não nulos e c é um inteiro qualquer. Vamos trabalhar (2.3) sob a condição de que a e b sejam números primos entre si, ou seja, que o máximo divisor comum entre a e b seja 1. Isto pode ser feito, pois

qualquer que seja a situação, podemos nos restringir a esta condição imposta sob a e b. De fato, suponha que o máximo divisor comum entre a e b seja $d \neq 1$. Então, podemos escrever $a = a_1 d$ e $b = b_1 d$, em que a_1 e b_1 são primos entre si. Dessa forma, a equação (2.3) torna-se

$$a_1 dx + b_1 dy + c = 0,$$

ou ainda,

$$(a_1 x + b_1 y)d + c = 0.$$

Assim, dividindo a equação acima por d e se dando conta de que d divide c, obtemos uma outra equação dada por

$$a_1 x + b_1 y + c_1 = 0,$$

em que $c_1 = c/d$, cujos coeficientes a_1 e b_1 tem máximo divisor comum igual a 1.

Observação: Note que se o máximo divisor comum de a e b dividir c, a equação (2.3) possui solução inteira. Com efeito, seja $d = \text{mdc}(a, b)$. Então, como $d|c$, existe $p \in \mathbb{Z}$ tal que $c = pd$. Além disso, existem $n, m \in \mathbb{Z}$ tais que $d = ma + nb$ e, portanto,

$$c = p(ma + nb) = (pm)a + (pn)b.$$

Como pm e pn são números inteiros, segue o que queríamos mostrar.

Estudaremos a equação (2.3) em dois casos. No primeiro, vamos supor que o coeficiente c é identicamente nulo. Já no segundo, consideraremos o caso em que c é qualquer número inteiro diferente de zero.

Primeiro caso: Se $c = 0$, então a equação (2.3) torna-se

$$ax + by = 0,$$

em que a e b são números inteiros primos entre si. Resolvendo esta equação com respeito a x, obtemos

$$x = -\frac{b}{a}y.$$

Sendo assim, x será um número inteiro somente quando a divide y. Isto quer dizer que existe $t \in \mathbb{Z}$ tal que $y = at$. Substituindo este valor de y na equação $x = -(b/a)y$, obtemos

$$x = -\frac{b}{a}y = -\frac{b}{a} \cdot at = -bt,$$

onde $t \in \mathbb{Z}$. Logo, todas as soluções inteiras da equação considerada são da forma:

$$\begin{cases} x &= -bt \\ y &= at, \end{cases}$$

onde $t \in \mathbb{Z}$.

Segundo caso: Consideramos agora o caso em que $c \neq 0$ e tentemos obter as soluções inteiras para a equação (2.3). Para tanto, demonstraremos um teorema que nos diz que para obter *todas* as soluções inteiras da equação (2.3), é suficiente obter uma solução particular, ou seja, se encontramos x_0 e y_0 inteiros tais que

$$ax_0 + by_0 + c = 0,$$

então encontramos todos os números inteiros que satisfazem a equação desejada.

A partir de agora, quando x e y satisfizerem a equação (2.3), escreveremos simplesmente $[x, y]$ para designar que o par x, y é solução desta equação.

Teorema 3. Sejam a e b números primos entre si e $[x_0, y_0]$ qualquer solução da equação (2.3). Então, todas as soluções inteiras desta equação são dadas pelas fórmulas

$$\begin{cases} x &= x_0 - bt \\ y &= y_0 + at, \end{cases} \tag{2.4}$$

onde $t \in \mathbb{Z}$.

Demonstração. Seja $[x_0, y_0]$ uma solução qualquer de (2.3). Então, das igualdades $ax + by + c = 0$ e $ax_0 + by_0 + c = 0$, obtemos

$$ax + by + c = ax_0 + by_0 + c,$$

o que acarreta que

$$ax - ax_0 + by - by_0 = 0,$$

ou ainda, que

$$y - y_0 = a \cdot \frac{(x_0 - x)}{b}.$$

Como $y - y_0$ é um número inteiro e o máximo divisor comum entre a e b é igual a 1, temos que b divide $x_0 - x$, ou seja, existe $t \in \mathbb{Z}$ tal que $x_0 - x = bt$. Logo,

$$y - y_0 = a \cdot \frac{bt}{b} = at,$$

donde $x = x_0 - bt$ e $y = y_0 + at$, onde $t \in \mathbb{Z}$. Demonstramos, então, que qualquer solução de (2.3) é da forma (2.4). Resta-nos mostrar que, de fato, (2.4) é solução de (2.3). Com efeito, sejam x_1 e y_1 tais que $x_1 = x_0 - bt$ e $y_1 = y_0 + at$, onde $t \in \mathbb{Z}$.

Então

$$\begin{aligned} ax_1 + by_1 + c &= a(x_0 - bt) + b(y_0 + at) + c \\ &= ax_0 - abt + by_0 + bat + c \\ &= ax_0 + by_0 + c - abt + abt \\ &= ax_0 + by_0 + c \\ &= 0, \end{aligned}$$

já que $[x_0, y_0]$ é uma solução de (2.3). □

Em suma, sendo conhecida uma solução inteira da equação (2.3), as demais soluções desta natureza são obtidas através das fórmulas (2.4). Devido a isso, nosso problema se resume a encontrar uma solução $[x_0, y_0]$ qualquer de (2.3), no caso em que $c \neq 0$. Para tanto, faremos uso de **frações contínuas** consideraremos um exemplo que nos dará a ideia central de como trataremos o caso geral.

Considere a equação

$$127x - 52y + 1 = 0.$$

Estamos interessados em encontrar uma solução inteira para esta equação, utilizando um método, descrito a seguir, feito através de relações entre os coeficientes da equação.

Primeiramente consideramos a fração irredutível 127/52 e separamos sua parte inteira do seguinte modo:

$$\frac{127}{52} = 2 + \frac{23}{52},$$

que ainda pode ser escrita como segue

$$\frac{127}{52} = 2 + \frac{1}{\frac{52}{23}}.$$

Agora, fazemos o mesmo com a fração 52/23, obtemos

$$\frac{52}{23} = 2 + \frac{6}{23} = 2 + \frac{1}{\frac{23}{6}}.$$

Utilizando este mesmo raciocínio para a fração 23/6, temos que

$$\frac{23}{6} = 3 + \frac{5}{6} = 3 + \frac{1}{\frac{6}{5}}$$

e, portanto, podemos escrever

$$\frac{127}{52} = 2 + \frac{1}{2 + \frac{1}{3 + \frac{1}{\frac{6}{5}}}}.$$

Agora, como $6/5 = 1 + 1/5$, podemos ainda escrever

$$\frac{127}{52} = 2 + \frac{1}{2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{5}}}}.$$

Esta última expressão para a fração 127/52 é chamada a **fração contínua** desta fração. Omitindo a fração 1/5 da expressão anterior, temos que a fração contínua

transforma-se em

$$2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1+0}}}=2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1}}}=2+\cfrac{1}{2+\cfrac{1}{4}}=2+\cfrac{1}{\cfrac{9}{4}}=2+\frac{4}{9}=\frac{22}{9}.$$

Além disso, temos que

$$\frac{127}{52}-\frac{22}{9}=-\frac{1}{52\cdot 9}.$$

Isto implica que

$$\frac{127}{52}\cdot\frac{9}{9}-\frac{22}{9}\cdot\frac{52}{52}=-\frac{1}{52\cdot 9},$$

ou seja,

$$127\cdot 9-52\cdot 22+1=0.$$

Assim, se $x_0=9$ e $y_0=22$, então $[x_0,y_0]$ é solução da equação $127x-52y+1=0$ e, pelo Teorema 3, todas as soluções inteiras desta equação são da forma

$$\begin{cases} x &= 9+52t, \\ y &= 22+127t, \end{cases} \quad \text{onde } t\in\mathbb{Z}.$$

Agora, como faremos para obter uma solução qualquer de uma dada equação com coeficientes inteiros, sendo $c\neq 0$? O exemplo anterior, nos permite conjecturar que, para achar uma solução particular da equação (2.3), é preciso desenvolver a fração a/b em uma fração contínua, omitindo o seu último termo e fazendo os cálculos feitos anteriormente. É o que faremos a seguir.

Seguiremos os passos do exemplo anterior. Considere a fração irredutível a/b. Denote por q_1 e por r_2 o quociente e o resto da divisão de a por b, respectivamente. Assim, podemos escrever

$$a=q_1b+r_2,\ \text{com } r_2<b.$$

Sejam agora q_2 e r_3 o quociente e o resto da divisão de b por r_2. Então

$$b = q_2 r_2 + r_3, \text{ com } r_3 < r_2.$$

Da mesma maneira, podemos considerar os números $q_3, q_4, \ldots$ e $r_4, r_5, \ldots$ se relacionando da seguinte maneira:

$$r_2 = q_3 r_3 + r_4, \text{ com } r_4 < r_3,$$

$$r_3 = q_4 r_4 + r_5, \text{ com } r_5 < r_4$$

e assim por diante. Os quocientes $q_1, q_2, \ldots$ das divisões feitas anteriormente são chamados de **quocientes incompletos** e cumprem a seguinte condição:

$$b > r_2 > r_3 > r_4 > \cdots \geq 0, \tag{2.5}$$

isto é, formam uma sequência decrescente de números positivos. Como a quantidade de números inteiros entre b e 0 é finita, em um determinado momento, o procedimento acima estaciona, com resto 0. Assim, se r_n é o último resto não nulo em (2.5), então $r_{n+1} = 0$ e, portanto, temos que

$$a = q_1 \cdot b + r_2,$$

$$b = q_2 \cdot r_2 + r_3,$$

$$r_2 = q_3 \cdot r_3 + r_4,$$

$$\vdots$$

$$r_{n-2} = q_{n-1} \cdot r_{n-1} + r_n,$$

$$r_{n-1} = q_n \cdot r_n + 0.$$

Estas equações podem ser escritas da seguinte forma:

$$\frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_2}},$$

$$\frac{b}{r_2} = q_2 + \frac{1}{\frac{r_2}{r_3}},$$

$$\vdots$$

$$\frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},$$

$$\frac{r_{n-1}}{r_n} = q_n.$$

Podemos, então, substituir o valor do número b/r_2 na primeira expressão, o valor do número r_2/r_3 na segunda expressão e, assim sucessivamente, até encontrarmos uma expressão para a fração a/b dada por

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{1}{q_{n-2} + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}}$$

Considerando a fração contínua de a/b, podemos omitir frações a partir do primeiro quociente q_1. As expressões obtidas depois desta omissão são chamadas de **frações reduzidas**. Temos que a primeira fração reduzida, denotada por δ_1, é obtida omitindo a fração $1/q_2$:

$$\delta_1 = q_1 < \frac{a}{b}.$$

A desigualdade é justificada a seguir: como

$$\frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_2}}$$

e, b e r_2 são números positivos, segue que $a/b > q_1$.

A segunda fração reduzida é obtida omitindo a fração a partir do termo $1/q_3$:

$$\delta_2 = q_1 + \frac{1}{q_2} > \frac{a}{b},$$

em que a desigualdade é justificada a seguir: como

$$\frac{b}{r_2} = q_2 + \frac{r_3}{r_2},$$

temos que

$$q_2 = \frac{b}{r_2} - \frac{r_3}{r_2} = \frac{b - r_3}{r_2} < \frac{b}{r_2},$$

pois $r_2 > 0$, ou seja,

$$\frac{1}{q_2} > \frac{r_2}{b}.$$

Agora,

$$\frac{a}{b} = q_1 + \frac{r_2}{b} < q_1 + \frac{1}{q_2},$$

como queríamos.

