Frações Contínuas e Equação de Pell

Por Gabriel Bastos e João Lemos

Resumo

Dentro do estudo de equações diofantinas, uma identidade especial é a *equação de Pell*, que assume a forma $x^2 - Ay^2 = 1$, onde A é um inteiro positivo que não é quadrado. Estamos interessados nas soluções $(x, y) \in \mathbb{Z}^2$ (no caso em que A é um quadrado perfeito, digamos $A = B^2$, teríamos então $(x + By)(x - By) = 1$, o que nos dá apenas as soluções $x = \pm 1$, $y = 0$).
O objetivo deste artigo é demonstrar que existem infinitas soluções inteiras da equação de Pell quando A não é quadrado perfeito, além de estudar as equações $x^2 - Ay^2 = c$, $c \in \mathbb{Z}$ e $mx^2 - ny^2 = \pm 1$ (sempre estaremos em soluções inteiras). Este material também aborda a teoria de frações contínuas - uma diferente forma de representar os números reais, - e como essa representação dos reais facilita na procura por soluções inteiras da equação de Pell.

1 Introdução à Equação de Pell

Nesta seção é apresentado de uma forma intuitiva o que a Equação de Pell significa, e alguns problemas introdutórios relacionados ao tema são resolvidos. Nenhum teorema será demonstrado no momento (isso será feito na seção 3).
Começamos com o seguinte

Exemplo 1.1. *Encontre todos os inteiros positivos n tais que o triângulo de lados $n-1$, n e $n+1$ possui área inteira.*

Solução. A fórumla de Heron para a área do triângulo fornece que, sendo S a área do triângulo de lados $a = n - 1$, $b = n$ e $c = n + 1$,

$$S = \sqrt{\left(\frac{a+b+c}{2}\right)\left(\frac{-a+b+c}{2}\right)\left(\frac{a-b+c}{2}\right)\left(\frac{a+b-c}{2}\right)} = \frac{n}{2}\sqrt{3(n^2-4)}.$$

Disso segue que

$$4S^2 = 3n^2(n^2 - 4).$$

Portanto, n é par, digamos $n = 2k$, e então

$$S^2 = 12k^2(k^2 - 1).$$

Portanto, $3(k^2 - 1)$ deve ser um quadrado perfeito, e então é múltiplo de 9, de modo que podemos escrever

$$3(k^2 - 1) = 9\ell^2 \Longrightarrow k^2 - 3\ell^2 = 1.$$

Assim, o problema se resume a encontrar todas as soluções de $X^2 - 3Y^2 = 1$. Isso pode parecer difícil, e de fato, como existem infinitas soluções (sabemos disso, já que isso é uma Equação de Pell!), devemos caracterizá-las de algum modo. A seguinte identidade vai nos ajudar bastante:

$$(x^2 - 3y^2)(z^2 - 3t^2) = (xz - 3yt)^2 - 3(xt - yz)^2.$$

Isso nos diz que, se os pares (x, y) e (z, t) são soluções de $X^2 - 3Y^2 = 1$, então $(xz - 3yt, xt - yz)$ também é, de modo que conseguimos gerar diversas soluções. Assim, procuremos algumas soluções. Se $X = 1$, obtemos $Y = 0$, uma "solução trivial", já que ela não ajuda a gerar mais soluções:

$$(x^2 - 3y^2)(1^2 - 3 \cdot 0^2) = (x - 3y \cdot 0)^2 - 3(x \cdot 0 - y)^2 = x^2 - 3y^2.$$

