Equação de Pell Generalizada

Semana Olímpica 2020 - Natal - RN

Rafael Filipe - rafaelfilipedoss@gmail.com

O objetivo deste material não é focar nas demonstrações por trás dos teoremas relacionados a equação de Pell. Para isso você pode consultar [1], que expõe muito bem o tema. Aqui nos restringiremos a bem aplicar os teoremas em problemas em olimpíadas ao redor do mundo, muitas deles bem recentes, mostrando que é um tema recorrente.

1 A equação de Pell

Equação de Pell é qualquer equação da forma $x^2 - Dy^2 = 1$, em que D é um inteiro positivo que não seja quadrado perfeito. O interesse principal é encontrar as soluções inteiras positivas dessa equação.

O primeiro teorema importante que precisamos saber é o seguinte:

Teorema 1.1. *Seja D um inteiro positivo diferente de um quadrado perfeito. Então a equação $x^2 - Dy^2 = 1$ possui solução não trivial em inteiros positivos, ou seja, com $x + y\sqrt{D} > 1$.*

Com isso sabemos que toda equação de Pell tem solução. Portanto, dentre todas as soluções com $x + y\sqrt{D} > 1$, podemos tomar uma *solução minimal*, ou seja, que possui $x + y\sqrt{D}$ mínimo.

Na realidade, um fato importante é que a solução minimal é também a que possui o menor x e o menor y. Este fato auxiliará bastante quando precisarmos encontrar a solução minimal, pois sabendo disso podemos testar os valores iniciais de x (ou y) e certamente a primeira que encontrarmos será a minimal.

Mas por que precisamos encontrar a minimal? Por conta do seguinte teorema:

Teorema 1.2. *Seja D um inteiro positivo diferente de um quadrado perfeito. Seja (x_1, y_1) a solução minimal da equação $x^2 - Dy^2 = 1$. Então, a solução geral (x_n, y_n) com $x_n, y_n \in \mathbb{Z}_{>0}$ é tal que*

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n.$$

Então, encontrando a solução minimal, podemos encontrar todas as solução da equação! Mas nem sempre encontrar a solução minimal é fácil. Muitas vezes a solução é grande e fica inviável testar vários casos. Ao final desta seção mostraremos um método que pode facilitar os cálculos.

Podemos definir x_n e y_n de maneira recorrente, tomando o conjugado:

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n \Rightarrow x_n - y_n\sqrt{D} = (x_1 - y_1\sqrt{D})^n$$

$$\Rightarrow x_n = \frac{(x_1 + y_1\sqrt{D})^n + (x_1 - y_1\sqrt{D})^n}{2} \text{ e } y_n = \frac{(x_1 + y_1\sqrt{D})^n - (x_1 - y_1\sqrt{D})^n}{2\sqrt{D}}.$$

Interpretando essas fórmulas como soluções de recorrências lineares, não é difícil perceber que (x_n) e (y_n) satisfazem a recorrência $u_{n+2} - 2x_1u_{n+1} + u_n = 0,\ \forall\ n \geq 1$.

Um método rápido de encontrar a solução minimal é olhando para a fração contínua de $\sqrt{D}$. Escrevendo $\sqrt{D} = [a_0; a_1, a_2, ..., a_k]$, então

$$\frac{x_1}{y_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{k-1}}}}}$$

se k é par e

$$\frac{x_1}{y_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{2k-1}}}}}$$

se k é ímpar.

Por exemplo, para encontrar a solução minimal de $x^2 - 41y^2 = 1$, basta escrever a fração contínua de $\sqrt{41}$:

$$\sqrt{41} = 6 + (\sqrt{41} - 6) = 6 + \frac{1}{\frac{\sqrt{41}+6}{5}} = 6 + \frac{1}{2 + \frac{\sqrt{41}-4}{5}} = 6 + \frac{1}{2 + \frac{5}{\sqrt{41}+4}} =$$

$$= 6 + \frac{1}{2 + \frac{1}{\frac{\sqrt{41}+4}{5}}} = 6 + \frac{1}{2 + \frac{1}{2 + \frac{\sqrt{41}-6}{5}}} = 6 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{41}+6}}} = 6 + \frac{1}{2 + \frac{1}{2 + \frac{1}{12 + (\sqrt{41}-6)}}}$$

e então começará a repetir de modo que $\sqrt{41} = [6; 2, 2, 12]$. Logo, sendo o período 3 (ímpar), temos que ir até o a_5 para achar a solução minimal:

$$\frac{x_1}{y_1} = 6 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{12 + \cfrac{1}{2 + \frac{1}{2}}}}} = \frac{2049}{320}.$$

Portanto, a solução minimal é $(2049, 320)$, e seria inviável encontrá-la à mão!

Exemplo 1.3. Prove que existem infinitos n tais que $1 + 2 + 3 + ... + n$ é um quadrado perfeito.

