Aritmética no estudo de retas e cônicas

Thais Ester Gonçalves thais.ester@aluno.ufop.edu.br
Universidade Federal de Ouro Preto, Ouro Preto, MG, Brazil

Geraldo César Gonçalves Ferreira geraldocesar@ufop.edu.br
Universidade Federal de Ouro Preto, Ouro Preto, MG, Brazil

Resumo

Neste trabalho aritmética e geometria são vistas em um único foco, através dos resultados obtidos por Fermat, Diofanto, Euclides, entre outros matemáticos. Nesta ligação entre a Aritmética e a Geometria, buscaremos soluções inteiras ou racionais de equações polinomiais de duas variáveis, de grau um ou dois, com coeficientes inteiros, o que neste caso é equivalente a encontrarmos pontos de coordenadas inteiras ou racionais em retas e cônicas. Como aplicação exibiremos todos os números inteiros que podem ser escritos como soma de dois quadrados e demonstraremos o último Teorema de Fermat para o caso em que $n = 3$.

Palavras-chave

Aritmética, Geometria, Fermat.

1 Introdução

A aritmética e a geometria se fazem presentes em todo momento do nosso cotidiano e são utilizadas desde os primórdios, sendo consideradas as áreas mais antigas da matemática. Para os pitagóricos, segundo Pinedo e Pinedo apud [11], um ponto era chamado de um, uma reta de dois, uma superfície de três e um sólido, de quatro. Assim, "os pontos geravam retas, que geravam superfícies, que geravam sólidos, que formavam o universo". Neste trabalho, buscamos estudar a aritmética e a geometria em um único foco através dos resultados obtidos por Fermat, Diofanto, Euclides, entre outros matemáticos. Iniciamos estudando existência de pontos de $\mathbb{Z} \times \mathbb{Z}$ em retas no plano cartesiano $\mathbb{R} \times \mathbb{R}$, o algoritmo de Euclides e equações diofantinas lineares. Na segunda seção, introduzimos a aritmética em cônicas estudando, basicamente, o Método das Secantes e Tangentes de Fermat, cuja bibliografia principal é dada por [7]. Por fim, na terceira seção, buscamos números inteiros que podem ser escritos como soma de dois quadrados, introduzindo o descenso infinito de Fermat, enunciando e demonstrando o último teorema de Fermat no caso em que $n = 3$.

2 Aritmética em retas

A aritmética juntamente com a geometria são os ramos mais antigos da matemática. A aritmética em retas, também conhecida como aritmética linear, estuda equações e inequações com coeficientes inteiros em busca de soluções inteiras. Nesta seção, buscaremos soluções para equações do tipo $bx + cy = a$, que são denominadas diofantinas (homenagem ao matemático Diofanto). Essas equações serão vistas como retas no plano, sendo cada solução representada por um ponto. Para essa seção, usaremos [7] como principal referência.

2.1 Pontos inteiros em retas e o algoritmo de Euclides

Iniciaremos obtendo uma condição necessária e suficiente para a existência de pontos de $\mathbb{Z}^2$ em uma reta no plano $\mathbb{R}^2$.

Proposição 2.1. *Seja $l = \{(x, y) \in \mathbb{R}^2 | bx + cy = a\}$ uma reta com coeficientes inteiros a, b e c. Suponha que a reta possua um ponto inteiro $(x_0, y_0) \in \mathbb{Z}^2$. Seja $w = (-\gamma, \beta)$ o vetor diretor inteiro e irredutível da reta l, então todos os pontos inteiros da reta são $(x_k, y_k) = (x_0 + k\gamma, y_0 - k\beta)$, $k \in \mathbb{Z}$.*

Demonstração. Primeiramente, demonstraremos que estes pontos são pontos inteiros da reta, substituindo-os na equação de l. Sabemos que, a menos de sinal, $w = \frac{1}{d}v$, sendo $v = (c, -b)$ e $d = \text{mdc}(b, c)$ (w é o vetor diretor irredutível da reta l). Então:

$$\begin{aligned} bx + cy &= bx_k + cy_k \\ &= b(x_0 + k\gamma) + c(y_0 - k\beta) \\ &= bx_0 + bk\gamma + cy_0 - ck\beta \\ &= bx_0 + bk\left(\frac{-c}{d}\right) + cy_0 - ck\left(\frac{-b}{d}\right) \\ &= bx_0 + cy_0 \end{aligned}$$

Como $(x_0, y_0) \in l$, temos que $bx_0 + cy_0 = a$. Portanto, está demonstrado que estes pontos são pontos inteiros da reta.

Agora, vamos demonstrar que esses pontos são todos os pontos inteiros da reta.

Suponhamos que exista um outro ponto inteiro $Q = (x', y') \in l$. Digamos que este ponto Q está entre dois pontos inteiros P_k e P_{k+1} pertencentes à l. Estes pontos são colineares e originam dois triângulos retângulos semelhantes que possuem hipotenusa sobre l e catetos nas direções horizontal e vertical, como na figura 1:

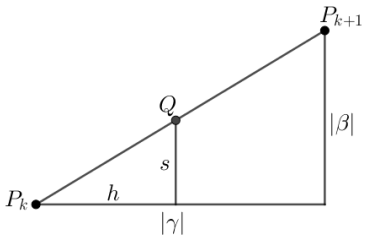

Figura 1: Triângulos retângulos semelhantes

Sejam h e s medidas dos catetos do triângulo menor, horizontal e vertical, respectivamente, e $|\gamma|$ e $|\beta|$ medidas dos catetos do triângulo maior, horizontal e vertical respectivamente. Dessa forma, temos que $h < |\gamma|$ e $s < |\beta|$. Além disso, pela proporcionalidade, temos que

$$\frac{h}{s} = \frac{|\gamma|}{|\beta|}$$

e isto é um absurdo, pois $h, s, |\gamma|$ e $|\beta|$ são números inteiros (pois os pontos P_k, P_{k+1} e Q são inteiros) e, por hipótese, mdc$(\gamma, \beta) = 1$, ou seja, a fração $\dfrac{|\gamma|}{|\beta|}$ é irredutível.

Portanto, todos os pontos inteiros da reta são $(x_k, y_k) = (x_0 + k\gamma, y_0 - k\beta)$, $k \in \mathbb{Z}$. □

Dados dois números inteiros a e b, como usual, usaremos a notação $a|b$ para dizermos que b é divisível por a. Estudaremos o algoritmo de Euclides para o cálculo do mdc de dois números inteiros.

Lema 2.1. *Sejam b, c e d números inteiros. Se $d|b$ e $d|c$, então para todo número inteiro k temos que $d|(b - kc)$. Além disso, $mdc(b, c) = mdc(c, b - kc)$.*

Demonstração. Sejam b, c e d números inteiros tais que $d|b$ e $d|c$. Assim, podemos

escrever $b = dq_1$ e $c = dq_2$ com $q_1, q_2 \in \mathbb{Z}$. A diferença desses números é:

$$b - c = dq_1 - dq_2 = d(q_1 - q_2), \quad q_1, q_2 \in \mathbb{Z}$$

Note que se $d|c$ então $d|kc$ para todo $k \in \mathbb{Z}$:

$$kc = kdq_2, \quad kdq_2 \in \mathbb{Z}$$

Daí, como $d|b$, então d divide a diferença $(b - kc)$.
Agora, se $d|c$ e $d|(b - kc)$, então d divide a soma $(b - kc) + (kc) = b$, ou seja, $d|b$ e $d|c$. Concluímos, então, que $mdc(b, c) = mdc(c, b - kc)$. □

Teorema 2.1 (Algoritmo de Euclides)**.** *Sejam $b > c > 0$ dois números inteiros. Se $c|b$ então $(b, c) = c$, caso contrário:*

$$\textit{mdc}(b, c) = \textit{mdc}(c, r_1) = \textit{mdc}(r_1, r_2) = ... = \textit{mdc}(r_{n-1}, r_n) = \textit{mdc}(r_n, 0) = r_n,$$

onde

$$\begin{gathered} b = cq_1 + r_1, \ \ 0 \leq r_1 < c \\ c = r_1q_2 + r_2, \ \ 0 \leq r_2 < r_1 \\ r_1 = r_2q_3 + r_3, \ \ 0 \leq r_3 < r_2 \\ \vdots \\ r_{n-2} = r_{n-1}q_n + r_n, \ \ 0 \leq r_n < r_{n-1} \end{gathered}$$

com r_n sendo o último resto não nulo e $q_i \in \mathbb{Z}$ para todo $i \in \mathbb{N}$.

Demonstração. Consideremos $b > c > 0$. Se $c|b$, então c é o maior divisor natural de b e c, consequentemente $\text{mdc}(b, c) = c$.

Suponhamos então que $c \nmid b$, pela divisão euclidiana de b por c sabemos que existem um quociente $q_1 \in \mathbb{Z}$ e um resto $r_1 \in \mathbb{N}$ tais que:

$$b = cq_1 + r_1 \Rightarrow r_1 = b - cq_1 \ , \ \ 0 \leq r_1 < c.$$

Assim, temos duas possibilidades:
1) $r_1|c$, e, neste caso, pelo Lema 2.1,

$$r_1 = \text{mdc}(c, r_1) = \text{mdc}(c, b - cq_1) = \text{mdc}(c, b)$$

e termina o algoritmo.
2) $r_1 \nmid c$, e, neste caso, podemos efetuar a divisão de c por r_1, obtendo

$$c = q_2 r_1 + r_2 \Rightarrow r_2 = c - q_2 r_1\ ,\ \ 0 < r_2 < r_1.$$

Novamente, temos duas possibilidades:
1) $r_2 | r_1$, e, neste caso, pelo Lema 2.1,

$$r_2 = \text{mdc}(r_1, r_2) = \text{mdc}(r_1, c - q_2 r_1) = \text{mdc}(r_1, c) = \text{mdc}(b - cq_1, c) = \text{mdc}(b, c)$$

e termina o algoritmo.
2) $r_2 \nmid r_1$, e, neste caso, podemos efetuar a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 q_3 + r_3 \Rightarrow r_3 = r_1 - r_2 q_3\ ,\ \ 0 < r_3 < r_2.$$

Esse procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais $c > r_1 > r_2 > ...$ que não possui menor elemento, o que não é possível pelo Princípio da Boa Ordenação.
Portanto, para algum $n \in \mathbb{N}$, temos que $r_n | r_{n-1}$, o que implica que $mdc(b, c) = r_n$. □

2.2 Algoritmo de Euclides de maneira prática:

Uma maneira prática para o cálculo do mdc(b, c) utilizando o Teorema 2.1 é feita em [8]. O método consiste em dividir b por c encontrando um quociente q_1 e um resto r_1. Em seguida organizamos estes números em um diagrama:

	q_1	
b	c	
	r_1	

Feito isto, repetimos r_1 ao lado de c e dividimos c por r_1 resultando em um quociente q_2 e um resto r_2. Novamente, escrevemos r_2 ao lado de r_1 e dividimos r_1 por r_2 obtendo um quociente q_3 e um resto r_3. Repetimos este processo enquanto for possível e organizamos todos os números no diagrama, como segue:

	q_1	q_2	...	q_n	q_{n+1}
b	c	r_1	...	r_{n-1}	$r_n = mdc(b,c)$
	r_1	r_2	...	r_n	

Lema 2.2 (Algoritmo Estendido de Euclides - Lema de Bèzout)**.** *Sejam b e c números inteiros, $b > c > 0$, e seja $d = mdc(b, c)$. Então existem números inteiros x e y tais que $bx + cy = d$. Além disso, os inteiros x e y podem ser efetivamente calculados a partir de um algoritmo finito.*