Se $X = 2$, obtemos $Y = 1$, e com essa solução conseguimos mais soluções (note que, para qualquer escolha de sinais, $(\pm 2, \pm 1)$ temos uma solução):

$$x^2 - 3y^2 = (x^2 - 3y^2)\left((2\delta)^2 - 3\lambda^2\right) = (2x\delta - 3y\lambda)^2 - 3(x\lambda - 2y\delta)^2 = (2x\delta - 3y\lambda)^2 - 3(2y\delta - x\lambda)^2,$$

onde $\delta, \lambda \in \{-1, 1\}$. Escolhendo os sinais de forma conveniente, concluímos que $\delta = 1, \lambda = -1$ diz que (x, y) é solução se, e só se, $(2x + 3y, x + 2y)$ é solução. Além disso, $\delta = \lambda = 1$ diz que (x, y) é solução se, e só se, $(2x - 3y, 2y - x)$ é solução.
Isso já nos permite caracterizar um conjunto infinito de soluções! Definindo $x_1 = 2$, $y_1 = 1$, e

$$x_{n+1} = 2x_n + 3y_n, \quad y_{n+1} = x_n + 2y_n,$$

sabemos que todos os pares (x_n, y_n) são solução de $X^2 - 3Y^2 = 1$. É claro que $x_n, y_n > 0$, mas nós precisamos nos preocupar apenas com soluções inteiras positivas, já que $(\pm x, \pm y)$ é solução independentemente dos sinais escolhidos.
Apesar desse avanço, ainda temos que responder à seguinte pergunta: existem outras soluções além das parametrizadas na nossa recorrência? Intuitivamente, a resposta é não, já que os "saltos"entre soluções são os menores possíveis, pois $(2, 1)$ é a menor solução de inteiros positivos (a que minimiza x e y).
Vamos então mostrar por indução no valor de x que, se existe $y > 0$ inteiro satisfazendo $x^2 - 3y^2 = 1$, então $x = x_n$ para algum n. Os casos iniciais são triviais de se verificar. Caso tal y não exista, não há o que fazer. Caso $x^2 - 3y^2 = 1$ possua solução, então $(2x - 3y, 2y - x)$ também é solução, e

$$2x > 3y \iff 4x^2 > 9y^2 = 3(x^2 - 1)$$
$$2y \geq x \iff 4y^2 \geq x^2 = 3y^2 + 1.$$

Mas como $4y^2 = 3y^2 + 1 \implies y = 1 \implies x = 2 = x_1$. Logo podemos supor $4y^2 > 3y^2 + 1$, de modo que $(2x - 3y, 2y - x)$ é uma solução positiva, e como

$$2x - 3y < x \iff x < 3y \iff x^2 = 3y^2 + 1 < 9y^2,$$

segue que $2x - 3y = x_m$ para algum m, e consequentemente $2y - x = y_m$. Mas

$$x = 2(2x - 3y) + 3(2y - x) = 2x_m + 3y_m = x_{m+1},$$

o que completa a indução! Então os valores de n pedidos no enunciado são da forma $2x_m$, $m \geq 1$. □

Essa solução pode até parecer um pouco mágica, e até que tudo foi mera coincidência. Façamos mais um exemplo para convencê-lo de que talvez esse não seja o caso.

Exemplo 1.2. *Sejam F_n e L_n as sequência de Fibonacci e Lucas, que são definidas por*

$$F_0 = 0, F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n,$$

e

$$L_0 = 2, L_1 = 1, \quad L_{n+2} = L_{n+1} + L_n.$$

Mostre que (x, y) é uma solução de inteiros positivos de $5x^2 - y^2 = 4$ se, e só se, $(x, y) = (F_{2n-1}, L_{2n-1})$ para algum $n \geq 1$.

Solução. Como no exemplo anterior, vamos procurar, a partir de alguma solução (x, y), alguma solução menor, e então utilizar indução. Podemos aplicar a mesma ideia do exemplo anterior:

$$(x^2 - 5y^2)(z^2 - 5t^2) = (xz - 5yt)^2 - 5(xt - yz)^2.$$

Assim, encontrando uma solução para $X^2 - 5Y^2 = 1$, podemos encontrar mais soluções para $X^2 - 5Y^2 = -4$. A menor solução da primeira equação é $(9, 4)$. Com isso concluímos que (x, y) é solução de $X^2 - 5Y^2 = -4$ se, e só se, $(9x - 20y, 9y - 4x)$ é solução. Usemos indução no valor de x para mostrar que todas as soluções são da forma $(x, y) = (L_{2n+1}, F_{2n+1})$. Vamos supor que (x, y) é uma solução com $x \geq 21 \iff y \geq 9$ e que, para todo valor menor de x, se existe solução, ela é da forma desejada (as soluções com $y < 9$ podem ser encontradas à mão, e são (L_1, F_1), (L_3, F_3) e (L_5, F_5), e isso é suficiente para a indução). Note que

$$9x > 20y \iff 81(5y^2 - 4) = 81x^2 > 400y^2 \iff 5y^2 > 81 \cdot 4 \impliedby y \geq 9$$
$$9y > 4x \iff 81y^2 > 16x^2 = 16(5y^2 - 4).$$

Isso mostra que $(9x - 20, 9y - 4x)$ é uma solução em inteiros positivos, e como

$$9x - 20y < x \iff 2x < 5y \iff 4(5y^2 - 4) = 4x^2 < 25y^2,$$

segue existe $n \geq 1$ tal que

$$\begin{cases} 9x - 20y = L_{2n+1} \\ -4x + 9y = F_{2n+1} \end{cases} \iff \begin{cases} x = 9L_{2n+1} + 20F_{2n+1} \\ y = 4L_{2n+1} + 9F_{2n+1} \end{cases}.$$

Agora, temos que mostrar x, y estão nas sequências de Lucas e Fibonacci, respectivamente. Como determinar o índice? Sabemos que F_{2n+1} e L_{2n+1} satisfazem a mesma recorrência linear $a_{2n+1} = 3a_{2n-1} - a_{2n-3}$, e então qualquer combinação linear delas também satisfaz essa recorrência linear. Ou seja, basta olharmos os dois termos iniciais de cada uma das sequências $9L_{2n+1} + 20F_{2n+1}$ e $4L_{2n+1} + 9F_{2n+1}$; caso sejam números de Lucas e Fibonacci, todos os próximos termos serão. Vejamos:

$$9L_1 + 20F_1 = 29 = L_7 \quad \text{e} \quad 9L_3 + 20F_3 = 76 = L_9,$$

e

$$4L_1 + 9F_1 = 13 = F_7 \quad \text{e} \quad 4L_3 + 9F_3 = 43 = F_9.$$

Com isso, podemos concluir que $x = L_{2n+7}$ e $y = F_{2n+7}$, e portanto são números de Lucas e Fibonacci com índice ímpar, como queríamos mostrar. Isso termina a indução. □

Na solução desse problema, demos um salto da solução (L_{2n+1}, F_{2n+1}) para $(L_{2(n+3)+1}, F_{2(n+3)+1})$. Por que não pulamos de (L_{2n+1}, F_{2n+1}) para $(L_{2(n+1)+1}, F_{2(n+1)+1})$? Ainda mais, assumimos na indução que $y \geq 9$, e para $y < 9$ temos apenas três soluções (L_1, F_1), (L_3, F_3) e (L_5, F_5). Ou seja, como o nosso salto tem "tamanho 3"(de n para $n + 3$), dessas três soluções podemos saltar para qualquer outra. Tudo parece bastante coincidência, mas na verdade não é! Veja a seção 3.3 para explicações desse fato.

Antes de vermos mais alguns exemplos, vamos dar uma olhada nas soluções que encontramos para as equações $X^2 - 3Y^2 = 1$ e $X^2 - 5Y^2 = -4$. Ambas satisfazem recorrências, sendo que a primeira parece um pouco mais complicada; $x_1 = 2$, $y_1 = 1$ e

$$x_{n+1} = 2x_n + 3y_n, \quad y_{n+1} = x_n + 2y_n.$$

Mas podemos simplificar um pouco:

$$2y_{n+1} - x_{n+1} = y_n \implies x_n = 2y_n - y_{n-1},$$

e então

$$y_{n+1} = x_n + 2y_n = 4y_n - y_{n-1} \implies y_{n+1} = 4y_n - y_{n-1}$$

(note que podemos extender x_n e y_n "para trás", isto é, definir x_n e y_n com $n < 1$ ainda satisfzendo a relação de recorrência. Por isso é válido dizer que $x_n = 2y_n - y_{n-1}$). Façamos um processo similar para encontrar x_n como recorrência linear:

$$2x_{n+1} - 3y_{n+1} = x_n \implies 3y_n = 2x_n - x_{n-1},$$

de modo que

$$x_{n+1} = 2x_n + 3y_n = 4x_n - x_{n-1} \implies x_{n+1} = 4x_n - x_{n-1}.$$

Portanto, x_n e y_n satisfazem a mesma recorrência linear! Ao resolver essa recorrência, vamos encontrar que

$$x_n = \frac{(2+\sqrt{3})^n + (2-\sqrt{3})^n}{2} \quad \text{e} \quad y_n = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{2\sqrt{3}}.$$

Voltando para as soluções de $X^2 - 5Y^2 = -4$, que são da forma (L_{2n+1}, F_{2n+1}), já sabemos que

$$L_n = \alpha^n + \beta^n \quad \text{e} \quad F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

onde $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$. Vejamos portanto o que descobrimos sobre a conjunto de soluções de $X^2 - 3Y^2 = 1$ e $X^2 - 5Y^2 = -4$:

1. Ambas satisfazem recorrências lineares;
2. As soluções gerais são encontradas a partir de soluções pequenas;
3. As fórmulas para uma solução de $X^2 - 3Y^2 = 1$ podem ser parametrizadas em função de números do conjunto $\mathbb{Q}[\sqrt{3}] \stackrel{\text{def}}{=} \{a + b\sqrt{3} \colon a, b \in \mathbb{Q}\}$, enquanto as soluções de $X^2 - 5Y^2 = -4$ podem ser parametrizadas em função de números do conjunto $\mathbb{Q}[\sqrt{5}] \stackrel{\text{def}}{=} \{a + b\sqrt{5} \colon a, b \in \mathbb{Q}\}$.

De fato, existem resultados similares para qualquer equação do tipo Pell; veja a seção 3 para mais detalhes.
Por fim, exploremos mais a identidade

$$(x^2 - Ay^2)(z^2 - At^2) = (xz - Ayt)^2 - A(xt - yz)^2. \tag{1}$$

Isso está nos dizendo que o conjunto $\{x^2 - Ay^2 : x, y \in \mathbb{Z}\}$ é fechado sobre a operação de multiplicação. Inspirado nos exemplos acima, podemos fatorar $x^2 - Ay^2 = (x + y\sqrt{A})(x - y\sqrt{A})$. Definindo $\mathbb{Q}[\sqrt{A}] \stackrel{\text{def}}{=} \{a + b\sqrt{A} : a, b \in \mathbb{Q}\}$, $\mathbb{Z}[\sqrt{A}] \stackrel{\text{def}}{=} \{a + b\sqrt{A} : a, b \in \mathbb{Z}\}$ e a função *norma* $N : \mathbb{Q}[\sqrt{A}] \to \mathbb{Q}$ por $N(\alpha) = \alpha \cdot \overline{\alpha}$, onde $\alpha = a + b\sqrt{A} \in \mathbb{Q}[\sqrt{A}]$ e $\overline{\alpha} = a - b\sqrt{A}$. Qualquer equação do tipo Pell é equivalente a resolver a equação

