Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 11

Equações Diofantinas Quadráticas

1 Ternas Pitagóricas

As triplas de números inteiros positivos (a, b, c) que satisfazem a equação

$$a^2 + b^2 = c^2$$

são denominadas *triplas ou ternas pitagóricas*, já que correspondem aos comprimentos dos lados de um triângulo retângulo de lados inteiros pelo teorema de Pitágoras.

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 $p \mid \text{mdc}(a, b)$, por exemplo, então $p \mid a^2 + b^2 = c^2 \implies p \mid c$, logo $(\frac{a}{p}, \frac{b}{p}, \frac{c}{p})$ também é tripla pitagórica. Uma tripla pitagórica cujos termos são primos relativos dois a dois se denomina *tripla pitagórica primitiva*.

Daqui a e b não podem ser pares ao mesmo tempo, portanto podemos supor sem perda de generalidade que a é ímpar. Além disso, como $(2k+1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$ e $(2k)^2 \equiv 0 \pmod 4$, quadrados perfeitos são congruentes ou a 0 ou a 1 módulo 4. Portanto b não pode ser ímpar pois caso contrário $c^2 \equiv a^2 + b^2 \equiv 2 \pmod 4$, um absurdo. Resumindo, temos que b é par e c é ímpar. Por outro lado,

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

Temos $\text{mdc}(c-a, c+a) = \text{mdc}(2c, c+a) = 2$ pois $\text{mdc}(a, c) = 1 \implies \text{mdc}(c, c+a) = 1$ e $c+a$ é par. Logo $\frac{c+a}{2}$ e $\frac{c-a}{2}$ são coprimos e seu produto é um quadrado perfeito. Pelo teorema Fundamental da Aritmética, cada um destes fatores deve ser o quadrado de um número natural. Assim,

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

com $\text{mdc}(m, n) = 1$. Escrevendo a, b, c em termos de m e n, obtemos portanto

Proposição 1. *As ternas pitagóricas primitivas* (a, b, c) *são da forma*

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

com $\text{mdc}(m, n) = 1$ *e* $m + n$ *ímpar.*

A condição de $m + n$ ser ímpar garante a primitividade da tripla: como $\text{mdc}(m, n) = 1$ temos $\text{mdc}(m^2, m^2 + n^2) = 1$ e portanto $\text{mdc}(a, c) = \text{mdc}(m^2 - n^2, m^2 + n^2) = \text{mdc}(2m^2, m^2 + n^2) = \text{mdc}(2, m^2 + n^2)$, que é igual a 1 se, e só se, $m^2 + n^2$ é ímpar, isto é, se m e n têm paridades distintas. Todas as demais triplas pitagóricas podem ser obtidas a partir de uma tripla pitagórica primitiva, multiplicando seus termos por uma constante.

Como uma aplicação do resultado anterior, consideremos o seguinte

Exemplo 2. *Encontrar todas as triplas de inteiros positivos* (a, b, c) *tais que* a^2, b^2 *e* c^2 *estão em progressão aritmética.*

Solução: O problema se reduz a encontrar todas as triplas (a, b, c) tais que

$$a^2 + c^2 = 2b^2$$

e, como no caso das ternas pitagóricas, basta considerar o caso em que a, b, c são dois a dois primos entre si. Temos que a e c têm igual paridade (logo são ímpares pois $\text{mdc}(a, c) = 1$ por hipótese) e portanto existem inteiros r e s tais que $c = r + s$ e $a = r - s$ (é só fazer $r = \frac{c+a}{2}$ e $s = \frac{c-a}{2}$). Substituindo temos que

$$a^2 + c^2 = (r - s)^2 + (r + s)^2 = 2(r^2 + s^2) = 2b^2.$$

Logo (r, s, b) é uma tripla pitagórica, que é primitiva pois qualquer divisor comum de r e s é um divisor comum de a e c. Portanto existem inteiros m e n tais que $r = m^2 - n^2$, $s = 2mn$ e $b = m^2 + n^2$ (ou $r = 2mn$ e $s = m^2 - n^2$, que fornecerá uma outra solução simétrica). Conclui-se que