Analogamente, obtemos o restante das frações reduzidas:

$$\delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}},$$

$$\delta_4 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4}}}$$

que satisfazem as desigualdades $\delta_3 < a/b$ e $\delta_4 > a/b$. Portanto, seguindo por indução poderíamos demonstrar as seguintes relações:

$$\delta_1 < \delta_3 < \ldots < \delta_{2k-1} < \frac{a}{b},$$

$$\delta_2 > \delta_4 > \ldots > \delta_{2k} > \frac{a}{b},$$

onde $k \in \mathbb{N}$. Observe que as relações de ordem entre os δ_i's são fornecidas através das relações de ordem entre os q_i's. Por exemplo, é claro que $\delta_1 < \delta_3$, pois $\frac{1}{q_2+\frac{1}{q_3}}$ é um número positivo. Por outro lado, como

$$\delta_4 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4}}},$$

e $\frac{1}{q_3+\frac{1}{q_4}} > 0$, segue que $\delta_4 < q_1 + \frac{1}{q_2} = \delta_2$.

Agora, denote por

$$\delta_k = \frac{P_k}{Q_k}$$

a k-ésima fração reduzida de a/b, onde $1 \leq k \leq n$. Vamos encontrar a lei de formação dos numeradores e denominadores dessas frações reduzidas. Vejamos o que acontece com os primeiros δ_i's:

$$\delta_1 = q_1 = \frac{q_1}{1} = \frac{P_1}{Q_1} \Rightarrow P_1 = q_1 \text{ e } Q_1 = 1,$$

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_1 q_2 + 1}{q_2} = \frac{P_2}{Q_2} \Rightarrow P_2 = q_1 q_2 + 1 \text{ e } Q_2 = q_2,$$

$$\delta_3 = q_1 + \frac{1}{q_2 + \dfrac{1}{q_3}} = q_1 + \frac{q_3}{q_2 q_3 + 1} = \frac{q_1 q_2 q_3 + q_1 + q_3}{q_2 q_3 + 1} = \frac{P_3}{Q_3}$$

e, assim, $P_3 = q_1 q_2 q_3 + q_1 + q_3$ e $Q_3 = q_2 q_3 + 1$, ou seja,

$$P_3 = P_2 q_3 + P_1 \quad \text{e} \quad Q_3 = Q_2 q_3 + Q_1.$$

Vamos demonstrar, usando indução sobre k, que

$$P_k = P_{k-1} q_k + P_{k-2} \quad \text{e} \quad Q_k = Q_{k-1} q_k + Q_{k-2}, \tag{2.6}$$

Com efeito, suponha que (2.6) é válido para algum $k \geq 3$ e provemos que é válido para $k+1$, ou seja, da hipótese de indução, temos que

$$\delta_k = \frac{P_k}{Q_k} = \frac{P_{k-1} q_k + P_{k-2}}{Q_{k-1} q_k + Q_{k-2}}.$$

Agora, substituindo q_k por $q_k + \frac{1}{q_{k+1}}$ na expressão acima, obtemos que:

$$\frac{P_{k-1}\left(q_k + \dfrac{1}{q_{k+1}}\right) + P_{k-2}}{Q_{k-1}\left(q_k + \dfrac{1}{q_{k+1}}\right) + Q_{k-2}} = \frac{P_{k-1} q_k + P_{k-2} + P_{k-1} \cdot \dfrac{1}{q_{k+1}}}{Q_{k-1} q_k + Q_{k-2} + \dfrac{1}{q_{k+1}} \cdot Q_{k-1}} = \frac{P_k q_{k+1} + P_{k-1}}{Q_k q_{k+1} + Q_{k-1}} = \delta_{k+1}.$$

Por outro lado, $\delta_{k+1} = \dfrac{P_{k+1}}{Q_{k+1}}$ e, portanto,

$$P_{k+1} = P_k q_{k+1} + P_{k-1} \quad \text{e} \quad Q_{k+1} = Q_k q_{k+1} + Q_{k-1}.$$

Assim, (2.6) é válido para qualquer inteiro $k \geq 3$.

A seguir, vamos provar que a diferença $\delta_k - \delta_{k-1}$ entre as frações reduzidas

cumprem a seguinte igualdade

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}}, \tag{2.7}$$

em que $k > 1$. Com efeito,

$$\delta_k - \delta_{k-1} = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_k Q_{k-1} - Q_k P_{k-1}}{Q_k Q_{k-1}}.$$

Usando (2.6), obtemos

$$\begin{aligned} P_k Q_{k-1} - Q_k P_{k-1} &= (P_{k-1}q_k + P_{k-2})Q_{k-1} - (Q_{k-1}q_k + Q_{k-2})P_{k-1} \\ &= P_{k-1}q_k Q_{k-1} + P_{k-2}Q_{k-1} - Q_{k-1}q_k P_{k-1} - Q_{k-2}P_{k-1} \\ &= -(P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2}) \\ &= (-1)(P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2}). \end{aligned}$$

Note que a expressão $P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2}$ é o mesmo que $P_k Q_{k-1} - Q_k P_{k-1}$ fazendo k igual a $k-1$ na segunda equação. Fazendo os mesmo cálculos para $P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2}$, obtemos

$$P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2} = (-1)(P_{k-2}Q_{k-3} - Q_{k-2}P_{k-3}).$$

Continuando dessa forma, tem-se que

$$\begin{aligned} P_kQ_{k-1} - Q_kP_{k-1} &= (-1)(P_{k-1}Q_{k-2} - Q_{k-1}P_{k-2}) \\ &= (-1)^2(P_{k-2}Q_{k-3} - Q_{k-2}P_{k-3}) \\ &= \ldots\ \ldots\ \ldots \\ &= (-1)^{k-2}(P_2Q_1 - Q_2P_1) \\ &= (-1)^{k-2}[(q_1q_2 + 1)\cdot 1 - q_2q_1] \\ &= (-1)^{k-2}. \end{aligned}$$

Portanto,

$$\begin{aligned} \delta_k - \delta_{k-1} &= \frac{P_kQ_{k-1} - Q_kP_{k-1}}{Q_kQ_{k-1}} \\ &= \frac{(-1)^{k-2}}{Q_kQ_{k-1}} \\ &= \frac{(-1)^k}{Q_kQ_{k-1}} \end{aligned}$$

para todo inteiro $k > 1$. Note que, pela definição das frações reduzidas, temos $\delta_n = a/b$. Agora, fazendo $k = n$ na equação (2.7), obtemos

$$\delta_n - \delta_{n-1} = \frac{(-1)^n}{Q_nQ_{n-1}},$$

ou seja,

$$\frac{a}{b} - \delta_{n-1} = \frac{(-1)^n}{bQ_{n-1}}, \tag{2.8}$$

já que $Q_n = b$.

Finalmente, voltemos para a equação (2.3). De (2.8), temos que

$$\frac{a}{b} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n}{bQ_{n-1}}$$

que é o mesmo que

$$\frac{a}{b} \cdot \frac{Q_{n-1}}{Q_{n-1}} - \frac{P_{n-1}}{Q_{n-1}} \cdot \frac{b}{b} = \frac{(-1)^n}{bQ_{n-1}}.$$

Simplificando a última equação, obtemos simplesmente

$$aQ_{n-1} - bP_{n-1} = (-1)^n.$$

Ou ainda,

$$aQ_{n-1} + b(-P_{n-1}) + (-1)^{n-1} = 0.$$

Multiplicando esta última equação por $(-1)^{n-1}c$, obtemos

$$a[(-1)^{n-1}cQ_{n-1}] + b[(-1)^n cP_{n-1}] + c = 0.$$

Assim, deduzimos que $[x_0, y_0]$ dado por

$$x_0 = (-1)^{n-1}cQ_{n-1} \quad \text{e} \quad y_0 = (-1)^n cP_{n-1}$$

é uma solução da equação (2.3) e pelo teorema anterior, todas as soluções inteiras desta equação tem a seguinte forma:

$$\begin{cases} x &= (-1)^{n-1}cQ_{n-1} - bt \\ y &= (-1)^n cP_{n-1} + at, . \end{cases}$$

onde $t \in \mathbb{Z}$. Isto prova o seguinte teorema:

Teorema 4. O par $[x_0, y_0]$ dado por

$$\begin{cases} x_0 &= (-1)^{n-1} cQ_{n-1} \\ y_0 &= (-1)^n cP_{n-1}, \end{cases}$$

é uma solução da equação (2.3) e, portanto, todas as soluções inteiras desta equação são dadas pelas fórmulas a seguir:

$$x = (-1)^{n-1} cQ_{n-1} - bt \quad \text{e} \quad y = (-1)^n cP_{n-1} + at,$$

onde $t \in \mathbb{Z}$.

Capítulo 3

Algumas Equações do Segundo Grau com Três Incógnitas

Neste capítulo, apresentaremos alguns exemplos de equações de segundo grau com três incógnitas como o título nos sugere.

3.1 A equação de Pitágoras $x^2 + y^2 = z^2$

Exemplo 3. (Equação de Pitágoras) Vamos encontrar todas as soluções inteiras da equação do segundo grau com três incógnitas dada a seguir

$$x^2 + y^2 = z^2. \tag{3.1}$$

Solução: Geometricamente, as soluções inteiras desta equação são determinadas por aqueles números inteiros que satisfazem os *triângulos de Pitágoras*, isto é, triângulos retângulos que têm como catetos e hipotenusa tais números. Vamos determinar todos os esses números analiticamente.

Denotando por d o máximo divisor comum de x e y, então existem números inteiros x_1 e y_1 que satisfazem as equações abaixo:

$$x = x_1 d \quad \text{e} \quad y = y_1 d$$

com x_1 e y_1 primos entre si e, portanto, a equação (3.1) torna-se a equação abaixo:

$$x_1^2 d^2 + y_1^2 d^2 = z^2,$$

ou ainda,

$$(x_1^2 + y_1^2) d^2 = z^2.$$

Isto quer dizer que z^2 é divisível por d^2 e, portanto, existe p inteiro tal que $z^2 = p \cdot d^2$, donde p também deve ser um quadrado, isto é, existe $z_1 \in \mathbb{Z}$ tal que $p = z_1^2$. Assim, $z^2 = z_1^2 d^2$, donde $z = z_1 d$.

Agora, a equação (3.1) pode ser expressa como segue

$$(x_1^2 + y_1^2) d^2 = z_1^2 d^2$$

e simplificando o termo d^2, temos

$$x_1^2 + y_1^2 = z_1^2.$$

A equação acima obtida tem a mesma forma que a inicial com uma nova informação: x_1 e y_1 não possuem divisores em comum, exceto o número 1. Com isso, para resolver a equação (3.1) é suficiente atacar o problema considerando x e y primos entre si. Suponhamos, portanto, que isto acontece. Sendo assim, podemos assumir que ou x ou y é um número ímpar, digamos x. Passando y^2 ao segundo membro da equação

(3.1), obtemos

$$x^2 = z^2 - y^2,$$

ou ainda,

$$x^2 = (z + y)(z - y). \tag{3.2}$$

Denotando por d_1 o máximo divisor comum de $z + y$ e $z - y$, temos

$$z + y = ad_1 \quad \text{e} \quad z - y = bd_1, \tag{3.3}$$

com a e b são primos entre si. Substituindo as equações de (3.3) na equação (3.2), obtemos:

$$\begin{aligned} x^2 &= (z + y)(z - y) \\ &= ad_1 \cdot bd_1 \\ &= abd_1^2. \end{aligned}$$

Desde que a e b não têm divisores em comum, a igualdade obtida acima é válida somente quando a e b forem quadrados perfeitos, isto é, quando existirem u e v inteiros tais que

$$a = u^2 \quad \text{e} \quad b = v^2.$$

Sendo assim, temos que

$$x^2 = u^2 v^2 d_1^2$$

e, então

$$x = uvd_1. \tag{3.4}$$

Vamos encontrar agora os valores de y e z usando as equações (3.3). Adicionando

tais equações, obtemos

$$(z + y) + (z - y) = ad_1 + bd_1,$$

ou seja,

$$\begin{aligned} 2z &= ad_1 + bd_1 \\ &= u^2 d_1 + b^2 d_1 \\ &= (u^2 + v^2) d_1. \end{aligned}$$

Logo,

$$z = \frac{u^2 + v^2}{2} \cdot d_1. \tag{3.5}$$

Agora, subtraindo a segunda equação da primeira em (3.3), temos que

$$(z - y) - (z + y) = bd_1 - ad_1,$$

ou seja,

$$-2y = bd_1 - ad_1.$$

Logo,

$$\begin{aligned} 2y &= ad_1 - bd_1 \\ &= u^2 d_1 - v^2 d_1 \\ &= (u^2 - v^2) d_1 \end{aligned}$$

e, assim,

$$y = \frac{u^2 - v^2}{2} \cdot d_1. \tag{3.6}$$

Lembrando que x é ímpar, temos de (3.4) que os números inteiros u, v e d_1 também

são ímpares. Disso, temos que d_1 é necessariamente igual a 1, já que do contrário, as equações (3.4) e (3.6) nos mostrariam que x e y possuiriam um divisor comum $d_1 \neq 1$, o que contradiz a hipótese inicial de que eles são primos entre si.