Solução: Sabemos que

$$1 + 2 + ... + n = \frac{n(n+1)}{2}.$$

Logo, para essa soma ser um quadrado perfeito, devemos ter:

$$\frac{n(n+1)}{2} = m^2 \iff n^2 + n = 2m^2 \iff 4n^2 + 4n = 8m^2 \iff$$

$$\iff (2n+1)^2 = 8m^2 + 1 \iff (2n+1)^2 - 2(2m)^2 = 1,$$

que é a equação de Pell $x^2 - 2y^2 = 1$, a qual sabemos que possui infinitas soluções.

Mas repare que devemos verificar se existem infinitas soluções com x ímpar e y par. Analisando a paridade de cada lado, x é sempre ímpar e, analisando módulo 8, temos que y tem que ser par. Logo, temos infinitos valores de n, como desejado.

□

Exemplo 1.4. Suponha que n é um natural tal que $m = 2 + \sqrt{28n^2+1}$ é um inteiro. Mostre que m é um quadrado perfeito.

Solução: Seja $t = \sqrt{28n^2+1}$. Temos então que $t^2 - 28n^2 = 1$ e queremos mostrar que $m = 2(1+t)$ é um quadrado perfeito. Veja que

$$t^2 - 28n^2 = 1 \iff t^2 - 7(2n)^2 = 1$$

e então podemos olhar para as soluções da equação de Pell $x^2 - 7y^2 = 1$ com y par. A solução minimal dessa equação é $8 + 3\sqrt{7}$ e então

$$x_k + y_k\sqrt{7} = (8 + 3\sqrt{7})^k.$$

Note que $y_1 = 3$ e $y_2 = 48$ e sabemos que (y_k) satisfaz a recorrência $y_{k+2} - 16y_{k+1} + y_k = 0$. Logo, não é difícil perceber que y_k é par para k par e ímpar para k ímpar.

Portanto, se $(t, 2n)$ é solução de $x^2 - 7y^2 = 1$, então $(t, 2n) = (x_k, y_k)$ para algum $k = 2\ell$.

Temos então que:

$$t = \frac{(8+3\sqrt{7})^{2\ell} + (8-3\sqrt{7})^{2\ell}}{2} \Rightarrow 2(1+t) = (8+3\sqrt{7})^{2\ell} + (8-3\sqrt{7})^{2\ell} + 2 = ((8+3\sqrt{7})^{\ell} + (8-3\sqrt{7})^{\ell})^2.$$

Portanto, $m = ((8+3\sqrt{7})^{\ell} + (8-3\sqrt{7})^{\ell})^2 = (2x_\ell)^2$ é o quadrado de um inteiro.

□

Exemplo 1.5. Seja n um inteiro tal que $3n+1$ e $4n+1$ são ambos quadrados perfeitos. Prove que 56 divide n.

Solução: Temos que $3n + 1 = a^2$ e $4n + 1 = b^2$. Isolando n nas duas equações:

$$n = \frac{a^2-1}{3} = \frac{b^2-1}{4} \Rightarrow 4a^2 - 3b^2 = 1 \iff (2a)^2 - 3b^2 = 1.$$

Devemos então olhar para as soluções de $x^2 - 3y^2 = 1$ com x par. A solução minimal é $2 + \sqrt{3}$ e então

$$x_k + y_k\sqrt{3} = (2 + \sqrt{3})^k.$$

Temos então que $x_1 = 2$, $x_2 = 7$ e (x_n) satisfaz $x_{n+2} - 4x_{n+1} + x_n = 0$ e então x_k é par para k ímpar. Portanto, $2a = x_{2\ell+1}$ para algum ℓ. Queremos mostrar que 56 divide n, então basta mostrar que 56 divide $a^2 - 1$.

Se mostrarmos que $a \equiv \pm 1 \pmod 7$ e que a é ímpar, temos $a^2 \equiv 1 \pmod 7$ e $a^2 \equiv 1 \pmod 8$ e então 56 divide $a^2 - 1$, já que 7 e 8 são primos entre si.

Veja que

$$a \equiv \pm 1 \pmod 7 \iff 2a \equiv \pm 2 \pmod 7 \iff x_{2\ell+1} \equiv \pm 2 \pmod 7,$$
$$a \equiv 1 \pmod 2 \iff 2a \equiv 2 \pmod 4 \iff x_{2\ell+1} \equiv \pm 2 \pmod 4.$$

Analisando a recorrência $\pmod 7$, temos que os restos são

$$2, 0, -2, -1, -2, 0, 2, 1, 2, 0, ...$$

e começa a repetir. Logo, nos ímpares é sempre $\pm 2 \pmod 7$, como desejado.

Finalmente, analisando $\pmod 4$, temos que os restos são

$$2, 3, 2, 1, 2, 3, ...$$

e começa a repetir. Logo, nos ímpares é sempre $2 \pmod 4$. Portanto, temos que 56 divide n, como desejado.