$$N(\alpha) = c, \alpha \in \mathbb{Z}[\sqrt{A}], c \in \mathbb{Z}.$$

Além do mais, sabemos que a norma é multiplicativa, ou seja, $N(\alpha\beta) = N(\alpha)N(\beta)$ para todos $\alpha, \beta \in \mathbb{Q}[\sqrt{A}]$, já que isso é equivalente à equação (1). Caso A não seja quadrado perfeito, então todo elemento $\alpha \in \mathbb{Q}[\sqrt{A}]$ possui representação única, isto é, $p + q\sqrt{A} = r + s\sqrt{A}$, $p, q, r, s \in \mathbb{Q}$, então $p = r$ e $q = r$. Isso nos garante que, caso a equação $N(\alpha) = 1$ possua alguma solução não trivial, ou seja, $\alpha \neq 1$, então ela possui infinitas, pois α^n será solução para todo n, e $\alpha^n = \alpha^m \implies m = n$ assumindo que A não é quadrado perfeito.
Finalizamos esta seção com mais alguns exemplos de como ideias relacionadas à equação de Pell podem ser aplicadas.

Exemplo 1.3. *Encontre o menor inteiro positivo para o qual $n+1$ e $3n+1$ são quadrados perfeitos.*

Solução. Queremos achar o menor n tal que

$$b^2 = n + 1 \text{ e } a^2 = 3n + 1 \implies a^2 - 3b^2 = -2.$$

A fim de achar o menor n procuraremos a menor solução, que nesse caso é $(1, 1)$ mas essa não conta porque $n = 0$ não vale. Então procuramos a próxima solução, que é $(5, 3)$. Logo $n = 8$. □

Exemplo 1.4. *Encontre o menor inteiro positivo para o qual $19n + 1$ e $95n + 1$ são quadrados perfeitos.*

Solução. Queremos achar o menor n tal que

$$b^2 = 19n + 1 \text{ e } a^2 = 95n + 1 \implies a^2 - 5b^2 = -4$$

Para isso ser suficiente temos que garantir que $b \equiv \pm 1 \pmod{19}$. Por outro lado, do exemplo 1.2, sabemos que todas as soluções são da forma $(a, b) = (L_{2n+1}, F_{2n+1})$. Logo, o problema se resume a encontrar o menor n tal que $F_{2n+1} \equiv \pm 1 \pmod{19}$, e ainda temos de verificar se $L_{2n+1}^2 \equiv 1 \pmod{95}$. Isso pode ser um pouco trabalhoso, já que o primeiro número de Fibonacci com a propriedade desejada é $F_{17} = 1597$. Outro cálculo diz que $L_{17}^2 = 3571^2 \equiv 1 \pmod{95}$. Portanto, o número desejado é

$$n = \frac{F_{17}^2 - 1}{19} = 134232.$$

□

Exemplo 1.5. *Encontre todos os pares de inteiros positivos (x, y) tais que $x(x + y) = y^2 + 1$.*

Solução. Manipulamos para transformar a equação em uma Pell:

$$x(x + y) = y^2 + 1 \Leftrightarrow x^2 = y^2 - xy + 1 \Leftrightarrow 5x^2 = 4y^2 - 4xy + x^2 + 4 \Leftrightarrow (2y - x)^2 - 5x^2 = -4.$$

Mas já sabemos a solução geral dessa equação! Devemos ter $2y - x = L_{2n+1}, x = F_{2n+1}$, ou seja, $x = F_{2n+1}$ e $y = \frac{F_{2n+1} + L_{2n+1}}{2}$. □

Exemplo 1.6. *Determine todos os inteiros a tais que $x^2 + axy + y^2 = 1$ possui infinitas soluções $(x, y) \in \mathbb{Z}^2$.*

Solução. Analisando a equação dada como uma equação quadrática em x, queremos que o discrimante seja quadrado perfeito:

$$a^2y^2 - 4y^2 + 4 = T^2 \implies T^2 - (a^2-4)y^2 = 4.$$

Caso $a^4 - 4$ não seja quadrado perfeito e $a^2 - 4 > 0$, sabemos que essa equação possui infinitas soluções, já que a equação $X^2 - (a^2-4)Y^2 = 1$ possui infinitas soluções (vamos assumir isso por enquanto; para uma demonstração, veja o Teorema 3.1), e $T^2 - (a^2-4)y^2 = 4$ possui uma solução $(T, y) = (a, 1)$. A verificação disso pode ser feita utilizando a multiplicatividade da norma. Mas $a^2 - 4 = b^2 \implies (a+b)(a-b) = 4$, e é trivial que as únicas soluções são $a = \pm 2, b = 0$. Logo, $|a| > 2$ nos diz que $a^2 - 4 > 0$ não é quadrado perfeito. Basta analisar os casos $|a| = 1, 2$. Se $|a| = 2$, queremos resolver

