Equações Diofantinas

Prof. Dr. Vinícius Wasques

Universidade Estadual Paulista "Júlio de Mesquita Filho" - Campus Rio Claro

06 de julho de 2020

Equações Diofantinas

Uma equação Diofantina é uma equação polinomial para a qual procuramos soluções inteiras ou racionais.

Nas aulas anteriores estudamos equações do seguinte tipo:

$$ax + by = c$$

com a, b e c inteiros dados, e procuramos os pares (x, y) que satisfazem a equação.

Equações do tipo $ax + by = c$ são equações diofantinas de grau 1.

Nessa aula estudaremos outras equações diofantinas, começando com

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

chamadas de ternas pitagóricas.

As triplas de números inteiros positivos (a, b, c) que satisfazem a equação acima são denominadas triplas ou ternas pitagóricas.

Vamos encontrar todas as ternas pitagóricas (a, b, c).

Podemos supor que a, b, c são primos relativos dois a dois, pois se houver um primo p tal que $p|mdc(a, b)$, então

$$p|a^2 + b^2 = c^2 \Rightarrow p|c,$$

logo

$$\left(\frac{a}{p}, \frac{b}{p}, \frac{c}{p}\right)$$

também é tripla pitagórica.

Uma tripla pitagórica cujos termos são primos relativos dois a dois se denomina tripla pitagórica *primitiva*.

Como estamos supondo que a e b são primos entre si, então a e b não podem ser pares ao mesmo tempo. Portanto podemos supor sem perda de generalidade que a é ímpar.

Além disso,

$$(2k+1)^2 = 4k^2 + 4k + 1 \equiv \ 1 \ (mod \ 4)$$

e

$$(2k)^2 \equiv \ 0 \ (mod \ 4)$$

Logo, quadrados perfeitos são congruentes ou a 0 ou a 1 módulo 4.

Portanto b não pode ser ímpar pois caso contrário

$$c^2 = a^2 + b^2 \equiv 2 \ (mod \ 4),$$

chegando em um absurdo.

Logo, temos que b é par e portanto c é ímpar.

Por outro lado,

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

Temos

$$mdc(c-a, c+a) = mdc(2c, c+a) = 2$$

pois

$$mdc(a, c) = 1 \Rightarrow mdc(c, c+a) = 1$$

e $c + a$ é par.

Logo $\frac{c+a}{2}$ e $\frac{c-a}{2}$ são primos entre si e seu produto é um quadrado perfeito.

Pelo teorema Fundamental da Aritmética, cada um destes fatores deve ser o quadrado de um número natural. (verifique esse fato)

Assim

$$\frac{c+a}{2} = m^2, \quad \frac{c-a}{2} = n^2, \quad b = 2mn,$$

com $mdc(m, n) = 1$.

Esse resultado pode ser enunciado da seguinte forma:

Proposição

As ternas pitagóricas primitivas (a, b, c) são da forma

$$\frac{c+a}{2} = m^2, \quad \frac{c-a}{2} = n^2, \quad b = 2mn,$$

com $mdc(m, n) = 1$ e $m + n$ ímpar

Exemplo:

A terna (7,24,25) é uma tripla pitagórica primitiva, pois

$$\frac{7+25}{2} = 16 = 4^2$$

$$\frac{25-7}{2} = 9 = 3^2$$

$$24 = 2.4.3$$

com $mdc(4,3) = 1$ e $4+3$ ímpar

Observação

A condição de que m + n seja um número ímpar garante a primitividade da tripla, isto é, como $mdc(m, n) = 1$ temos

$$mdc(m^2, m^2 + n^2) = 1$$

e portanto (verifique as igualdades abaixo)

$$\begin{aligned} mdc(a, c) &= mdc(m^2 - n^2, m^2 + n^2) \\ &= mdc(2m^2, m^2 + n^2) \\ &= mdc(2, m^2 + n^2), \end{aligned}$$

que é igual a 1 se, e só se, $m^2 + n^2$ é ímpar.

As soluções inteiras primitivas da equação

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

estão em bijeção via aplicação

$$\phi(x, y, z) = \left(\frac{x}{z}, \frac{y}{z}\right)$$

com as soluções racionais da equação

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

Exercício

Os pontos racionais (x, y) da circunferência de equação $x^2 + y^2 = 1$ são todos os pontos da forma:

$$(x, y) = (1, 0)$$

e

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

com $t \in \mathbb{Q}$.

