Métodos em Equações Diofantinas

Prof. George Lucas

Semana Olímpica 2023 - Nível 2

Uma equação diofantina é uma equação da forma $f(x_1, x_2, \ldots, x_n) = 0$ onde f é uma função de $n \geq 2$ variáveis. Geralmente queremos achar soluções (possivelmente todas) inteiras (ou naturais) $(x_1, x_2, \ldots, x_n)$ dessa equação.

É claro que as soluções dessa equação dependem tanto de f quanto de n , o que torna o estudo das equações diofantinas extremamente interessante. Vejamos a seguir alguns métodos que podem nos ajudar a resolver equações desse tipo.

1 O método da decomposição.

Esse método é relativamente simples. Se temos uma equação da forma

$$f_1(x_1, x_2, \ldots, x_n) f_2(x_1, x_2, \ldots, x_n) \ldots f_k(x_1, x_2, \ldots, x_n) = a,$$

onde $f_1, f_2, \ldots, f_k$ são funções fixas que levam cada n-úpla de inteiros em um número inteiro e $a \in \mathbb{Z}$ também fixo, então teremos que:

$$f_1(x_1, x_2, \ldots, x_n) = a_1$$
$$f_2(x_1, x_2, \ldots, x_n) = a_2$$
$$\ldots$$
$$f_k(x_1, x_2, \ldots, x_n) = a_k$$

Onde $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ e $a_1 a_2 \ldots a_k = a$.

Exemplo 1: Determine todas as soluções inteiras (x, y) da equação $x^2 - y^2 = 2023$.

Solução: Fatorando obtemos $(x + y)(x - y) = 2023$. Assim, $x + y = a_1$ e $x - y = a_2 \rightarrow x = \frac{a_1 + a_2}{2}$, $y = \frac{a_1 - a_2}{2}$, onde $a_1 a_2 = 2023$. Olhando para os divisores de 2023 vemos que (a_1, a_2) pode assumir os pares

$$(1,2023), (7,289), (17,119), (119, 17), (289,7), (2023,1), (-1,-2023),$$
$$(-7, -289), (-17, -119), (-119, -17), (-289, -7), (-2023, -1),$$

obtendo respectivamente as soluções

$$(1012,-1011), (148,-141), (68,-51), (68,51), (148,141), (1012,1011),$$
$$(-1012,1011), (-148, 141), (-68, 51), (-68, -51), (-148,-141), (-1012, -1011),$$

que são todas as soluções do problema.

Exemplo 2: Determine todas as soluções inteiras da equação

$$(x^2 + 1)(y^2 + 1) + 2(x - y)(1 - xy) = 4(1 + xy).$$

Solução: Abrindo alguns termos da equação acima obtemos:

$$x^2y^2 - 2xy + 1 + x^2 + y^2 - 2xy + 2(x-y)(1-xy) = 4,$$

o que nos dá

$$(xy-1)^2 + (x-y)^2 - 2(x-y)(xy-1) = 4$$

$$\Leftrightarrow \big(xy - 1 - (x-y)\big)^2 = 4$$

$$\Leftrightarrow (x+1)(y-1) = \pm 2$$

e assim $(x+1,\ y-1)$ só podem assumir os valores

$$(2,1),\ (-2,-1),\ (1,2),\ (-1,\ -2),\ (2,\ -1),\ (-2,\ 1),\ (1,\ -2),\ (-1,\ 2),$$

obtendo os pares (x, y), respectivamente,

$$(1,\ 2),\ (-3,\ 0),\ (0,\ 3),\ (-2,\ -1),\ (1,\ 0),\ (-3,\ 2),\ (0,\ -1),\ (-2,\ 3)$$

que são todas as soluções do problema.

2 O método de cotar por desigualdades

Este método consiste em encontrar intervalos finitos nos quais as váriáveis podem se encontrar dado que para os demais valores é possível provar que ambos os lados da igualdade são diferentes através de uma sequência de desigualdades estritas.

Exemplo 3: Determine todos os pares de números inteiros (x, y) que satisfazem

$$x^3 + y^3 = (x+y)^2$$

Solução: Fatorando o lado esquerdo, obtemos: $(x+y)(x^2 - xy + y^2) = (x+y)^2$. Assim, se $x + y = 0$, isto é, $(x, y) = (k, -k)$, com $k \in \mathbb{Z}$ é sempre solução. Suponhamos então agora que $x + y \neq 0$. Cancelando o fator $x + y$ de ambos os lados, obtemos:

$$x^2 - xy + y^2 = x + y \Rightarrow 2x^2 - 2xy + 2y^2 = 2x + 2y$$

Obtendo $(x-y)^2 + x^2 - 2x + y^2 - 2y = 0 \Leftrightarrow (x-y)^2 + (x-1)^2 + (y-1)^2 = 2$. E com isso, se $x - y \neq 0,\ x - 1 \neq 0,\ y - 1 \neq 0$, obtemos

$$(x-y)^2 + (x-1)^2 + (y-1)^2 \geq 1 + 1 + 1 = 3 \Rightarrow 2 \geq 3$$

Uma contradição. Logo $x = y$ ou $x = 1$ ou $y = 1$.