□

Problemas

1. Encontre todos os triângulos cujos lados são inteiros consecutivos e cuja área é inteira.
2. (Romênia TST 2000) Mostre que existem infinitos inteiros (x, y, z, t) com $\text{mdc}(x, y, z, t) = 1$ tais que
$$x^3 + y^3 + z^2 = t^4.$$
3. (Longlist 1990) Prove que existem infinitos inteiros positivos n tais que $\frac{1^2+2^2+\cdots+n^2}{n}$ é um quadrado.
4. Sejam d, k inteiros positivos tais que d não é um quadrado perfeito Mostre que existem infinitos pares de inteiros positivos (x, y) tais que k divide y e $x^2 - dy^2 = 1$.
5. Prove que existem infinitos quadrados perfeitos que podem ser escritos na forma $1 + 2^{x^2} + 2^{y^2}$, em que x e y são inteiros positivos.
6. Resolva $(x + 1)^3 - x^3 = y^2$ nos inteiros positivos.
7. Resolva $(x - y)^5 = x^3 - y^3$ nos inteiros positivos.
8. Existem inteiros $a, b > 1$ tais que $ab + 1$ e $ab^3 + 1$ sejam ambos quadrados perfeitos?
9. Determine todos os pares (x, y) com $x, y \in \mathbb{Z}_{>0}$ tais que: $\binom{x-1}{y} = \binom{x}{y-1}$.
10. (Bulgária 1999) Prove que a equação $x^3 + y^3 + z^3 + t^3 = 1999$ tem infinitas soluções inteiras.
11. (China TST 2002) Determine todos os inteiros não negativos m e n tais que $(2^n - 1)(3^n - 1) = m^2$.

2 A equação de Pell Generalizada

Aqui vamos estudar equações do tipo $x^2 - Dy^2 = c$, com D inteiro positivo diferente de quadrado perfeito e c inteiro qualquer.

Infelizmente não garantimos a existência de soluções. Uma condição necessária é que $\left(\frac{c}{D}\right) = 1$, mas esta condição não é suficiente. De fato, a equação $x^2 - 3y^2 = 7$ não possui solução e podemos verificar isso analisando módulo 4.

Mas, caso exista alguma solução, não só temos infinitas soluções como também podemos encontrar todas as soluções. Porém, nesse caso não temos necessariamente apenas uma família de soluções, gerada por uma solução minimal.

É possível que haja um conjunto de soluções fundamentais, cada uma gerando uma família. Isso se torna mais claro com o seguinte teorema:

Teorema 2.1. *Seja D um inteiro positivo que não seja quadrado perfeito. Suponha que a equação $x^2 - Dy^2 = c$ possua solução com x, y inteiros positivos. Seja $x_1 + y_1\sqrt{D}$ a solução minimal da equação $x^2 - Dy^2 = 1$. Então toda solução (x, y) de $x^2 - Dy^2 = c$ com $x, y \in \mathbb{Z}_{\geq 0}$ pode ser escrita na forma*

$$x + y\sqrt{D} = (u + v\sqrt{D})(x_1 + y_1\sqrt{D})^k,$$

para algum par de inteiros $u, v \in \mathbb{Z}_{>0}$ com $u^2 - Av^2 = c$ e $u + v\sqrt{D} < (x_1 + y_1\sqrt{D})\sqrt{|c|}$ e algum $k \in \mathbb{Z}_{\geq 0}$.

É fácil verificar que todo número da forma $x+y\sqrt{D} = (u+v\sqrt{D})(x_1+y_1\sqrt{D})^k$ é solução da equação $x^2-Dy^2 = c$. Portanto, o teorema acima caracteriza todas as soluções da equação $x^2 - Dy^2 = c$. Basta procurarmos todos os pares $(u, v) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ (note que u e v podem ser 0) que satisfaçam

$$u + v\sqrt{D} < (x_1 + y_1\sqrt{D})\sqrt{|c|} \qquad (*)$$

e gerar as famílias para cada um deles, ou seja, sendo (u_1, v_1), (u_2, v_2), ..., (u_r, v_r) os pares, basta multiplicá-los por potências de $x_1 + y_1\sqrt{D}$ e temos todas as soluções. Além disso, note que (u_n) e (v_n) também satisfazem a recorrência $t_{n+2} - 2x_1t_{n+1} + t_n = 0,\ \forall\ n \geq 1$.

Repare que nada impede que tenhamos redundância de soluções, isto é, que existam pares tais que

$$u_i + v_i\sqrt{D} = (u_j + v_j\sqrt{D})(x_1 + y_1\sqrt{D})^k$$

e então uma família estaria contida na outra.

Neste ponto é importante que você não tenha medo de fazer contas. Para lidar com $(*)$, em geral tentamos estimar o intervalo de valores para u e v e testamos todos os casos, para ver quais os possíveis pares (u_i, v_i).

Uma maneira alternativa é notar que, considerando que k pode ser negativo (e nesse caso encontraríamos soluções com alguma das coordenadas negativas), cada família possui exatamente uma raíz $u + v\sqrt{D}$ tal que $1 < u + v\sqrt{D} \leq x_1 + y_1\sqrt{D}$. Dessa forma, basta procurar soluções nesse intervalo com $u, v \in \mathbb{Z}$.

Outra coisa que pode ajudar é analisar a equação módulo alguns primos e tentar descobrir os restos que u e v devem ter na divisão por esses primos. Isso pode diminuir bastante a quantidade de casos para se testar.

Exemplo 2.2. Resolva a equação $x^2 - 5y^2 = 4$ nos inteiros positivos.