Assim, substituindo $t = \frac{m}{n}$ com $m, n \in \mathbb{Z}$ e $mdc(m, n) = 1$, obtemos as soluções racionais

$$\left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2}\right),$$

que correspondem às ternas pitagóricas $(m^2 - n^2, 2mn, m^2 + n^2)$.

Equações Diofantinas Quadráticas e Somas de Quadrados

Aqui vamos buscar um critério para determinar quando uma equação do tipo

$$ax^2 + by^2 + cz^2 = 0$$

tem solução não nula, generalizando as triplas pitagóricas.

Teorema de Legendre

Sejam a, b, c inteiros livres de quadrados, primos entre si, dois a dois, e não todos do mesmo sinal.

A equação

$$ax^2 + by^2 + cz^2 = 0$$

tem solução não trivial com x, y e z inteiros se, e somente se,

$(-bc)$ é quadrado módulo a,

$(-ac)$ é quadrado módulo b e

$(-ab)$ é quadrado módulo c.

Demonstração

($\Rightarrow$) Note que, pela simetria da equação temos que $-bc$ é quadrado módulo a. De fato, podemos supor que x, y e z são primos entre si dois a dois, pois se $d|mdc(x,y)$ então d^2 divide cz^2, mas c é livre de quadrados, portanto $d|z$.

Agora como $by^2 + cz^2 \equiv 0 \ (mod \ a)$ segue que

$$b^2y^2 \equiv -bcz^2 \ (mod \ a)$$

Note que z deve ser primo entre si com a, pois se p é primo tal que $p|a$ e $p|z$, teremos que $p|by^2$, mas $mdc(a, b) = 1$, segue que $p|y$ o que contradiz o fato de y e z serem primos entre si.

Assim, z é invertível módulo a, e logo

$$(byz^{-1})^2 \equiv -bc \ (mod \ a)$$

e portanto $-bc$ é quadrado módulo a.

De modo similar pode ser provado que $(-ac)$ é quadrado módulo b e $(-ab)$ é quadrado módulo c.

($\Leftarrow$) Podemos supor, sem perda de generalidade, que $a < 0, b < 0$ e $c > 0$. Por hipótese, existe $u \in \mathbb{Z}$ tal que $u^2 \equiv -bc \ (mod\ a)$. Assim, temos que

$$\begin{aligned}
ax^2 + by^2 + cz^2 &\equiv by^2 + cz^2 \ (mod\ a) \\
&\equiv b^{-1}((by)^2 + bcz^2) \ (mod\ a) \\
&\equiv b^{-1}((by)^2 - u^2z^2) \ (mod\ a) \\
&\equiv b^{-1}(by - uz)(by + uz) \ (mod\ a) \\
&\equiv (y - b^{-1}uz)(by + uz) \ (mod\ a) \\
&\equiv L_1(x, y, z)M_1(x, y, z) \ (mod\ a)
\end{aligned}$$

sendo $L_1(x, y, z) = d_1x + e_1y + f_1z$, $M_1(x, y, z) = g_1x + h_1y + i_1z$, com $d_1 = g_1 = 0$, $e_1 = 1$, $f_1 = -b^{-1}u$, $h_1 = b$ e $i_1 = u$.

De modo similar, temos que

$$ax^2 + by^2 + cz^2 \equiv L_2(x, y, z)M_2(x, y, z)\ (mod\ b)$$

e

$$ax^2 + by^2 + cz^2 \equiv L_3(x, y, z)M_3(x, y, z)\ (mod\ c)$$

com

$L_k(x, y, z) = d_k x + e_k y + f_k z$ e $M_k(x, y, z) = g_k x + h_k y + i_k z$
para $k = 2, 3$.

Como a, b e c são primos entre si dois a dois, podemos pelo teorema chinês dos restos encontrar duas formas lineares

$$L(x, y, z) = dx + ey + fz$$

e

$$M(x, y, z) = gx + hy + iz$$

tais que

$$L \equiv L_1 \ (mod \ a), L \equiv L_2 \ (mod \ b) \quad \text{e} \quad L \equiv L_3 \ (mod \ c),$$

e

$$M \equiv M_1 \ (mod \ a), M \equiv M_2 \ (mod \ b) \quad \text{e} \quad M \equiv M_3 \ (mod \ c),$$

Verifique esse fato! (note que basta resolver o sistema de congruências coeficiente a coeficiente)

Logo

$$ax^2 + by^2 + cz^2 \equiv L(x, y, z)M(x, y, z) \; (mod \; abc).$$

Consideremos agora todas a triplas $(x, y, z) \in \mathbb{Z}^3$ com $0 \leq x \leq \sqrt{|bc|}$, $0 \leq y \leq \sqrt{|ac|}$ e $0 \leq z \leq \sqrt{|ab|}$.

