POLOS OLÍMPICOS DE TREINAMENTO INTENSIVO

Problemas Resolvidos

Nível 2

Equações diofantinas III

Material elaborado por Valentino Amadeus Sichinel

Problemas

Problema 1. Encontre todas as soluções em inteiros x, y, z, t da equação:

$$x^2 + y^2 + z^2 = 8t - 1.$$

Problema 2. Encontre todas as soluções em inteiros positivos da equação

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1.$$

Problema 3. Mostre que para todo inteiro z existem inteiros x e y tais que

$$x^2 - y^2 = z^3.$$

Problema 4. Encontre todas as soluções de

$$1 + x + x^2 + x^3 = 2^y$$

em inteiros positivos x e y.

Problema 5. Mostre que a equação diofantina

$$5m^2 - 6mn + 7n^2 = 1988$$

não possui solução nos inteiros.

Problema 6 (Rússia 1996)**.** Sejam x, y, p, n, k números inteiros positivos tais que

$$x^n + y^n = p^k.$$

Prove que, se $n > 1$ é ímpar, e p é um número primo, então n é uma potência de p.

Problema 7 (OBM 2009)**.** Prove que não existem inteiros positivos x e y tais que

$$x^3 + y^3 = 2^{2009}.$$

Soluções

1. Um quadrado perfeito só pode deixar resto 0, 1 ou 4, quando dividido por 8. Dessa forma, se x, y e z são inteiros, $x^2 + y^2 + z^2$ pode deixar qualquer resto quando dividido por 8, à exceção de 7.

Como $8t - 1 \equiv 7 \pmod 8$, seja qual for $t \in \mathbb{Z}$, concluímos que não existem inteiros x, y, z, t satisfazendo a equação enunciada.

2. Seja (a, b, c) uma solução. Sem perdas, suponhamos que $a \geq b \geq c$. Como

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1 \iff ab + bc + ca = abc \iff bc = a(bc - b - c), \tag{1}$$

bc é divisível por a. Dessa forma, existe k inteiro positivo tal que $bc = ak$. Substituindo no lado direito da última igualdade acima, ficamos com

$$bc = a(ak - b - c).$$

Se $k \geq 3$, isso nos dá

$$bc = a(ak - b - c) \geq a(3a - b - c) \geq a(3a - a - a) \geq a^2.$$

Por outro lado, $a \geq b \geq c$ implica $a^2 \geq bc$, com igualdade se, e somente se, $a = b = c$. Daí, $a = b = c$. Substituindo na equação original, obtemos

$$\frac{3}{a} = 1,$$

o que implica $a = 3$.

Dessa forma, encontramos a primeira solução $(a, b, c) = (3, 3, 3)$.

Restam somente os casos $k = 2$ e $k = 1$.

Se $k = 2$, temos $bc = 2a$, donde

$$bc = a(bc - b - c) \Rightarrow 2a = a(bc - b - c) \Rightarrow 2 = bc - b - c \Rightarrow 2 + c = bc - b. \tag{2}$$

Portanto, neste caso, $b \mid 2 + c$. Como $b \geq c \geq 2$, segue que ou $2 + c = 2b$, caso em que $b = c = 2$, ou $2 + c = b$. Não podemos ter $b = c = 2$ porque, nesse caso, teríamos $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1 + \frac{1}{a}$. Logo, $c + 2 = b$.

Substituindo em (2), encontramos

$$b = bc - b \Rightarrow 1 = c - 1 \Rightarrow c = 2.$$

Assim, $c = 2$, $b = c + 2 = 4$, e temos $a = \frac{bc}{2} = 4$.

Isso nos leva à nossa segunda solução: $(a, b, c) = (4, 4, 2)$.

Resta, agora, apenas o caso $k = 1$. Neste caso, temos $bc = a$.

Substituindo em (1), ficamos com

$$bc = a(bc - b - c) \Rightarrow a = a(bc - b - c) \Rightarrow 1 = bc - b - c \Rightarrow 1 + c = b(c - 1). \tag{3}$$

b divide $c + 1$. Como $b \geq c$ e $b \geq 2$, só podemos ter $b = c + 1$. Substituindo em (3), encontramos

$$1 + c = b(c - 1) \Rightarrow b = b(c - 1) \Rightarrow 1 = c - 1 \Rightarrow c = 2.$$

Logo, $c = 2$, $b = c + 1 = 3$, $a = bc = 6$, e temos uma terceira solução: $(a, b, c) = (6, 3, 2)$.