Demonstração. Como no Teorema 2.1 considere $r_1, r_2 \cdots, r_n$ dados por

$$b = cq_1 + r_1, \;\; 0 \leq r_1 < b$$

$$c = r_1q_2 + r_2, \;\; 0 \leq r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, \;\; 0 \leq r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \;\; 0 \leq r_n < r_{n-1}$$

onde $r_n = d$ é o o último resto não nulo. A última igualdade pode ser reescrita como:

$$r_n = r_{n-2} - r_{n-1}q_n \tag{1}$$

Além disso, ao dividirmos r_{n-3} por r_{n-2}, obtemos um quociente q_{n-1} e um resto r_{n-1}, podendo também rescrever da seguinte forma:

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \Rightarrow r_{n-1} = r_{n-3} - r_{n-2}q_{n-1} \tag{2}$$

Substituindo 2 em 1, temos:

$$r_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = (q_{n-1}q_n + 1)r_{n-2} - r_{n-3}q_n$$

Nomeamos $x_{n-2} = q_{n-1}q_n + 1$ e $y_{n-2} = -q_n$. Temos que $x_{n-2}, y_{n-2} \in \mathbb{Z}$ e

$$r_n = x_{n-2}r_{n-2} + y_{n-2}r_{n-3}. \tag{3}$$

Repetindo este processo um número finito de vezes, veremos que existem $x_1, y_1 \in \mathbb{Z}$ tais que

$$d = r_n = x_1r_2 + y_1r_1 \tag{4}$$

Contudo $r_1 = b - cq_1$ e $r_2 = c - r_1q_2$. Substituindo r_1 e r_2 em 4:

$$r_n = x_1(c-r_1q_2)+y_1(b-cq_1) = x_1(c-(b-cq_1)q_2)+y_1(b-cq_1) = b(y_1-x_1q_2)+c(x_1+x_1q_1q_2-y_1q_1)$$

Denotando $x = (y_1 - x_1q_2)$ e $y = (x_1 + x_1q_1q_2 - y_1q_1)$, temos que $x, y \in \mathbb{Z}$ e

$$bx + cy = r_n = d.$$

□

2.3 Equações diofantinas lineares de duas variáveis

Uma equação diofantina linear de duas variáveis é uma equação do tipo $bx + cy = a$ tal que a, b e $c \in \mathbb{Z}$ com b, c não nulos. Esta equação recebe este nome em homenagem ao matemático Diofanto e, para estudá-las, usaremos [4] e [10] como referências.

Vejamos, como motivação, dois exemplos de problemas que envolvem a equação diofantina:

Exemplo 2.1. *Uma costureira possui* 63 *metros de tecido e deseja cortá-lo em tiras de 2 ou 4 metros de forma que não sobre nenhum retalho. De quantas maneiras a costureira consegue cortar este tecido?*

Resolver este problema é o mesmo que resolver a equação diofantina $2x+4y = 63$. Neste exemplo é fácil perceber que a equação não possui solução inteira, uma vez que temos soma de pares resultando em um número ímpar. Mas, no geral, quando uma equação desse tipo terá soluções?

Exemplo 2.2. *Uma pessoa possui* $R\$\ 60,00$ *deseja comprar maçãs e laranjas,*

sendo que cada maçã custa $R\$\ 3,00$ *e cada laranja custa* $R\$\ 5,00$. *Quantas dessas frutas ela pode comprar gastando todo o dinheiro?*

Resolver este problema é buscar soluções inteiras para a equação $3x+5y = 60$. Uma solução para este problema é $x = 10$ e $y = 6$, ou seja, comprar 10 maçãs e 6 laranjas. Mas há outras soluções? Como encontrá-las?

Ao estudar uma equação diofantina linear de duas variáveis, buscamos saber se ela possui soluções inteiras e, em caso positivo, encontrar todas as soluções.

Teorema 2.2. *Sejam* $a, b, c \in \mathbb{Z}$ *e* $d =$*mdc*(b, c) *com* b, c *não nulos. A equação diofantina* $bx + cy = a$ *possui solução inteira se, e somente se,* $d|a$*, e neste caso todas as soluções são da forma* $x = x_0 - \frac{c}{d}k$ *e* $y = y_0 + \frac{b}{d}k$*, com* $k \in \mathbb{Z}$*, sendo* (x_0, y_0) *uma solução particular.*

Demonstração. Sejam x_0 e y_0 soluções da equação, ou seja,

$$bx_0 + cy_0 = a$$

Seja $d = \text{mdc}(b, c)$. Como $d|b$ e $d|c$, podemos escrever $b = q_1 d$ e $c = q_2 d$, com $q_1, q_2 \in \mathbb{Z}$. Substituindo b e c na equação acima, temos:

$$q_1 dx_0 + q_2 dy_0 = a \Rightarrow d(q_1 x_0 + q_2 y_0) = a$$

com $q_1 x_0 + q_2 y_0 \in \mathbb{Z}$ donde $d = mdc(b, c)|a$.

Reciprocamente seja $d = \text{mdc}(b, c)$ e $k \in \mathbb{Z}$ tal que $a = kd$. Pelo Lema 2.2, existem números inteiros x e y tais que

$$d = bx + cy.$$

Multipliquemos essa equação por k:

$$dk = bxk + cyk.$$

Logo $a = b(xk) + c(yk)$ e (xk, yk) é uma solução da equação. A afirmação que

todas as soluções são da forma $x = x_0 - \frac{c}{d}k$ e $y = y_0 + \frac{b}{d}k$, sendo (x_0, y_0) uma solução particular segue da Proposição 2.1. □

Corolário 2.1. *Se b e c são coprimos, ou seja, mdc$(b, c) = 1$, então a equação $bx + cy = a$ possui soluções inteiras, para todo número inteiro a.*

Demonstração. Pelo Lema 2.2 existem inteiros x_0 e y_0 tais que:

$$bx_0 + cy_0 = 1$$

Consequentemente $\tilde{x_0} = ax_0$ e $\tilde{y_0} = ay_0$ satisfazem a equação $bx + cy = a$. □

Observação 2.1. *Se equação $bx + cy = 1$ possui soluções inteiras, então mdc$(b, c) = 1$. Com efeito, seja $d =$ mdc(b, c). Como $d|b$, $d|c$ então, $d|(bx + cy)$. Ainda como $bx + cy = 1$, segue que $d|1$ e como $d > 0$ temos que $d = 1$.*

Teorema 2.3. *Seja (x_0, y_0) uma solução particular da equação $bx + cy = a$ com mdc$(b, c) = 1$. Então essa equação possui infinitas soluções e todas são da forma $(x_0 + ck, y_0 - bk), k \in \mathbb{Z}$.*

Demonstração. Segue diretamente do Teorema 2.2. □

Exemplo 2.3. *Encontre o conjunto solução da equação $162x + 48y = 6$.*

Inicialmente, vamos encontrar o mdc$(162, 48)$ para verificarmos se esta equação possui solução inteira. Utilizando o algoritmo de Euclides, temos que $mdc(162, 48) = 6$ e como $6|6$, a equação possui solução.

	3	**2**	**1**	**2**	
162	**48**	**18**	**12**	**6**	
	18	**12**	**6**		

Observe que não é trivial encontrar uma solução particular para esta equação.

No entanto, do algoritmo de Euclides decorre que

$$162 = 3.48 + 18 \Rightarrow 18 = 162 - 3.48$$

$$48 = 2.18 + 12 \Rightarrow 12 = 48 - 2.18$$

$$18 = 1.12 + 6 \Rightarrow 6 = 18 - 1.12$$

Com isso, podemos escrever:

$$\begin{aligned} 6 &= 18 - 1.12 \\ 6 &= 18 - 1.(48 - 2.18) \\ 6 &= 3.18 - 1.48 \\ 6 &= 3.(162 - 3.48) - 1.48 \\ 6 &= 3.162 - 10.48 \\ 6 &= 162.3 + 48.(-10) \end{aligned}$$

Assim, temos que $x = 3$ *e* $y = -10$ *é uma solução para a equação* $162x + 48y = 6$*.*

Conhecendo uma solução podemos encontrar todas as outras a partir dela. Para isto, vamos dividir toda a equação pelo mdc$(162, 48)$*. Assim, a equação fica da forma* $27x + 8y = 1$ *com mdc*$(27, 8) = 1$*.*

Logo, pelo Teorema 2.3, temos que o conjunto solução da equação $162x + 48y = 6$ *é*

$$S = \{(3 + 8k, -10 - 27k) | k \in \mathbb{Z}\}$$

Observação 2.2. *No exemplo 2.3 trabalhamos com a equação* $162x + 48y = 6$ *com o intuito de utilizarmos o Algoritmo de Euclides de forma prática. No entanto, sabendo que* $mdc(162, 48) = 6$*, podemos dividir toda a equação por* 6 *e trabalhar com a equação* $27x + 8y = 1$*, que é mais simples e requer menos trabalho, uma vez que efetuamos divisões com números menores.*

3 Aritmética em cônicas

As cônicas são curvas algébricas planas definidas por um polinômio de grau 2. Nesta seção sobre a aritmética em cônicas, novamente usaremos [7] como prinicpal referência.

Vejamos as formas canônicas com coeficientes inteiros das cônicas:

- Parábolas: $\{(x, y) \in \mathbb{R}^2 \,|ax^2 + by = 0\}, a \neq 0, b \neq 0.$
- Hipérboles: $\{(x, y) \in \mathbb{R}^2 \,|ax^2 - by^2 = c\}, a > 0, b > 0, c > 0.$
- Elipses: $\{(x, y) \in \mathbb{R}^2 \,|ax^2 + by^2 = c\}, a > 0, b > 0, c > 0.$

Neste artigo trabalharemos apenas com elipses e hipérboles, mas todos os resultados dessa seção valem também para a parábola.

Proposição 3.1. *Sejam $C : ax^2 \pm by^2 = c$ e $r : y = mx + n$ uma cônica e uma reta de coeficientes racionais. Se essa cônica C e essa reta r se interceptam em um ponto racional, o outro ponto de intercessão também será racional.*

Demonstração. Sejam $ax^2 \pm by^2 = c$ e $y = mx + n$ equações de uma cônica e uma reta, respectivamente. Para encontrar a interseção entre a reta e cônica, devemos resolver o sistema gerado por suas equações, substituindo a equação da reta na equação da cônica:

$$\begin{gathered} ax^2 \pm by^2 = c \\ ax^2 \pm b(mx + n)^2 = c \\ (a \pm bm^2)x^2 \pm (2bmn)x \pm (n^2b) - c = 0. \end{gathered}$$

Observemos que o sistema se resume em uma equação do segundo grau de uma variável do tipo $Ax^2 + Bx + C = 0$. Além disso, se a reta e a cônica possuem coeficientes racionais, então $A, B, C \in \mathbb{Q}$, pois a soma, subtração e produto de racionais resulta em um racional.

