Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 2

Prof. Samuel Feitosa

Aula 12

# Equações Diofantinas II

Continuaremos nosso estudo das equações diofantinas abordando agora algumas equações quadráticas. Começaremos peloo clássico problema das ternas pitagóricas.

Desejamos encontrar todas as soluções $(x, y, z)$ da equação:

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

em inteiros positivos. Seja $d = mdc(x, y)$. Como $d^2 \mid z^2$, segue que $d \mid z$ e que $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ também é solução. Além disso, podemos concluir que:

$$mdc(x/d, y/d) = mdc(x/d, z/d) = mdc(y/d, z/d) = 1.$$

Uma terna que é solução e possui a propriedade de que quaisquer dois de seus termos são primos entre si, será chamada de solução primitiva. Assim, toda solução $(x, y, z)$ é da forma $(dx_1, dy_1, dz_1)$ onde $(x_1, y_1, z_1)$ é uma solução primitiva. Para cumprimirmos nosso objetivo, bastará nos concentrarmos em encontrar todas as soluções primitivas. Analisando a equação módulo 4 e lembrando que todo quadrado perfeito pode deixar apenas os restos 0 ou 1, concluímos que exatamente um dentre $x$ e $y$ é par. Suponha sem perda de generalidade que $y$ seja par. Fatorando a equação, obtemos:

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

Como $mdc((z+x)/2, (z-x)/2) = 1$, concluímos que $(z+x)/2$ e $(z-x)/2$ devem ser ambos quadrados perfeitos, i.e., existem inteiros positivos $r$ e $s$, com $r > s$ e $mdc(r, s) = 1$, tais que $(z + x)/2 = r^2$ e $(z - x)/2 = s^2$ (veja o primeiro problema proposto). Consequentemente, $x = r^2 - s^2$, $y = 2rs$ e $z = r^2 + s^2$. Reciprocamente, se $(x, y, z) = (r^2 - s^2, 2rs, r^2 + s^2)$, temos:

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

O próximo teorema resume nossa discussão original:

**Teorema 1.** *Todas as soluções primitivas de $x^2+y^2=z^2$ com $y$ par são da forma $x=r^2-s^2$, $y=2rs$ e $z=r^2+s^2$, onde $r$ e $s$ são inteiros de paridade oposta com $r>s>0$ e $mdc(r,s)=1$.*

**Exemplo 2.** *Encontre todas as ternas pitagóricas $(a,b,c)$ tais que $a+b+c=1000$.*

Seja $k=mdc(a,b,c)$ e suponha sem perda de generalidade que $b/k$ é par. Pelo teorema anterior, $(a,b,c)=(k(x^2-y^2),k(2xy),k(x^2+y^2))$, onde $x>y$, $mdc(x,y)=1$ e pelo menos um dentre $x$ e $y$ par. Assim, $(x^2-y^2)+2xy+(x^2+y^2)=2x(x+y)$ é um divisor de 1000. Com mais razão, $x(x+y)\mid 500$. Usando que $mdc(x,x+y)=1$ e a fatoração em primos de 500, podemos concluir que um deles é uma potência de 5 e o outro uma potência de 2. Veja que $x$ não pode ser uma potência de 5 pois nesse caso $y$ deveria ser ímpar para garantir que $x+y$ seja uma potência de 2. Assim, $x\mid 500$ e $x=2^k$, produzindo como possibilidades $x=1,2$ ou 4. Analisando cada um desses casos e levando em conta que $y<x$, é fácil encontrar que $x=4$ e $y=1$ são as únicas opções possíveis. Nesse caso, $x=15, y=8$ e $z=17$. Consequentemente, $(a,b,c)=(20\cdot 15, 20\cdot 8, 20\cdot 17)$.

**Exemplo 3.** *Mostre que se $a$, $b$ e $c$ são inteiros positivos tais que $a^2+b^2=c^2$, então $(ab)^4+(bc)^4+(ca)^4$ é um quadrado perfeito.*

Veja que:

$$(ab)^4+(bc)^4+(ca)^4=(a^2b^2+b^4)^2+(a^2b^2)^2+(a^2b^2+a^4)^2=(a^4+a^2b^2+b^4)^2.$$

**Exemplo 4.** *Encontre todas as soluções de $x^2+2y^2=z^2$ em inteiros positivos com $mdc(x,y,z)=1$.*

Como $2y^2\equiv 0 \pmod 2$, devemos ter $x\equiv z \pmod 2$. Além disso, se fosse $x\equiv z\equiv 0 \pmod 2$ teríamos $4\mid z^2-x^2=2y^2$ e consequentemente $2\mid y$, contradizendo a hipóstese $mdc(x,y,z)=1$. Fatorando a expressão, temos:

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

Como $mdc(x,z)=1$ e ambos são ímpares; $mdc(z-x,z+x)=2$ e apenas um deles é côngruo à 2 (mod 4). Temos dois casos a considerar: 1) $z+x\equiv 0 \pmod 4$ e $z-x\equiv 2 \pmod 4$. Nesse caso, $y^2=(z-x)/2\cdot(z+x)$ com $mdc((z-x)/2,(z+x))=1$. Daí, existem inteiros positivos $r$ e $s$ tais que $(z-x)/2=r^2$ e $(z+x)/2=s^2$, produzindo a solução $(x,y,z)=((s^2-2r^2)/2, rs, (2r^2+s^2)/2)$ com $mdc(r,s)=1$ e $s\equiv 0 \pmod 2$. Um raciocínio análogo para o caso $z+x\equiv 2 \pmod 4$ e $z-x\equiv 0 \pmod 4$ produz $(x,y,z)=((2s^2-r^2)/2, rs, (r^2+2s^2)/2)$ com $mdc(r,s)=1$ e $r\equiv 0 \pmod 2$.

**Problema 5.** *(USAMO 1976) Encontre todas as soluções naturais da equação*

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

A equação pode ser reescrita como:

$$c^2=(a^2-1)(b^2-1)-1.$$

Se pelo menos um dentre $a$ ou $b$ é ímpar, teremos $c^2 \equiv 3 \pmod 4$. Como os quadrados perfeitos só podem deixar resto 0 ou 1 (mod 4), temos um absurdo. Portanto, $a$, $b$ e consequentemente $c$ são números pares. Seja $k$ o maior inteiro tal que $2^k$ divida esses três números. Assim, $a = 2^x$, $b = 2^k y$, $c = 2^k z$ onde pelo menos um dentre $x, y$ e $z$ ímpar. Assim,

$$x^2 + y^2 + z^2 = 2^{2r} x^2 y^2.$$

Como $r > 0$, $x^2 + y^2 + z^2 \equiv 0 \pmod 4$. Entretanto, isso não é possível se um dentre os $x, y, z$ é ímpar pois a soma só poderia ser congruente à $1, 2, 3 \pmod 4$.

**Exemplo 6.** *(Extraído de [1]) Determine todas as ternas $(a, b, c)$ de inteiros positivos tais que $a^2 = 2^b + c^4$.*

Como $a^2 = 2^b + c^4 \iff (a - c^2)(a + c^2) = 2^b$, pelo Teorema Fundamental da Aritmética existem dois naturais $m > n$ tais que $m + n = b$, $a - c^2 = 2^n$ e $a + c^2 = 2^m$. Subtraindo as duas últimas equações, obtemos que $2c^2 = 2^m - 2^n$, assim $c^2 = 2^{n-1}(2^{m-n} - 1)$. Como $2^{n-1}$ e $2^{m-n} - 1$ são primos entre si e o seu produto é um quadrado perfeito (i.e. os expoentes das potências de primos distintos são pares), novamente pelo Teorema Fundamental da Aritmética $2^{n-1}$ e $2^{m-n} - 1$ devem ser ambos quadrados perfeitos, logo $n - 1$ é par e $2^{m-n} - 1 = (2k-1)^2$ para algum inteiro positivo $k$. Como $2^{m-n} = (2k-1)^2 + 1 = 4k(k-1) + 2$ é divisível por 2 mas não por 4, temos $m - n = 1$. Assim, fazendo $n - 1 = 2t$, temos que todas as soluções são da forma $(a, b, c) = (3 \cdot 2^{2t}, 4t + 3, 2^t)$ com $t \in \mathbb{N}$ e é fácil verificar que todos os números desta forma são soluções.

O próximo exemplo ilustrará o método da descida de Fermat que faz uso do princípio da boa ordenação: todo subconjunto não vazio de inteiros positivos possui um elemento mínimo.