$$x^2 + y^2 \pm 2xy = 1 \implies (x \pm y)^2 = 1,$$

que possui infinitas soluções para qualquer escolha do sinal. Caso $|a| = 1$, como a equação

$$T^2 + 3y^2 = 4$$

possui finitas soluções, então há finitos valores para (x, y). Então a resposta é todos os a com $|a| > 1$. □

2 Frações Contínuas

O conjunto dos números reais $\mathbb{R}$ possui uma definição formal complicada. Entretanto, sabemos que todo número real pode ser bem aproximado por números racionais. De fato, dado um número real r, existe um inteiro $\lfloor r \rfloor$ tal que $\lfloor r \rfloor \leq r < \lfloor r \rfloor + 1$. Escrevendo a representação decimal de $r - \lfloor r \rfloor$:

$$r - \lfloor r \rfloor = 0, a_0a_1a_2\ldots, \quad a_i \in \{0, 1, \ldots, 9\},$$

e definindo $r_n = \sum_{i=0}^{n} 10^{n-i}a_i$, temos que $0 \leq r - \left(\lfloor r \rfloor + \frac{r_n}{10^n}\right) \leq \frac{1}{10^n}$, o que é uma aproximação com um erro bem pequeno caso n seja grande. Mais geralmente, temos que $\left|r - \frac{\lfloor pr \rfloor}{p}\right| \leq \frac{1}{p}$ para todo natural p, de modo que existe uma aproximação de r por um racional de denominador p com erro menor que $1/p$.

A representação decimal de r é dada através das aproximações fornecidas pela escolha de $p = 10^n$. Devido à praticidade de trabalhar com a representação decimal, ela tornou-se a mais comum dentre as diversas formas de representar os reais. Entretanto, a escolha da base 10 pode ocultar aproximações mais eficientes (com erro menor em relação ao denominador). Por exemplo,

$$\left|\pi - \frac{355}{113}\right| < \frac{1}{3000000} < \left|\pi - \frac{3141592}{1000000}\right| \quad \text{e} \quad \left|e - \frac{19}{7}\right| < \frac{1}{200} < \left|e - \frac{271}{100}\right|,$$

e isso mostra que $\frac{355}{113}$ e $\frac{19}{7}$ aproximam π e e, respectivamente, com um erro menor que aproximações decimais de denominadores muito maiores.

Mas como encontrar as aproximações mais eficientes de um número real? A maneira de obtê-las é através da representação por *frações contínuas* de um número real. Esta seção, portanto, apresenta ao leitor tal forma de representar os números reais.

Dado um real x, definimos

$$\alpha_0 = x, \quad a_0 = \lfloor \alpha_0 \rfloor$$
$$\text{e, se } \alpha_n \notin \mathbb{Z}, \alpha_{n+1} = \frac{1}{\alpha_n - a_n} \text{ para todo } n \geq 0. \qquad (\times)$$

Se $\alpha_n \in \mathbb{Z}$ para algum n, definimos então

$$x = [a_0; a_1, a_2, \ldots, a_n] \overset{\text{def}}{=} a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}.$$

Caso $\alpha_n \notin \mathbb{Z}$ para todo n, temos então

$$x = [a_0; a_1, a_2, \ldots] \overset{\text{def}}{=} a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}.$$