- Se $x = y$: $2(x-1)^2 = 2 \Rightarrow x = 2$ (note que se $x = 0$ então $x + y = 0$)
- Se $x = 1$ ($y = 1$ é análogo): $2(y-1)^2 = 2 \Rightarrow y = 0$ ou 2

E assim obtemos as demais soluções: $(2,2),\ (1,0),\ (1,2),\ (0,1),\ (2,1)$.

Exemplo 4: Encontre todas as soluções inteiras (x, y) da equação

$$x^3 + (x+1)^3 + (x+2)^3 + (x+3)^3 + (x+4)^3 + (x+5)^3 + (x+6)^3 + (x+7)^3 = y^3$$

Solução: Abrindo o lado esquerdo da equação, obtemos

$$8x^3 + 84x^2 + 420x + 784 = y^3 \quad (1)$$

Inicialmente façamos o caso $x > 0$ (e consequentemente $y > 0$). Como

$$84x^2 = 3 \cdot (2x)^2 \cdot 7,$$

a equação nos remete a pensar em

$$(2x+7)^3 = 8x^3 + 84x^2 + 294x + 343 = y^3 - 126x - 441 < y^3 \Rightarrow 2x + 7 < y.$$

Por outro lado,

$$(2x+8)^3 = 8x^3 + 96x^2 + 384x + 512 = y^3 + 12x^2 - 36x - 272.$$

Hmmm... meio chato, mas

$$(2x+9)^3 = 8x^3 + 108x^2 + 486x + 729$$
$$= y^3 + 24x^2 + 66x - 55$$
$$\geq y^3 + 24 + 66 - 55 > y^3$$
$$\Rightarrow 2x + 9 > y$$

Perfeito! E assim $2x + 7 < y < 2x + 9 \Rightarrow y = 2x + 8$

Substituindo na equação (1): $8x^3 + 84x^2 + 420x + 784 = (2x+8)^3$. E assim:

$$8x^3 + 84x^2 + 420x + 784 = 8x^3 + 96x^2 + 384x + 512 \Leftrightarrow 12x^2 - 36x - 272 = 0.$$

Assim:

$$12(x^2 - 3x) = 272 \Rightarrow 272 \text{ é múltiplo de } 12 \text{ (Absurdo!)}$$

Logo, não há solução para $x > 0$.

Se $x = 0 \rightarrow 784 = y^3$ (Absurdo!). Resta então fazer o caso $x < 0$. Tomando $x = -t$, com $t > 0$ em (1), obtemos:

$$-8t^3 + 84t^2 - 420t + 784 = y^3.$$

Para $y = -r$:

$$8t^3 - 84t^2 + 420t - 784 = r^3 \ (2)$$

Como $(2t-7)^3 = 8t^3 - 84t^2 + 294t - 343 = r^3 - 126t + 441$, temos que para $t \geq 4$:

$$(2t-7)^3 = r^3 - 126t + 441 < r^3 \Rightarrow 2t - 7 < r.$$

Note que se

- $t = 1$: $8 - 84 + 420 - 784 = r^3 \rightarrow r^3 = -440$ (Absurdo!)
- $t = 2$: $8 \cdot 2^3 - 84 \cdot 2^2 + 420 \cdot 2 - 784 = r^3 \rightarrow r^3 = -216 \rightarrow r = -6$
- $t = 3$: $8 \cdot 3^3 - 84 \cdot 3^2 + 420 \cdot 3 - 784 = r^3 \rightarrow r^3 = -64 \rightarrow r = -4$
- Para $t \geq 4$ temos $2t - 7 < r$. Além disso:
  $$(2t-5)^3 = 8t^3 - 60t^2 + 150t - 125 = r^3 + 24t^2 - 270t + 659 \ldots$$

puxa... mas veja que

$$(2t-4)^3 = 8t^3 - 48t^2 + 96t - 64$$
$$= r^3 + 36t^2 - 324t + 720$$
$$= r^3 + 36(t^2 - 9t + 20)$$
$$= r^3 + 36(t-4)(t-5).$$

Assim, $2t - 4 > r$ quando $t \geq 6$ e $r = 2t - 4$ se $t = 4$ ou 5. Para $t \geq 6$:

$$t - 7 < r < 2t - 4 \Rightarrow r = 2t - 5 \ ou \ 2t - 6.$$

Note que em (2) r é par, e assim $r = 2t - 6$. Substituindo:

$$8t^3 - 84t^2 + 420t - 784 = (2t-6)^3 = 8t^3 - 72t^2 + 216t - 216$$

$$\Rightarrow 12t^2 - 204t + 568 = 0 \Rightarrow 568 = 12(17t - t^2) \Rightarrow 568 \text{ é múltiplo de } 12 \text{ (Absurdo!).}$$

Logo os pares (t,r) em (2) são $(2,-6)$, $(3,\ -4)$, $(4,\ 4)$, $(5,\ 6)$ o que nos dá os pares (x,y) sendo, respectivamente, $(-2,6)$, $(-3,4)$, $(-4,-4)$, $(-5,-6)$.

Observe que alguns problemas de Equações Diofantinas vão exigir certo trabalho braçal...