**Exemplo 7.** *Determine todas as soluções da equação $x^4 + y^4 = z^2$ em inteiros positivos com $mdc(x, y) = 1$.*

Como $(x^2)^2 + (y^2)^2 = z^2$ e $mdc(x^2, y^2) = 1$, podemos usar o primeiro teorema para concluir que existem $u$ e $v$ tais que $x^2 = u^2 - v^2$, $y^2 = 2uv$, $z = u^2 + v^2$, $u > v > 0$ e $mdc(u, v) = 1$ (Estamos assumindo sem perda de generalidade que $x$ é ímpar). Se $u$ é par, então $v$ será ímpar e teremos $x^2 \equiv 3 \pmod 4$. Como isso é um absurdo, $u$ deve ser ímpar e $v$ deve ser par. Sendo assim, $(y/2)^2 = u \cdot v/2$ com $mdc(u, v/2) = 1$. Devemos ter $u = r^2$, $v/2 = s^2$, com $mdc(r, s) = 1$, $r, s > 0$, $r$ ímpar e $y = 2rs$. Além disso, como $x^2 + v^2 = u^2$, obtemos $x^2 + 4s^2 = r^4$. Como $mdc(r, 2s) = 1$, novamente pelo primeiro teorema, existem $m$ e $n$ tais que $x = m^2 - n^2$, $2s^2 = 2mn$ e $r^2 = m^2 + n^2$ com $mdc(m, n) = 1$ e $m > n > 0$. Como $mn = s^2$, podemos escrever $m = f^2$ e $n = g^2$ com $f, g > 0$ e $mdc(f, g) = 1$. Portanto, $r^2 = f^4 + g^4$. Note que dada a solução em inteiros positivos $(x, y, z)$, obtivemos outra solução $(f, g, r)$, também nos inteiros positivos, com $0 < r < z$. Isso nos diz que existe uma infinidade decrescente de possíveis valores para o inteiro positivo $z$ e naturalmente obtemos uma contradição do princípio da boa ordenação. Sendo assim, a equação anterior não possui solução nos inteiros positivos.

**Observação 8.** *Outra maneira de formalizar o argumento anterior é escolher dentre as ternas nos inteiros positivos que são soluções, aquela com $z$ mínimo. A nova terna $(f, g, r)$ caracterizaria um absurdo.*

**Exemplo 9.** *Prove que para todo inteiro $n > 2$, existem inteiros positivos $p$ e $q$ tais que $n^2 + q^2 = p^2$.*

Fatorando a expressão, obtemos $n^2 = (p-q)(p+q)$. Se $n$ é ímpar, podemos encontrar $p$ e $q$ tais que $p+q = n^2$ e $p-q = 1$, bastando para isso resolver o sistema originado, obtendo $(n, q, p) = (n, \frac{n^2-1}{2}, \frac{n^2+1}{2})$. Se $n$ é par, podemos fazer algo semelhante e encontrar $p$ e $q$ tais que $p+q = n^2/2$ e $p-q = 2$, cuja solução é $(n, q, p) = (n, \frac{n^2}{4} - 1, \frac{n^2}{4} + 1)$.

**Exemplo 10.** *(Extraído de [3]) Prove que a equação*

$$x^2 + y^2 + z^2 + w^2 = 2xyzw \tag{1}$$

*não possui soluções inteiras positivas.*

Por contradição, suponha que (1) possua pelo menos uma solução não-trivial, digamos $(x_0, y_0, z_0, w_0)$. Se $x_0, y_0, z_0, w_0$ forem todos ímpares, o lado esquerdo é um múltiplo de 4 e o lado direito não. Se apenas um ou três deles forem pares, o lado esquerdo é ímpar e o direito é par. Se dois deles forem pares e dois forem ímpares, o lado direito é um múltiplo de quatro e o esquerdo não. Desse modo, $x_0, y_0, z_0, w_0$ são todos pares, ou seja, $x_0 = 2x_1$, $y_0 = 2y_1$, $z_0 = 2z_1$ e $w_0 = 2w_1$. Substituindo em (1) e dividindo por quatro, concluímos que $x_1, y_1, z_1, w_1$ satisfazem a igualdade

$$x_1^2 + y_1^2 + z_1^2 + w_1^2 = 8x_1y_1z_1w_1.$$

Com uma análise de paridades análoga à acima, obtemos $x_1 = 2x_2$, $y_1 = 2y_2$, $z_1 = 2z_2$ e $w_1 = 2w_2$, e daí

$$x_2^2 + y_2^2 + z_2^2 + w_2^2 = 32x_2y_2z_2w_2.$$

Procedendo dessa maneira, $x_0, y_0, z_0, w_0$ devem ser todos múltiplos de $2^n$, qualquer que seja $n \geq 1$. Então $x_0 = y_0 = z_0 = w_0 = 0$, absurdo.