Agora, como $a = u^2$ e $b = v^2$, e a e b são primos entre si, segue que existem números inteiros r e s tais que

$$ar + bs = 1,$$

ou ainda,

$$u^2r + v^2s = 1.$$

Mas

$$u^2r + v^2s = u(ur) + v(vs) = 1,$$

em que ur e vs são ainda números inteiros. Logo, u e v também são primos entre si. Além disso, de (3.3) temos que

$$ad_1 - bd_1 = 2y$$

e, portanto,

$$a - b = \frac{2y}{d_1} > 0,$$

isto é, $b < a$. Fazendo $d_1 = 1$ em (3.4), (3.5) e (3.6), obtemos as fórmulas

$$x = uv, \quad y = \frac{u^2 - v^2}{2} \quad \text{e} \quad z = \frac{u^2 + v^2}{2}, \tag{3.7}$$

das quais são todos os números inteiros positivos livres de divisores comuns que verificam a equação (3.1), já que u e v são primos entre si. De fato, as relações (3.7)

verificam a equação (3.1) como nos mostra os cálculos abaixo:

$$\begin{aligned} x^2 + y^2 &= (uv)^2 + \left(\frac{u^2 - v^2}{2}\right)^2 \\ &= u^2v^2 + \frac{(u^2)^2 - 2u^2v^2 + (v^2)^2}{4} \\ &= \frac{4u^2v^2 + (u^2)^2 - 2u^2v^2 + (v^2)^2}{4} \\ &= \frac{(u^2)^2 + 2u^2v^2 + (v^2)^2}{4} \\ &= \frac{(u^2 + v^2)^2}{2^2} \\ &= z^2. \end{aligned}$$

Colocando alguns valores inteiros para u e v, primos entre si, nas fórmulas em (3.7), podemos encontrar soluções inteiras para a equação (3.1). Por exemplo, se $u = 3$ e $v = 1$ então temos a equação satisfeita para $x = 3$, $y = 4$ e $z = 5$: $3^2 + 4^2 = 5^2$. Ou ainda se $u = 5$ e $v = 1$, a equação é satisfeita para $x = 5$, $y = 12$ e $z = 13$.

Note ainda que as fórmulas em (3.7) nos dão as soluções inteiras da equação (3.1) quando x, y e z não possuem divisores em comum. Todas as demais soluções inteiras desta equação, podem ser obtidas multiplicando as soluções encontradas com (3.7) por um número inteiro d, já que se x_0, y_0, z_0 é uma solução de (3.1) dx_0, dy_0, dz_0 também é, pois

$$\begin{aligned} (dx_0)^2 + (dy_0)^2 &= d^2x_0^2 + d^2y_0^2 \\ &= d^2(x_0^2 + y_0^2) \\ &= d^2z_0^2 \\ &= (dz_0)^2. \end{aligned}$$

Observação: O problema anterior também pode ser resolvido de forma geo-

métrica, se "parametrizamos racionalmente" o círculo unitário, como mostraremos a seguir (confira [9]). Considere a equação do círculo C

$$x^2 + y^2 = 1. \tag{3.8}$$

Denotemos por $(0, t)$ o ponto de interseção da reta L que passa por $(-1, 0)$ e por um ponto do círculo C com o eixo dos y's, como nos mostra a Figura 3.1.

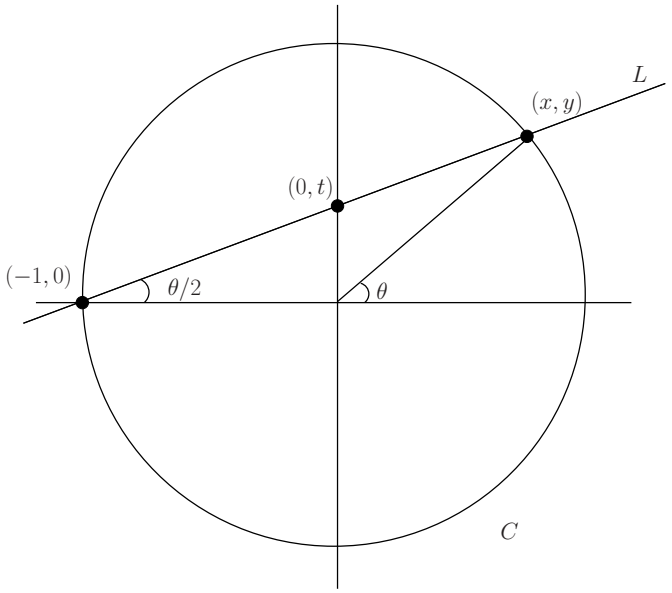

Figura 3.1: Interseção da reta L com o círculo C.

Se conhecemos os valores de x e y, então podemos determinar o valor de t sem muitas dificuldades. De fato, a equação da reta L é dada por

$$y = t(1 + x), \tag{3.9}$$

já que L passa pelos pontos $(-1, 0)$ e $(0, t)$. Como o ponto (x, y) pertence tanto a L como a C, segue de (3.8) e (3.9) que

$$1 - x^2 = y^2 = t^2(1 + x)^2. \tag{3.10}$$

Para t fixado, (3.10) é uma equação quadrática cujas raízes são as primeiras coordenadas dos pontos de interseção entre a reta L e o círculo C. Sabemos que $x = -1$ é uma dessa raízes, pois o ponto $(-1, 0)$ pertence a L e a C. Para encontrar a outra raiz, suponha que $x \neq -1$. Então, em (3.10), podemos cancelar o termo $(1 + x)$ em ambos os membros e obter a seguinte equação:

$$1 - x = t^2(1 + x).$$

Assim,

$$1 - x = t^2 + t^2 x,$$

ou seja,

$$x + t^2 x = 1 - t^2.$$

Portanto, $(1 + t^2)x = 1 - t^2$, isto é,

$$x = \frac{1 - t^2}{1 + t^2}.$$

Agora, como $y = t(1 + x)$, segue que

$$y = t\left(1 + \frac{1 - t^2}{1 + t^2}\right) = t\left(\frac{1 + t^2 + 1 - t^2}{1 + t^2}\right) = \frac{2t}{1 + t^2}.$$

Sendo assim, obtemos a *parametrização do círculo*:

$$x = \frac{1 - t^2}{1 + t^2} \quad \text{e} \quad y = \frac{2t}{1 + t^2}. \tag{3.11}$$

Note que se x e y são números racionais, então t também será um número racional. Reciprocamente, se t é racional, então x e y também serão pelas equações obtidas em (3.11). Então, esta é a maneira de obtermos "pontos racionais" no círculo, a saber, escolhendo um número racional qualquer para t. Isto fornecerá todos os pontos

racionais exceto $(-1, 0)$ de C.

Estas fórmulas podem ser usadas para resolver o problema de descrever todos os triângulos de Pitágoras. Estamos novamente interessados em solucionar o problema (3.1) do exemplo 3, ou seja, queremos todos os números inteiros X, Y e Z que satisfaçam a equação

$$X^2 + Y^2 = Z^2. \tag{3.12}$$

Como já vimos no exemplo 3, é suficiente estudarmos este problema no caso de X, Y e Z serem primos entre si. Note que o ponto (x, y), onde

$$x = \frac{X}{Z} \quad \text{e} \quad y = \frac{Y}{Z}$$

é um ponto racional do círculo $x^2 + y^2 = 1$, já que

$$x^2 + y^2 = \frac{X^2}{Z^2} + \frac{Y^2}{Z^2} = 1$$

e X, Y e Z são números inteiros, fazendo uso da equação (3.12). Como X e Y são números primos entre si, eles não podem ser ambos pares. Afirmamos que eles também não podem ser ambos ímpares. Primeiramente, note que se um número $p = 2k + 1$, onde $k \in \mathbb{Z}$, é um número ímpar, então

$$p^2 = (2k + 1)^2 = 4k^2 + 4k + 1,$$

ou seja, $p^2 - 1$ é divisível por 4. Lembrando disso, suponha que X e Y sejam ambos ímpares. Então, $X^2 + Y^2 - 2$ é divisível por 4 pelo que acabamos de mencionar. Mas $X^2 + Y^2 = Z^2$ e Z^2 é tal que: ou Z^2 é divisível por 4 ou $Z^2 - 1$ é divisível por 4. Então, X e Y *não* podem ser ambos ímpares. Assumimos, sem perda de generalidade, que X é ímpar e que Y é par.

Como (x, y) é um ponto racional no círculo, existe algum $t \in \mathbb{Q}$ que nos fornece

o x e o y nas fórmulas de (3.11). Escreva, então, $t = m/n$, na sua forma reduzida, em que m e n são números inteiros. Portanto,

$$\frac{X}{Z} = x = \frac{1 - \dfrac{m^2}{n^2}}{1 + \dfrac{m^2}{n^2}} = \frac{n^2 - m^2}{n^2 + m^2},$$

e

$$\frac{Y}{Z} = y = \frac{2 \cdot \dfrac{m}{n}}{1 + \dfrac{m^2}{n^2}} = \frac{2mn}{n^2 + m^2}.$$

Como X/Z e Y/Z estão em suas formas reduzidas, existe $\lambda \in \mathbb{Z}$ tal que

$$\lambda Z = n^2 + m^2 \ , \ \lambda Y = 2mn \text{ e } \lambda X = n^2 - m^2.$$

Vamos mostrar que $\lambda = 1$. Com efeito, como λ divide $n^2 + m^2$ e $n^2 - m^2$ temos que λ também divide

$$(n^2 + m^2) + (n^2 - m^2) = 2n^2$$

e

$$(n^2 + m^2) - (n^2 - m^2) = 2m^2.$$

Mas m e n são primos entre si. Portanto, λ divide 2, ou seja, $\lambda = 1$ ou $\lambda = 2$. Se $\lambda = 2$, então

$$n^2 - m^2 = \lambda X = 2X$$

é divisível por 2 e não por 4, já que estamos supondo que X é ímpar. Logo, $n^2 - m^2 - 2$ é divisível por 4. Vamos justificar esta última afirmação. Com efeito, como X é ímpar, X pode se escrever como $X = 2k + 1$, onde $k \in \mathbb{Z}$. Daí, $2X = 4k + 2$ e, portanto,

$$n^2 - m^2 - 2 = 2X - 2 = 4k + 2 - 2 = 4k,$$

donde $n^2 - m^2 - 2$ é divisível por 4. Mas n^2 é tal que: ou n^2 é divisível por 4 ou $n^2 - 1$ é divisível por 4. O mesmo vale para m^2. Logo, não pode acontecer de $n^2 - m^2 - 2$ ser divisível por 4. Logo, $\lambda = 1$.