Nota 1: Sim, eu sei que vocês pensaram que em (2) temos que r é par e, substituindo $r = 2k$ a conta ficava bem mais rápida (De fato!), mas escolhi o caminho mais "chato" de maneira proposital como um incentivo para vocês não desistirem tão fácil assim de uma conta extensa.

Nota 2: Existe uma solução alternativa para o caso $x < 0$. Basta você perceber pela equação inicial que (x,y) é solução se, e somente se, $(-x-7,-y)$ é, e com isso, já que não há solução com $x \geq 0$ também não haverá com $x \leq -7$, restando apenas testar $x \in \{-1,-2,-3,-4,-5,-6\}$.

3 O método de parametrização

Sabe aqueles problemas "Prove que tal equação possui infinitas soluções inteiras". Para isso você não precisa achar todas elas, basta achar uma família infinita de soluções. Nesses tipos de problemas tentamos simplificá-los assumindo particularidades e parametrizando as variáveis por outras variáveis mas em menor quantidade, diminuindo o número de variáveis e deixando a equação mais agradável. (Mas é claro, pode ser que a sua nova equação não tenha infinitas soluções, o que torna a escolha de uma parametrização um trabalho não-trivial). Vejamos alguns exemplos para ficar mais claro:

Exemplo 5: Mostre que existem infinitas triplas de inteiros (x,y,z) tais que

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

Solução: Como eu disse acima, "chutar" uma parametrização é um trabalho não-trivial e para isso precisamos de alguma estratégia. Por exemplo, note que se tomarmos $z = -y$ o lado esquerdo da igualdade fica apenas x^3 obtendo assim a equação $x^3 = x^2 + 2y^2$ o que nos dá (a menos que $x = 0$) que x^2 divide $2y^2$. Então que tal fazermos x dividindo y , isto é, $y = mx$? A equação fica

$$x^3 = x^2 + 2m^2x^2$$

e assim $x = 0$ ou $x = 2m^2 + 1$, onde m é um inteiro qualquer. Assim,

$$\left(2m^2+1,\ m(2m^2+1),\ -m(2m^2+1)\right)$$

é solução da equação para todo $m \in \mathbb{Z}$.

Nota: Note que provamos que a equação acima tem infinitas soluções, apesar de não termos encontrado todas (veja que $(0,0,0)$ é solução, mas não é da forma acima).

Exemplo 6: Dados inteiros positivos a e b , demonstre que a equação

$$x^2 - 2axy + (a^2 - 4b)y^2 + 4by = z^2$$

tem infinitas soluções inteiras positivas (x,y,z).

Solução: Podemos reescrever como

$$(x-ay)^2 - 4by^2 + 4by = z^2 \Leftrightarrow (x-ay)^2 + b = z^2 + b(2y-1)^2.$$

Olha só!! Uma diferença de quadrados! Reescreva como

$$(x - ay + z)(x - ay - z) = b((2y - 1)^2 - 1).$$

Para nossa sorte $(2y - 1)^2 - 1 = 4y^2 - 4y$ é múltiplo de 4 . Agora, em particular, vamos tomar:

$$x - ay + z = \frac{(2y - 1)^2 - 1}{2}$$

$$x - ay - z = 2b$$

E assim, resolvendo o sistema nas variáveis x e z :

$$x = \frac{(2y - 1)^2 - 1}{4} + b + ay = y^2 - y + b + ay$$

$$z = \frac{(2y - 1)^2 - 1}{4} - b = y^2 - y - b$$

Logo, $(t^2 - t + b + at,\ t,\ t^2 - t - b)$ satisfaz a equação para todo $t \in \mathbb{Z}$.

Além disso, se tomarmos $t > 0$ tal que $t^2 - t > b$ (por exemplo $t \geq 2b$) garantimos que x, y, z são inteiros positivos. Note novamente que não achamos todas as soluções, apenas provamos que existem infinitas.

4 O método da aritmética modular

Sabe aqueles problemas que você sofre a bessa e no final descobre que era só usar uma congruência em um módulo específico? Então... Utilizar alguns módulos podem simplificar (as vezes até concluir) determinadas equações diofantinas! Vejamos adiante alguns exemplos disso.

Exemplo 7: Demonstre que a equação

$$(x + 1)^2 + (x + 2)^2 + \cdots + (x + 2001)^2 = y^2$$

não possui solução inteira (x, y).

Solução: Vamos analisar a equação $mod\ 3$:

$$\frac{2001}{3}((x + 1)^2 + (x + 2)^2 + x^2) \equiv y^2 (mod\ 3) \Rightarrow 667(3x^2 + 6x + 5) \equiv y^2 (mod\ 3)$$

$$\Rightarrow y^2 \equiv 667 \cdot 5 \equiv 1 \cdot 2 \equiv 2 (mod\ 3),$$

uma contradição, pois nenhum quadrado perfeito é congruente a $2\ mod\ 3$.

Nota: Mas qual a motivação para pensar $mod\ 3$? Bem, temos 2001 quadrados perfeitos consecutivos e 2001 é múltiplo de 3 , né? Não custa tentar... E será que $mod\ 23$ ou $mod\ 29$ funcionária com essa mesma ideia? (Pense sobre)

Exemplo 8: Demonstre que a equação

$$x^5 - y^2 = 4$$

não tem solução inteira (x, y).