Solução: O primeiro passo é encontrar a solução minimal da equação $x^2 - 5y^2 = 1$. Testando os valores de y, temos que a solução minimal é $9 + 4\sqrt{5}$. Pelo **Teorema 2.1**, as soluções de $x^2 - 5y^2 = 4$ são dadas por

$$x_n + y_n = (u + v\sqrt{5})(9 + 4\sqrt{5})^n,$$

em que $u, v > 0$ são tais que $u^2 - 5v^2 = 4$ e $u + v\sqrt{5} < (9 + 4\sqrt{5})\sqrt{4} = 18 + 8\sqrt{5}$. Note que $= 18^2 - 5.8^2 = 4$, de modo que se tiver alguma outra solução menor, devemos ter $v < 8$. Testando $v = 0, 1, 2, ..., 7$, obtemos as soluções 2, $3 + \sqrt{5}$ e $7 + 3\sqrt{5}$. Portanto, as soluções da equação são dadas por

$$x_n + y_n\sqrt{5} = (3 + \sqrt{5})(9 + 4\sqrt{5})^n,$$

$$x_n + y_n\sqrt{5} = (7 + 3\sqrt{5})(9 + 4\sqrt{5})^n,$$

$$x_n + y_n\sqrt{5} = 2(9 + 4\sqrt{5})^n.$$

□

Exemplo 2.3. Determine todos os triângulos retângulos com lados inteiros cujos catetos são números consecutivos.

Solução: Por Pitágoras, basta encontrarmos as soluções da equação $n^2 + (n+1)^2 = m^2$. Reescrevendo a equação, obtemos

$$n^2 + (n+1)^2 = m^2 \iff 2n^2 + 2n + 1 = m^2 \iff 4n^2 + 4n + 2 = 2m^2 \iff (2n+1)^2 - 2m^2 = -1.$$

Então, devemos olhar para a equação $x^2 - 2y^2 = -1$ em que x é sempre ímpar, mas veja que x é sempre ímpar. Logo, basta encontrarmos todas as soluções. Novamente, a minimal de $x^2 - 2y^2 = 1$ é $3 + 2\sqrt{2}$ e então toda solução de $x^2 - 2y^2 = -1$ se escreve como:

$$u_k + v_k\sqrt{2} = (u + v\sqrt{2})(3 + 2\sqrt{2})^k,$$

com $u, v > 0$ e $u + v\sqrt{2} < (3 + 2\sqrt{2})\sqrt{|1|}$ e $u^2 - 2v^2 = -1$. Da desigualdade, obtemos $v < \frac{3}{\sqrt{2}} + 2 < 5$ e então basta testarmos $v = 0, 1, 2, 3, 4$. Analisando todos os casos obtemos a solução $1 + \sqrt{2}$.

Portanto, as soluções são $u_k + v_k\sqrt{2} = (1 + \sqrt{2})(3 + 2\sqrt{2})^k$ e usando que $3 + 2\sqrt{2} = (1 + \sqrt{2})^2$, temos que:

$$u_k + v_k\sqrt{2} = (1 + \sqrt{2})^{2k+1}$$

Logo, os triângulos são os triângulos com lados $n = \frac{u_k - 1}{2}$, $n+1 = \frac{u_k+1}{2}$ e $m = v_k$.

□

Você também pode utilizar Pell para construir exemplos em alguns problemas que não estão diretamente relacionados a equações diofantinas.

Exemplo 2.4. Prove que existem infinitos n tais que n^2+1 divide $n!$.

Solução: Sabemos que a equação $n^2+1 = 2m^2$ possui infinitas soluções. Vamos mostrar que para pares (m,n) que suficientemente grandes que satisfazem essa equação também satisfazem que $2m^2|n!$.

Primeiramente, como 4 não divide n^2+1, temos que m é sempre ímpar. Logo, basta mostrarmos que $m^2|n!$, já que claramente $n!$ tem fator 2.

Note que $m \leq n$. Sabemos que se m é composto, então $m|(m-1)!$. Logo, $m^2|m!$ e como $m \leq n$, $m!|n!$ e então $m^2|n!$, como desejado.

Veja que para m primo isso não é verdade. Logo, basta mostrarmos que existem infinitas soluções de $n^2+1 = 2m^2$ com m composto. Sabemos que as soluções da equação são dadas por $n_k + m_k\sqrt{2} = (1+\sqrt{2})^{2k+1}$ e que a sequência (m_k) satisfaz $m_{k+2} - 6m_{k+1} + m_k = 0$, $m_0 = 1$, $m_1 = 7$. Portanto, m_1 é múltiplo de 7 e, como toda recorrência módulo algum número é periódica, segue que existem infinitos múltiplos de 7. Portanto, temos infinitos valores de m compostos, como desejado.