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

e é fácil verificar que tal tripla cumpre o pedido. □

As soluções inteiras primitivas da equação $x^2 + y^2 = z^2$ estão claramente em bijeção, via $(x, y, z) \mapsto (x/z, y/z)$, com as soluções *racionais* da equação $x^2 + y^2 = 1$. Estas, por sua vez, podem ser facilmente obtidas através do seguinte método geométrico:

Teorema 3. *Os pontos racionais* (x, y) *(isto é, com ambas as coordenadas* $x, y \in \mathbb{Q}$*) da circunferência de equação* $x^2 + y^2 = 1$ *são todos os pontos da forma*

$$(x, y) = (1, 0) \qquad e \qquad (x, y) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1}\right) \qquad com\ t \in \mathbb{Q}.$$

Demonstração. Considere a reta passando pelos pontos $(1, 0)$ e $(0, t)$ com $t \in \mathbb{Q}$, ou seja, a reta de equação $y = -t(x - 1)$. Esta reta intercepta a circunferência em dois pontos: $(1, 0)$ e $(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1})$.

Agora observe que $(0,t) \mapsto (\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1})$ estabelece uma bijeção entre os pontos racionais do eixo y e os pontos racionais P da circunferência $x^2+y^2=1$, menos o ponto $(1,0)$. De fato, é claro que se $t \in \mathbb{Q}$ então $(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1})$ é um ponto racional da circunferência. Reciprocamente, dado um ponto racional $P \neq (1,0)$ da circunferência, temos que a reta que une P a $(1,0)$ admite uma equação com coeficientes racionais, logo intercepta o eixo y em um ponto $(0,t)$ com $t \in \mathbb{Q}$. Isto completa a demonstração. □

Assim, substituindo $t = \frac{m}{n}$ com $m, n \in \mathbb{Z}$ e $\text{mdc}(m,n) = 1$, obtemos as soluções racionais $(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2})$, que correspondem às ternas pitagóricas $(m^2-n^2, 2mn, m^2+n^2)$.

2 Soma de Quadrados

Vamos provar um resultado devido a Legendre que fornece um critério para determinar quando uma equação do tipo $ax^2+by^2+cz^2=0$ tem solução não nula e que dá uma generalização natural das triplas pitagóricas.

Teorema 4 (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 $(x,y,z) \neq (0,0,0)$ 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. Vamos primeiro mostrar a necessidade. Basta ver pela simetria da equação que $-bc$ é quadrado módulo a. De fato, podemos supor que x, y e z são primos relativos dois a dois, pois se $d \mid \text{mdc}(x,y)$ então d^2 divide cz^2, mas c é livre de quadrados, portanto $d \mid z$. Agora como $by^2+cz^2 \equiv 0 \pmod{a}$ segue que $b^2y^2 \equiv -bcz^2 \pmod{a}$. Note que z deve ser primo com a, pois se p é primo tal que $p \mid a$ e $p \mid z$, teremos que $p \mid by^2$, mas $\text{mdc}(a,b)=1$, segue que $p \mid y$ o que contradiz o fato de y e z serem primos entre si. Assim, z é invertível módulo a, e logo $(byz^{-1})^2 \equiv -bc \pmod{a}$.

Provemos agora a suficiência. Podemos supor, sem perda de generalidade, que $a<0$, $b<0$ e $c>0$. Por hipótese, existe $u \in \mathbb{Z}$ tal que $u^2 \equiv -bc \pmod{a}$. Assim, módulo a, temos que