Solução: Quadrados são legais, quintas potências... hm... esse tipo de problema remete muito ao pequeno teorema de Fermat ($a^{p-1} \equiv 1 (mod\ p)$ quando p primo e a não múltiplo de p). Que tal então achar um primo p tal que 5 divide $p - 1$?

Vejamos $p = 11$. Note que o pequeno teorema de Fermat nos diz que $x^{10} \equiv 0$ ou $1\ (mod\ 11)$. Assim:

$$x^5 \equiv 0,1,-1\ (mod\ 11) \Rightarrow y^2 \equiv 7,\ 8\ ou\ 6\ (mod\ 11),$$

uma contradição, uma vez que nenhum quadrado admite alguma dessas 3 congruências $mod\ 11$. (verifique!)

Nota 1: Quando estudamos resíduos quadráticos, uma das primeiras coisas que aprendemos é que dado p primo ímpar, existem exatamente $\frac{p-1}{2}$ resíduos quadráticos (não-nulos) $mod\ p$. Mas esse teorema pode ser generalizado pelo lema abaixo:

Lema: Seja $d > 1$ um inteiro positivo e $p \equiv 1\ (mod\ d)$ um primo. Então existem exatamente $\frac{p-1}{d}$ resíduos d-ésimas potências (não-nulas) $mod\ p$, isto é, existem $\frac{p-1}{d}$ congruências não-nulas a tal que existe $x \in \mathbb{Z}$ com $x^d \equiv a(mod\ p)$.

Prova: Tome g uma raiz primitiva $mod\ p$. Então as congruências não-nulas $mod\ p$ são dadas por $g^1,\ g^2,\ \ldots,\ g^{p-1}$. Obviamente $g^d,\ g^{2d},\ \ldots,\ g^{\frac{p-1}{d}d}$ são resíduos d-ésimas potências $mod\ p$. Além disso, se $g^k,\ 1 \leq k \leq p-1$ é raiz d-ésima $mod\ p$, então existe x não-nulo $mod\ p$ com

$$x^d \equiv g^k(mod\ p) \Rightarrow (g^k)^{\frac{p-1}{d}} \equiv (x^d)^{\frac{p-1}{d}} \equiv\ x^{p-1} \equiv 1(mod\ p)$$

$$\Rightarrow k\frac{p-1}{d} \text{ é múltiplo de } p-1 \Rightarrow \frac{k^{\frac{p-1}{d}}}{p-1} \in \mathbb{Z} \Rightarrow \frac{k}{d} \in \mathbb{Z} \Rightarrow k \in \left\{d,\ 2d,\ \ldots,\ \frac{p-1}{d}d\right\},$$

como queríamos. $Q.E.D.$

A partir desse lema, x^5 só poderia assumir $\frac{11-1}{5} = 2$ congruências não-nulas $mod\ 11$ (são elas 1 e -1), enquanto y^2 poderia assumir $\frac{11-1}{2} = 5$ congruências não-nulas $mod\ 11$ (são elas $1,\ 3,\ 4,\ 5$ e 9).

Nota 2: 31 também é um primo $\equiv 1\ (mod\ 5)$. Entretanto 11 era o menor primo com aquela propriedade, o que provavelmente economizaria nosso tempo e grafite (mas claro, poderia ser que ele não funcionasse. Felizmente tivemos sorte). Além disso, braçalmente, ao testarmos o 31 nessa ideia, ele não funciona... Tururu.

5 O método de Indução

Suponha que tenhamos uma sequência de equações diofantinas: $F_1,\ F_2,\ F_3,\ \ldots$ e o problema nos pede para provar que F_n tem solução para todo n . Nessas situações, uma ideia que pode funcionar é aplicar indução em n , isto é, que existe um n_0 tal que $F_1,\ F_2,\ \ldots,\ F_{n_0}$ têm solução e que para todo $k \geq n_0 + 1$: Se $F_1,\ F_2,\ \ldots,\ F_{k-1}$ têm solução, então F_k tem solução.

Exemplo 9: Prove que para todo $n \geq 3$ existem inteiros positivos $x_1,\ x_2,\ \ldots,\ x_n$ distintos dois a dois tais que

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = 1.$$

Solução: Para $n = 3$ temos $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$.

Suponha agora que para algum $k \geq 3$ o resultado vale para $n = k$, isto é, existam inteiros positivos $2 \leq x_1 < x_2 < x_3 < \cdots < x_k$ tais que $\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} = 1$. Assim, dividindo ambos os lados por 2 :

$$\frac{1}{2x_1} + \frac{1}{2x_2} + \cdots + \frac{1}{2x_k} = \frac{1}{2} \rightarrow \frac{1}{2} + \frac{1}{2x_1} + \frac{1}{2x_2} + \cdots + \frac{1}{2x_k} = 1$$

e de fato $2 \leq 2 < 2x_1 < 2x_2 < \cdots < 2x_k$. Isso mostra que o resultado vale para $n = k + 1$.

Nossa indução está completa!