As raízes da equação do segundo grau fornecem abcissas dos pontos de interseção. Sabemos, pelas relações de Girard, que o produto das raízes é $\dfrac{C}{A}$, que é um

número racional. Então se tivermos uma raiz racional, a outra também será. □

3.1 Método das tangentes e das secantes de Fermat:

Sejam C uma cônica, $P_1 \in C$ um ponto e r uma reta que não passa por P_1. Seja t a reta paralela a r passando por P_1 e $P_2 = C \cap t$ (sendo P_1 e P_2 não necessariamente distintos). Considere a função:

$$\begin{aligned} \lambda : C \setminus \{P_1, P_2\} &\rightarrow r \\ Q &\rightarrow \overline{P_1 Q} \cap r = R(Q) \end{aligned}$$

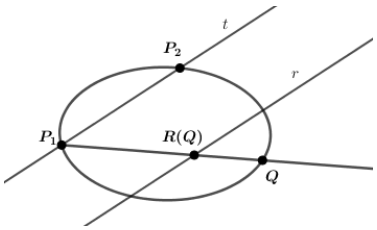

Figura 2: Representação geométrica da função λ.

λ é uma função invertível com inversa

$$\begin{aligned} \lambda^{-1} : r &\rightarrow C \setminus \{P_1, P_2\} \\ R &\rightarrow \overline{P_1 R} \cap C = Q(R) \end{aligned}$$

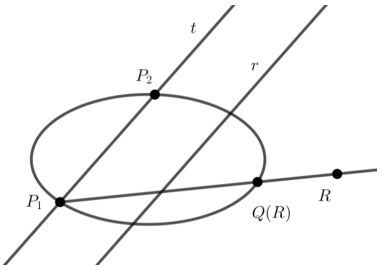

Figura 3: Inversa da função λ.

O Lema 3.1 é o análogo da Proposição 2.1 para pontos do conjunto $\mathbb{Q}^2$ em uma reta com coeficientes racionais.

Lema 3.1. *Seja $l = \{(x, y) \in \mathbb{R}^2 | bx+cy = a\}$ uma reta com coeficientes racionais a, b e c. Suponha que a reta possua um ponto racional $(x_0, y_0) \in \mathbb{Q}^2$. Os pontos $(x_k, y_k) = (x_0 + kc, y_0 - kb)$, são pontos da reta para todo $k \in \mathbb{Q}$.*

Demonstração. Os pontos $(x_k, y_k) = (x_0 + kc, y_0 - kb)$ satisfazem a equação da reta para todo $k \in \mathbb{Q}$. □

Teorema 3.1. *Seja $C \subset \mathbb{R}^2$ uma cônica com coeficientes racionais. Se o conjunto $\mathbb{Q} \times \mathbb{Q} \cap C$ é não vazio, então ele possui uma infinidade de pontos.*

Demonstração. Sejam C uma cônica de coeficientes racionais, $P \in \mathbb{Q} \times \mathbb{Q} \cap C$ e r uma reta com coeficientes racionais qualquer que não passa por P. Seja R pertencente à $\mathbb{Q}^2 \cap r$ e considere a reta determinada pelos pontos R e P. Seja Q o outro ponto de interseção da reta r com a cônica C. Note que pode ocorrer dos pontos P e Q serem os mesmos, se este for o caso tomamos outro ponto da reta em $\mathbb{Q}^2$. Sabemos pela Proposição 3.1 que Q é um ponto racional. Dessa forma, relacionamos os pontos racionais de r com os pontos racionais de C. Agora, pelo Lema 3.1, r possui infinitos pontos racionais, donde, C terá infinitos outros pontos racionais, como queríamos mostrar. □

Vejamos um exemplo do método das tangentes e das secantes de Fermat.

Exemplo 3.1. *Seja $C = \{(x, y) \in \mathbb{R}^2 \mid x^2+y^2 = 1\}$. Usamos o ponto $P = (-1, 0)$ e a reta $r = \{(0, t) \mid t \in \mathbb{R}\}$ para aplicar o Método de Fermat. Dados a cônica, o ponto P e a reta r, tracemos uma reta s paralela a r passando por P e tomemos um ponto $Q = (x, y)$ qualquer, obtendo a função*

$$\begin{aligned} \lambda : C \setminus \{P\} &\to r \\ Q &\to \overline{PQ} \cap r \end{aligned}$$

Pela Figura 4, podemos observar dois triângulos semelhantes. Assim,

$$\frac{y}{x+1} = \frac{t}{1} \Rightarrow t = \frac{y}{x+1}$$

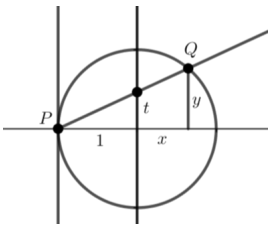

Figura 4: Representação geométrica da função λ.

Logo, a função λ é:

$$\begin{aligned} \lambda : C \setminus \{P\} &\rightarrow l \\ (x, y) &\rightarrow \left(0, \frac{y}{x+1}\right) \end{aligned}$$

Agora, vamos encontrar a inversa dessa função, ou seja, λ^{-1}. Sabemos que $t = \frac{y}{x+1} \Rightarrow y = t(x+1)$. Então, substituindo y na equação da cônica, temos:

$$\begin{gathered} x^2 + y^2 = 1 \\ x^2 + (t(x+1))^2 = 1 \\ x^2 + (tx+t)^2 = 1 \\ x^2 + (tx)^2 + 2t^2x + t^2 = 1 \\ (1+t^2)x^2 + 2t^2x + t^2 - 1 = 0 \end{gathered}$$

Observe que a equação acima é uma equação do segundo grau na variável x e que $x = -1$ é uma raiz dessa equação (é a interseção, P, que já conhecemos). Pelas relações de Girard, sabemos que o produto das raízes x_1 e x_2 dessa equação é igual a:

$$x_1.x_2 = \frac{t^2-1}{1+t^2}$$

Como $x_1 = -1$, segue que:

$$x_2 = \frac{1-t^2}{1+t^2}$$

Logo, temos a raiz $x_t = \frac{1-t^2}{1+t^2}$. Substituindo x_t em y_t:

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

Portanto,

$$\begin{aligned} \lambda^{-1} : r &\rightarrow C \setminus \{P\} \\ Q &\rightarrow \overline{PQ} \cap C \\ (0,t) &\rightarrow \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \end{aligned}$$

No próximo exemplo, além de mostrar a infinitude de pontos do Teorema 3.1, daremos uma descrição para esses pontos, como será visto mais adiante no Teorema 3.2.

Exemplo 3.2. *Considere agora o círculo* $C = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 2\}$. *Um ponto racional neste círculo é* $(1,1)$. *Considere a família de retas passando por esse ponto* $r_t : y - 1 = t(x-1)$. *Se* $t \in \mathbb{Q}$, *então cada uma dessas retas é secante ao círculo em um outro ponto* P_t *racional. Então, todos os outros pontos racionais desse círculo são:*

$$\left(\frac{t^2-2t-1}{t^2+1}, \frac{-t^2-2t+1}{t^2+1}\right)$$

Sabemos que $r_t : y - 1 = t(x-1) \Rightarrow y = tx - t + 1$. *Então, vamos substituir* y *na equação do círculo:*

$$\begin{gathered} x^2 + y^2 = 2 \\ x^2 + (tx - t + 1)^2 = 2 \\ x^2 + t^2x^2 - 2t^2x + 2tx + t^2 - 2t + 1 = 2 \\ (1+t^2)x^2 + (-2t^2 + 2t)x + (t^2 - 2t - 1) = 0 \end{gathered}$$

Pelas relações de Girard, o produto das raízes é dado por $x_0.x_t = \dfrac{t^2-2t-1}{1+t^2}$. *Como* $x_0 = 1$, *temos que* $x_t = \dfrac{t^2-2t-1}{1+t^2}$. *Substituindo* x_t *em* r_t*:*

$$\begin{aligned} y &= tx - t + 1 \\ y &= t\left(\frac{t^2 - 2t - 1}{1 + t^2}\right) - t + 1 \\ y &= \frac{t^3 - 2t^2 - t}{1 + t^2} - t + 1 \\ y &= \frac{-t^2 - 2t + 1}{t^2 + 1} \end{aligned}$$

Logo, todos os outros pontos racionais de C são $\left(\frac{t^2 - 2t - 1}{t^2 + 1}, \frac{-t^2 - 2t + 1}{t^2 + 1}\right)$.

Teorema 3.2. *Seja* $C \subset \mathbb{R}^2$ *a cônica de equação* $ax^2 + by^2 = c$ *com* $a, b, c \in \mathbb{Q}$. *Se* $P_0 = (x_0, y_0) \in \mathbb{Q}^2 \cap C$, *então todos os outros pontos do conjunto* $\mathbb{Q}^2 \cap C$ *são da forma*

$$\left(\frac{bt^2x_0 - 2bty_0 - ax_0}{bt^2 + a}, \frac{-bt^2y_0 - 2atx_0 + ay_0}{bt^2 + a}\right)$$

em que $t \in \mathbb{Q}$, $bt^2 + a \neq 0$.