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

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

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

e

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

onde $L_k(x,y,z) = d_kx+e_ky+f_kz$, $M_k(x,y,z) = g_kx+h_ky+i_kz$, $k = 2,3$. Como a, b e c são primos entre si dois a dois, podemos pelo teorema chinês dos restos encontrar duas formas lineares $L(x,y,z) = dx+ey+fz$, $M(x,y,z) = gx+hy+iz$ tais que $L \equiv L_1 \pmod a$, $L \equiv L_2 \pmod b$ e $L \equiv L_3 \pmod c$, e $M \equiv M_1 \pmod a$, $M \equiv M_2 \pmod b$ e $M \equiv M_3 \pmod c$ (basta resolver o sistema de congruências coeficiente a coeficiente). Logo

$$ax^2 + by^2 + cz^2 \equiv L(x,y,z)M(x,y,z) \pmod{abc}.$$

Consideremos agora todas a triplas $(x,y,z) \in \mathbb{Z}^3$ com $0 \le x \le \sqrt{|bc|}$, $0 \le y \le \sqrt{|ac|}$ e $0 \le z \le \sqrt{|ab|}$. Temos $(\lfloor\sqrt{|bc|}\rfloor + 1)(\lfloor\sqrt{|ac|}\rfloor + 1)(\lfloor\sqrt{|ab|}\rfloor + 1) > abc$ de tais triplas, donde 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 $L(x_1,y_1,z_1) \equiv L(x_2,y_2,z_2) \pmod{abc} \iff L(x_1-x_2, y_1-y_2, z_1-z_2) \equiv 0 \pmod{abc}$, donde, fazendo $\tilde{x} = x_1 - x_2$, $\tilde{y} = y_1 - y_2$ e $\tilde{z} = z_1 - z_2$, temos

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

Note que $(\tilde{x},\tilde{y},\tilde{z}) \neq (0,0,0)$, $|\tilde{x}| < \sqrt{|bc|}$, $|\tilde{y}| < \sqrt{|ac|}$ e $|\tilde{z}| < \sqrt{|ab|}$ (de fato, como a, b, c são dois a dois coprimos e livre de quadrados, não pode ocorrer a igualdade). Como $a, b < 0$ e $c > 0$ temos que

$$-2abc = a|bc| + b|ac| < a\tilde{x}^2 + b\tilde{y}^2 \le a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \le c\tilde{z}^2 < |ab|c = abc.$$

Como $abc \mid a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2$, devemos então ter $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = 0$, o que resolve o problema, ou $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = -abc$, mas, nesse caso, temos

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

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

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* $(x,y) \in \mathbb{Q}^2$. De fato, fazendo $\tilde{x} = x + \frac{B}{2A}y$ (podemos supor que $A \neq 0$, se não fazemos uma mudança de coordenadas como $y = \tilde{y} + x$), a curva fica da forma $\tilde{A}\tilde{x}^2 + \tilde{C}\tilde{y}^2 + \tilde{D}\tilde{x} + \tilde{E}\tilde{y} + \tilde{F} = 0$, e, fazendo $\overline{x} = \tilde{x} + \frac{\tilde{D}}{2\tilde{A}}$ e $\overline{y} = \tilde{y} + \frac{\tilde{E}}{2\tilde{C}}$, a curva fica da forma $\overline{A}\overline{x}^2 + \overline{C}\overline{y}^2 + \overline{F} = 0$. Multiplicando pelo mmc dos denominadores dos coeficientes, podemos supor que $\overline{A}, \overline{C}$ e $\overline{F}$ são inteiros, e, escrevendo $\overline{A} = k^2\hat{A}$, $\overline{C} = l^2\hat{C}$ e $\overline{F} = m^2\hat{F}$, com $\hat{A}, \hat{C}$ e $\hat{F}$ livre de quadrados, obtemos fazendo $\hat{x} = \frac{k}{m}\overline{x}$ e $\hat{y} = \frac{l}{m}\overline{y}$ a expressão $\hat{A}\hat{x}^2 + \hat{C}\hat{y}^2 + \hat{F} = 0$. Assim fazendo $\hat{x} = \frac{p}{q}$ e $\hat{y} = \frac{r}{q}$, obtemos a equação