Nota 1: É possível exibir explicitamente os $x_i s$ da solução acima: $x_i = 2^i$ para $i = 1,2, \ldots, n-2$,$x_{n-1} = 3 \cdot 2^{n-3}$, $x_n = 3 \cdot 2^{n-2}$.

Nota 2: Existem outros exemplos de soluções $(x_1, x_2, \ldots, x_n)$ para tal problema, veja alguns:

(i) $x_i = \frac{(i+1)!}{i}$ para $i = 1,2, \ldots, n-1$ e $x_n = n!$; (spoiler do $P1$ da OBM 2020 do $N3$)
(ii) $x_i = 2^i$ para $i = 1,2, \ldots, n-2$ e $x_{n-1} = 2^{n-2} + 1$, $x_n = 2^{n-2}(2^{n-2} + 1)$;
(iii) $x_i = a_i$ para $i = 1,2, \ldots, n-1$ e $x_n = a_n - 1$, onde a sequência $(a_i)_{i \geq 1}$ satisfaz

$$a_1 = 2 \text{ e } a_{k+1} = a_k^2 - a_k + 1 \text{ para todo } k \geq 1.$$

Como exercício deixamos o leitor provar que tais soluções funcionam.

Exemplo 10: Prove que para todo inteiro positivo $n \geq 3$ existem inteiros positivos ímpares x e y tais que

$$7x^2 + y^2 = 2^n.$$

Solução: Para $n = 3 : 7 \cdot 1^2 + 1^2 = 2^3$. Suponha agora que para algum $k \geq 3$ tenhamos que para $n = k$ o enunciado é verdadeiro. Isto é, existem inteiros positivos ímpares x e y tais que $7x^2 + y^2 = 2^k$.

Assim, $2^{k+1} = 14x^2 + 2y^2$. É interessante tentarmos escrever

$$14x^2 + 2y^2 = 7(ax + by)^2 + (cx + dy)^2,$$

onde $ax + by,\ cx + dy$ são inteiros ímpares. Abrindo, obtemos:

$$14x^2 + 2y^2 = (7a^2 + c^2)x^2 + (7b^2 + d^2)y^2 + (14ab + 2cd)xy.$$

Basta então fazermos $7a^2 + c^2 = 14;\ 7b^2 + d^2 = 2;\ 14ab + 2cd = 0.$

Meio estranho porque obviamente a segunda equação não tem solução inteira.... Mas $a,\ b,\ c,\ d$ não precisam ser inteiros 😊! Na real, se você multiplicar a segunda equação por $4 : 7(2b)^2 + (2d)^2 = 8$ (parece que já vimos isso antes...). Que tal tomar $2b,\ 2d\ \in \{-1, +1\}$, isto é, $b,\ d\ \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}$?

Ok, vamos tentar $b = d = \frac{1}{2}$: A terceira equação nos dá $c = -7a$. Substituindo na primeira equação, obtemos $56a^2 = 14 \Rightarrow a \in \left\{-\frac{1}{2},\ \frac{1}{2}\right\}$.

Se $(a, b, c, d) = \left(\frac{1}{2},\ \frac{1}{2},\ -\frac{7}{2},\ \frac{1}{2}\right)$:

$$2^{k+1} = 7\left(\frac{x+y}{2}\right)^2 + \left(\frac{-7x+y}{2}\right)^2$$

Bem, como x e y são ímpares, $\frac{x+y}{2}$ é inteiro e $\frac{-7x+y}{2} = \frac{x+y}{2} - 4x$ é um inteiro de mesma paridade. Assim, se $\frac{x+y}{2}$ é ímpar, então $\left|\frac{-7x+y}{2}\right|$ também será e assim achamos solução para $n = k + 1$.

Mas e se $\frac{x+y}{2}$ é par? Então $\frac{x-y}{2} = \frac{x+y}{2} - y$ é ímpar, e assim tomando $(a, b, c, d) = \left(-\frac{1}{2},\ \frac{1}{2},\ \frac{7}{2},\ \frac{1}{2}\right)$ obtemos:

$$2^{k+1} = 7\left(\frac{-x+y}{2}\right)^2 + \left(\frac{7x+y}{2}\right)^2$$

E de fato $\left|\frac{-x+y}{2}\right|$ é um inteiro positivo ímpar e $\frac{7x+y}{2} = 4x + \frac{y-x}{2}$ também vai ser um inteiro positivo ímpar. Assim encontramos uma solução para $n = k + 1$.

Nota: Veja que caso o problema pedisse a existência de inteiros positivos (não necessariamente ímpares) que satisfizessem o problema, isso o tornaria bem mais fácil, pois se $n = 2k + 3$ tome $(x, y) = (2^k,\ 2^k)$, e se $n = 2k + 4$ tome $(x, y) = (2^k,\ 3 \cdot 2^k)$.

6 O método da descida de Fermat

Em geral, o método da descida de Fermat é dado por: Considere as proposições $P(1),\ P(2),\ P(3),\ \ldots$. Suponha que $P(1)$ é falsa e que se $k > 1$ tal que $P(k)$ é verdadeira, então existe $1 < j < k$ tal que $P(j)$ é verdadeira. Isso nos implica que $P(n)$ é falsa para todo n .