**Exemplo 11.** *(Extraído de [3]) Encontre todas as quadrúplas $(x, y, z, k)$ de números inteiros, com $x, y, z > 0$ e $k \geq 0$, tais que*

$$x^6 + y^6 + z^6 = 4826 \cdot 7^k.$$

Vamos mostrar o seguinte fato:

$$(x, y, z, k) \text{ é solução, com } k \geq 1 \iff (x/7, y/7, z/7, k-6) \text{ é solução, e nesse caso } k \geq 6.$$

($\Longrightarrow$) Temos $x^6 + y^6 + z^6 \equiv 0 \pmod 7$. Como $x^6, y^6, z^6 \equiv 0$ ou $1 \pmod 7$, devemos ter $x, y, z$ múltiplos de 7. Daí, $7^6 | 4826 \cdot 7^k \Rightarrow 7^6 | 7^k \Rightarrow k \geq 6$. Ademais, vale a igualdade

$$\left(\frac{x}{7}\right)^6 + \left(\frac{y}{7}\right)^6 + \left(\frac{z}{7}\right)^6 = 4826 \cdot 7^{k-6},$$

ou seja, $(x/7, y/7, z/7, k-6)$ também é solução.
($\Longleftarrow$) Claro.

O fato acima garante que podemos ir subtraindo 6 de $k$ e retirando um fator 7 de $x$, $y$, $z$ enquanto $k \geq 1$, até que o expoente de 7 no lado direito da igualdade seja 0. Em outras palavras, existe $n \geq 0$ tal que $k = 6n$, com $x = 7^n \cdot x_0$, $y = 7^n \cdot y_0$, $z = 7^n \cdot z_0$, e

$$x_0{}^6 + y_0{}^6 + z_0{}^6 = 4826.$$

A equação acima só tem a solução $(1, 3, 4)$ e suas permutações. Assim, as soluções da equação original são $(7^n, 3 \cdot 7^n, 4 \cdot 7^n, 6n)$, $n \geq 0$, e suas permutações nas três primeiras coordenadas.

## Problemas Propostos

**Problema 12.** *Mostre que se $a \cdot b = x^2$ e $mdc(a, b) = 1$ então existem $r$ e $s$ tais que $a = r^2$ e $b = s^2$.*

**Problema 13.** *Prove que todas as soluções positivas da equação $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$ com $mdc(x, y, z) = 1$ são dadas por*

$$(x, y, z) = (r^4 - s^4, 2rs(r^2 + s^2), rs(r^2 - s^2))$$

*ou*

$$(x, y, z) = (2rs(r^2 + s^2), r^4 - s^4, rs(r^2 - s^2)),$$

*onde $r > s > 0$, $mdc(r, s) = 1$ e $r$ e $s$ de paridades opostas.*

**Problema 14.** *Encontre todos os pares de racionais $(x, y)$ tais que $x^2 + y^2 = 1$.*

**Problema 15.** *Resolva simultaneamente em inteiros positivos:*

$$\begin{aligned} a^2 + b^2 &= c^2 \\ a^2 + c^2 &= d^2 \end{aligned}$$

*onde $a, b, c$ e $d$ são inteiros positivos relativamente primos entre si dois dois.*

**Problema 16.** *(Torneio das Cidades 1997) Prove que a equação*

$$x^2 + y^2 - z^2 = 1997$$

*tem infinitas soluções inteiras $(x, y, z)$.*

**Problema 17.** *Encontre todas as soluções inteiras de $x^2 + y^2 + z^2 = t^2$.*

**Problema 18.** *Encontre todas as soluções de $5m^2 + n^2 = 5^{2011}$*

**Problema 19.** *Encontre todas as soluções em números naturais $m$ e $n$ da equação:*

$$m^2 = 1 + 2 + \ldots + n.$$

## 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.

[2] E. Carneiro, O. Campos and F. Paiva, Olimpíadas Cearenses de Matemática 1981-2005 (Níveis Júnior e Senior), Ed. Realce, 2005.

[3] S. B. Feitosa, B. Holanda, Y. Lima and C. T. Magalhães, Treinamento Cone Sul 2008. Fortaleza, Ed. Realce, 2010.

[4] D. Fomin, A. Kirichenko, Leningrad Mathematical Olympiads 1987-1991, MathPro Press, Westford, MA, 1994.

[5] D. Fomin, S. Genkin and I. Itenberg, Mathematical Circles, Mathematical Words, Vol. 7, American Mathematical Society, Boston, MA, 1966.

[6] I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction to the Theory of Numbers.