□

Problemas

1. Mostre que as soluções da equação $5x^2 - y^2 = 4$ são $(x,y) = (F_{2n-1}, L_{2n-1})$, em que (F_k) é a sequência de Fibonacci e (L_k) é a sequência de Lucas.
2. Encontre o menor inteiro positivo n para o qual $19n+1$ e $95n+1$ sejam ambos quadrados perfeitos.
3. Seja p um número primo. Mostre que a equação $x^2 - py^2 = -1$ tem solução se, e só se, p é da forma $4k+1$.
4. Encontre todos os naturais n tais que $n+1$ e $3n+1$ são ambos quadrados perfeitos.
5. Encontre todos os pares de inteiros positivos (x,y) tais que $x(x+y) = y^2+1$.
6. (Irlanda 1995) Encontre todos os inteiros a tais que a equaçao $x^2 + axy + y^2 = 1$ possua infinitas soluções (x,y) inteiras.
7. (a) Seja k um inteiro positivo. Mostre que a equação $x^2 - (k^2-1)y^2 = -1$ não possui solução inteira.

   (b) Seja k um inteiro diferente de quadrado perfeito. Mostre que existe A tal que a equação $x^2-(a^2-1)y^2 = k$ não possui solução inteira para todo a tal que $a > A$.
8. (Vietnã 1992) Encontre todos os pares de inteiros positivos (x,y) satisfazendo a equação $x^2+y^2-5xy+5 = 0$.
9. (Irã 2013) Seja $p = n^2+1$ um primo. Determine as soluções inteiras da equação $x^2 - (n^2+1)y^2 = n^2$.
10. (Shortlist 2016) Seja a um inteiro positivo diferente de quadrado perfeito e considere a equação

$$k = \frac{x^2 - a}{x^2 - y^2}.$$

Seja A o conjunto dos inteiros positivos k para os quais a equação admite solução em $\mathbb{Z}^2$ com $x > \sqrt{a}$, e seja B o conjunto dos inteiros positivos para os quais a equação admite solução em $\mathbb{Z}^2$ com $0 \leq x < \sqrt{a}$. Mostre que $A = B$.

11. (China TST 2018) Determine todos os pares de inteiros positivos (x, y) tais que $(xy + 1)(xy + x + 2)$ é um quadrado perfeito.

12. (Romênia TST 2011) Mostre que existem infinitos inteiros positivos n tais que $n^2 + 1$ possui dois divisores positivos cuja diferença é n.

13. Sejam x e y inteiros tais que $\dfrac{x^2+1}{y^2} + 4$ é o quadrado de um inteiro. Prove que esse quadrado é igual a 9.

14. (Vingança 2019) Para todo inteiro positivo x, defina $P(x)$ como sendo o maior divisor primo de x. Prove que existem infinitos n tais que $P(n^2 + 1) < n.\pi^{-2019}$.

15. (OIbM 1989) Demonstrar que existe uma infinidade de pares (x, y) de números naturais tais que $2x^2 - 3x - 3y^2 - y + 1 = 0$.

16. (Longlist 1989) Determine o maior número real c tal que para todo $n \in \mathbb{N}$ temos $\{n \cdot \sqrt{2}\} \geq \frac{c}{n}$ em que $\{x\}$ é a parte fracionária de x. Determine ainda para este c, todos os $n \in \mathbb{N}$ para os quais $\{n \cdot \sqrt{2}\} = \frac{c}{n}$.

17. Prove que existem infinitos n tais que
    (a) $\lfloor n\sqrt{2} \rfloor$ é um quadrado perfeito.
    (b) $\lfloor n\sqrt{5} \rfloor$ é um quadrado perfeito.

18. (Vingança 2014)
    (a) Prove que para todo n natural $\text{mdc}(n, \lfloor n\sqrt{2} \rfloor) < \sqrt[4]{8}\sqrt{n}$.
    (b) Prove que existem infinitos n tais que $\text{mdc}(n, \lfloor n\sqrt{2} \rfloor) > \sqrt[4]{7.99}\sqrt{n}$.

19. (a) Prove que se n é um inteiro positivo, então $\{n\sqrt{5}\} > \dfrac{\sqrt{5}}{10n}$.
    (b) Prove que $c = \dfrac{\sqrt{5}}{10}$ é a maior constante com essa propriedade.

20. (Coreia 2019) Sejam m, n, k inteiros positivos satisfazendo as equações $m^2 + 1 = 2n^2$ e $2m^2 + 1 = 11k^2$. Determine o resto da divisão de n por 17.

21. (USA TST 2001) Determine todos os pares de inteiros não negativos (m, n) tais que $(m + n - 5)^2 = 9mn$.

3 Um Truque Especial

Nesta seção iremos ilustrar como aplicar equação de Pell para resolver algumas equações Diofantinas que podem ser bem mais difíceis com outras técnicas.