Isto prova que todos os triângulos de Pitágoras podem ser obtidos pelas relações

$$X = n^2 - m^2 \ , \ Y = 2mn \ , \ Z = n^2 + m^2,$$

em que n e m são primos entre si e, X e Y têm paridades opostas. Compare este resultado ao que obtemos no exemplo 3.

3.2 A equação $x^2 + 2y^2 = z^2$

Exemplo 4. Vamos obter todas as soluções da equação

$$x^2 + 2y^2 = z^2, \tag{3.13}$$

onde x, y e z são inteiros positivos e primos entre si.

Solução: Primeiramente, observemos que se x, y, z é uma solução de (3.13), onde x, y e z não têm divisor comum diferente de 1, então eles são dois a dois primos entre si. De fato, suponha, por absurdo, que x e y sejam múltiplos de um número primo $p > 2$. Então, da igualdade (3.13), podemos escrever

$$\left(\frac{x}{p}\right)^2 + 2\left(\frac{y}{p}\right)^2 = \left(\frac{z}{p}\right)^2$$

multiplicando ambos os membros por $1/p^2$. Logo, como $x = n_1 p$ e $y = n_2 p$, para alguns $n_1, n_2 \in \mathbb{Z}$, segue que

$$\left(\frac{n_1 p}{p}\right)^2 + 2\left(\frac{n_2 p}{p}\right)^2 = \left(\frac{z}{p}\right)^2,$$

ou seja,

$$(n_1^2 + 2n_2^2) \cdot p^2 = z^2.$$

Então, p^2 divide z^2 e, portanto, p divide z. Isto quer dizer que z também é múltiplo de p, contradizendo o fato de que o máximo divisor comum entre x, y e z é 1. O mesmo acontece se considerarmos que x e z ou y e z são múltiplos de um primo $p > 2$.

Afim de que o máximo divisor comum entre x, y e z seja igual a 1, observemos que x deverá ser um número ímpar. É o que vamos provar agora. Com efeito, se x é um número par, o primeiro membro da equação (3.13) será um número par e, portanto, z também será. Sendo assim, x^2 e z^2 são múltiplos de 4. Logo, existem n_1 e n_2 inteiros tais que $x^2 = 4n_1$ e $z^2 = 4n_2$, donde

$$\begin{aligned} 2y^2 &= z^2 - x^2 \\ &= 4n_2 - 4n_1 \\ &= 4(n_2 - n_1), \end{aligned}$$

ou seja, $2y^2$ é divisível por 4 e, portanto, y é divisível por 2. Isto quer dizer que se x for um número par, então os números y e z também serão pares, mas isto contradiz novamente a hipótese feita sobre estes três números de que seu máximo divisor comum é 1. Segue, então, que na solução sem divisor comum diferente de 1, o termo x deve ser ímpar e, assim, z também será, já que se z fosse par então teríamos que $x^2 = z^2 - 2y^2$ também seria par.

Agora, passando x^2 ao segundo membro da equação (3.13), obtemos

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

Vamos provar que o máximo divisor comum de $z + x$ e $z - x$ é igual a 2. Com

efeito, seja d este máximo divisor comum e provemos que $d = 2$. Temos que

$$z + x = kd \quad \text{e} \quad z - x = ld,$$

em que k e l são números inteiros primos entre si. Adicionando e subtraindo estas duas últimas equações, obtemos que

$$2z = (k + l)d \quad \text{e} \quad 2x = (k - l)d.$$

Mas z e x são números ímpares e primos entre si e, por isso, $\text{mdc}(2z, 2x) = 2$. Daí,

$$\text{mdc}(d(k + l), d(k - l)) = d \cdot \text{mdc}(k + l, k - l).$$

Veja que $d|2z$ e $d|2x$. Dado que $\text{mdc}(z, x) = 1$, segue que $d|2$. Logo, $d = 1$ ou $d = 2$. Se d fosse 1, então teríamos nas equações

$$z + x = dk = 1 \cdot k = k \quad \text{e} \quad z - x = d \cdot l = 1 \cdot l = l.$$

Mas como z e x são ímpares, então a soma e a diferença seria par, ou seja, k e l seriam pares, mas isso é um absurdo, pois eles não primos entre si. Logo, $d = 2$, ou seja,

$$\text{mdc}(z + x, z - x) = 2,$$

ou ainda,

$$\text{mdc}\left(\frac{z + x}{2}, \frac{z - x}{2}\right) = 1.$$

Assim, $\frac{z+x}{2}$ ou $\frac{z-x}{2}$ é ímpar. Consequentemente, temos duas possibilidades: ou os números

$$z + x \quad \text{e} \quad \frac{z - x}{2}$$

são primos entre si ou os números

$$\frac{z+x}{2} \quad \text{e} \quad z-x$$

são primos entre si. No primeiro caso, da igualdade

$$(z+x) \cdot \frac{z-x}{2} = y^2$$

temos que

$$z+x = n^2 \quad \text{e} \quad z-x = 2m^2$$

e no segundo caso, a igualdade

$$\frac{z+x}{2} \cdot (z-x) = y^2$$

acarreta que

$$z+x = 2m^2 \quad \text{e} \quad z-x = n^2,$$

em que n e m são inteiros positivos. Note que m é necessariamente ímpar, pois se fosse par, seu quadrado também seria e, portanto, o número

$$\frac{z-x}{2} = m^2$$

seria par e os números $z+x$ e $\frac{z-x}{2}$ não seriam primos entre si, já que estamos no caso em que $\frac{z-x}{2}$ é ímpar e, portanto, $z+x$ é par. O mesmo ocorre para o segundo caso.

Assim, resolvendo o sistema linear do primeiro caso, temos que

$$z = \frac{n^2+2m^2}{2} \quad , \quad x = \frac{n^2-2m^2}{2} \quad \text{e} \quad y = nm$$

e resolvendo o sistema do segundo, que

$$z = \frac{n^2 + 2m^2}{2} \quad , \quad x = \frac{2m^2 - n^2}{2} \quad \text{e} \quad y = nm$$

em que m é um número ímpar. Assim, a fórmula geral que representa a solução x, y, z da equação (3.13) é dada por

$$x = \pm\frac{1}{2} \cdot (n^2 - 2m^2) \quad , \quad y = mn \quad \text{e} \quad z = \frac{1}{2} \cdot (n^2 + 2m^2),$$

em que m é ímpar. Mas para que x e z sejam números inteiros, é preciso que n seja par. Sendo assim, se $n = 2b$ e $m = a$, então todas as soluções inteiras da equação (3.13) com x, y e z positivos sem divisor comum diferente de 1 são dadas por

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

em que a e b são positivos sendo a um número ímpar.

Finalmente, note que estas fórmulas encontradas, de fato, correspondem as soluções da equação (3.13) com as condições impostas sobre x, y e z como nos mostra os cálculos a seguir:

$$\begin{aligned} x^2 + 2y^2 &= [\pm(a^2 - 2b^2)]^2 + 2(2ab)^2 \\ &= (a^2)^2 - 2 \cdot a^2 2b^2 + (2b^2)^2 + 2 \cdot 4a^2b^2 \\ &= (a^2)^2 - 4a^2b^2 + (2b^2)^2 + 8a^2b^2 \\ &= (a^2)^2 + 4a^2b^2 + (2b^2)^2 \\ &= (a^2 + 2b^2)^2 \\ &= z^2. \end{aligned}$$

3.3 A equação "negativa" de Pitágoras $x^{-2} + y^{-2} = z^{-2}$

Exemplo 5. Estamos agora interessados em resolver a equação

$$x^{-2} + y^{-2} = z^{-2} \tag{3.14}$$

para x, y e z números naturais.

Solução: Note que (3.14) é o mesmo que

$$x^2 + y^2 = \left(\frac{xy}{z}\right)^2 \tag{3.15}$$

já que

$$\begin{aligned} x^{-2} + y^{-2} = z^{-2} &\Rightarrow \frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2} \\ &\Rightarrow \frac{y^2 + x^2}{x^2 y^2} = \frac{1}{z^2} \\ &\Rightarrow x^2 + y^2 = \frac{x^2 y^2}{z^2} = \left(\frac{xy}{z}\right)^2. \end{aligned}$$

Isso implica que z divide xy e que $x^2 + y^2$ é um quadrado perfeito, ou seja, existe $t \in \mathbb{N}$ tal que

$$x^2 + y^2 = t^2$$

e, portanto,

$$t = \frac{xy}{z}. \tag{3.16}$$

Seja $d = \text{mdc}(x, y, t)$ o máximo divisor comum entre x, y e t. Então, podemos escrever $x = ad$, $y = bd$ e $t = cd$, onde a, b e c são números naturais relativamente

primos entre si. Portanto, de (3.16), segue que

$$cd = \frac{(ad)(bd)}{z},$$

ou seja,

$$z = \frac{(ad)(bd)}{cd} = \frac{abd^2}{cd} = \frac{abd}{c}. \tag{3.17}$$

Lembrando que $\text{mdc}(a, b, c) = 1$, segue que c divide d, já que d é um número natural. Portanto, existe $k \in \mathbb{N}$ tal que $d = kc$ e, portanto, as equações $x = ad$, $y = bd$, $t = cd$ e (3.17) transformam-se em

$$x = kac,\ y = kbc,\ t = kc^2 \text{ e } z = kab.$$

De $t^2 = x^2 + y^2$, temos que

$$a^2 + b^2 = c^2, \tag{3.18}$$

em que a, b e c são relativamente primos entre si. Do Exemplo 3, temos que as soluções de (3.18) são

$$a = m^2 - n^2,\ b = 2mn,\ c = m^2 + n^2,$$

em que os inteiros m e n satisfazem as condições da equação apresentada naquele exemplo. Portanto, as soluções da equação (3.14) são

$$\begin{cases} x = kac = k(m^2 - n^2)(m^2 + n^2) = k(m^4 - n^4), \\ y = kbc = k(2mn)(m^2 + n^2) = 2kmn(m^2 + n^2), \\ z = kab = k(m^2 - n^2)(2mn) = 2kmn(m^2 - n^2), \end{cases}$$

em que $k, m, n \in \mathbb{N}$ e $m > n$.

3.4 A equação de Fermat $x^4 + y^4 = z^4$

Para resolver a equação de Fermat $x^4 + y^4 = z^4$, precisamos primeiramente resolver a equação $x^4 + y^4 = z^2$, como fazemos no Exemplo 6. A equação desejada é tratada no Exemplo 7.

Exemplo 6. Provaremos que a equação

$$x^4 + y^4 = z^2 \tag{3.19}$$

não possui solução inteira.

Solução: Pelo aspecto da equação (3.19), é suficiente mostrar o resultado para x, y e z estritamente positivos. Suponhamos, por absurdo, que (3.19) possua uma solução não trivial, isto é, existe um terno (x_1, y_1, z_1) que satisfaz tal equação. Considere que z_1 seja o menor número natural com esta propriedade. Nosso objetivo é chegar em uma contradição sobre a minimalidade de z_1.

Da mesma maneira que fizemos no Exemplo 3, podemos supor, sem perda de generalidade, que o máximo divisor comum entre x_1, y_1 e z_1 seja igual a 1. De fato, se existe uma solução tal que x_1 e y_1 tenham um máximo divisor comum igual a $d > 1$, então

$$x_1 = dx_2' \quad \text{e} \quad y_1 = dy_2',$$

onde $\text{mdc}(x_2', y_2') = 1$. Assim, a equação (3.19) se transforma na equação

$$(x_2')^4 + (y_2')^4 = \left(\frac{z_1}{d^2}\right)^2 = (z_2')^2. \tag{3.20}$$

Mas como x_2' e y_2' são números inteiros, temos que z_2' também é um número inteiro. Se z_2' e y_2' tivessem mdc igual a $k > 1$, então, segundo a igualdade (3.20), $(x_2')^2$ seria divisível por k e, portanto, x_2' e y_2' não poderiam ser primos entre si, contrariando

a hipótese de ser $\text{mdc}(x_2', y_2') = 1$. Sendo assim, basta considerarmos o caso em que os números que compõe a solução de (3.19) são todos primos entre si.