Portanto, as soluções inteiras positivas para a equação do enunciado são, a menos de permutação,[1] $(3, 3, 3)$, $(4, 4, 2)$ e $(6, 3, 2)$.

[1] Lembre-se de que supomos, no início da solução, que $a \geq b \geq c$.

3. Seja z um inteiro. Temos

$$x^2 - y^2 = z^3 \iff (x-y)(x+y) = z^3.$$

Se conseguirmos mostrar que existem x e y tais que $x - y = z$ e $x + y = z^2$, teremos resolvido o problema.

Ora, o sistema

$$\begin{cases} x - y = z \\ x + y = z^2 \end{cases}$$

é fácil de resolver: sua única solução é

$$(x, y) = \Big(\frac{z^2+z}{2}, \frac{z^2-z}{2}\Big).$$

Como tanto $\frac{z^2+z}{2}$ quanto $\frac{z^2-z}{2}$ são inteiros, isso mostra que somos capazes de obter os inteiros por que procurávamos.

4. Podemos fatorar o lado esquerdo da equação: temos

$$1 + x + x^2 + x^3 = \frac{x^4-1}{x-1} = \frac{(x^2-1)(x^2+1)}{x-1} = \frac{(x-1)(x+1)(x^2+1)}{x-1} = (x+1)(x^2+1).$$

Dessa forma, queremos inteiros positivos x e y tais que

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

Para que seu produto seja uma potência de 2, $(x+1)$ e (x^2+1) devem ser ambos potências de 2. Os únicos restos que um quadrado perfeito pode deixar quando divido por 4, no entanto, são 0 e 1. Dessa forma, (x^2+1) deixa resto 1 ou 2 quando dividido por 4. Como x deve ser positivo, (x^2+1) não pode ser igual a 1 e, portanto (sendo potência de 2), não pode deixar resto 1 quando dividido por 4. Dessa forma, (x^2+1) deixa resto 2 quando dividido por 4. Como a única potência de 2 que iguala tal feito é 2, devemos ter $x^2 + 1 = 2$.

Como x é positivo, segue que $x = 1$. De $1 + x + x^2 + x^3 = 2^y$ concluímos que $4 = 2^y$, isto é, $y = 2$.

Portanto, a única solução em inteiros positivos para a equação apresentada é

$$(x, y) = (1, 2).$$

5. Seja (m, n) uma hipotética solução inteira para a equação. Veja que

$$\begin{aligned}
5m^2 - 6mn + 7n^2 = 1988 &\iff 100m^2 - 120mn + 140n^2 = 20 \cdot 1988 \\
&\iff 100m^2 - 120mn = 20 \cdot 1988 - 140n^2 \\
&\iff 100m^2 - 120mn + 36n^2 = 20 \cdot 1988 - 140n^2 + 36n^2 \\
&\iff (10m - 6n)^2 = 20 \cdot 1988 - 104n^2,
\end{aligned}$$

donde $20 \cdot 1988 - 104n^2$ há de ser um quadrado perfeito.

(Obs.: Você poderia ter chegado à mesma conclusão através da fórmula de Bhaskara.)

Dessa forma, $20 \cdot 1988$ é um quadrado perfeito módulo 13 (veja que $13 \mid 104$). Será que isso acontece de fato?

Uma fatoração rápida mostra-nos que $1988 = 4 \cdot 7 \cdot 71$. Assim, $20 \cdot 1988 = 16 \cdot 5 \cdot 7 \cdot 71$ é quadrado módulo 13 se, e somente se, $5 \cdot 7 \cdot 71$ é quadrado módulo 13. No entanto,[1]

$$\begin{aligned}
\left(\frac{5 \cdot 7 \cdot 71}{13}\right) &= \left(\frac{5}{13}\right) \cdot \left(\frac{7}{13}\right) \cdot \left(\frac{71}{13}\right) \\
&= \left(\frac{13}{5}\right) \cdot \left(\frac{13}{7}\right) \cdot \left(\frac{6}{13}\right) \\
&= (-1) \cdot (-1) \cdot \left(\frac{2}{13}\right) \cdot \left(\frac{3}{13}\right) \\
&= \left(\frac{2}{13}\right) \cdot \left(\frac{13}{3}\right) \\
&= (-1) \cdot 1 \\
&= -1.
\end{aligned}$$

A contradição mostra que não existe solução inteira (m, n) para a equação $5m^2 - 6mn + 7n^2 = 1988$, tal como queríamos.