A ideia acima é interessante para provarmos que determinadas equações diofantinas não possuem solução. Além disso, uma leve variação desse método pode nos ajudar a achar todas as soluções de uma equação diofantina a partir de "soluções minimais" (Se tais soluções minimais não existem... Então não há soluções). Ué, mas o que seriam essas tais "soluções minimais"? Vamos com calma...

Exemplo 11: Determine todas as soluções inteiras (x, y, z) da equação

$$x^3 + 2y^3 = 4z^3$$

Solução: É claro que $(0,0,0)$ é solução. Seja então (caso exista) $(x, y, z) \neq (0,0,0)$ uma outra solução. Vendo a equação $mod\ 2$ descobrimos que x é par, então $x = 2a$ com $a \in \mathbb{Z}$.

Substituindo: $4a^3 + y^3 = 2z^3$. Novamente, por $mod\ 2$, y é par, então $y = 2b,\ b \in \mathbb{Z}$.

Substituindo: $2a^3 + 4b^3 = z^3$. Novamente, por $mod\ 2$, z é par, então $z = 2c,\ c \in \mathbb{Z}$.

Substituindo: $a^3 + 2b^3 = 4c^3$. O que nos dá que (a, b, c) é solução da equação inicial.

Ou seja, se (x, y, z) é solução, então x, y, z são pares e $\left(\frac{x}{2},\ \frac{y}{2},\ \frac{z}{2}\right)$ é solução. Vamos chamar de "minimal" uma solução $(x, y, z) \neq (0,0,0)$ que minimiza $|x| + |y| + |z|$. Então se $(x_0,\ y_0,\ z_0)$ é solução minimal, então $\left(\frac{x_0}{2},\ \frac{y_0}{2},\ \frac{z_0}{2}\right) \neq (0,0,0)$ também é solução. Entretanto $\left|\frac{x_0}{2}\right| + \left|\frac{y_0}{2}\right| + \left|\frac{z_0}{2}\right| < |x_0| + |y_0| + |z_0|$, contradizendo a minimalidade de $(x_0,\ y_0,\ z_0)$. Uma contradição. Logo, não existem soluções $(x, y, z) \neq (0,0,0)$, sendo $(0,0,0)$ a única solução.

Interessante, não?

Exemplo 12: Encontre todas as soluções inteiras positivas (m, n) da equação

$$(n^2 - mn - m^2)^2 = 1.$$

Solução: Seja (m, n) uma solução (se houver), então:

$$1 = (n^2 - mn - m^2)^2 = ((n - m)^2 + mn - 2m^2)^2$$

$$= ((n - m)^2 + m(n - m) - m^2)^2 = \big(m^2 - m(n - m) - (n - m)\big)^2,$$

o que nos dá que $(n - m,\ m)$ é uma solução inteira.

Note ainda que $n^2 - mn - m^2 = \pm 1 \rightarrow n^2 = m^2 + mn \pm 1 \geq m^2 \rightarrow n \geq m$. Além disso, se $(m, n) \neq (1,1)$ (que também é uma solução), então $n > m \rightarrow n - m > 0$. Além disso, para $(m, n) \neq (1,1)$:

$$n^2 = m^2 + mn \pm 1 \leq m^2 + mn + 1$$

$$\Rightarrow n \leq \frac{m^2}{n} + m + \frac{1}{n} \leq \frac{m^2}{m+1} + m + \frac{1}{m+1} \leq \frac{m^2+m}{m+1} + m = 2m \Rightarrow n \leq 2m$$

com igualdade se, e somente se, $m = 1,\ n = m + 1 \rightarrow (m, n) = (1,2)$ (que magicamente também é solução).

Logo, se $(m, n) \neq (1,1)$ é solução, então $m < n \leq 2m$ e $(n - m,\ m)$ é solução.

Vamos chamar de minimal as soluções (m, n) que minimizam $m + n$. Assim, se $(m, n) \neq (1,1)$ é solução, ela não é minimal, pois $(n - m, m)$ é solução e $(n - m) + m < m + n$. Logo, $(1,1)$ é a única solução minimal. Agora considere a seguinte operação sobre um par de inteiros positivos (a, b) tal que $a < b \leq 2a$: $(a, b) \longmapsto (b - a,\ a)$. Ao realizarmos sucessivas operações começando por uma solução (m, n), em algum momento será impossível realizar a operação (afinal, a soma das entradas sempre diminui a cada operação... isso é uma monovariante). Seja então (m_0, n_0) o par final. Tal par surgiu de $(n_0,\ m_0 + n_0)$ e $n_0 < m_0 + n_0 \leq 2n_0$, mas como não podemos aplicar a operação em $(m_0,\ n_0)$ isso nos indica que a afirmação $[m_0 < n_0 \leq 2m_0]$ é falsa. Como $(m_0,\ n_0)$é solução do problema, a afirmação $[n_0 \leq 2m_0]$ é verdadeira, sendo portanto falsa a afirmação $[m_0 < n_0]$ e assim obtemos $m_0 \geq n_0$, mas por (m_0, n_0) ser solução, então $(m_0, n_0) = (1,1)$.