Demonstração. Seja $r_t : y - y_0 = t(x - x_0)$ a família de retas que passa por P_0. Para cada t racional, temos que r_t possui coeficientes racionais, visto que $P_0 \in \mathbb{Q}^2 \cap C$. Dessa forma, pela Proposição 3.1 r_t será secante ou tangente à cônica em outro ponto do conjunto $\mathbb{Q}^2 \cap C$. Assim, substituindo a equação da reta $y = y_0 + t(x - x_0)$ na equação da cônica obtemos uma equação de grau 2:

$$ax^2 + b(y_0 + t(x - x_0))^2 = c$$

$$(a + bt^2)x^2 + (2by_0t - 2bt^2x_0)x + (by_0^2 - 2by_0tx_0 + bt^2x_0^2 - c) = 0 \quad (5)$$

Como $P_0 \in C$, podemos escrever C da seguinte maneira:

$$C : ax^2 + by^2 = c \Rightarrow ax_0^2 + by_0^2 = c \Rightarrow by_0^2 - c = -ax_0^2 \quad (6)$$

Substituindo o resultado anterior, 6, na equação 5, temos:

$$(a+bt^2)x^2+(2by_0t-2bt^2x_0)x+(-2by_0tx_0+bt^2x_0^2-ax_0^2)=0 \qquad (7)$$

Se a cônica $C: ax^2+by^2=c$ for uma elipse, então $a,\ b$ e c são ambos positivos ou negativos e, portanto, $a+bt^2$ é sempre positivo ou negativo para todo t real. Em particular, concluímos que $a+bt^2\neq 0$ será não nulo para todo t racional. Todavia, se C for uma hipérbole, temos que $a>0$ e $b<0$ ou $a<0$ e $b>0$ e, neste caso, $t_0=\sqrt{\dfrac{-a}{b}}$ e $t_1=-\sqrt{\dfrac{-a}{b}}$ são soluções reais da equação $a+bt^2=0$. Se t_0 (respectivamente t_1) é um número racional então temos a reta $r_{t_0}: y-y_0=t_0(x-x_0)$ (respectivamente r_{t_1}). Substituindo $t^2=-\dfrac{a}{b}$ na equação (7), temos:

$$+\left(2by_0t-2b\left(-\frac{a}{b}\right)x_0\right)x+\left(-2by_0tx_0+b\left(-\frac{a}{b}\right)x_0^2-ax_0^2\right)=0\Rightarrow$$

$$(2by_0t+2ax_0)x=-(-2by_0tx_0-ax_0^2-ax_0^2)\Rightarrow$$

$$(2by_0t+2ax_0)x=(2by_0t+2ax_0)x_0\Rightarrow$$

$$x=x_0.$$

Daí, como era de se esperar, uma vez que o coeficiente do termo quadrático x^2 da equação (7) se anula, temos uma equação do primeiro grau na qual, por construção, x_0 é solução. Portanto, a única solução da equação (7) é o ponto x_0 e, portanto, a reta $r_{t_0}: y-y_0=t_0(x-x_0)$ (respectivamente r_{t_1}) é tangente a cônica no ponto (x_0,y_0).

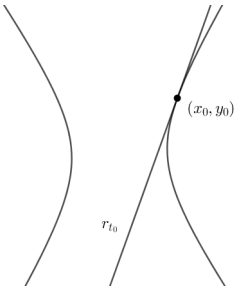

Figura 5: Hipérbole com reta r_{t_0} tangente no ponto (x_0,y_0).

Excetuando-se este caso particular da hipérbole no qual $\sqrt{\frac{-a}{b}}$ é um número racional, no caso geral o coeficiente do termo quadrático $(a + bt^2)$ é não nulo para todo $t \in \mathbb{Q}$. Deste modo, Pelas relações de Girard, se x_0 e x_t são raízes, então:

$$\begin{aligned} x_0 \,.\, x_t &= \left(\frac{-2by_0tx_0 + bt^2x_0^2 - ax_0^2}{a + bt^2}\right) \\ x_t &= \left(\frac{-2by_0t + bt^2x_0 - ax_0}{a + bt^2}\right) \end{aligned}$$

Para encontrarmos a coordenada y_t, vamos substituir o valor de x_t na equação de r_t:

$$\begin{aligned} y_t &= y_0 + t(x_t - x_0) \\ y_t &= y_0 + t\left(\frac{-2by_0t + bt^2x_0 - ax_0}{a + bt^2} - x_0\right) \\ y_t &= \frac{-bt^2y_0 - 2atx_0 + ay_0}{a + bt^2} \end{aligned}$$

Portanto, a partir de $P_0 = (x_0, y_0)$, concluímos que todos os outros pontos do conjunto $\mathbb{Q} \cap C$ são da forma

$$\left(\frac{bt^2x_0 - 2bty_0 - ax_0}{a + bt^2}, \frac{-bt^2y_0 - 2atx_0 + ay_0}{a + bt^2}\right),$$

$t \in \mathbb{Q}$ e $a + bt^2 \neq 0$ □

4 Soma de dois quadrados

Nesta seção estudaremos as propriedades de um número inteiro que pode ser escrito como soma de dois quadrados, isto é, buscaremos soluções inteiras para a equação $x^2 + y^2 = n$. A ideia de representar um número como soma de dois quadrados pode surgir naturalmente, como ao buscar triângulos retângulos de lados inteiros.Utilizaremos o método da secante de Fermat e o Teorema 3.2, que parametriza o conjunto de pontos $\mathbb{Q}^2$ em cônicas com coeficientes racionais, serão de fundamental importância para a conclusão dos resultados dessa seção.

Teorema 4.1. *Seja $n \in \mathbb{N}$, então n é soma de dois quadrados de racionais que não são inteiros se, e somente se, n for soma de dois quadrados de inteiros.*

Demonstração. Para a demonstração desde teorema, usaremos [7] como referência.

Suponhamos que $n \in \mathbb{N}$ seja soma de dois quadrados racionais, ou seja, $n = p_1^2 + p_2^2$ com $p_1, p_2 \in \mathbb{Q}$ e $p_1, p_2 \notin \mathbb{Z}$.

Seja $P = (p_1, p_2)$ um ponto do círculo $x^2+y^2 = n$ e seja $M = (m_1, m_2) \in \mathbb{Z}^2$ tal que $|m_1 - p_1| \leq \frac{1}{2}$ e $|m_2 - p_2| \leq \frac{1}{2}$.

Se a reta l que contém o segmento $\overline{MP}$ for tangente ao círculo $x^2 + y^2 = n$, teremos o triângulo OPM retângulo no ponto de tangência, em P, como na Figura 6.

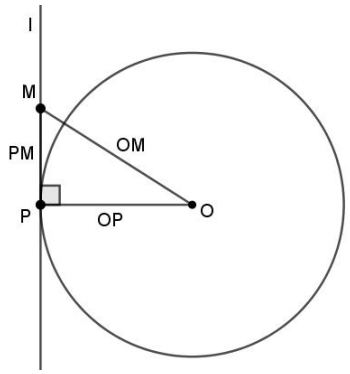

Figura 6: Círculo $x^2 + y^2 = n$.

Dessa forma, pelo Teorema de Pitágoras, teremos $||\overline{OM}||^2 = ||\overline{OP}||^2 + ||\overline{PM}||^2$. No entanto, sabemos que:
$||\overline{OM}||^2 \in \mathbb{Z}$, pois $M, O \in \mathbb{Z}^2$
$||\overline{OP}||^2 = (\sqrt{(p_1 - 0)^2 + (p_2 - 0)^2})^2 = p_1^2 + p_2^2 = n \in \mathbb{N}$
Logo $||\overline{PM}||^2 \in \mathbb{Z}$ uma vez que $||\overline{OM}||^2$ e $||\overline{OP}||^2$ são números inteiros.
Contudo $||\overline{PM}||^2 = (\sqrt{(m_1 - p_1)^2 + (m_2 - p_2)^2})^2 = |m_1 - p_1|^2 + |m_2 - p_2|^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. Como $||\overline{PM}||^2 \neq 0$, temos que $||\overline{PM}||^2 \notin \mathbb{Z}$, o que é uma contradição.

Logo, concluímos que l é secante ao círculo.

A reta l e o círculo $x^2+y^2=n$ possuem coeficientes racionais e se interceptam em um ponto $P \in \mathbb{Q}^2$. Dessa forma, pelo método das secantes de de Fermat, temos um outro ponto $Q=(q_1,q_2) \in \mathbb{Q}^2$ de interseção.

Seja d o mmc dos denominadores das frações irredutíveis p_1, p_2 que definem P. Vamos definir $c = d||\overline{PM}||^2$. Como $||\overline{PM}||^2 \leq \frac{1}{2}$, temos que $c < d$. Assim:

$$c = d||\overline{PM}||^2 = d(|m_1-p_1|^2+|m_2-p_2|^2) =$$
$$d[m_1^2+m_2^2+p_1^2+p_2^2-2(p_1m_1+p_2m_2)] = d[m_1^2+m_2^2+n-2(p_1m_1+p_2m_2)] \in \mathbb{Z}.$$

O ponto Q, interseção entre a reta e o círculo, pode ser obtido da seguinte forma:

$$Q = P + t(M-P) = (p_1,p_2) + t[(m_1,m_2)-(p_1,p_2)] =$$
$$(p_1+t(m_1-p_1), p_2+t(m_2-p_2)),\ t \in \mathbb{Q}$$

O produto escalar $\langle Q,Q\rangle = \langle (q_1,q_2),(q_1,q_2)\rangle = q_1^2+q_2^2 = n$, já que Q pertence ao círculo $x^2+y^2=n$.

Seja $v = M-P = (m_1-p_1, m_2-p_2)$. Então:

$$Q = P + tv$$
$$Q \cdot Q = (P+tv)\cdot(P+tv)$$
$$n = P\cdot P + 2t(P\cdot v) + t^2(v\cdot v)$$

Como P é um ponto do círculo, temos que $P\cdot P = n$. Logo, $2t(P\cdot v)+t^2(v\cdot v)$ deve ser igual a 0.

Temos ainda que $v\cdot v = ||\overline{PM}||^2 = \frac{c}{d}$. Logo,

$$2t(P\cdot v)+t^2(v\cdot v) = 0$$
$$t(2(P\cdot v)+t(v\cdot v)) = 0$$
$$2(P\cdot v)+t(v\cdot v) = 0$$
$$t = \frac{-2(P\cdot v)}{(v\cdot v)}$$

$$t = \frac{-2(p_1(m_1 - p_1) + p_2(m_2 - p_2))}{\frac{c}{d}}$$
$$t = \frac{-2(p_1m_1 + p_2m_2 - n)}{\frac{c}{d}}$$
$$t = \frac{d(2n - 2(p_1m_1 + p_2m_2))}{c}$$
$$ct = d(2n - 2(p_1m_1 + p_2m_2)) \tag{8}$$

Sabemos que: $\frac{c}{d} = m_1^2 + m_2^2 + p_1^2 + p_2^2 - 2(p_1m_1 + p_2m_2)$. Então, a equação 8 pode ser escrita como:

$$\begin{aligned} ct &= d(2n - 2(p_1m_1 + p_2m_2)) \\ ct &= d(2n + \frac{c}{d} - n - m_1^2 - m_2^2) \\ ct &= c + d(n - m_1^2 - m_2^2). \end{aligned}$$

Para concluir a prova, vamos mostrar que cq_1 e cq_2 são números inteiros. Para isso, multipliquemos q_i, $i = 1, 2$, por c.

$$Q = P + t(M - P)$$
$$q_i = p_i + t(m_i - p_i)$$
$$cq_i = cp_i + (ct)(m_i - p_i)$$
$$cq_i = cp_i + [c + d(n - m_1^2 - m_2^2)](m_i - p_i)$$
$$cq_i = cp_i + cm_i - cp_i + d(n - m_1^2 - m_2^2)(m_i - p_i)$$
$$cq_i = cm_i + d(n - m_1^2 - m_2^2)(m_i - p_i)$$

Os números c, m_i, n, dp_1 e dp_2, são inteiros. Logo, cq_i é inteiro e portanto o mmc dos denominadores das frações q_1 e q_2 que definem o ponto Q são menores ou iguais a c que por sua vez é menor do que o mmc dos denominadores das frações p_1 e p_2 que definem o ponto P.