Vejamos algumas propriedades que os números x_1, y_1 e z_1 possuem. Usando as observações iniciais do Exemplo 3, podemos afirmar que

(1) $\text{mdc}(x_1, y_1) = 1$,

(2) $\text{mdc}(y_1, z_1) = 1$,

(3) $\text{mdc}(z_1, x_1) = 1$,

(4) x_1 e y_1 possuem paridades distintas.

Na verdade, dos resultados do Exemplo 3, teríamos que $\text{mdc}(x_1^2, y_1^2) = \text{mdc}(y_1^2, z_1) = \text{mdc}(z_1, x_1^2) = 1$, mas estas últimas igualdades implicam em (1), (2) e (3), respectivamente. Por exemplo, como $\text{mdc}(x_1^2, y_1^2) = 1$, temos que existem números inteiros $p, q \in \mathbb{Z}$ tais que

$$px_1^2 + qy_1^2 = 1.$$

Mas tal equação ainda pode ser reescrita sob a forma

$$(px_1)x_1 + (qy_1)y_1 = 1,$$

isto é, existe números inteiros $r = px_1$ e $s = qy_1$ tais que

$$rx_1 + sy_1 = 1.$$

Isto quer dizer que $\text{mdc}(x_1, y_1) = 1$. As igualdades (2) e (3) são justificadas analogamente. A justificativa para (4) é ainda simples. Pelo Exemplo 3, teríamos que x_1^2 e y_1^2 possuem paridades distintas, ou seja, um deles é par enquanto o outro é ímpar. Mas isso é o mesmo que provar que se x_1 e y_1 possuem a mesma paridade, então x_1^2 e y_1^2 também possuem e, de fato, isso acontece. Então (4) está justificado.

Feitas essas observações, suponha, sem perda de generalidade, que x_1 é ímpar e y_1 é par. Sendo y_1 par, temos que z_1 deve ser ímpar por causa de (2). Vamos provar agora que

$$\text{mdc}(z_1 - x_1^2, z_1 + x_1^2) = 2. \tag{3.21}$$

Com efeito, se d divide $z_1 - x_1^2$ e $z_1 + x_1^2$, então d divide $(z_1 - x_1^2) + (z_1 + x_1^2) = 2z_1$ e também divide $(z_1 + x_1^2) - (z_1 - x_1^2) = 2x_1^2$. Mas como vale (3) e z_1 é ímpar, segue que $d = 2$ e (3.21) está provado.

Agora, como (x_1, y_1, z_1) é solução de (3.19), segue que $x_1^4 + y_1^4 = z_1^2$ e, então,

$$y_1^4 = z_1^2 - x_1^4.$$

Já que y_1 é um número par, existe $k \in \mathbb{N}$ tal que

$$(z_1 - x_1^2)(z_1 + x_1^2) = y_1^4 = (2k)^4 = 16k^4 = 2 \cdot 8 \cdot k^4.$$

Logo, como vale (3.21), temos que um dos números $(z_1 - x_1^2)$ e $(z_1 + x_1^2)$ é divisível por 2 e *não* por 4, e o outro é divisível por 8.

A seguir, vamos mostrar que

$$y_1 = 2ab, \text{ com } \text{mdc}(a, b) = 1. \tag{3.22}$$

Já vimos que $(z_1 - x_1^2)(z_1 + x_1^2) = y_1^4$ e que um dos números que fazem parte dessa fatoração de y_1^4 é divisível por 2 e não por 4, e o outro é divisível por 8. Denotaremos por s a parcela que é divisível por 2 e não por 4, e por t a parcela que é divisível por 8. Ficamos, então, com a seguite expressão:

$$y_1^4 = s \cdot t. \tag{3.23}$$

Assim, existem inteiros positivos s' e t' tais que

$$s = 2s' \quad \text{e} \quad t = 8t', \text{ com } \text{mdc}(s', t') = 1. \tag{3.24}$$

Para mostrar que vale (3.22), vamos mostrar que existem a e b naturais tais que

$$s' = a^4 \quad \text{e} \quad t' = b^4, \text{ com } \text{mdc}(a, b) = 1. \tag{3.25}$$

As igualdades em (3.25) são provadas da seguinte maneira: mostraremos que se p é um número primo que divide s' (ou seja, vamos supor que o primo p faça parte da fatoração de s'), então p^4 também divide s' (ou seja, p^4 também faz parte da fatoração de s'). Suponha, primeiramente, que $p \neq 2$ seja um primo que divide s'. Como $s = 2s'$ não é divisível por 4, temos que p *não* pode dividir 8 nem 2. Mas p divide s' e, portanto, p *não* pode dividir t', já que s' e t' são primos entre si. Agora, já que p divide s', temos que p também divide y_1^4 por (3.23), o que implica que p divide y_1. Mas se p é um número primo dividindo y_1, temos que p^4 divide y_1^4. Sendo $p \neq 2$ e $p^4 | y_1^4 = 2s' \cdot 8t'$, segue que $p^4 | s' \cdot t'$, já que p não divide 2 nem 8. Só que p *não* divide t' e como $\text{mdc}(s', t') = 1$, temos que p^4 divide s'. O caso em que $p = 2$ *não* pode acontecer, porque como $s = 2s'$ não é divisível por 4, s' *não* pode ser divisível por 2.

O que provamos afinal? Mostramos que qualquer primo que divide s', aparece quatro vezes na fatoração de s' e como podemos fatorar o número s' em fatores de primos, resulta que existe $a \in \mathbb{N}$ tal que

$$s' = a^4.$$

Então, combinando (3.23) e (3.24), teremos que

$$y_1^4 = 2a^4 \cdot 8t' = (2a)^4 \cdot t'$$

o que implica que t' é também uma potência de 4, ou seja, existe $b \in \mathbb{N}$ com $\text{mdc}(a, b) = 1$ tal que $t' = b^4$. Ficamos, então, com

$$y_1^4 = (2a)^4 \cdot b^4,$$

isto é, provamos (3.22). Observando, portanto, (3.24), temos duas situações: ou

$$z_1 - x_1^2 = 2a^4 \quad \text{e} \quad z_1 + x_1^2 = 8b^4, \tag{3.26}$$

ou

$$z_1 - x_1^2 = 8b^4 \quad \text{e} \quad z_1 + x_1^2 = 2a^4, \tag{3.27}$$

com $\text{mdc}(a, b) = 1$ e a é ímpar (podemos supor isso sem perda de generalidade). Suponha que a situação (3.26) acontece. Então fazendo a diferença entre a segunda e primeira equação, obtemos

$$2x_1^2 = 8b^4 - 2a^4.$$

Dividindo esta última equação por 2, ficamos com

$$x_1^2 = 4b^4 - a^4.$$

Logo, $x_1^2 + a^4 = 4b^2$. Isto quer dizer que 4 divide $x_1^2 + a^2$, ou seja, $x_1^2 \equiv -a^4 \pmod 4$. Agora, como x_1 é um número ímpar, temos que

$$x_1 \equiv 1 \pmod 4 \quad \text{ou} \quad x_1 \equiv 3 \equiv -1 \pmod 4.$$

O mesmo acontece para a, já que a também é um número ímpar. Logo,

$$x_1^2 \equiv 1 \pmod 4$$

ou

$$x_1^2 \equiv 3^2 = 9 \equiv 1 \pmod 4.$$

Daí, $x_1 \equiv 1 \pmod 4$ e também $a \equiv 1 \pmod 4$. Assim, ficamos com as seguintes congruências:

$$x_1^2 \equiv 1 \pmod 4, \tag{3.28}$$

$$x_1^2 \equiv -a^4 \pmod 4 \quad \text{e} \quad -a^4 \equiv -1 \pmod 4. \tag{3.29}$$

Usando as propriedades, obtemos de (3.29) que $x_1^2 \equiv -1 \pmod 4$. Assim, como (3.28) é equivalente a $1 \equiv x_1^2 \pmod 4$, temos que $1 \equiv -1 \pmod 4$, pela transitividade da congruência, e isto é um absurdo, já que 4 não divide 2. Portanto, a situação (3.26) *não* pode ocorrer. Portanto, a única situação possível é a (3.27).

Valendo das equações (3.27), obtemos $2a^4 - 8b^4 = 2x_1^2$, que é o mesmo que $a^4 - x_1^2 = 4b^2$. Mostraremos que como $\text{mdc}(a, b) = 1$, temos que $\text{mdc}(a, x_1) = 1$. De fato, seja d um número que divide a e x_1 ao mesmo tempo. Então, d divide a^4 e x_1^2 e, por conseguinte, divide $a^4 - x_1^2 = 4b^4$, ou seja, d divide $4b^4$. Como d divide a e a é um número ímpar, temos que d *não* divide 4 e, portanto, divide b^4. Se d não fosse 1, poderíamos tomar um primo p que dividisse d e, portanto, tal primo dividiria a e b^4, ou seja, este primo dividiria a e b ao mesmo tempo. Isto implica que $p = 1$, o que é uma contradição, já que 1 não é primo. Vamos usar que $\text{mdc}(a, x_1) = 1$ em seguida.

Novamente das equações (3.27), temos que $z_1 = a^4 + 4b^4$, onde $0 < a < z_1$ e

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

Agora, como $\text{mdc}(a, x_1) = 1$, podemos fazer os mesmos cálculos de (3.21), para concluir que

$$\text{mdc}(a^2 - x_1, a^2 + x_1) = 2.$$

Fazendo uso das mesmas ideias que utilizamos para chegar nas situações (3.26) e (3.27), e os argumentos que usamos para mostrar que (3.26) não pode ocorrer, podemos concluir que existem x_2 e y_2 primos entre si tais que $b = x_2y_2$ e

$$\begin{cases} a^2 - x_1 = 2x_2^4, \\ a^2 + x_1 = 2y_2^4. \end{cases}$$

Pondo $a = z_2$ e somando estas duas últimas equações, obtemos que $2z_2^2 = 2x_2^4 + 2y_2^4$, ou seja,

$$x_2^4 + y_2^4 = z_2^2,$$

com $0 < z_2 < z_1$ e isto contradiz a minimalidade de z_1.

Exemplo 7. (Equação de Fermat para $n = 4$) A equação

$$x^4 + y^4 = z^4 \tag{3.30}$$

não possui solução inteira.

Solução: Sabemos, pelo Exemplo 6, que a equação $x^4 + y^4 = z^2$ não possue soluções inteiras. Se (3.30) possui uma solução (x_1, y_1, z_1) é porque este terno satisfaz

$$x_1^4 + y_1^4 = z_1^4 = (z_1^2)^2.$$

Assim, como $z_1 \in \mathbb{Z}$, temos que $z_1^2 \in \mathbb{Z}$. Pondo $z_2 = z_1^2$, temos que existe um terno (x_1, y_1, z_2) tal que

$$x_1^4 + y_1^4 = z_2^2,$$

o que contradiz o Exemplo 6.

Observação: É possível provar que a equação de Fermat $x^3 + y^3 = z^3$ também *não* possui soluções inteiras, mas isto é mais complicado.

3.5 O Último Teorema de Fermat

Nessa seção, contaremos uma pouco da história do Último Teorema de Fermat (confira [10]).