Exemplo 3.1 (OBM 2010) Encontre todos os pares (a, b) de inteiros positivos tais que

$$3^a = 2b^2 + 1.$$

Solução: Se a é par, analisando módulo 4, vemos que b tem que ser par. Logo, sendo $a = 2\ell$ e $b = 2k$, temos que

$$3^{2\ell} - 1 = 8k^2 \iff \left(\frac{3^\ell - 1}{2}\right)\left(\frac{(3^\ell + 1}{2}\right) = 2k^2.$$

Temos que mdc $\left(\frac{3^\ell-1}{2}, \frac{3^\ell+1}{2}\right) = 1$. Logo, temos dois casos:

$$\begin{cases} \frac{3^\ell-1}{2} = u^2 \\ \frac{3^\ell+1}{2} = 2v^2 \end{cases} \text{ ou } \begin{cases} \frac{3^\ell-1}{2} = 2u^2 \\ \frac{3^\ell+1}{2} = v^2 \end{cases}$$

No primeiro caso, a segunda equação nos dá $3^\ell = 4v^2 - 1 = (2v+1)(2v-1)$. Como mdc$(2v+1, 2v-1) = 1$, temos que $2v+1 = 3^x$ e $2v-1 = 3^y$ com $x+y = \ell$, $x > y$. Subtraindo as duas, obtemos $3^x - 3^y = 2$. Se $y > 0$, então 3 divide 2, absurdo. Logo $y = 0 \Rightarrow v = 1 \Rightarrow \ell = 1 \Rightarrow a = 2, b = 2$. No segundo caso, a primeira equação nos dá $3^\ell = 4u^2 + 1$. Mas então 3 divide $u^2 + 1$, absurdo, já que -1 não é resíduo quadrático módulo 3. Portanto, para a par, temos a solução $(a, b) = (2, 2)$.

Resta verificar o caso a ímpar. Seja $a = 2\ell + 1$. A equação passa a ser

$$3^{2\ell+1} = 2b^2 + 1 \Rightarrow (2b)^2 - 6(3^\ell)^2 = -2.$$

Vamos encontrar as soluções da equação $x^2 - 6y^2 = -2$. A solução minimal da equação $x^2 - 6y^2 = 1$ é $5+2\sqrt{6}$. Em seguida, pelo Teorema 2.1, devemos procurar as soluções $u, v \geq 0$ tais que $u^2 - 6v^2 = -2$ e $u + v\sqrt{6} < (5+2\sqrt{6})\sqrt{3}$. Note que

$$v\sqrt{6} < (5 + 2\sqrt{6})\sqrt{3} \Rightarrow v < \frac{5}{\sqrt{2}} + 2\sqrt{3} < \frac{5}{1,4} + 4 < 8 \Rightarrow v \leq 7.$$

Devemos testar $v = 0, 1, 2, .., 7$. Testando todas, vemos que a única solução é $u + v\sqrt{6} = 2 + \sqrt{6}$. Portanto, a solução geral da equação $x^2 - 6y^2 = -2$ é dada por

$$x_n + y_n\sqrt{6} = (2 + \sqrt{6})(5 + 2\sqrt{6})^n.$$

Voltando ao problema, queremos encontrar todas as soluções em que x_n é uma potência de 3. Sabemos que a sequência (y_n) satisfaz a recorrência $y_{n+2} - 10y_{n+1} + y_n = 0$, $y_0 = 1$, $y_1 = 9$. Queremos saber para quais os x_n que são potências de 3. Para isso, vamos analisar o período da recorrência (mod 27) para saber quando temos um múltiplo de 27 (veja que esses são os candidatos a ser potência de 3). Analisando os restos obtemos

$$1, 9, 8, -10, 0, 10, -8, -9, -1, -1, -9, -8, 10, 0, -10, 8, 9, 1, 1, 9, ...$$

de modo que o período módulo 27 é 18 e os múltiplos de 27 aparecem em $18k + 4$ e $18k + 13$.

Vamos agora analisar a mesma sequência módulo 17. Temos os seguintes restos:

$$1, 9, 4, -3, 0, 3, -4, 8, -1, -1, 8, -4, 3, 0, -3, 4, -8, 1, 1, 9, ...$$

de modo que o período módulo 17 é 18 e os múltiplos de 17 aparecem em $18k + 4$ e $18k + 13$.

Dessa forma, sempre que houver um múltiplo de 27, este número também é múltiplo de 17. Portanto, não pode haver nenhuma potência de 3 maior que 9 na sequência. Então, os únicos valores de y_n que são potências são $y_0 = 1$ e $y_1 = 9$, os quais nos dão as soluções $(a, b) = (1, 1)$ e $(a, b) = (5, 11)$.

Portanto, as soluções são $(1, 1)$, $(2, 2)$ e $(5, 11)$.

□

Lendo a solução você pode ter achado muito mágico escolher módulo 17, e mais mágico ainda que justamente nos mesmos índices tenham coincidido os múltiplos de 17 e 27. Mas na verdade não é tão mágico assim.

Note que essa parte final se traduz no seguinte problema: temos uma recorrência de 2ª ordem e queremos mostrar que não podemos ter potências arbitrariamente grandes de um certo número m entre seus termos.

A idéia então consiste em olhar a recorrência módulo alguma potência m^k mais baixa para saber quais os candidatos a serem as potências na recorrência. Sendo T o período módulo m^k, escolhe-se então um primo p com o mesmo período T e então analisamos os restos módulo p dos termos da sequência que são múltiplos de m^k para ver se há algo de interessante. Nem sempre funciona, mas é uma idéia a se tentar.

Em nosso caso, os termos eram múltiplos de p e por isso concluímos que, se há alguma potência, então ela tem que ser no máximo m^{k-1}. Mas podem acontecer outras coisas, por exemplo, o resto módulo p não ser um resíduo possível para potências de m módulo p, ou alguma outra propriedade que impessa que seja potência de m.