6. Antes de mais nada, mostraremos que podemos supor que $p \nmid x$ e $p \nmid y$.

Escrevamos $x = p^a x'$ e $y = p^b y'$, com $p \nmid x'$ e $p \nmid y'$. Sem perdas, suponhamos que $a \geq b$. Temos então

$$p^{na} x'^n + p^{nb} y'^n = p^k \;\Rightarrow\; p^{n(a-b)} x'^n + y'^n = p^{k-nb}.$$

Se $a - b \neq 0$, o lado esquerdo da igualdade acima não é divisível por p. Logo, nesse caso, temos de ter $p^{k-nb} = 1$. Mas

$$p^{n(a-b)} x'^n + y'^n \geq p^{a-b} + 1.$$

Absurdo! Logo, $a - b = 0$, e (1) reescreve-se como

$$x'^n + y'^n = p^{k-nb},$$

com $p \nmid x'$ e $p \nmid y'$.

Como a conclusão a que queremos chegar diz respeito a n somente, segue daí que podemos supor, sem perdas, que $p \nmid x$ e $p \nmid y$.

Voltemos então ao cenário original, desta vez com nossa mais nova suposição em mãos (isto é, a de que p não divide nem x, nem y).

Por absurdo, suponhamos que existe um primo $q \neq p$ tal que $q \mid n$, e seja l tal que $n = ql$. Como l é ímpar (l não pode ser par, porque n é ímpar), podemos escrever

$$x^n + y^n \;=\; (x^q)^l + (y^q)^l \;=\; \big(x^q + y^q\big)\big((x^q)^{l-1} - (x^q)^{l-2} y^q + \cdots - x^q (y^q)^{l-2} + (y^q)^{l-1}\big).$$

Assim, já que $x^n + y^n$ é uma potência de p, $x^q + y^q$ também é uma potência de p.

Uma fatoração similar à que utilizamos acima nos dá

$$x^q + y^q \;=\; (x + y)(x^{q-1} - x^{q-2} y + \cdots - x y^{q-2} + y^{q-1}).$$

Daí, vem que

$$x + y \;\equiv\; 0 \pmod{p}, \quad \text{isto é,} \quad x \;\equiv\; -y \pmod{p}$$

[1] A partir daqui, nesta solução, $\left(\frac{a}{b}\right)$ é o *símbolo de Legendre*. Nas igualdades que se seguem, utilizamos várias vezes a Lei da Reciprocidade Quadrática.

e

$$x^{q-1} - x^{q-2}y + \cdots - xy^{q-2} + y^{q-1} \equiv 0 \pmod{p}.$$

Substituindo a primeira na segunda, ficamos com

$$y^{q-1} + y^{q-1} + \cdots + y^{q-1} + y^{q-1} \equiv 0 \pmod{p},$$

isto é,

$$qy^{p-1} \equiv 0 \pmod{p}.$$

Mas $p \nmid q$, já que p e q são primos distintos. Por outro lado, $p \nmid y$. Absurdo!

A contradição mostra que a hipótese que fizemos é absurda. Portanto, não existe primo q, distinto de p, que divide n e, assim, n é uma potência de p.

7. Pelo Pequeno Teorema de Fermat, $2^6 \equiv 1 \pmod{7}$. Daí,

$$2^{2009} \equiv 2^{6\cdot 334+5} \equiv (2^6)^{334} \cdot 2^5 \equiv 2^5 \equiv 32 \equiv 4 \pmod{7}.$$

Por outro lado, os possíveis restos de um cubo perfeito módulo 7 são 0, 1 e 6, donde os possíveis resto da soma de dois cubos perfeitos módulo 7 são 0, 1, 2, 5 e 6. Assim, não é possível que existam inteiros x e y tais que

$$x^3 + y^3 = 2^{2009}.$$