Pierre de Fermat foi um matemático francês do século XVII, que fez muitas descobertas na teoria dos números. O livro grego *Arithmetica* iniciou Fermat nos estudos em Matemática e, neste livro, ele costumava fazer anotações em suas margens. Tais anotações foram perdidas com o passar do tempo, mas ainda podem ser lidas em um livro publicado anos após sua morte por seu filho. Em uma dessas anotações, Fermat escreveu uma pequena observação que deixaria futuros matemáticos curiosos, obcecados e desconfiados: tratava de um dos problemas mais famosos de todos os tempos e ficou conhecido como o *Último Teorema de Fermat*.

Este problema não foi resolvido durante séculos, apesar de seu enunciado ser tão simples que qualquer um pode entender. Por exemplo, podemos nos perguntar quais são as soluções inteiras da equação $x^2 + y^2 = z^2$, como fizemos no Exemplo 3 (vide Figura 3.2). Esta equação nada mais é do que o *Teorema de Pitágoras* que aprendemos quando ainda somos crianças. Rapidamente somos ensinados que, por exemplo, $3^2+4^2 = 5^2$ ou que $5^2+12^2 = 13^2$. Portanto, é natural se questionar, como Fermat o fez, se existem soluções inteiras para as equações $x^3+y^3 = z^3$, $x^4+y^4 = z^4$, $x^5 + y^5 = z^5$ e assim por diante. Mais geralmente, nos perguntamos quais são as soluções inteiras da equação

$$x^n + y^n = z^n \tag{3.31}$$

para qualquer $n \in \mathbb{N}$. Voltando a observação que Fermat havia deixado em seu livro, ele escreveu simplesmente que a equação (3.31) *não* tinha soluções inteiras, para qualquer $n \in \mathbb{N}$. Mais do que isso, ele escreveu que poderia provar tal resultado só que as margens daquele livro eram curtas demais para conter sua demonstração.

Esse não foi o último problema que Fermat deixou para os futuros matemáticos.

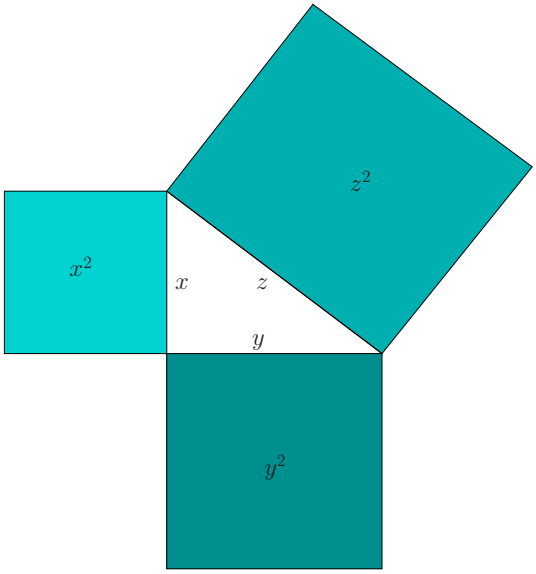

Figura 3.2: Representação geométrica do Teorema de Pitágoras.

Como já mencionado, ele costumava escrever muitas coisas nas margens daquele livro trazendo muitos questionamentos sobre a validade de alguns resultados. Com o passar do tempo, vários matemáticos tomaram tais anotações como desafios e resolveram um por um. O último a ser resolvido foi o problema (3.31) e, por isso, é chamado de *Último* Teorema de Fermat.

Esse problema ficou sem solução por aproximadamente 300 anos e desafiou muitos matemáticos durante todo esse tempo. Por exemplo, Gauss, Galois, Kummer, Euler e Sophie Germain foram importantes nomes que tentaram atacar esse problema e não conseguiram uma solução. Depois de algum tempo, vários matemáticos começaram a duvidar se, de fato, Fermat possuia uma demonstração.

No início dos anos 1970, um novo nome começou a surgir na Matemática. Andrew Wiles começou a estudar Matemática na Universidade de Cambridge sob a orientação do professor John Coates. Segundo ele, Wiles era dono de ideias profundas e que sempre o considerou um matemático que teria grande futuro, mas não acreditava que ele fosse capaz de demonstrar um problema como o Último Teorema

de Fermat. Nessa época, muitos acreditavam que esse problema não poderia ser solucionado, inclusive Coates que incentivou Wiles a não seguir tentando enfrentar este problema. Por isso, Andrew começou a estudar equações elípticas e deixou um pouco de lado o problema de Fermat.

Entretanto, um professor da Universidade de Princeton chamado Goro Shimura, juntamente com seus colegas, continuaram com o sonho de conseguir uma demonstração para o problema de Fermat. Dentro desse grupo havia um jovem chamado Utaka Taniyama. Juntamente com Shimura, Taniyama estudou funções modulares e em 1955, em um congresso, Taniyama enunciou dois problemas em aberto. Um desses problemas ficou conhecida como *Conjectura de Taniyama-Shimura* e tal conjectura, caso estivesse correta, ligava as teorias de formas modulares e curvas elípicas. Infelizmente, em 1958, Taniyama suicidou-se e não pôde ver a grande contribuição do seu trabalho no decorrer dos anos seguintes.

Naquele tempo, ninguém pensava que a conjectura de Taniyama-Shimura teria alguma ligação com o Último Teorema de Fermat até o começo dos anos 1980. Em 1985, Gerhard Frey, um matemático alemão, supos que se há uma solução para a equação (3.31), existe uma curva elíptica que contraria a Conjectura de Taniyama-Shimura. Isto quer dizer que se o problema de Fermat fosse falso, então a Conjectura de Taniyama-Shimura também seria. Dito de outra maneira, se Taniyama-Shimura fosse verdadeiro, então Fermat seria verdadeiro. Essa conjectura de Frey ficou conhecida como *Conjectura Épsilon* e foi Kenneth Ribet quem a provou.

Nesse momento, Andrew abandonou todas as suas pesquisas e começou a trabalhar em cima da Conjectura de Taniyama-Shimura e isso durou sete anos. Nos dois primeiros anos, Andrew não teve progresso algum, tentando arranjar uma estratégia que pudesse dar certo. Apenas depois de 4 anos, em 1991, é que Wiles conseguiu algo para avançar em sua pesquisa. Depois de seis anos de silêncio, ele falou de seu progresso sobre a solução da Conjectura de Taniyama-Shimura para um professor da

Universidade de Princeton chamado Nick Katz. Mais ainda, ele falou que achava que tinha conseguido provar tal conjectura. Andrew decidiu, então, expor suas ideias em conferências das quais Nick poderia assistir e ver se realmente sua demonstração estava correta, e em Maio de 1993 Andrew Wiles acreditava ter provado o Último Teorema de Fermat.

Um dia após Andrews apresentar sua demonstração, todos os jornais ao redor do mundo publicaram que ele tinha provado o Último Teorema de Fermat e logo ficou famoso. Só que depois de algum tempo, Andrew descobriu que havia um erro no final de sua demonstração. Depois disso, Andrew começou a trabalhar neste erro e convidou seu antigo aluno, Richard Taylor, para estudar com ele, mas nada conseguiu até então. Depois de uma grande persistência, Andrew conseguiu consertar seu erro e, de fato, provou um dos principais problemas do século. Portanto, a Conjectura de Taniyama-Shimura foi provada e, portanto, o último Teorema de Fermat.

Capítulo 4

Equações de Pell

Neste capítulo, vamos determinar todas os números inteiros que satisfazem a *equação de Pell*, isto é, equações do segundo grau com duas incógnitas da forma

$$x^2 - Ay^2 = 1,$$

em que A é um número inteiro positivo que não é um quadrado perfeito, isto é, não existe um número inteiro a tal que $A = a^2$.

Para resolver este tipo de equação, devemos primeiramente observar o método de desenvolvimento em frações contínuas de números irracionais, como por exemplo, números irracionais do tipo $\sqrt{A}$. Segundo o Algoritmo de Euclides, qualquer número racional se desenvolve em fração contínua com um número finito de termos, ao contrário dos números irracionais, cujas frações contínuas que os representam são infinitas. Desenvolvamos em fração contínua, por exemplo, o número irracional $\sqrt{2}$.

Note que

$$(\sqrt{2} - 1)(\sqrt{2} + 1) = 2 - 1 = 1$$

e, portanto,

$$\sqrt{2}-1=\frac{1}{\sqrt{2}+1}$$

que pode ser escrito ainda como segue

$$\sqrt{2}-1=\frac{1}{2+(\sqrt{2}-1)}.$$

Assim, tendo em vista a última igualdade acima, temos que:

$$\sqrt{2}-1=\frac{1}{2+(\sqrt{2}-1)}=\frac{1}{2+\dfrac{1}{2+(\sqrt{2}-1)}},$$

ou seja,

$$\sqrt{2}=1+\frac{1}{2+(\sqrt{2}-1)}=1+\frac{1}{2+\dfrac{1}{2+(\sqrt{2}-1)}}.$$

Substituindo novamente o termo entre parênteses, obtemos ainda que

$$\sqrt{2}=1+\frac{1}{2+\dfrac{1}{2+\dfrac{1}{2+(\sqrt{2}-1)}}}.$$

Continuando este procedimento, obteremos o seguinte desenvolvimento para $\sqrt{2}$ em fração contínua:

$$\sqrt{2}=1+\frac{1}{2+\dfrac{1}{2+\dfrac{1}{2+\dfrac{1}{2+\ddots}}}}. \tag{4.1}$$

Observe que o procedimento para o desenvolvimento em fração contínua, aplicado

anteriormente, é baseado na utilização de identidades do tipo

$$(\sqrt{m^2+1}-m)\cdot(\sqrt{m^2+1}+m)=1,$$

que não é válido para quaisquer números irracionais. Este procedimento pode ser usado naqueles casos que o número inteiro A pode se expressar na forma

$$A=m^2+1,$$

em que m é um número inteiro não nulo. Por exemplo, em nosso caso temos que $m=1$, já que

$$\sqrt{2}=\sqrt{1^2+1}=\sqrt{1+1}.$$

O mesmo poderia ser feito para $\sqrt{5}$, já que

$$\sqrt{5}=\sqrt{2^2+1}.$$

A título de curiosidade, para o caso geral, existem procedimentos relativamente simples para o desenvolvimento de um número irracional $\sqrt{A}$ em frações contínuas.

Fazendo o mesmo que fizemos para o caso das frações contínuas finitas, podemos formar uma sequência de frações reduzidas $\delta_1, \delta_2, \delta_3, \ldots$ para a fração contínua infinita (4.1), da seguinte maneira:

$$\delta_1 = 1 \text{ e, portanto, } \delta_1 < \sqrt{2};$$

$$\delta_2 = 1+\frac{1}{2}=\frac{3}{2} \text{ e, portanto, } \delta_2 > \sqrt{2};$$

$$\delta_3 = 1+\frac{1}{2+\dfrac{1}{2}}=\frac{7}{5} \text{ e, portanto, } \delta_3 < \sqrt{2};$$

$$\delta_4 = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2}}} = \frac{17}{12} \text{ e, portanto, } \delta_4 > \sqrt{2};$$

e assim por diante. Tendo em vista o procedimento de formação das frações reduzidas do capítulo anterior, podemos deduzir as seguintes relações:

$$\delta_1 < \delta_3 < \cdots < \delta_{2_k+1} < \ldots < \sqrt{2},$$

$$\delta_2 > \delta_4 > \cdots > \delta_{2k} > \ldots > \sqrt{2}.$$

Em geral, se tomarmos o desenvolvimento em fração contínua infinita de um número irracional α,

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots}},$$

então conseguimos ainda as seguintes desigualdades para as frações reduzidas

$$\delta_1 < \delta_3 < \ldots < \delta_{2k+1} < \ldots < \alpha < \delta_{2k} < \ldots < \delta_4 < \delta_2. \tag{4.2}$$

Da mesma forma que denotamos anteriormente, façamos

$$\delta_k = \frac{P_k}{Q_k},$$

em que

$$\begin{cases} P_k &= P_{k-1}q_k &+ P_{k-2} \\ Q_k &= Q_{k-1}q_k &+ Q_{k-2} \end{cases}$$

são as mesmas obtidas em (2.6), já que em momento algum da dedução destas fórmulas, foi exigida a hipótese de que a fração contínua fosse finita. Consequentemente,

a relação (2.7) continua válida:

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}} \tag{4.3}$$

Por exemplo, note que para as frações reduzidas de $\sqrt{2}$, temos que

$$\delta_3 - \delta_2 = \frac{7}{5} - \frac{3}{2} = \frac{-1}{10} = \frac{-1}{5 \cdot 2}$$

e

$$\delta_4 - \delta_3 = \frac{17}{12} - \frac{7}{5} = \frac{1}{60} = \frac{1}{12 \cdot 5},$$

que coincidem com os resultados obtidos na relação (4.3).