Portanto, ao realizarmos sucessivamente a operação em cima de uma solução, eventualmente chegaremos ao par $(1,1)$ (a nossa solução minimal). Logo todas as soluções são geradas a partir de $(1,1)$ realizando a operação inversa, isto é, $(a, b) \longmapsto (b,\ a + b)$. Veja:

$$(1,1) \longmapsto (1,2) \longmapsto (2,3) \longmapsto (3,5) \longmapsto (5,8) \longmapsto \cdots$$

Esta é exatamente a sequência das soluções! Indutivamente prova-se que os termos da sequência são dados por $(F_n,\ F_{n+1}),\ n \geq 1$, onde $(F_k)_{k \geq 1}$ é a sequência de Fibonacci.

Nota: A sequência de Fibonacci é dada por $F_1 = F_2 = 1$ e $F_{k+1} = F_k + F_{k-1}$, $k \geq 2$.

Sua fórmula fechada é dada por $F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$.

Bem, mostramos nesse material 6 métodos bem úteis para resolvermos equações diofantinas, e caso seja necessário, você pode usar mais de um método para resolver um problema, não pense que cada problema exige um único método (na verdade, eles costumam ter até mais de uma solução, então crie a sua!).

7 Problemas

1. Determine todos os inteiros positivos n tais que a equação

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

possui solução inteira (x, y).

2. Seja n um inteiro positivo e $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ sua fatoração em primos. Prove que a equação

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$$

possui exatamente $(2\alpha_1 + 1)(2\alpha_2 + 1) \dots (2\alpha_k + 1)$ soluções inteiras positivas (x, y).

3. Encontre todas as soluções inteiras (x, y) de

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

4. Determine todos os pares de inteiros (x, y) que satisfazem

$$x^6 + 3x^3 + 1 = y^4$$

5. Resolva a equação abaixo nos inteiros positivos (a, b, c):

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = \frac{3}{5}$$

6. Determine todos os pares de primos (p, q) que satisfazem $p^3 - q^5 = (p + q)^2$.
7. Determine todas as triplas (x, y, z) de inteiros positivos tais que

$$(x + y)^2 + 3x + y + 1 = z^2$$

8. Resolva nos inteiros positivos a seguinte equação:

$$x^2 + y^2 + z^2 + w^2 = 3(x + y + z + w)$$

9. Sejam t, m, n inteiros positivos com $m \neq n$. Prove que a equação

$$x^2 + y^2 = (m^2 + n^2)^t$$

Possui solução inteira positiva (x, y).

10. Seja $n \geq 2$ um inteiro positivo. Prove que a equação

$$x^n + y^n = z^{n+1}$$

Admite solução inteira positiva (x, y).

11. Resolva a equação abaixo nos inteiros (x, y, z):

$$x^2 + xy = y^2 + xz$$

12. Sejam x, y, z inteiros positivos satisfazendo

$$(x + 1)^2 + (x + 2)^2 + \cdots + (x + 99)^2 = y^z$$

Prove que $z = 1$.

13. Encontre todos os pares de inteiros positivos (x, y) tais que

$$3^x - 2^y = 7$$

14. Encontre todas as $14-$ úplas de inteiros $(x_1, x_2, \ldots, x_{14})$ tais que

$$x_1^4 + x_2^4 + \cdots + x_{14}^4 = 15999$$

15. Prove que existe n_0 inteiro positivo tal que para todo $n \geq n_0$ existem números inteiros positivos $x_1, x_2, \ldots, x_n$ que satisfazem

$$\frac{1}{x_1^3} + \frac{1}{x_2^3} + \frac{1}{x_3^3} + \cdots + \frac{1}{x_n^3} = 1$$

16. Prove que para cada inteiro positivo n a equação

$$x^2 + xy + y^2 = 7^n$$

Admite solução inteira positiva (x, y).

17. Prove que a equação

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

Admite infinitas soluções inteiras positivas (x, y).

18. Resolva a equação

$$x^4 + y^4 + z^4 = 9u^4$$

Nos inteiros (x, y, z, u).

19. Resolva nos inteiros positivos a equação

$$2^x - 1 = xy$$

20. Resolva nos inteiros positivos (a, b, c, d) o sistema:

$$a^2 + 1 = bc$$

$$b^2 + 1 = ad$$

21. Encontre todas as soluções (a, b, c, n) de inteiros que satisfazem

$$6(6a^2 + 3b^2 + c^2) = 5n^2$$

22. (IMO 1997) Ache todos os pares de inteiros positivos (x, y) satisfazendo a equação

$$x^{(y^2)} = y^x$$

23. (OBM 2021) Uma tripla de inteiros positivos (a, b, c) é chamada *miranha* se
    - $\cdot$ a divide $bc + 1$
    - $\cdot$ b divide $ac + 1$
    - $\cdot$ c divide $ab + 1$

Determine todas as triplas miranhas.