Temos

$$(\lfloor\sqrt{|bc|}\rfloor + 1)(\lfloor\sqrt{|ac|}\rfloor + 1)(\lfloor\sqrt{|ab|}\rfloor + 1) > abc$$

Verifique essa afirmação.

Pelo Princípio da Casa dos Pombos existem duas triplas distintas dentre elas, (x_1, y_1, z_1) e (x_2, y_2, z_2), com

$$\begin{aligned} L(x_1, y_1, z_1) &\equiv L(x_2, y_2, z_2)\ (mod\ abc) \\ &\Leftrightarrow \\ L(x_1 - x_2, y_1 - y_2, z_1 - z_2) &\equiv 0\ (mod\ abc), \end{aligned}$$

Fazendo $\bar{x} = x_1 - x_2$, $\bar{y} = y_1 - y_2$ e $\bar{z} = z_1 - z_2$, temos

$$a\bar{x}^2 + b\bar{y}^2 + c\bar{z}^2 \equiv L(\bar{x}, \bar{y}, \bar{z})M(\bar{x}, \bar{y}, \bar{z}) \equiv 0\ (mod\ abc)$$

Note que $(\bar{x}, \bar{y}, \bar{z} \neq (0,0,0)$, $|\bar{x}| < \sqrt{|bc|}$, $|\bar{y}| < \sqrt{|ac|}$ e $|\bar{z}| < \sqrt{|ab|}$, uma vez que como a, b, c são dois a dois primos entre si e livre de quadrados, não pode ocorrer a igualdade.

Como $a, b < 0$ e $c > 0$ temos que

$$
\begin{aligned}
-2abc = a|bc| + b|ac| &< a\bar{x}^2 + b\bar{y}^2 \\
&\leq a\bar{x}^2 + b\bar{y}^2 + c\bar{z}^2 \\
&\leq c\bar{z}^2 \\
&< |ab|c \\
&= abc.
\end{aligned}
$$

Como $abc | a\bar{x}^2 + b\bar{y}^2 + c\bar{z}^2$, devemos então ter $a\bar{x}^2 + b\bar{y}^2 + c\bar{z}^2 = 0$, o que resolve o problema, ou

$$a\bar{x}^2 + b\bar{y}^2 + c\bar{z}^2 = -abc,$$

mas, nesse caso, temos

$$\begin{aligned} 0 &= (a\bar{x}^2 + b\bar{y}^2 + c\bar{z}^2 + abc)(\bar{z}^2 + ab) \\ &= a(\bar{x}\bar{z} + b\bar{y})^2 + b(\bar{y}\bar{z} - a\bar{x})^2 + c(\bar{z}^2 + ab)^2 \end{aligned}$$

o que nos dá a solução $(\bar{x}\bar{z} + b\bar{y}, \bar{y}\bar{z} - a\bar{x}, \bar{z}^2 + ab)$ com $\bar{z}^2 + ab \neq 0$.

O teorema de Legendre permite determinar quando uma curva algébrica plana de grau 2,

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$$

com $A, B, C, D, E \in \mathbb{Q}$, possui algum ponto racional $(x, y) \in \mathbb{Q}^2$.

Referências

MARTINEZ, F.E.B; MOREIRA, C.G.T; SALDANHA, N.,T.; TENGAN, E. Teoria dos Números. Um passeio com Primos e outros Números Familiares pelo Mundo Inteiro. IMPA, 2013.

GRAHAM, R. L., KNUTH, D. E., PATASHNIK, O
Matemática Concreta. LTC, São Paulo, 1995

NIVEN, I. E.; ZUCKERMAN, N.S. An Introduction to the Theory of Numbers, NY, John Wiley & Sons, 1991.

Contato

Prof. Dr. Vinícius Wasques

email: viniciuswasques@gmail.com

Departamento de Matemática

site: `https://viniciuswasques.github.io/home/`