Analogamente ao que foi feito com o ponto $P = (p_1, p_2)$ tomemos $U = (u_1, u_2) \in \mathbb{Z}^2$ tal que $|u_1 - q_1| \leq \frac{1}{2}$ e $|u_2 - q_2| \leq \frac{1}{2}$. Repetindo todas as contas teremos que a reta que contém o segmento $\overline{UQ}$ é secante ao círculo $x^2 + y^2 =$

n interceptando este em outro ponto $R = (r_1, r_2) \in \mathbb{Q}^2$, tal que o mmc dos denominadores das frações r_1 e r_2 que definem o ponto R é menor do que o mmc dos denominadores das frações q_1 e q_2 que definem o ponto Q o qual é menor do que o mmc dos denominadores das frações p_1 e p_2 que definem o ponto P.

Deste modo, se (x_0, y_0) é uma solução racional de $x^2 + y^2 = n$, então podemos construir uma sequência $(x_j, y_j) \in \mathbb{Q}$ de soluções tal que o mmc dos denominadores de x_{j+1} e y_{j+1} é menor do que o mmc dos denominadores de x_j e y_j.

Repetindo este processo um número finito de vezes encontraremos um ponto $V = (v_1, v_2)$ cujo os denominadores das frações v_1 e v_2 possuem mmc igual a 1, ou seja, V pertence a $\mathbb{Z}^2$.

Reciprocamente suponhamos que $n \in \mathbb{Z}$ seja soma de dois quadrados de inteiros, ou seja, $n = a_1^2 + a_2^2$ com $a_1, a_2 \in \mathbb{Z}$. Seja $A = (a_1, a_2) \in \mathbb{Z}^2$ um ponto do círculo $x^2 + y^2 = n$. Pelo Teorema 3.2 podemos parametrizar o conjunto dos ponto racionais de um círculo a partir de um ponto racional. Assim, vamos encontrar os outros pontos racionais do círculo $x^2 + y^2 = n$ a partir do ponto A. O teorema nos diz que estes pontos são do tipo:

$$\left(\frac{t^2 a_1 - 2ta_2 - a_1}{t^2 + 1}, \frac{-t^2 a_2 - 2ta_1 + a_2}{t^2 + 1} \right), t \in \mathbb{Q}$$

ou seja, pontos racionais. Logo, conseguimos escrever n como soma de dois quadrados de racionais, com denominador diferente de 1. □

A seguir enunciaremos um lema que garante que se dois números inteiros podem ser escritos como soma de dois quadrados, o produto entre eles também pode. Este lema será usado na demonstração de um teorema que nos fornece condições para identificar primos que são soma de dois quadrados. Para a demonstrações de ambos os resultados, usaremos [13] como referência.

Lema 4.1. *Se a e b são dois números inteiros tais que cada um é soma de dois quadrados, então o produto ab também é soma de dois quadrados.*

Demonstração. Sejam a e b dois números que podem ser escritos como soma de dois quadrados, ou seja, $a = x^2 + y^2$ e $b = w^2 + z^2$, com x, y, w e $z \in \mathbb{Z}$. Observe que o produto desses números é:

$$\begin{aligned} ab &= (x^2 + y^2)(w^2 + z^2) \\ ab &= x^2w^2 + x^2z^2 + y^2w^2 + y^2z^2 \\ ab &= x^2w^2 + y^2z^2 + x^2z^2 + y^2w^2 \end{aligned}$$

Somar e subtrair um mesmo termo não altera a igualdade. Então,

$$\begin{aligned} ab &= x^2w^2 + y^2z^2 + x^2z^2 + y^2w^2 + 2(xw)(yz) - 2(xw)(yz) \\ ab &= x^2w^2 + 2(xw)(yz) + y^2z^2 + x^2z^2 - 2(xz)(yw) + y^2w^2 \\ ab &= (xw + yz)^2 + (xz - yw)^2 \end{aligned}$$

Logo, $ab = m^2 + n^2$ com $m = xw + yz$ e $n = xz - yw$, ou seja, o produto de a e b também é soma de dois quadrados. □

Teorema 4.2. *Seja p um número primo. A equação $x^2 + y^2 = p$ possui solução inteira se, e somente se, $p = 2$ ou $p \equiv 1 \pmod 4$.*

Demonstração. Suponha $p = x^2 + y^2$ com x e y inteiros. Observe que se a é um número inteiro, $a^2 \equiv 0 \pmod 4$ ou $a^2 \equiv 1 \pmod 4$. De fato, os possíveis restos de $a \in \mathbb{Z}$ por 4 são $0, 1, 2$ e 3. Assim,

$$\begin{aligned} a \equiv 0 \pmod 4 &\Rightarrow a^2 \equiv 0 \pmod 4 \\ a \equiv 1 \pmod 4 &\Rightarrow a^2 \equiv 1 \pmod 4 \\ a \equiv 2 \pmod 4 &\Rightarrow a^2 \equiv 2^2 = 4 \equiv 0 \pmod 4 \\ a \equiv 3 \pmod 4 &\Rightarrow a^2 \equiv 3^2 = 9 \equiv 1 \pmod 4 \end{aligned}$$

Dessa forma, na equação $x^2 + y^2 = p$, temos as seguintes possibilidades:

•$x^2 \equiv y^2 \equiv 0 \pmod 4 : x^2 + y^2 \equiv 0 + 0 \pmod 4 \Rightarrow p \equiv 0 \pmod 4$

•$x^2 \equiv y^2 \equiv 1 \pmod 4 : x^2 + y^2 \equiv 1 + 1 \pmod 4 \Rightarrow p \equiv 2 \pmod 4$

•$x^2 \equiv 0 \pmod 4$ e $y^2 \equiv 1 \pmod 4 : x^2 + y^2 \equiv 0 + 1 \pmod 4 \Rightarrow p \equiv 1 \pmod 4$

Observe que a condição $x^2 \equiv 1 \pmod 4$ e $y^2 \equiv 0 \pmod 4$ é equivalente à terceira possibilidade. Como p é primo, então $p = 2$ ou $p \equiv 1 \pmod 4$.

Reciprocamente se $p = 2$, $x = 1$ e $y = 1$ satisfazem esta equação. Logo, se $p = 2$ a equação $x^2 + y^2 = p$ possui solução inteira. Vamos verificar se o mesmo ocorre para $p \equiv 1 \pmod 4$. vamos demonstrar que todo $p \equiv 1 \pmod 4$ pode ser escrito como soma de dois quadrados.

Seja $k = [\sqrt{p}]$, ou seja, k o maior número inteiro que é menor ou igual a $\sqrt{p}$. Como p é primo, então $\sqrt{p}$ não é um número inteiro. Dessa forma, $k < \sqrt{p} < k+1$.

Fixado um inteiro x consideremos a função $f(a, b) = a + bx$ e tomemos os pares de inteiros (a, b) tais que $0 \leq a \leq k$ e $0 \leq b \leq k$. O número de pares ordenados (a, b) possíveis é $(k + 1)(k + 1) = (k + 1)^2$. Como $(k + 1) > \sqrt{p}$, então $(k + 1)^2 > (\sqrt{p})^2$. Logo, o número de pares (a, b) é maior que p.

Sabemos que o conjunto de todas as classes residuais módulo p possui exatamente p elementos, então se considerarmos $f(a, b)$ módulo p, teremos mais números do que classes de resíduos e, pelo princípio da casa dos pombos, existem dois pares inteiros distintos (a_1, b_1) e (a_2, b_2) tais que $f(a_1, b_1) \equiv f(a_2, b_2) \pmod p$, ou seja, $a_1 + b_1x \equiv a_2 + b_2x \pmod p$.

Subtrair um mesmo termo nos dois membros de uma congruência não a altera.

Assim, podemos escrever:

$$\begin{aligned} a_1 + b_1x - a_2 &\equiv a_2 + b_2x - a_2 \pmod{p} \\ a_1 + b_1x - a_2 &\equiv b_2x \pmod{p} \\ a_1 + b_1x - a_2 - b_1x &\equiv b_2x - b_1x \pmod{p} \\ a_1 - a_2 &\equiv b_2x - b_1x \pmod{p} \\ a_1 - a_2 &\equiv -x(b_1 - b_2) \pmod{p} \end{aligned}$$

Podemos elevar a congruência ao quadrado sem alterá-la. Então,

$$\begin{aligned} (a_1 - a_2)^2 &\equiv [-x(b_1 - b_2)]^2 \pmod{p} \\ (a_1 - a_2)^2 &\equiv (-x)^2(b_1 - b_2)^2 \pmod{p} \\ (a_1 - a_2)^2 &\equiv x^2(b_1 - b_2)^2 \pmod{p} \end{aligned}$$

Se p é da forma $4q + 1$ (que é o mesmo que $p \equiv 1 \pmod 4$) então existe $x \in \mathbb{Z}$ tal que $x^2 \equiv -1 \pmod p$, sendo p um número primo. Para a demonstração deste resultado, consultar o Teorema 1.3, na página 3, da referência bibliográfica [13]. Dessa forma,

$$(a_1 - a_2)^2 \equiv -1(b_1 - b_2)^2 \pmod{p}$$

Denotemos $m = a_1 - a_2$ e $n = (b_1 - b_2)$. Assim, a congruência pode ser escrita como

$$\begin{aligned} m^2 &\equiv -n^2 \pmod{p} \\ m^2 + n^2 &\equiv -n^2 + n^2 \pmod{p} \\ m^2 + n^2 &\equiv 0 \pmod{p} \end{aligned}$$

Dessa forma, concluímos que $p|(m^2 + n^2)$.

Por construção (a_1, b_1) e (a_2, b_2) são pares ordenados distintos, ou seja, m e n não podem ser nulos. Assim, $m^2 + n^2 > 0$. Ainda a_1 e a_2 são inteiros e pertencem

ao intervalo $[0, k]$, então $m = a_1 - a_2$ pertence ao intervalo $-k \leq m \leq k$ e, analogamente, temos $n = b_1 - b_2$ com $-k \leq n \leq k$. Como $k < \sqrt{p}$, então $|m| < \sqrt{p}$ e $|n| < \sqrt{p}$. Consequentemente, $m^2 < (\sqrt{p})^2 = p$ e $n^2 < (\sqrt{p})^2 = p$. Assim, $m^2 + n^2 < p + p = 2p$. Deste modo $m^2 + n^2$ é um inteiro divisível por p e $0 < m^2 + n^2 < 2p$, o que implica que, $m^2 + n^2 = p$.

□

Proposição 4.1. *Sejam a, b e m inteiros com $m > 0$ e mdc$(a, m) = d$. A congruência $ax \equiv b \pmod{m}$ não possui nenhuma solução se $d \nmid b$ e possui exatamente d soluções incongruentes módulo m se $d|b$.*

Demonstração. Para esta demonstração, usaremos [13] como referência.

Dado que a e b são inteiros, temos que $ax \equiv b \pmod{m}$ se, e somente se, $m|(ax - b)$ e existe um $y \in \mathbb{Z}$ tal que $ax - b = my$, ou seja, que $ax - my = b$. Observe que $ax - my = b$ é uma equação diofantina e pelo Teorema 2.2 sabemos que se $d \nmid b$ esta equação não possui solução.