$$\hat{A}p^2 + \hat{C}r^2 + \hat{F}q^2 = 0.$$

Podemos supor $\mathrm{mdc}(\hat{A}, \hat{C}, \hat{F}) = 1$ (se não dividimos por $\mathrm{mdc}(\hat{A}, \hat{C}, \hat{F})$) e que $\mathrm{mdc}(p, r, q) = 1$. Além disso, se $\mathrm{mdc}(\hat{A}, \hat{C}) = d$ devemos ter $d \mid \hat{F}q^2$, e logo $d \mid q$ (pois d é livre de quadrados), donde $q = dq'$, e obtemos a equação

$$\frac{\hat{A}}{d}p^2 + \frac{\hat{C}}{d}r^2 + (\hat{F}d)q'^2 = 0$$

com $\frac{\hat{A}}{d}, \frac{\hat{C}}{d}, \hat{F}d$ livres de quadrados e

$$\left|\frac{\hat{A}}{d}\frac{\hat{C}}{d}\hat{F}d\right| = \left|\frac{\hat{A}\hat{C}\hat{F}}{d}\right| < |\hat{A}\hat{C}\hat{F}| \quad \text{se } d > 1.$$

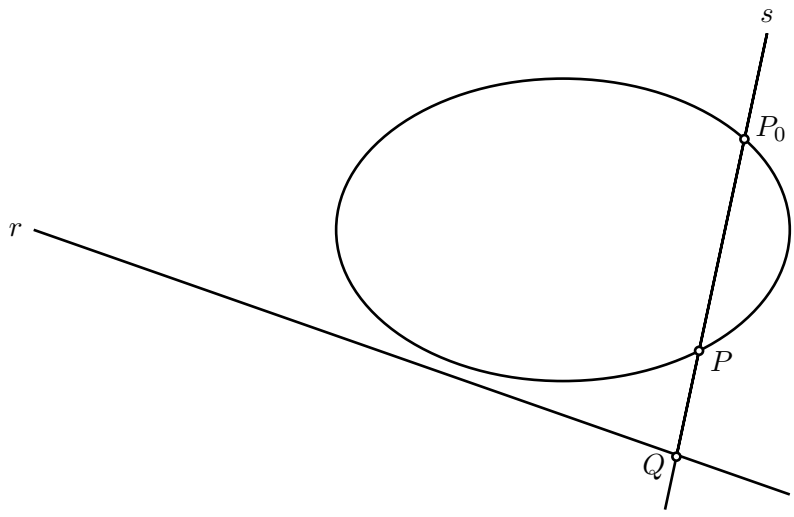
Após algumas reduções deste tipo, obtemos uma equação equivalente como nas hipóteses do teorema de Legendre, que pode então ser usado para decidir a existência de um ponto racional na curva. Note que a hipótese sobre a, b, c não terem o mesmo sinal no teorema de Legendre equivale à existência de pontos reais não triviais na curva.

Se há algum ponto racional (x_0, y_0) numa tal curva, então há infinitos. Isto pode ser visto a partir do exemplo a seguir, que ilustra o método geométrico que permite encontrar todos os pontos racionais explicitamente.

Exemplo 5. *Encontre todos os pontos racionais da elipse*

$$\frac{x^2}{5/2} + \frac{y^2}{5/3} = 1.$$

Solução: É fácil encontrar um destes pontos racionais, digamos $(x, y) = (1, 1)$. Para encontrar os demais, começamos traçando uma reta r de coeficientes racionais paralela à reta tangente à elipse no ponto $P_0 = (1, 1)$. Derivando a equação da elipse em relação à x, obtemos $\frac{2x}{5/2} + \frac{2yy'}{5/3} = 0$ e assim $y' = -2/3$ para $(x, y) = (1, 1)$. Portanto podemos tomar (por exemplo) a reta r de equação $y = -\frac{2}{3}x - 2$. Agora, para um ponto $P \neq P_0$ da elipse, seja s a reta que liga P a $P_0 = (1, 1)$; como esta reta não é paralela a r, temos que r e s determinam um ponto Q, como na figura a seguir.