Em particular, utilizando (4.3), temos que

$$\begin{aligned} \delta_{2k} - \delta_{2k+1} &= -(\delta_{2k+1} - \delta_{2k}) \\ &= -\left[\frac{(-1)^{2k+1}}{Q_{2k+1}Q_{2k}}\right] \\ &= -\left[\frac{(-1)^{2k} \cdot (-1)}{Q_{2k+1}Q_{2k}}\right] \\ &= \frac{1}{Q_{2k+1}Q_{2k}}. \end{aligned}$$

Provado isto, vamos mostrar que a seguinte desigualdade é válida:

$$0 < P_{2k} - \alpha Q_{2k} < \frac{1}{Q_{2k+1}}, \tag{4.4}$$

onde $\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots}}$. Com efeito, temos que

$$\alpha < \delta_{2k} = \frac{P_{2k}}{Q_{2k}},$$

ou seja,

$$\alpha Q_{2k} < P_{2k}$$

e, portanto,

$$P_{2k} - \alpha Q_{2k} > 0.$$

Isto prova uma das desigualdades de (4.4). Além disso, sabemos que

$$\delta_{2k+1} < \alpha < \delta_{2k},$$

para cada $k \in \mathbb{N}$, donde $-\delta_{2k+1} > -\alpha$. Logo,

$$\delta_{2k} - \alpha < \delta_{2k} - \delta_{2k+1} = \frac{1}{Q_{2k+1}Q_{2k}}.$$

Mas $\delta_{2k} = \frac{P_{2k}}{Q_{2k}}$ e, portanto,

$$\frac{P_{2k}}{Q_{2k}} - \alpha < \frac{1}{Q_{2k+1}Q_{2k}}.$$

Multiplicando esta última desigualdade por Q_{2k}, obtemos

$$P_{2k} - \alpha Q_{2k} < \frac{1}{Q_{2k+1}},$$

provando assim a outra desigualdade de (4.4).

Vamos aplicar agora os resultados obtidos para resolver a equação

$$x^2 - 2y^2 = 1. \tag{4.5}$$

Podemos escrever o primeiro membro da equação acima como segue

$$x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y).$$

Agora, consideramos que $x = P_{2k}$ e $y = Q_{2k}$, onde P_{2k} e Q_{2k} são, respectivamente, o numerador e o denominador da fração reduzida correspondente do desenvolvimento de $\sqrt{2}$ em fração contínua. Vamos mostrar que, para cada $k \in \mathbb{N}$, $[x = P_{2k}, y = Q_{2k}]$ é solução da equação (4.5).

De fato, podemos escrever

$$P_{2k}^2 - 2Q_{2k}^2 = (P_{2k} - \sqrt{2}Q_{2k})(P_{2k} + \sqrt{2}Q_{2k}) \tag{4.6}$$

Agora, note que o primeiro membro da última igualdade é um número inteiro e, portanto, o segundo membro também o é. Vamos mostrar que o número $P_{2k}^2 - 2Q_{2k}^2$ é maior do que 0 e menor do que 2 e, portanto, terá que ser igual a 1. Com efeito, utilizando a desigualdade (4.4) com $\alpha = \sqrt{2}$, temos

$$0 < P_{2k} - \sqrt{2}Q_{2k} < \frac{1}{Q_{2k+1}} \tag{4.7}$$

Assim, como $P_{2k} + \sqrt{2}Q_{2k} > 0$, temos que o seguno membro de (4.6) é positivo e, portanto,

$$P_{2k}^2 - 2Q_{2k}^2 > 0.$$

Por outro lado, de $P_{2k} - \alpha Q_{2k} < \frac{1}{Q_{2k+1}}$, temos

$$\begin{aligned} P_{2k} - \sqrt{2}Q_{2k} &< \frac{1}{Q_{2k+1}} \\ &= \frac{1}{Q_{2k}q_{2k+1} + Q_{2k-1}} \\ &= \frac{1}{2Q_{2k} + Q_{2k-1}} \\ &< \frac{1}{2Q_{2k}}, \end{aligned}$$

já que $q_{2k+1} = 2$. Mas de (4.2), temos que

$$\delta_{2k} = \frac{P_{2k}}{Q_{2k}} > \sqrt{2}$$

e, portanto,

$$\sqrt{2}Q_{2k} < P_{2k}.$$

Somando P_{2k} em ambos os lados da última desigualdade, tem-se que

$$P_{2k} + \sqrt{2}Q_{2k} < 2P_{2k}.$$

Sendo assim, obtemos as seguintes desigualdades para as expressões que compõe a multiplicação do segundo membro de (4.6):

$$P_{2k} - \sqrt{2}Q_{2k} < \frac{1}{2Q_{2k}},$$

$$P_{2k} + \sqrt{2}Q_{2k} < 2P_{2k}.$$

Multiplicando estas duas desigualdades, obtemos que

$$(P_{2k} - \sqrt{2}Q_{2k}) \cdot (P_{2k} + \sqrt{2}Q_{2k}) < \frac{2P_{2k}}{2Q_{2k}} = \frac{P_{2k}}{Q_{2k}},$$

ou seja,

$$P_{2k}^2 - 2Q_{2k}^2 < \frac{P_{2k}}{Q_{2k}}.$$

Assim, de (4.7), tem-se que

$$\begin{aligned} P_{2k}^2 - 2Q_{2k}^2 &< \frac{P_{2k}}{Q_{2k}} \\ &= \frac{1}{Q_{2k}} \cdot P_{2k} \\ &< \frac{1}{Q_{2k}} \left(\sqrt{2} Q_{2k} + \frac{1}{Q_{2k+1}} \right) \\ &= \sqrt{2} + \frac{1}{Q_{2k} Q_{2k+1}} \end{aligned}$$

e como $k \geq 1$,

$$\frac{1}{Q_{2k} Q_{2k+1}} \leq \frac{1}{Q_2 Q_3} = \frac{1}{2 \cdot 5} = \frac{1}{10}.$$

Portanto,

$$\begin{aligned} P_{2k}^2 - 2Q_{2k}^2 &< \sqrt{2} + \frac{1}{Q_{2k} Q_{2k+1}} \\ &< \sqrt{2} + \frac{1}{10} \\ &< 2. \end{aligned}$$

Sendo assim, temos que

$$0 < P_{2k}^2 - 2Q_{2k}^2 < 2,$$

ou seja,

$$P_{2k}^2 - 2Q_{2k}^2 = 1.$$

Portanto, $[P_{2k}, Q_{2k}]$ são as soluções da equação $x^2 - 2y^2 = 1$, para cada $k \geq 1$. Entretanto, não sabemos se tais soluções são todas as soluções possíveis desta equação.

Naturalmente, surge a pergunta de como obter todas as soluções inteiras da equação

$$x^2 - Ay^2 = 1 \Leftrightarrow x + \sqrt{A}y = \frac{1}{x - \sqrt{A}y}, \tag{4.8}$$

em que A é um número inteiro positivo e $\sqrt{A}$ é um número irracional. Para encontrar todas essas soluções, devemos conhecer pelo menos uma solução particular. De acordo com o que fizemos para a equação (4.5), podemos concluir que equações dessa natureza possuem, de fato, soluções. A partir de agora, vamos estudar o problema de obter todas as soluções inteiras de (4.8) sendo conhecida uma determinada solução. Não vamos nos preocupar aqui se a equação (4.8) possui, pelo menos, uma solução inteira diferente da trivial $x = 1$ e $y = 0$. Assumiremos que isto sempre ocorre.

Suponha que a equação (4.8) possui uma solução não trivial $[x_0, y_0]$ com $x_0 > 0$, $y_0 > 0$ e

$$x_0^2 - Ay_0^2 = 1. \tag{4.9}$$

Diremos que a solução $[x_0, y_0]$ é **mínima** se, pondo $x = x_0$ e $y = y_0$, o número $x + \sqrt{A}y$ é o menor valor possível entre todos os seus valores ao substituir x e y por todas as possíveis soluções positivas não nulas da equação (4.8). Por exemplo, a solução mínima da equação (4.5) é $[x_0 = 3, y_0 = 2]$, já que a equação não possui soluções inteiras positivas menores do que essa, como é fácil de comprovar ao substituirmos os números inteiros positivos menores do que 3 e 2. Na verdade, a solução mais próxima desta equação é quando $x = 17$ e $y = 12$, mas **não** temos que

$$17 + 12\sqrt{2} < 3 + 2\sqrt{2}.$$

Vamos provar agora que uma solução mínima da equação (4.8) tem que ser única. De fato, suponha que existem duas soluções mínimas $[x_1, y_1]$ e $[x_2, y_2]$ que dão um

mesmo valor ao número $x + \sqrt{A}y$. Logo,

$$x_1 + \sqrt{A}y_1 = x_2 + \sqrt{A}y_2. \tag{4.10}$$

Daí,

$$x_1 - x_2 = (y_2 - y_1)\sqrt{A}.$$

Mas $\sqrt{A}$ é um número irracional, enquanto que x_1, x_2, y_1 e y_2 são números inteiros. Isto é um absurdo, pois $(y_2 - y_1)\sqrt{A} \notin \mathbb{Q}$ e $x_1 - x_2 \in \mathbb{Q}$. Esta contradição nos dá que $x_1 = x_2$ e $y_1 = y_2$. Portanto, a solução mínima é única.

Provemos uma outra propriedade muito importante das soluções da equação (4.8). Seja $[x_1, y_1]$ uma dessas soluções. Então

$$x_1^2 - Ay_1^2 = 1,$$

ou ainda,

$$(x_1 + \sqrt{A}y_1)(x_1 - \sqrt{A}y_1) = 1. \tag{4.11}$$

Elevemos os dois membros da equação (4.11) ao número $n \in \mathbb{N}$. Ficamos com a seguinte expressão:

$$(x_1 + \sqrt{A}y_1)^n(x_1 - \sqrt{A}y_1)^n = 1.$$

Pela fórmula do binômio de Newton, obtemos

$$\begin{aligned} (x_1 + \sqrt{A}y_1)^n &= x_1^n + nx_1^{n-1}\sqrt{A}y_1 + \frac{n(n-1)}{2}x_1^{n-2}Ay_1^2 + \cdots + (\sqrt{A})^n y_1^n \\ &:= x_n + \sqrt{A}y_n. \end{aligned} \tag{4.12}$$

pois $(\sqrt{A})^n$ é igual a A^k se $n = 2k$ e $(\sqrt{A})^n$ é igual a $A^k\sqrt{A}$ se $n = 2k + 1$. Vamos

mostrar que os números x_n e y_n também satisfazem a equação (4.8). Com efeito, da igualdade (4.13) podemos trocar o sinal de $\sqrt{A}$ e obter que

$$(x_1 - \sqrt{A}y_1)^n = x_n - \sqrt{A}y_n.$$

Daí,

$$\begin{aligned} 1 &= (x_1 + \sqrt{A}y_1)^n(x_1 - \sqrt{A}y_1)^n \\ &= (x_n + \sqrt{A}y_n)(x_n - \sqrt{A}y_n) \\ &= x_n^2 - Ay_n^2, \end{aligned}$$

ou seja, $[x_n, y_n]$ é uma solução da equação (4.8). Finalmente, podemos demonstrar o seguinte teorema que, além de encerrar este capítulo, nos dá todas as soluções da equação (4.8), desde que saibamos qual é a solução mínima desta equação.