Por outro lado, se $d|b$, novamente pelo Teorema 2.2, esta equação possui infinitas soluções e são todas da forma $x = x_0 - \left(\frac{m}{d}\right) k$ e $y = y_0 - \left(\frac{a}{d}\right) k$, sendo (x_0, y_0) uma solução particular dessa equação e $k \in \mathbb{Z}$.

Assim, a congruência $ax \equiv b \pmod{m}$ irá possuir infinitas soluções que serão da forma $x = x_0 - \left(\frac{m}{d}\right) k$. Estamos interessados na quantidade de soluções que são duas a duas incongruentes módulo m, uma vez que toda solução particular determina, automaticamente, uma infinidade de soluções congruentes entre si. Se x_1 e x_2 forem congruentes módulo m, temos:

$$\begin{aligned} x_0 - \left(\frac{m}{d}\right) k_1 &\equiv x_0 - \left(\frac{m}{d}\right) k_2 \pmod{m} \\ x_0 - x_0 - \left(\frac{m}{d}\right) k_1 &\equiv x_0 - x_0 - \left(\frac{m}{d}\right) k_2 \pmod{m} \\ - \left(\frac{m}{d}\right) k_1 &\equiv - \left(\frac{m}{d}\right) k_2 \pmod{m} \end{aligned} \tag{9}$$

mas a congruência 9 equivale à:

$$k_1 \equiv k_2 \left(\mod \frac{m}{\frac{m}{\text{mdc}\left(\frac{m}{d}, m\right)}} \right) \tag{10}$$

como mdc $\left(\frac{m}{d}, m\right) = \frac{m}{d}$, a congruência 10 equivale à:

$$k_1 \equiv k_2 \pmod{d}.$$

Portanto, as soluções incongruentes são da forma $x = x_0 - \left(\frac{m}{d}\right) k$, onde k percorre um sistema completo de resíduos módulo d. □

Teorema 4.3. *Um número $n \in \mathbb{N}$ pode ser escrito como soma de dois quadrados se, e somente se, tiver a fatoração da forma:*

$$n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} ... q_s^{\beta_s}$$

com p_i e q_j primos, $p_i \equiv 1 \pmod 4$ e $q_j \equiv 3 \pmod 4$, $i = 1, 2, ..., r$ e $j = 1, 2, ..., s$ sendo todos os expoentes β_j pares.

Demonstração. Suponhamos que o número n tenha a fatoração $n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} ... q_s^{\beta_s}$ e vamos provar que n pode ser escrito como soma de dois quadrados.

Todo número da forma 2^{α} pode ser representado como soma de dois quadrados. De fato,

$$\text{se } \alpha \text{ é par, temos } 2^{\alpha} = (2^{\frac{\alpha}{2}})^2 + 0^2$$
$$\text{se } \alpha \text{ é ímpar, temos } 2^{\alpha} = (2^{\frac{\alpha-1}{2}})^2 + (2^{\frac{\alpha-1}{2}})^2$$

Pelo Teorema 4.2, todo p primo com $p \equiv 1 \pmod 4$ pode ser escrito como soma de dois quadrados. Além disso, pelo Lema 4.1, se dois números são soma de dois quadrados, então o produto destes números também é. Dessa forma, todos os $p_i^{\alpha_i}$ podem ser representados como soma de dois quadrados, assim como $p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$. Então, basta mostrarmos que $q_j^{\beta_j}$ também pode ser representado como

soma de dois quadrados.

Por hipótese, temos que todos os β_j são pares, então cada β_h pode ser escrito como $\beta_h = 2k$, $k \in \mathbb{Z}$. Logo,

$$q_j^{\beta_j} = q_j^{2k} = (q_j^k)^2.$$

Mas $(q_j^k)^2 = (q_j^k)^2 + 0^2$, ou seja, $(q_j^k)^2 = q_j^{2k}$ pode ser representado como soma de dois quadrados. Como todos 2^α, $p_i^{\alpha_i}$ e $q_j^{\beta_j}$ podem ser representados como soma de dois quadrados, concluímos pelo Lema 4.1 que o produto $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} ... q_s^{\beta_s}$ também pode.

Reciprocamente suponhamos que n seja soma de dois quadrados e que exista um β_j ímpar. Sem perda de generalidade, podemos considerar β_1 como tal ímpar.

Sejam a e b números que satisfazem a equação $a^2 + b^2 = n$ e $d = \text{mdc}(a, b)$. Dessa forma, $d|a$ e $d|b$ e, assim, existem k_1 e k_2 inteiros tais que $a = dk_1$ e $b = dk_2$. Além disso, sabemos que ao dividir dois números pelo o mdc, eles tornam primos entre si. Então,

$$\begin{aligned} \text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) &= 1 \\ \text{mdc}\left(\frac{dk_1}{d}, \frac{dk_2}{d}\right) &= 1 \\ \text{mdc}(k_1, k_2) &= 1 \end{aligned}$$

Como $a = dk_1$ e $b = dk_2$ satisfazem a equação $a^2 + b^2 = n$, podemos escrever

$$\begin{aligned} (dk_1)^2 + (dk_2)^2 &= n \\ d^2k_1^2 + d^2k_2^2 &= n \\ d^2(k_1^2 + k_2^2) &= n \end{aligned}$$

Sendo $k = k_1^2 + k_2^2$, podemos escrever $d^2k = n$ e concluir que $d^2|n$. Observe que k é soma de dois quadrados e que $k = \dfrac{n}{d^2}$, ou seja, k e $\dfrac{n}{d^2}$ possuem a mesma decomposição em fatores primos. Assim, como β_1 é um expoente ímpar de q_1 em n e todos os expoentes da decomposição de d^2 são pares, concluímos que o

expoente de q_1 em k também deve ser ímpar, uma vez que na divisão os expoentes de q_1 em n e d^2 são subtraídos. Visto que o expoente de q_1 é ímpar, então existe um número inteiro s tal que $k = q_1^{2s+1}r = q_1^{2s}q_1^1 r = q_1 q_1^{2s} r$, ou seja, $q_1|k$.

Como $\text{mdc}(k_1, k_2) = 1$ pelo Corolário 2.1 existem x e y inteiros tal que $k_1x + k_2y = 1$. Elevando cada membro ao quadrado, obtemos:

$$\begin{aligned} (k_1x + k_2y)^2 &= (1)^2 \\ (k_1x)^2 + 2(k_1x)(k_2y) + (k_2y)^2 &= 1 \end{aligned}$$

$$k_1^2x^2 + 2k_1xk_2y + k_2^2y^2 = 1 \tag{11}$$

Vimos também que $q_1|k$, isto é, existe um t inteiro tal que $k = q_1t$. Por outro lado, sabemos que $k = k_1^2 + k_2^2$, logo,

$$\begin{aligned} k_1^2 + k_2^2 &= q_1t \\ k_2^2 &= q_1t - k_1^2 \end{aligned}$$

Lembremos que $b = dk_2$, sendo $d = \text{mdc}(a, b)$, então, $k_2 = \dfrac{b}{d}$ e vamos substituir este valor na equação 11.

$$\begin{aligned} k_1^2x^2 + 2k_1xk_2y + k_2^2y^2 &= 1 \\ k_1^2x^2 + 2k_1xy\frac{b}{d} + y^2(q_1t - k_1^2) &= 1 \\ k_1^2x^2 + 2k_1xy\frac{b}{d} + y^2q_1t - y^2k_1^2 &= 1 \end{aligned}$$

Agrupando os termos que contém k_1 e q_1:

$$\begin{aligned} k_1^2x^2 + 2k_1xy\frac{b}{d} + y^2q_1t - y^2k_1^2 &= 1 \\ k_1^2x^2 + 2k_1xy\frac{b}{d} - y^2k_1^2 + y^2q_1t &= 1 \\ \left(k_1x^2 + 2xy\frac{b}{d} - y^2k_1\right)k_1 + (y^2t)q_1 &= 1 \end{aligned}$$

Os números $u = k_1x^2 + 2xy\dfrac{b}{d} - y^2k_1$ e $v = y^2t$ são inteiros. Como $uk_1 + vq_1 = 1$, pela Observação 2.1 temos que mdc$(k_1, q_1) = 1$. De forma análoga, mdc$(k_2, q_1) = 1$. Sabemos que $q_1|k$, isto é, $k \equiv 0 \pmod{q_1}$. Mas $k = k_1^2 + k_2^2$, então

$$\begin{aligned} k &\equiv 0 \pmod{q_1} \\ k_1^2 + k_2^2 &\equiv 0 \pmod{q_1} \\ k_1^2 + k_2^2 - k_2^2 &\equiv 0 - k_2^2 \pmod{q_1} \\ k_1^2 &\equiv -k_2^2 \pmod{q_1} \end{aligned}$$

Por outro lado, como $1 = mdc(k_1, q_1)|k_2$, pela Proposição 4.1 sabemos que existe um x de forma que $k_1x \equiv k_2 \pmod{q_1}$. Deste modo:

$$\begin{aligned} k_1x &\equiv k_2 \pmod{q_1} \\ k_1^2x^2 &\equiv k_2^2 \pmod{q_1} \\ k_1^2x^2 + k_1^2 &\equiv k_2^2 - k_2^2 \pmod{q_1} \\ k_1^2(x^2 + 1) &\equiv 0 \pmod{q_1} \end{aligned}$$

Entretanto, como mdc$(k_1, q_1) = 1$, temos que $q_1 \nmid k_1$ e portanto $q_1 \nmid k_1^2$.

Vimos que $k_1^2(x^2 + 1) \equiv 0 \pmod{q_1}$, ou seja, que $q_1|k_1^2(x^2 + 1)$. Como q_1 é primo, $q_1|k_1^2$ ou $q_1|(x^2 + 1)$, mas $q_1 \nmid k_1^2$, então $q_1|(x^2 + 1)$, ou seja, $x^2 \equiv -1 \pmod{q_1}$. Mas, pelo Teorema 1.3 de [13], $x^2 \equiv -1 \pmod{q_1}$ se e somente se $p = 2$ ou $p \equiv 1 \mod 4$. Mas a equação $x^2 \equiv -1 \pmod{q_1}$ possui solução para $q_1 \equiv 3 \pmod 4$ o que nos dará uma contradição. Portanto, todos os β_j são pares. □

5 Descenso infinito de Fermat

O método do descenso infinito de Fermat (quando aplicável) permite mostrar que uma equação $f(x_1, x_2, ..., x_n) = 0$ não possui soluções inteiras positivas ou, sob certas condições, até mesmo encontrar todas as soluções inteiras desta equação. Para o estudo desde método, usaremos [6] e [13] como referências.

Ao considerarmos $A = \{(x_1, ..., x_n) \in \mathbb{Z}^n | f(x_1, ..., x_n) = 0\}$ sendo o conjunto solução de f e este diferente de vazio, queremos construir uma função $\phi : A \to \mathbb{N}$ e tomar a solução $(x_1, ..., x_n) \in A$ sendo $\phi(x_1, ..., x_n)$ a menor possível. O descenso consiste em obter, a partir desta solução mínima, uma ainda menor, o que nos leva a uma contradição provando que A é realmente vazio. Para ilustrar este método de Fermat, vejamos um exemplo.