Vamos mostrar que a associação $P \mapsto Q$ define uma bijeção entre os pontos racionais da elipse, excetuando o ponto P_0, e os pontos racionais da reta r.

Em primeiro lugar, se P é um ponto racional da elipse então a equação da reta s, que liga dois pontos racionais P e P_0, possui coeficientes racionais. Logo Q será um ponto racional, sendo a intersecção de duas retas r e s cujas equações têm coeficientes racionais.

Reciprocamente, suponha que $Q = (a, b)$ é um ponto racional de r. Então a equação da reta s, determinada pelos pontos racionais P_0 e Q, terá coeficientes racionais: $y - 1 = \frac{b-1}{a-1} \cdot (x - 1)$. Como a equação da elipse também tem coeficientes racionais, a intersecção $P \neq P_0$ de s com a elipse será um ponto racional, já que isolando y na equação de s e substituindo na equação da elipse obtemos uma equação quadrática com coeficientes racionais

$$\frac{2}{5}x^2 + \frac{3}{5}\Big(1 + \frac{b-1}{a-1} \cdot (x-1)\Big)^2 - 1 = 0.$$

Sabemos que a abscissa $x = 1$ de P_0 é uma das raízes, logo a outra raiz (que é a abscissa de P) é racional também pelas relações de Girard. Como P pertence à reta s cuja equação tem coeficientes racionais, a ordenada de P também será racional, ou seja, P será um ponto racional.

Após algumas contas, obtemos a seguinte fórmula para P em função de $Q = (a, b)$:

$$P = \Big(\frac{10a^2 + 90a + 21}{10a^2 + 24a + 87}, \frac{10a^2 - 20a - 111}{10a^2 + 24a + 87}\Big).$$

Assim, os pontos racionais P da elipse são obtidos fazendo a percorrer todos os racionais $a \in \mathbb{Q}$ juntamente com $a = \infty$, i.e., o limite para $a \to \infty$ na expressão acima, que fornece o ponto inicial $P_0 = (1, 1)$, que corresponde ao "ponto no infinito" de r, intersecção de r com a reta s tangente à elipse no ponto P_0 (no plano projetivo, é claro!). □

2.1 Soma de Dois Quadrados

Nesta seção, caracterizamos os números que são somas de dois quadrados.

Teorema 6. *Os únicos números que podem se expressar como soma de dois quadrados são os da forma $n = 2^s d^2 l$ onde s é um natural e l é um número livre de quadrados tais que seus fatores primos são da forma $4k + 1$.*

Começamos observando que se p é um primo da forma $4k+3$ que divide $n = a^2+b^2$, então $p \mid a$ e $p \mid b$. De fato, se isto não ocorresse, b seria invertível módulo p, logo de $a^2 \equiv -b^2 \pmod{p}$ teríamos que -1 é resíduo quadrático módulo p, o que é absurdo pois $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = -1$ já que $p \equiv 3 \pmod 4$. Logo $p^2 \mid n$ e repetindo o processo com $\frac{n}{p^2} = (\frac{a}{p})^2 + (\frac{b}{p})^2$ no lugar de n, concluímos que todo primo da forma $4k + 3$ aparece com expoente par na fatoração canônica de n. Assim, apenas os números da forma descrita no teorema podem ser soma de dois quadrados.

Agora todo natural n pode se expressar como $n = k^2 m$ onde k e m são inteiros positivos e m é livre de quadrados, donde se m pode se escrever como soma de dois quadrados $m = a^2 + b^2$ então o mesmo ocorre para $n = (ak)^2 + (bk)^2$. Além disso, se temos dois números que são soma de dois quadrados, digamos $m = a^2 + b^2$ e $n = c^2 + d^2$, então a seguinte identidade de números

complexos

$$\begin{aligned} mn &= (a^2+b^2)(c^2+d^2) = |a+bi|^2 \cdot |c+di|^2 \\ &= |(a+bi)(c+di)|^2 = |(ac-bd)+(ad+bc)i|^2 \\ &= (ac-bd)^2+(ad+bc)^2 \end{aligned}$$

mostra que seu produto também será soma de dois quadrados. Assim, para mostrar que todo n da forma descrita no teorema é soma de dois quadrados, basta mostrar que 2 e todo primo da forma $4k+1$ são somas de dois quadrados. Se $p=2$ temos que $2=1^2+1^2$ é soma de dois quadrados. Para o outro caso, precisamos do seguinte