Mas como escolher o primo p? Para isso, vamos provar o seguinte resultado:

Teorema 3.1. *Seja $p > 2$ um número primo e $a_{n+2} + ba_{n+1} + ca_n = 0$ uma recorrência de ordem 2, com a_0 e a_1 inteiros dados. Além disso, seja T_p o período da recorrência quando analisada módulo p, ou seja T_p é o menor inteiro positivo tal que $a_{n+T_p} = a_n$ para todo n. Então, sendo $\left(\frac{a}{p}\right)$ o símbolo de Legendre, vale que:*

(i) Se $\left(\frac{b^2-4c}{p}\right) = 1$, então $T_p | p-1$;

(ii) Se $\left(\frac{b^2-4c}{p}\right) = -1$, então $T_p | p^2-1$;

(iii) Se $b^2 - 4c \equiv 0 \pmod p$, então $p|T_p$ e $T_p|p(p-1)$.

Demonstração: Sabemos que a equação característica da recorrência $a_{n+2} + ba_{n+1} + ca_n = 0$ é $x^2 + bx + c = 0$.

Note que, como p>2, temos

$$x^2 + bx + c \equiv 0 \pmod p \iff 4x^2 + 4bx + 4c = 0 \pmod p \iff (2x+b)^2 \equiv b^2 - 4c \pmod p.$$

Portanto, a equação $x^2+bx+c = 0$ tem solução módulo p se, e somente se, b^2-4c é resíduo quadrático $\pmod p$. Vamos então dividir em 3 casos:

Caso 1: $b^2 - 4c$ é resíduo quadrático não nulo módulo p.

Se isso ocorre, então temos duas soluções distintas, digamos α e β, para a congruência. $x^2+bx+c \equiv 0 \pmod p$. Vamos mostrar por indução que

$$a_n \equiv A.\alpha^n + B.\beta^n \pmod p, \quad (**)$$

para certos A e B determinados a partir de a_0 e a_1.

Note que A e B devem satisfazer $A + B \equiv a_0 \pmod p$ e $A.\alpha + B.\beta \equiv a_1 \pmod p$. Isolando B na primeira e substituindo na segunda, basta encontrarmos A tal que

$$A.\alpha + (a_0 - A).\beta \equiv a_1 \pmod p \iff A(\alpha - \beta) \equiv a_1 - \beta.a_0 \pmod p.$$

Como $\alpha \not\equiv \beta \pmod p$, $\alpha - \beta$ é inversível e então podemos tomar tal A. Definindo A e B como soluções do sistema, temos que a igualdade $(**)$ vale para 0 e 1. Supondo válido para k e $k+1$, pela recorrência, temos

$$a_{k+2} \equiv -ba_{k+1} - ca_k \equiv -b(A.\alpha^{k+1} + B.\beta^{k+1}) - c(A.\alpha^k + B.\beta^k) \equiv A.\alpha^k(-b.\alpha - c) + B.\beta^k(-b.\beta - c) \pmod p$$

Mas $\alpha^2 + b\alpha + c \equiv 0 \pmod p$ e $\beta^2 + b\beta + c \equiv 0 \pmod p$. Substituindo na equação acima, obtemos

$$a_{k+2} \equiv A.\alpha^{k+2} + B.\beta^{k+2} \pmod p,$$

completando a indução.

Agora, seja T_p o período. Note que ele certamente existe. De fato, como a quantidade máxima de pares de números consecutivos na sequência $\pmod p$ é p^2 e temos infinitos pares, certamente existem dois iguais, e como cada termo é definido a partir de dois anteriores, certamente ela é periódica $\pmod p$ e esse período existe.

Procuramos então o menor número T_p tal que para todo n vale a igualdade

$$a_{n+T_p} \equiv a_n \pmod p \iff A.\alpha^{n+T_p} + B.\beta^{n+T_p} \equiv A.\alpha^n + B.\beta^n \pmod p \iff$$
$$\iff A.\alpha^n(\alpha^{T_p} - 1) \equiv B.\beta^n(1 - \beta^{T_p}) \pmod p.$$

Veja que se α ou β é múltiplo de p, por exemplo β, então $a_n \equiv A.\alpha^n \pmod p$ e então é fácil ver que $T_p = ord_p(\alpha)$ e sabemos que $T_p|p-1$. O mesmo vale se p divide A ou B. Suponha então que p não divide nenhuma das raízes e nem A e nem B. Temos então que

$$(\alpha\beta^{-1})^n(\alpha^{T_p} - 1) \equiv BA^{-1}.(1 - \beta^{T_p}) \pmod p.$$

Veja que, se $\alpha^{T_p} - 1 \not\equiv 0 \pmod p$, então $(\alpha\beta^{-1})^n$ é constante módulo p. Mas isso ocorre se, e somente se, $\alpha\beta^{-1} \equiv 1 \pmod p \iff \alpha \equiv \beta \pmod p$, absurdo! Portanto, $\alpha^{T_p} - 1 \equiv 0 \pmod p$ e $\beta^{T_p} - 1 \equiv 0 \pmod p$. Como T_p é mínimo, temos que $T_p = \text{mmc}(ord_p(\alpha), ord_p(\beta))$ e, sendo $p-1$ um múltiplo comum, temos que $T_p|p-1$, como desejado.