Exemplo 5.1. *(Fermat) Demonstre que a equação $x^4+y^4 = z^2$ não possui soluções inteiras positivas.*

Demonstração. Suponhamos que a equação $x^4 + y^4 = z^2$ possua uma solução inteira com $x, y, z > 0$. Assim, existe uma solução (a, b, c) no qual c é mínimo, visto que pelo Princípio da Boa Ordenação todo conjunto de inteiros positivos tem um menor elemento. Temos que a e b são primos entre si. De fato, se $d = \text{mdc}(a, b) > 1$ podemos substituir a e b por $\frac{a}{d}$ e $\frac{b}{d}$, respectivamente. Notemos que (a, b, c) é solução da equação $x^4+y^4 = z^2$, então $\left(\frac{a}{d}\right)^4 + \left(\frac{b}{d}\right)^4 = \frac{a^4+b^4}{d^4} = \left(\frac{c}{d^2}\right)^2$, ou seja, $\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2}\right)$ também é solução da equação e temos $\frac{c}{d^2} < c$, o que contradiz a minimalidade de c. (a^2, b^2, c) é um termo pitagórico primitivo (ver [8]), visto que $(a^2)^2 + (b^2)^2 = c^2$ e $\text{mdc}(a^2, b^2) = 1$. Assim, existem números inteiros positivos m e n, $m > n$, que são primos entre si de forma que

$$a^2 = m^2 - n^2, b^2 = 2mn \text{ e } c = m^2 + n^2.$$

A igualdade $a^2 = m^2 - n^2$ implica que $a^2 + n^2 = m^2$, ou seja, (a, n, m) é uma terna pitagórica primitiva. Como a e n são primos entre si, ambos números não podem ser pares, então suponhamos que a seja ímpar. Se n também for ímpar, temos:

$$a^2 = (2r + 1)^2 = 4r^2 + 4r + 1 = 4(r^2 + r) + 1 \Rightarrow a^2 \equiv 1 \pmod 4$$
$$n^2 = (4s + 1)^2 = 4s^2 + 4s + 1 = 4(s^2 + s) + 1 \Rightarrow n^2 \equiv 1 \pmod 4$$

Assim,

$$a^2 + n^2 \equiv 1 + 1 = 2 \pmod 4.$$

Mas $a^2 + n^2 = m^2$ e todo número ao quadrado é congruente a 0 ou 1 módulo 4 (ver [8]), o que nos leva à uma contradição. Portanto, n^2 deve ser par e, assim concluímos que m^2 é ímpar. Consequentemente, temos m ímpar e n par.

Já pela igualdade $b^2 = 2mn$, concluímos que b é par. Ainda mdc$(2n, m) = 1$, de fato, como m e n são coprimos, temos mdc$(n, m) = 1$, e isto implica que mdc$(2n, m) =$ mdc$(2, m)$, sendo mdc$(2, m) = 1$ ou 2. Mas mdc$(2, m) = 2$ é um absurdo, pois neste caso $2|m$ o que implica em m ser par, mas sabemos que m é ímpar. Então, mdc$(2n, m) =$ mdc$(2, m) = 1$.

Como $(2n)m = b^2$ é um quadrado perfeito, $2n$ e m também são. De fato, suponhamos que $2n$ não seja um quadrado perfeito. Neste caso, na fatoração de $2n$ existe um fator primo $p_i^{\alpha_i}$ com α_i ímpar, isto é, um fator que aparece um número ímpar de vezes no produto e como mdc$(2n, m) = 1$ este fator $p_i^{\alpha_i}$ não está na fatoração de m. Por outro lado, sabemos que $b^2 = (2n)n$ é um quadrado perfeito, então o fator p_i deve aparecer uma quantidade par de vezes, o que implica em um absurdo. Dessa forma, temos que $2n$ e m são ambos quadrados perfeitos e, então, existem inteiros positivos s e t tais que $2n = 4s^2$ e $m = t^2$.

Por outro lado, dado que $a^2 + n^2 = m^2$, então existirão inteiros positivos i e j, primos entre si tais que:

$$a = i^2 - j^2, n = 2ij \text{ e } m = i^2 + j^2$$

Assim, $s^2 = \dfrac{n}{2} = ij$, então i e j serão quadrados perfeitos, digamos $i = u^2$ e $j = v^2$.

Desta maneira $t^2 = m = i^2 + j^2$, $i = u^2$ e $j = v^2$. Logo,

$$t^2 = u^4 + v^4,$$

ou seja, (u, v, t) é outra solução para a equação original, $x^4 + y^4 = z^2$. No entanto,

$$t \leq t^2 = m \leq m^2 < m^2 + n^2 = c \Rightarrow t < c$$

Lembremos que $t \neq 0$, pois $m \neq 0$. Isto contradiz a minimalidade de c, concluindo a demonstração. □

6 O Último Teorema de Fermat

O Último Teorema de Fermat é um famoso teorema matemático conjecturado por Pierre de Fermat no qual afirma que a equação $x^n + y^n = z^n$ não possui solução inteira com x, y e z pertencentes a $\mathbb{Z}/\{0\}$ para $n > 2$.

De acordo com [5] e [14], Fermat, em 1637, afirmou ainda que conhecia a demonstração deste teorema, mas que na margem do papel não havia espaço para escrevê-la. Assim, este teorema desafiou diversos matemáticos durante mais de 300 anos em busca de uma demonstração. Foi somente em 1995 que o matemático Andrew Wiles [15] apresentou a demonstração desse teorema.

Neste trabalho, demonstraremos este teorema para o caso em que $n = 3$. Para isso, usaremos [2] e [12] como referências.

Lema 6.1. *Todas as soluções da equação $s^3 = a^2 + 3b^2$ em inteiros positivos tais que mdc$(a, b) = 1$ e s é ímpar são dadas por:*

$$s = u^2 + 3v^2,\ a = u(u^2 - 9v^2),\ b = 3v(u^2 - v^2),$$

com u, $v \in \mathbb{Z}$ e mdc$(u, 3v) = 1$.

Demonstração. Seja $\mho$ o conjunto de todos os inteiros da forma $a^2 + 3b^2$ com $a, b \in \mathbb{Z}$. $\mho$ é fechado para a multiplicação, visto que

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac \pm 3bd)^2 + 3(ad \mp bc)^2$$

sendo essa igualdade assegurada com os sinais correspondentes. Dado $s^3 = a^2 + 3b^2$, utilizando o hipótese de s ser ímpar e mdc$(a, b) = 1$ podemos escrever $s = u^2 + 3v^2$ com $u, v \in \mathbb{Z}$. A prova desta igualdade foge ao escopo deste trabalho, para a demonstração deste resultado, consultar a referência bibliográfica [12]: Lema 4.7, página 30.

Elevando s ao cubo, temos:

$$\begin{aligned}
s^3 &= (u^2+3v^2)^3 \\
s^3 &= (u^2+3v^2)(u^2+3v^2)^2 \\
s^3 &= (u^2+3v^2)(u^4+6u^2v^2+9v^4) \\
s^3 &= (u^2+3v^2)(u^4-6u^2v^2+9v^4+12u^2v^2) \\
s^3 &= (u^2+3v^2)[(u^2-3v^2)^2+3(2uv)^2] \\
s^3 &= [u(u^2-3v^2)-3v(2uv)]^2+3[u(2uv)+v(u^2-3v^2)]^2 \\
s^3 &= (u^3-3uv^2-6uv^2)^2+3(2vu^2+vu^2-3v^3)^2 \\
s^3 &= (u(u^2-9v^2))^2+3(3v(u^2-v^2))^2
\end{aligned}$$

Como, por hipótese, $s^3 = a^2+3b^2$, segue que $a = u(u^2-9v^2)$ e $b = 3v(u^2-v^2)$.

Daí, já que mdc$(a,b)=1$, então mdc$(u,3v)=1$. □

Teorema 6.1. *A equação $X^3+Y^3=Z^3$ não possui solução inteira, com X, Y e Z pertencentes a $\mathbb{Z}/\{0\}$.*

Demonstração. Suponhamos x, y e z números inteiros não nulos e, dois a dois, primos entre si tais que $x^3+y^3=z^3$. Note que sob estas hipóteses, x, y e z são números distintos.

Sabemos que x, y e z são primos entre si, então dois destes números não podem ser pares. Mas, se forem todos ímpares, teríamos que a soma de dois ímpares resulta em um ímpar, o que é falso. Portanto, exatamente um destes inteiros é par. É suficiente tomarmos x e y ímpares e z par uma vez que se considerarmos x par, y e z ímpares reescrevendo $z^3+(-y)^3=x^3$ teremos a soma de dois ímpares cúbicos resultando também em um número par cúbico. Deste modo, sejam x e y ímpares e z par.

Dentre todas as soluções da equação com as propriedades acima, escolhemos uma em que $|z|$ é a menor escolha possível.

Como x e y são ambos ímpares, sabemos que $(x+y)$ e $(x-y)$ são pares e assim

existem inteiros a e b tais que $(x+y) = 2a$ e $(x-y) = 2b$. Resolvendo o sistema gerado por estas duas últimas equações, temos que $x = a+b$ e $y = a-b$. Como x e y são não nulos e primos entre si, a e b também são não nulos com mdc$(a,b) = 1$. Além disso, dado que x e y são ímpares e sabendo que obtemos resultado ímpar apenas com a soma ou subtração de dois números de paridades diferentes, podemos concluir que a e b são de paridades diferentes. Agora, substituindo os valores de x e y na equação inicial, temos

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

Visto que o quadrado de um número, assim como multiplicar um número por 3, não altera a paridade e sabendo que a e b tem paridades diferentes, temos que (a^2+3b^2) é ímpar. Dado que z é um inteiro par, temos que $z^3 = (2j)^3 = 8j^3$ e $8|z^3$, portanto $8|2a(a^2+3b^2)$. Como (a^2+3b^2) é ímpar, temos que $8|2a$. Dessa forma, concluímos que a é par e, consequentemente, b é ímpar.

Uma vez que a é par e b é ímpar, o mdc$(2a, a^2+3b^2) = 1$ ou 3. De fato, seja q primo e q^k um fator comum dos termos acima, ou seja, $2a = q^k c$ e $(a^2+3b^2) = q^k d$. Como (a^2+3b^2) é ímpar, $q \neq 2$. Então, $q^k|a$ e, assim, $q^k|3b^2$. Visto que mdc$(a,b) = 1$ e que $q^k|a$, temos que $q^k \nmid b$. Como $q^k|3b^2$, concluímos que $k = 1$ e $q = 3$, ou seja, 3 é um possível fator comum a $2a$ e a^2+3b^2, assim como o 1, que é um fator comum a qualquer dois números. Dessa forma, consideremos os casos:

Caso 1: mdc$(2a, a^2+3b^2) = 1$

Neste caso, $3 \nmid a$, pois se ocorresse o contrário teríamos mdc$(2a, a^2+3b^2) \geq 3$. Da equação $z^3 = 2a(a^2+3b^2)$ e da fatoração única de inteiros em primos, temos que $(2a)$ e (a^2+3b^2) são cubos. Assim,

$$2a = r^3$$
$$a^2+3b^2 = s^3$$

onde s é ímpar e não é um múltiplo de 3 (pois $3 \nmid a$). Como s é ímpar e mdc$(a,b) = 1$, pelo Lema 6.1 podemos reescrever:

$$s = (u^2 + 3v^2)$$
$$a = u(u^2 - 9v^2)$$
$$b = 3v(u^2 - v^2)$$

com u, $v \in \mathbb{Z}$ e $mdc(u, 3v) = 1$.