Lema 7 (Lema de Thue). *Se $m>1$ é um número natural e a é um inteiro primo relativo com m então existem números naturais x e y não nulos menores do que ou iguais a $\sqrt{m}$ e tais que algum dos números $ax \pm y$ é divisível por m.*

Demonstração. Seja $q = \lfloor \sqrt{m} \rfloor$, então $q+1 > \sqrt{m}$ e portanto $(q+1)^2 > m$. Consideremos todos os $(q+1)^2$ números da forma $ax-y$ onde x e y tomam os valores $0, 1, \ldots, q$. Como só existem m restos ao se dividir um número por m, pelo Princípio da Casa dos Pombos dois dos números anteriores, digamos $ax_1 - y_1$ e $ax_2 - y_2$, são congruentes módulo m. Portanto a diferença $a(x_1 - x_2) - (y_1 - y_2)$ é divisível por m. Temos

$$0 \leq x_i, y_i \leq \sqrt{m} \implies |x_1 - x_2|, |y_1 - y_2| \leq \sqrt{m}.$$

Se $x_1 - x_2 = 0$ então $y_1 - y_2$ será divisível por m, o que implica $y_1 = y_2$, mas os pares (x_1, y_1) e (x_2, y_2) são diferentes, uma contradição. De igual forma, se $y_1 - y_2 = 0$ então $a(x_1 - x_2)$ será divisível por m, mas a e m são primos relativos, logo $m \mid x_1 - x_2$ e assim $x_1 = x_2$, outra contradição. Logo $x = |x_1 - x_2|$ e $y = |y_1 - y_2|$ satisfazem as condições do enunciado. □

Retomando o nosso problema inicial, se p é um número primo da forma $4k+1$, então $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1$, logo existe a tal que $p \mid a^2+1$. Aplicando o lema anterior, existem inteiros $0 < x, y < \sqrt{p}$ tais que algum dos números $ax \pm y$ é divisível por p, portanto o número $(ax+y)(ax-y) = a^2x^2 - y^2$ é divisível por p. Daqui

$$x^2 + y^2 = x^2 + a^2x^2 - a^2x^2 + y^2 = x^2(a^2+1) - (a^2x^2 - y^2)$$

é divisível por p, mas como $0 < x, y < \sqrt{p}$ então $0 < x^2 + y^2 < 2p$, portanto $p = x^2 + y^2$. Isto encerra a prova do teorema.

O método anterior pode ser aplicado para obter outras representações de números primos.

Exemplo 8. *Sejam $d \in \{1, 2, 3, 7\}$ e p é primo ímpar tal que $\left(\frac{-d}{p}\right) = 1$, então existem $e, f \in \mathbb{N}$ tais que $p = e^2 + df^2$.*

SOLUÇÃO: Seja $a \in \mathbb{N}$ tal que $a^2 \equiv -d \pmod{p}$. Pelo lema de Thue, existem inteiros x, y tais que $(x + ay)(x - ay) \equiv 0 \pmod{p} \iff p \mid x^2 + dy^2$ e $0 < x^2 + dy^2 < (d+1)p$. Assim, temos

$$x^2 + dy^2 = kp \qquad \text{com } k \in \{1, 2, \cdots, d\}.$$

Observemos que se $k = d$, x é múltiplo de d e fazendo $x = dz$ temos que $dz^2 + y^2 = p$. Assim podemos desconsiderar este caso e se $d = 1$ ou $d = 2$ o problema está resolvido. Consideremos agora os outros valores de d:

1. Se $d = 3$ então $x^2 + 3y^2 = p$ ou $2p$. No caso $x^2 + 3y^2 = 2p$ temos que x e y têm a mesma paridade, assim se x, y são pares temos que $4 \mid x^2 + 3y^2 = 2p$, que é contraditório, e no caso em que x, y ímpares temos que $x^2 \equiv y^2 \equiv 1 \pmod{8}$, portanto $2p = x^2 + 3y^2 \equiv 4 \pmod{8}$, que também é contraditório. Assim concluímos que $x^2 + 3y^2 = p$.