Caso 2: $b^2 - 4c \equiv 0 \pmod p$.

Esse caso é parecido com o anterior, salvo pelo início. Lembrando da resolução de recorrências, devemos lembrar que a fórmula muda um pouco quando há raiz dupla. Dessa forma, por indução, sendo α a raiz dupla, podemos mostrar que

$$a_n \equiv \alpha^n(An + B) \pmod p.$$

Portanto, queremos T_p mínimo tal que para todo n valha

$$\alpha^{n+T_p}(A(n + T_p) + B) \equiv \alpha^n(An + B) \pmod p.$$

Se α é divisível por p, temos que a_n é sempre múltiplo de p e o período é 1. Se p divide A, temos $a_n \equiv B.\alpha^n \pmod p$ e então novamente o períod será $ord_p(\alpha)$. Em todos esses dois casos, vale que $T_p|p(p-1)$. Suponha então que p não divida α e nem A. Então, podemos cancelar α^n e ficamos com

$$\alpha^{T_p}(A(n + T_p) + B) \equiv An + B \pmod p \iff n.A.(\alpha^{T_p} - 1) \equiv B - B.\alpha^{T_p} - T_p.\alpha^{T_p} \pmod p.$$

Novamente, como deve valer para todo n, devemos ter $A.(\alpha^{T_p} - 1) \equiv B - B.\alpha^{T_p} - A.T_p.\alpha^{T_p} \equiv 0 \pmod p$. Como $A \not\equiv 0 \pmod p$, devemos ter $\alpha^{T_p} - 1 \equiv 0 \pmod p$ e, além disso, pela segunda igualdade ainda temos que $T_p \equiv 0 \pmod p$. Nesse caso, portanto, pela minimalidade de p, temos $T_p = p.ord_p(\alpha)$ e vale que $T_p|p(p-1)$.

Caso 3: $b^2 - 4c$ não é resíduo quadrático módulo p.

Nesse caso, a equação não tem raiz. Mas, sendo $\Delta = \sqrt{b^2 - 4c}$, podemos tomar a extensão de $\mathbb{Z}_p$ definida pelo conjunto $\mathbb{K} = \{a + b.\Delta \mid a, b \in \mathbb{Z}_p\}$. Olhando para os elementos não nulos de $\mathbb{K}$, temos um grupo de ordem $p^2 - 1$ com a operação multiplicação. Pelo Teorema de Lagrange, temos então que

$$x^{p^2-1} \equiv 1 \pmod p, \forall\ x \in \mathbb{K}. \quad (***)$$

Se você não viu o Teorema de Lagrande, pode simplesmente reproduzir a demonstração do Teorema de Fermat!

Evidentemente, em $\mathbb{K}$ a equação $x^2 + bx + c = 0$ tem raiz, basta tomarmos as raízes que obtemos pela equação do 2° grau. Sejam então α e β essas raízes.

A partir de agora o problema segue de modo idêntico ao caso 1. Por indução podemos mostrar que $a_n \equiv A.\alpha^n + B.\beta^n \pmod{p}$ para certos $A, B \in \mathbb{K}$ e então procedemos do mesmo modo, obtendo novamente $T_p = \text{mmc}(ord_p(\alpha), ord_p(\beta))$. A diferença é que temos $(***)$ em vez do Teorema de Fermat e concluímos que $T_p|p^2-1$.

□

Note que no Exemplo 3.1 a equação característica é $x^2 - 10x + 1 = (x-5)^2 - 24$. Logo, desconsiderando os primos 2 e 3, basta que $18|p^2-1$. Dessa forma, fica mais natural chutar 17.

Problemas

1. (Sérvia TST 2019) Resolva nos inteiros não negativos a equação $2^x = 5^y + 3$.
2. (TCS 2013) Encontre todas as triplas de inteiros não negativos (k, m, n) tais que $2^k + 7^m - 9^n = 0$.
3. Prove que a única solução nos inteiros positivos para a equação $5^a - 3^b = 2$ é $a = b = 1$.
4. Provar que não existe inteiro n tal que $n^2 - 2$ é uma potência de 7 com expoente maior que 1.
5. Encontrar todos os inteiros positivos n tais que $3^n - 2$ é um quadrado perfeito.
6. Encontre todos os inteirso não negativos x, y tais que $2.3^x + 1 = 7.5^y$.
7. Determine todos os pares de inteiros positivos (m, n) tais que $7^n = m^2 + m + 1$.

4 Referências

[1] MARTINEZ, Fabio Brochero; et al. Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro. 3 ed. Rio de Janeiro: IMPA, 2013.

[2] GELCA, Răzvan; ANDREEESCU, Titu. Putnam & Beyond. Springer Science+Business Media, LLC 2007.

[3] ANDREESCU, Titu; ANDRICA, Dorin. Number Theory: Structures, Examples, and Problems. Springer Science+Business Media, LLC 2009.

"With great power, comes great responsibility" - Uncle Ben