Como b é ímpar, temos $3v(u^2 - v^2)$ ímpar. Sabemos que apenas o produto de dois ímpares resulta em um ímpar, então $3v$ e $(u^2 - v^2)$ devem ser ímpares. Assim, como 3 é um número ímpar, v também deve ser ímpar. E, se v é ímpar, u é par, já que a subtração de números de paridades distintas resulta em um ímpar. Além disso, temos que u é não nulo. Como $u|u$ e $v|3v$ então mdc$(u, v)|$mdc$(u, 3v)$ e daí mdc$(u, v) = 1$.

Seja q primo tal que $q|2u$. Como u é par, podemos afirmar que $q|u$. Suponhamos que $q|(u + 3v)$. Então, $q|(u + 3v) - u = 3v$, o que é um absurdo, pois mdc$(u, 3v) = 1$. Analogamente, suponhamos que $q|(u - 3v)$. Assim, $q|u - (u - 3v) = 3v$, que é um absurdo. Logo, mdc$(2u, u + 3v) =$ mdc$(2u, u - 3v) = 1$. Do mesmo modo se $\hat{q}$ é um primo tal que $\hat{q}|(u + 3v)$ e $\hat{q}|(u - 3v)$ então $\hat{q}|(u + 3v) + (u - 3v)$, ou seja, $\hat{q}|2u$, mas mdc$(2u, u + 3v) = 1$ o que implica $\hat{q} = 1$. O que nos dará um absurdo. Portanto podemos afirmar que $2u$, $(u + 3v)$, $(u - 3v)$ são primos dois a dois. Das igualdades

$$r^3 = 2a = 2.u(u^2 - 9v^2) = 2u(u - 3v)(u + 3v)$$

podemos concluir que $2u$, $(u + 3v)$, $(u - 3v)$ são cubos, ou seja,

$$2u = n^3$$
$$u - 3v = p^3$$
$$u + 3v = m^3$$

e temos que na terna (p, m, n) todos são diferentes de 0 (pois $u \neq 0$ e 3 não divide u), relativamente primos entre si dois a dois e satisfazem a equação $X^3 + Y^3 = Z^3$,

pois

$$\begin{aligned} 2u &= 2u \\ (u-3v)+(u+3v) &= (2u) \\ p^3+m^3 &= n^3 \end{aligned}$$

com n par (pois possui a mesma paridade de n^3) e $|z| > |n|$. De fato,

$$\begin{aligned} |z^3| &= |2a(a^2+3b^2)| \\ |z^3| &= |2.u(u^2-9v^2)(a^2+3b^2)| \\ |z^3| &= |2u(u-3v)(u+3v)(a^2+3b^2)| \\ |z^3| &= |n^3.p^3m^3.(a^2+3b^2)| \end{aligned}$$

Como b é ímpar, sabemos que $a^2+3b^2 \geq 3$. Então,

$$\begin{aligned} |z^3| &\geq |n^3.p^3m^3.3| \\ |z^3| &> |n^3| \\ |z| &> |n| \end{aligned}$$

No entanto, inicialmente havíamos escolhido (x, y, z) como solução da equação $X^3+Y^3=Z^3$ com $|z|$ sendo a menor escolha possível, ou seja, isso contradiz a escolha inicial.

Caso 2: mdc$(2a, a^2+3b^2) = 3$

Neste caso, a é múltiplo de 3, então escrevemos $a = 3c$. Como a é par, temos que c também é par. Além disso, $3 \nmid b$, já que mdc$(a, b) = 1$ e $3|a$. Dessa forma, temos que $(3c^2+b^2)$ é ímpar (pois c é par e b é ímpar e a soma de dois números de paridades diferentes resulta em um ímpar), ou seja $2 \nmid (3c^2+b^2)$ e ainda $3 \nmid (3c^2+b^2)$ (pois $3 \nmid b$) uma vez que mdc$(b, c) = 1$, o que implica $18 \nmid (3c^2+b^2)$ e consequentemente mdc$(18c, 3c^2+b^2) =$ mdc$(c, 3c^2+b^2) = 1$.

$$z^3 = 2a(a^2+3b^2) = 2(3c)[(3c)^2+3b^2] = 18c(3c^2+b^2).$$

De fato, pela fatoração única de inteiros, temos que $18c$ e $(3c^2 + b^2)$ são cubos, ou seja:

$$18c = r^3$$
$$3c^2 + b^2 = s^3$$

com s ímpar e $3|r$ uma vez que 3 é um fator de r^3. Novamente podemos utilizar o Lema 6.1 e escrever

$$s = (u^2 + 3v^2)$$
$$b = u(u^2 - 9v^2)$$
$$c = 3v(u^2 - v^2)$$

com $u, v \in \mathbb{Z}$ e mdc$(u, 3v) = 1$.

Como b é ímpar, temos que $u(u^2 - 9v^2)$ é ímpar e, então, u e $u^2 - 9v^2$ são ímpares. Como u é ímpar, podemos concluir que v é par. Além disso, temos que $v \neq 0$ (pois c é não nulo) e mdc$(u, v) = 1$ (consequência do Lema 6.1). Assim, usando o mesmo argumento do caso 1, é possível concluir que $2v$, $(u + v)$, $(u - v)$ são relativamente primos dois a dois. Da equação

$$r^3 = 18c = 18[3v(u^2 - v^2)] = 54v(u + v)(u - v)$$

temos que

$$\left(\frac{r}{3}\right)^3 = 2v(u + v)(u - v)$$

ou seja, $2v$, $(u + v)$, $(u - v)$ são cubos, isto é,

$$2v = n^3$$
$$u + v = p^3$$
$$u - v = -m^3$$

e temos que na terna (p, m, n) todos são diferentes de 0, relativamente primos entre

si dois a dois e satisfazem a equação $X^3 + Y^3 = Z^3$, pois

$$\begin{aligned} 2v &= 2v \\ (u+v)+(v-u) &= 2v \\ p^3 + (m^3) &= n^3 \end{aligned}$$

com $|n|$ par e $|z| > |n|$. De fato,

$$\begin{aligned} |z^3| &= |18c(3c^2+b^2)| \\ |z^3| &= |9.2.3v(u^2-v^2).(3c^2+b^2)| \\ |z^3| &= |27.2v(u^2-v^2).(3c^2+b^2)| \\ |z^3| &= |3^3.n^3.(-p^3m^3).(3c^2+b^2)| \\ |z^3| &= |3^3|.|n^3|.|(-p^3m^3)|.|(3c^2+b^2)| \end{aligned}$$

Como c e b são não nulos, temos que $(3c^2 + b^2) \geq 1$. Então,

$$\begin{aligned} |z^3| &> |3^3|.|n^3|.|(-p^3m^3)| \\ |z^3| &> |n^3| \\ |z| &> |n| \end{aligned}$$

Isto novamente contradiz a escolha inicial da terna (x, y, z) solução da equação $X^3 + Y^3 = Z^3$ com z sendo a menor escolha possível.

Dessa forma, a equação $X^3 + Y^3 = Z^3$ não possui solução. □

7 Conclusão

No século XVII René Descartes criou a Geometria Analítica, a qual possibilitou a fusão das áreas de Álgebra e Geometria, abrindo espaço para aplicações de Geometria em Teoria dos números e vice-versa. Pierre de Fermat, por exemplo, para se aprofundar no estudo das equações diofantinas, fez uso da Geometria Analítica. Desde então a junção entre Geometria e Aritmética tem sido amplamente usada na resolução de problemas envolvendo teoria dos números. Um exemplo

recente de problema envolvendo essa fusão, é uma generalização do Teorema 6.1 que consiste em demonstrar que :

$$x^3 + y^3 = z^n \quad x,\ y,\ z \in \mathbb{Z}/\{0\} \text{ não possui solução para } \ n \geq 3.$$

Bruin provou em [1] os casos $n = 4,\ 5$, Kraus fez em [9] o caso n primo com $17 \leq n < 10^4$ e Dahmen em [3] demonstrou para $n = 5, 7, 11, 13$. O problema se encontra em aberto para o restante dos valores de n.

8 Agradecimentos

À Universidade Federal de Ouro Preto - UFOP, ao Programa de Iniciação Científica e Mestrado - PICME e ao Programa de Educação Tutorial de Matemática - PETMAT UFOP, que permitiram o desenvolvimento deste trabalho.

Referências

[1] Nils Bruin. On powers as sums of two cubes. *Algorithmic number theory (edited by W. Bosma), Lecture Notes in Comput. Sci. 1838, Springer*, page 169–184, 2020.

[2] Salvador da Silva Bruno. O último teorema de fermat para n = 3. Master's thesis, Universidade Federal do Estado do Rio de Janeiro, Mestrado Profissional em Matemática em Rede Nacional, Rio de Janeiro, 2014.

[3] Sander Roland Dahmen. Classical and modular methods applied to diophantine equations. *University of Utrecht, Ph.D. thesis*, 2008.

[4] Gilda de La Rocque e João Bosco Pitombeira. Uma equação diofantina e suas resoluções. *Revista do Professor de Matemática*, 19:39–47, 1991.

[5] Stan Dolan. Fermat's method of descente infinie. *Mathematical Gazette*, 2011.

[6] Fabio Brochero Martinez; et. al. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. IMPA, Rio de Janeiro, 2016.

[7] Rodrigo Gondim. Aritmética em retas e cônicas. pages 6–31, Paraíba (SE), 2010. V Bienal da Sociedade Brasileira de Matemática.

[8] Abramo Hefez. *Aritmética*. SBM, Rio de Janeiro, 2016.

[9] Alain Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experimental Mathematics 7*, 1:1–13, 1998.

[10] Ricardo Vieira Lima. Equações diofantinas. Master's thesis, Universidade Federal de São João del-Rei, https://ufsj.edu.br/portal-repositorio/File/comat/tcc_Ricardo.pdf, 2017.

[11] Edi Jussara Candido Lorensatti. Aritmética: um pouco de história. Caxias do Sul (RS), 2012. IX ANPED SUL.

[12] Paulo Ribenboim. *Fermat's last theorem for amateurs*. Springer Science & Business Media, 2008.

[13] João Evangelista Cabral dos Santos et al. Números inteiros como soma de quadrados. 2013.

[14] Simon Lehna Singh. O Último teorema de fermat. *Rio de Janeiro: Editora Record.*, 1998.

[15] Andrew J Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 141:443–551, 1995.