24. (USA TST 2009) Ache todos os pares de inteiros positivos (m, n) tais que $mn - 1$ divide $(n^2 - n + 1)^2$.
25. (OCM 2014) Resolva os itens:

(a) Prove que existem inteiros positivos x, y e z tais que

$$13x^4 + 3y^4 - z^4 = 2013$$

(b) Prove que não existem inteiros positivos x, y e z tais que

$$13x^4 + 3y^4 - z^4 = 2014$$

26. (IMO) Sejam a, b inteiros positivos tais que $ab + 1$ divide $a^2 + b^2$. Prove que $\frac{a^2+b^2}{ab+1}$ é o quadrado de um inteiro.
27. (IMO 2012) Demonstre que para qualquer par de inteiros positivos (k, n), existem k inteiros positivos $m_1, m_2, \ldots, m_k$ tais que

$$1 + \frac{2^k - 1}{n} = \left(1 + \frac{1}{m_1}\right)\left(1 + \frac{1}{m_2}\right) \ldots \left(1 + \frac{1}{m_k}\right)$$

28. (Canadá 2009) Determine todos os pares de inteiros (a, b) tais que $3^a + 7^b$ é o quadrado de um inteiro.
29. (OBM 2011) Dizemos que um inteiro positivo é *chapa* quando ele é formado apenas por algarismos não-nulos e a soma dos quadrados de seus algarismos também é um quadrado perfeito. Prove que, para todo inteiro positivo n, existe um número chapa com n algarismos.

30. (OBM 2012) Determine se existem inteiros positivos n, a_1, a_2, …, a_{2012}, todos maiores ou iguais a 2 , tais que

$$n^2 = a_1^2 + a_2^3 + a_3^5 + \cdots + a_i^{p_i} + \cdots + a_{2012}^{p_{2012}}$$

em que p_ié o i-ésimo primo.

31. (Copa Europeia Júnior 2012) Encontre todas as quádruplas de inteiros positivos (a, b, n, p), com p primo, que satisfazem

$$a^{2013} + b^{2013} = p^n$$

32. (Copa Europeia Júnior) Encontre todos os pares (x, y) de inteiros positivos tais que xy divide $x^2 + 2y - 1$.
33. (CONE SUL 2007) Encontre todos os pares (x, y) de inteiros não-negativos que satisfazem

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

34. (CONE SUL 2011) Encontre todas as triplas de inteiros positivos (x, y, z) tais que

$$x^2 + y^2 + z^2 = 2011$$

35. (CONE SUL 2015) Prove que não existe par (m, n) de inteiros tal que

$$n^3 - 9n + 27 = 81m$$

36. (CIIM 2019) Determine todas as triplas de inteiros (x, y, z) que satisfazem a equação

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

37. (OBM 2021) Determine todas as triplas de inteiros não-negativos (a, b, c) tais que

$$a^2 + b^2 + c^2 = abc + 1$$

38. (CIIM 2020) Encontre todas as triplas de inteiros positivos (a, b, c) tais que as seguintes equações são ambas verdadeiras:

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

(ii) $a^3 + b^3 + 1 = (c - 1)^3$

39. (Ibero 2016) Encontre todos os primos $p,\ q,\ r,\ k$ tais que

$$pq + qr + rp = 12k + 1$$

40. (IMO 1994) Encontre todos os pares (m, n) de inteiros positivos tais que $\frac{n^3+1}{mn-1}$ é um número inteiro.
41. Determine todos os pares $(n,\ p)$ de inteiros positivos, com p primo tais que $p^n + n^2$ é o quadrado de um inteiro.
42. Dado n inteiro positivo, resolva a equação

$$1 + x_1 + 2x_1x_2 + 3x_1x_2x_3 + \cdots + (n-1)x_1x_2 \ldots x_{n-1} = x_1x_2 \ldots x_n$$

nos inteiros positivos distintos dois a dois $(x_1,\ x_2,\ \ldots,\ x_n)$.

43. Resolva nos inteiros positivos a seguinte equação:

$$7^x + x^4 + 47 = y^2$$

44. Determine todas as triplas de inteiros positivos $(x,\ k,\ n)$ tais que

$$3^k - 1 = x^n$$

45. Sejam $p,\ q,\ n$ inteiros positivos, com p primo tais que

$$2^p + 3^p = q^n$$

Prove que $n = 1$.

46. (Ibero 2015) Encontre todos os pares de inteiros (a, b) tais que

$$\left(b^2 + 7(a - b)\right)^2 = a^3b$$

47. (Ibero 2018) Seja $n \geq 2$ um inteiro. Encontre todas as soluções inteiras do sistema:

$$x_1 = (x_2 + x_3 + x_4 + \cdots + x_n)^{2018}$$

$$x_2 = (x_1 + x_3 + x_4 + \cdots + x_n)^{2018}$$

…

$$x_n = (x_1 + x_2 + x_3 + \cdots + x_{n-1})^{2018}$$

48. (IMO 1992) Encontre todos os inteiros $a,\ b,\ c$ com $1 < a < b < c$ tais que $(a - 1)(b - 1)(c - 1)$ é um divisor de $abc - 1$.
49. (Ibero 2008) Prove que não existem inteiros $x,\ y$ que satisfazem $x^{2008} + 1 = 21^y$
50. (IMO 2015) Encontre todas as triplas (a, b, c) de inteiros positivos tais que

$$ab - c,\ bc - a,\ ca - b$$

são potências de 2 , isto é, da forma 2^k com k inteiro não-negativo.

Referência

Andreescu, T., O introducere în studiul ecuatiilor diofantiene, Editora Gil, Zalau, 2003.