2. Se $d = 7$ então $x^2 + 7y^2 = ip$ com $i \in \{1, 2, 3, 4, 5, 6\}$. No caso que x, y são ímpares, como $x^2 \equiv y^2 \equiv 1 \pmod{8}$, temos que $x^2 + 7y^2 \equiv 0 \pmod{8}$, o que é contraditório, e no caso em que x, y são pares, dividimos toda a expressão por 4, logo podemos supor que i é ímpar. Assim resta considerar os casos em que $i = 3$ ou 5. Mas -7 não é resto quadrático módulo 3 nem 5, portanto $x^2 + 7y^2 = p$.

□

Problemas Propostos

Problema 9. *Encontrar todos os triângulos ABC tais que $\angle A = 2\angle B$ e seus lados a, b e c são inteiros.*

Problema 10. *Se no problema anterior fixamos $b = n$, quantos triângulos satisfazem as condições acima?*

Problema 11. *Dado um número inteiro n, de quantos triângulos retângulos com lados inteiros é n o comprimento de um cateto?*

Problema 12. *Dado um número inteiro n, de quantos triângulos retângulos com lados inteiros é n o comprimento da hipotenusa?*

Problema 13. *Demonstrar que a equação $x^2 + y^2 = 3z^2$ não tem soluções inteiras positivas.*

Problema 14. *Encontrar todas as soluções inteiras da equação $x^2 + y^2 = 5z^2$.*

Problema 15. *Encontrar infinitas triplas primitivas de números (a, b, c) tais que a^3, b^3 e c^3 estão em progressão aritmética.*

Problema 16. *Encontrar infinitas triplas primitivas de números (a, b, c) tais que a^4, b^4 e c^4 estão em progressão aritmética.*

Problema 17. *Demonstrar que todas as soluções inteiras de* $x^2 + y^2 + z^2 = t^2$ *são dadas por*

$$\begin{aligned} x &= d(m^2 - n^2 - p^2 + q^2) \\ y &= d(2mn - 2pq) \\ z &= d(2mp + 2nq) \\ t &= d(m^2 + n^2 + p^2 + q^2). \end{aligned}$$

Problema 18 (APMO2002)**.** *Encontrar todos os pares* m, n *de inteiros positivos tais que* $m^2 - n$ *divide* $m + n^2$ *e* $n^2 - m$ *divide* $m^2 + n$*.*

Problema 19 (APMO1999)**.** *Encontrar todos os pares* m, n *de inteiros tais que* $m^2 + 4n$ *e* $n^2 + 4m$ *são ambos quadrados perfeitos.*

Problema 20 (AusPol1994)**.** *Encontrar todas as soluções inteiras de*

$$\frac{(a+b)(b+c)(c+a)}{2} + (a+b+c)^3 = 1 - abc.$$

Problema 21 (IMO1982)**.** *Demonstre que se* n *é um inteiro positivo tal que a equação*

$$x^3 - 3xy^2 + y^3 = n$$

tem uma solução com x, y *inteiros, então ela tem ao menos três soluções inteiras. Mostre que esta equação não possui soluções inteiras para* $n = 2891$*.*

Problema 22 (OIbM2001)**.** *Seja* n *um inteiro positivo. Demonstrar que o número de soluções inteiras* (x, y) *da equação*

$$x^2 - xy + y^2 = n$$

é finito e múltiplo de 6.

Dicas e Soluções

Em breve.

Referências

[1] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.