Teorema 5. Qualquer solução de (4.8) é da forma:

$$\begin{cases} x_n = \dfrac{1}{2}[(x_0 + y_0\sqrt{A})^n + (x_0 - y_0\sqrt{A})^n] \\ \\ y_n = \dfrac{1}{2\sqrt{A}}[(x_0 + y_0\sqrt{A})^n - (x_0 - y_0\sqrt{A})^n] \end{cases} \tag{4.13}$$

onde $[x_0, y_0]$ é solução mínima.

Demonstração. Suponha, por absurso, que existe uma solução inteira $[x', y']$ da equação (4.8) tal que a igualdade

$$x' + \sqrt{A}y' = (x_0 + \sqrt{A}y_0)^n \tag{4.14}$$

não seja verdadeira para nenhum número natural n. Veja que, pelo que fizemos

anteriormente, se $[x_0, y_0]$ é uma solução de (4.8), então deveremos ter

$$(x_0 + \sqrt{A}y_0)^n = x_n + \sqrt{A}y_n.$$

Dizer que a solução $[x', y']$ não satisfaz a igualdade (4.14), é dizer que ela não é da forma (4.13). Chegando a um absurdo, teremos provado que (4.13) nos dá todas as soluções da equação (4.8).

Note primeiramente que a sequência

$$x_0 + \sqrt{A}y_0, (x_0 + \sqrt{A}y_0)^2, (x_0 + \sqrt{A}y_0)^3, \ldots$$

cresce ilimitadamente, já que $x_0, y_0 \geq 1$ e $x_0 + \sqrt{A}y_0 > 1$. Como $[x_0, y_0]$ é a solução mínima de (4.8), se $[x', y']$ for uma outra solução, temos, por definição, que

$$x' + \sqrt{A}y' > x_0 + \sqrt{A}y_0.$$

Portanto, é possível encontrar um número natural $n \geq 1$ tal que

$$(x_0 + \sqrt{A}y_0)^n < x' + \sqrt{A}y' < (x_0 + \sqrt{A}y_0)^{n+1}. \tag{4.15}$$

Agora, observe que

$$(x_0 + \sqrt{A}y_0)(x_0 - \sqrt{A}y_0) = x_0^2 - Ay_0^2 = 1 > 0,$$

ou seja, $x_0 - \sqrt{A}y_0 > 0$, já que $x_0 + \sqrt{A}y_0 > 0$. Logo, $(x_0 - \sqrt{A}y_0)^n > 0$ e, então,

multiplicando este fator em (4.15), as desigualdades não se alteram e ficamos com:

$$\begin{aligned}(x_0+\sqrt{A}y_0)^n(x_0-\sqrt{A}y_0)^n &< (x'+\sqrt{A}y')(x_0-\sqrt{A}y_0)^n \\ &< (x_0+\sqrt{A}y_0)^{n+1}(x_0-\sqrt{A}y_0)^n. \qquad (4.16)\end{aligned}$$

Agora, como

$$\begin{aligned}(x_0+\sqrt{A}y_0)^n(x_0-\sqrt{A}y_0)^n &= [(x_0+\sqrt{A}y_0)(x_0-\sqrt{A}y_0)]^n \\ &= (x_0^2-Ay_0^2)^n \\ &= 1^n \\ &= 1\end{aligned}$$

então,

$$\begin{aligned}(x_0+\sqrt{A}y_0)^{n+1}(x_0-\sqrt{A}y_0)^n &= (x_0+\sqrt{A}y_0)[(x_0+\sqrt{A}y_0)^n(x_0-\sqrt{A}y_0)^n] \\ &= x_0+\sqrt{A}y_0.\end{aligned}$$

Além disso,

$$\begin{aligned}(x'+\sqrt{A}y')(x_0-\sqrt{A}y_0)^n &= (x'+\sqrt{A}y')(x_n-\sqrt{A}y_n) \\ &= x'x_n-x'\sqrt{A}y_n+\sqrt{A}y'x_n-Ay'y_n \\ &= x'x_n-Ay'y_n+\sqrt{A}(y'x_n-x'y_n) \\ &:= \overline{x}+\sqrt{A}\overline{y},\end{aligned}$$

onde $\overline{x}$ e $\overline{y}$ são números inteiros. Com isso, a desigualdade (4.16) torna-se a seguinte:

$$1<\overline{x}+\sqrt{A}\overline{y}<x_0+\sqrt{A}y_0 \qquad (4.17)$$

Vamos demonstrar que $[\overline{x}, \overline{y}]$ é solução da equação (4.8) e assim chegar numa contradição, visto que $[x_0, y_0]$ é a solução mínima da equação. Com efeito, temos a igualdade

$$\overline{x} + \sqrt{A}\overline{y} = (x' + \sqrt{A}y')(x_0 - \sqrt{A}y_0)^n.$$

Trocando o sinal de $\sqrt{A}$, temos ainda que

$$\overline{x} - \sqrt{A}\overline{y} = (x' - \sqrt{A}y')(x_0 + \sqrt{A}y_0)^n.$$

Então

$$(\overline{x} + \sqrt{A}\overline{y})(\overline{x} - \sqrt{A}\overline{y}) = \overline{x}^2 - A\overline{y}^2.$$

Mas

$$\begin{aligned}
(\overline{x} + \sqrt{A}\overline{y})(\overline{x} - \sqrt{A}\overline{y}) &= (x' + \sqrt{A}y')(x_0 - \sqrt{A}y_0)^n(x' - \sqrt{A}y')(x_0 + \sqrt{A}y_0)^n \\
&= (x' + \sqrt{A}y')(x' - \sqrt{A}y')(x_0 + \sqrt{A}y_0)^n(x_0 - \sqrt{A}y_0)^n \\
&= ((x')^2 - A(y')^2)(x_0^2 - Ay_0^2)^n \\
&= 1,
\end{aligned}$$

já que $[x', y']$ e $[x_0, y_0]$ são soluções de (4.8).

Finalmente, vamos provar $\overline{x} > 0$ e que $\overline{y} > 0$. De fato, note que se $\overline{x} = 0$, então a igualdade

$$(\overline{x} + \sqrt{A}\overline{y})(\overline{x} - \sqrt{A}\overline{y}) = 1$$

torna-se

$$-A\overline{y}^2 = 1,$$

o qual não pode acontecer pois desde o início estamos supondo $A > 0$. Por outro lado, se $\overline{y} = 0$, então $\overline{x}^2 = 1$, que também não é possível acontecer, pois da desi-

gualdade (4.17), temos que $\overline{x} > 1$. Observemos ainda que $\overline{x}$ e $\overline{y}$ possuem o mesmo sinal. Com efeito, supondo que os sinais de $\overline{x}$ e $\overline{y}$ são diferentes, então $\overline{x}$ e $-\overline{y}$ têm o mesmo sinal. Comparando os valores absolutos das expressões $\overline{x} + \sqrt{A}\overline{y}$ e $\overline{x} - \sqrt{A}\overline{y} = \overline{x} + \sqrt{A}(-\overline{y})$, resulta que o valor absoluto da primeira expressão é menor do que o valor absoluto da segunda, já que na primeira $\overline{x}$ e $\overline{y}$ têm sinais trocados enquanto que na segunda, eles possuem o mesmo sinal, lembrando que $\sqrt{A} > 0$. Mas de (4.17), sabemos que

$$\overline{x} + \sqrt{A}\overline{y} > 1$$

e, portanto, $\overline{x} - \sqrt{A}\overline{y}$ também é maior do que 1, em valor absoluto. Mas

$$(\overline{x} + \sqrt{A}\overline{y})(\overline{x} - \sqrt{A}\overline{y}) = 1,$$

o que é um absurdo, pois a multiplicação de dois números maiores do que 1, é maior do que 1. Portanto, os sinais de $\overline{x}$ e $\overline{y}$ devem ser iguais e eles são não nulos. Assim, novamente da desigualdade (4.17), se deduz que ambos $\overline{x}$ e $\overline{y}$ são estritamente positivos.

Portanto, supondo que existe uma solução $[x', y']$ da equação (4.8) tal que a igualdade (4.14) não se estabeleça para nenhum valor natural de n, conseguimos determinar uma solução $[\overline{x}, \overline{y}]$ desta equação, onde $\overline{x}$ e $\overline{y}$ são números inteiros positivos e que satisfazem a desigualdade (4.17). Isto é um absurdo, pois contradiz a definção $[x_0, y_0]$ ser a solução mínima de (4.8). Com isso, supondo que existe uma solução que não satisfaz a igualdade (4.14), chegamos a uma contradição. Dito de outro modo, demonstramos que todas as soluções da equação (4.8) podem ser obtidas através da fórmula (4.14), isto é, qualquer solução $[x, y]$ desta equação se obtém através da igualdade

$$x + \sqrt{A}y = (x_0 + \sqrt{A}y_0)^n, \tag{4.18}$$

com $n \geq 0$, onde $[x_0, y_0]$ é a solução mínima de (4.8). Trocando o sinal de $\sqrt{A}$ na igualdade (4.18), obtemos que

$$x - \sqrt{A}y = (x_0 - \sqrt{A}y_0)^n, \tag{4.19}$$

Somando e substraindo as expressões (4.18) e (4.19), obtemos (4.13) com $x = x_n$ e $y = y_n$, que são fórmulas explícitas para a determinação das soluções $[x, y]$ da equação (4.8), onde x e y são números inteiros positivos. □

Exemplo 8. Na equação

$$x^2 - 2y^2 = 1,$$

temos que a solução mínima é $[3, 2]$. Portanto, todas as soluções desta equação são dadas pela fórmula

$$\begin{cases} x_n = \dfrac{1}{2}[(3+2\sqrt{2})^n + (3-2\sqrt{2})^n] \\ \\ y_n = \dfrac{1}{2\sqrt{2}}[(3+2\sqrt{2})^n - (3-2\sqrt{2})^n] \end{cases}$$

Quando $n = 2, 3$, por exemplo, tem-se que $[17, 12]$ e $[99, 70]$ são soluções inteiras da equação dada, como se pode verificar sem muitas dificuldades.

Referências Bibliográficas

[1] Alencar F., E. *Teoria Elementar dos Números* - 3 ed, Editora Nobel, São Paulo, 1992.

[2] Andreescu, T., Andrica, D., Cucurezeanu, I. *An Introduction to Diophantine Equations. A Problem-Based Approach*, Springer, 2010.

[3] Guelfond, A. O. *Resolución de Ecuaciones en Números Enteros*, Editorial MIR, Moscú, 1979.

[4] Hefez, A. *Elementos da Aritmética*, Rio de Janeiro, SBM, 2006.

[5] Martinez, F. B. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro* Rio de Janeiro, IMPA, 2010.

[6] Oliveira, K. I. M. e Fernández, A. J. C. *Iniciação à Matemática: um curso com problemas e soluções*, Rio de Janeiro, SBM, 2010.

[7] Santos, J. P. de O. *Introdução à Teoria dos Números*, Coleção Matemática Universitária, Rio de Janeiro, 1998.

[8] Shokranian, S. *Uma Introdução à Teoria dos Números*, Ciência Moderna, Rio de Janeiro, 2008.

[9] Silverman, J. H., Tate, J. *Rational Points on Elliptic Curves*, Springer, 1992.

[10] Singh, S. *O Último Teorema de Fermat*, Editora Record, São Paulo, 1998.