Provaremos adiante que tal representação, chamada de representação por frações contínuas de x, faz sentido.
Se a representação por frações contínuas de x for finita, então x é racional. A recíproca também vale: se $x = p/q$ $(q > 0)$, então os $a_i's$ vêm do algoritmo de Euclides:

$$\begin{aligned} p &= a_0 q + r_1 & 0 \leq r_1 < q \\ q &= a_1 r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 &= a_2 r_2 + r_3 & 0 \leq r_3 < r_2 \\ &\vdots & \vdots \\ r_{n-1} &= a_n r_n \end{aligned}$$

Segue que

$$x = p/q = a_0 + \frac{r_1}{q} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 \frac{1}{a_2 + \frac{r_2}{r_3}}} =$$

$$= \cdots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}.$$

Desse modo, a identificação dos racionais é muito mais simples levando em conta a representação por frações contínuas.
A partir de agora, suponha que x é irracional, e portanto $x = [a_0; a_1, a_2, \ldots]$. Definimos os números $p_n, q_n \in \mathbb{Z}$, com $q_n > 0$ e $\text{mdc}(p_n, q_n) = 1$ tais que $p_n/q_n = [a_0; a_1, a_2, \ldots, a_n]$ e dizemos que p_n/q_n é a n-ésima *reduzida* de x. Começamos com a seguinte

Proposição 2.1. *Seja $s_0, s_1, s_2, \ldots$ uma sequência de reais com $s_k > 0$ para $k > 0$. Definimos $x_0 = s_0$, $x_1 = s_0 s_1 + 1$ e $x_{n+2} = s_{n+2} x_{n+1} + x_n$, e também definimos $y_0 = 1$, $y_1 = s_1$ e $y_{n+2} = s_{n+2} y_{n+1} + y_n$. Então*

$$[s_0; s_1, s_2, \ldots, s_n] = s_0 + \cfrac{1}{s_1 + \cfrac{1}{s_2 + \ddots + \cfrac{1}{s_n}}} = \frac{x_n}{y_n}$$

para todo $n \geq 0$, e $x_{n+1} y_n - x_n y_{n+1} = (-1)^n$.

Demonstração. Fazemos indução em n. Os casos $n = 0, 1$ são imediatos por definição. Para $n = 2$, veja que

$$[s_0, s_1, s_2] = s_0 + \frac{1}{s_1 + \frac{1}{s_2}} = \frac{s_0 s_1 s_2 + s_0 + s_2}{s_1 s_2 + 1} = \frac{s_2(s_0 s_1 + 1) + s_0}{s_1 s_2 + 1} = \frac{s_2 x_1 + x_0}{s_2 y_1 + y_0} = \frac{x_n}{y_n}.$$

Se o resultado é verdadeiro para n, note que, trocando s_n por $s_n + \frac{1}{s_{n+1}}$ (e portanto trocando x_n por $(s_n + \frac{1}{s_{n+1}})x_{n-1} + x_{n-2}$ e y_n por $(s_n + \frac{1}{s_{n+1}})y_{n-1} + y_{n-2}$),

$$\begin{aligned} [s_0; s_1, s_2, \ldots, s_n, s_{n+1}] &= [s_0; s_1, s_2, \ldots, s_n + \frac{1}{s_{n+1}}] \\ &= \frac{(s_n + \frac{1}{s_{n+1}})x_{n-1} + x_{n-2}}{(s_n + \frac{1}{s_{n+1}})y_{n-1+y_{n-2}}} \\ &= \frac{s_{n+1}(s_n x_{n-1} + x_{n-2}) + x_{n-1}}{s_{n+1}(s_n y_{n-1} + y_{n-2}) + y_{n-1}} \\ &= \frac{s_{n+1} x_n + x_{n-1}}{s_{n+1} y_n + y_{n-1}} \\ &= \frac{x_{n+1}}{y_{n+1}}. \end{aligned}$$

Ainda precisamos mostrar a segunda afirmação. A prova é novamente por indução em n, sendo o caso $n = 0$ imediato e o caso $n = 1$ uma verificação trivial. Se $x_{n+1}y_n - x_n y_{n+1} = (-1)^n$, então

$$\begin{aligned} x_{n+2}y_{n+1} - x_{n+1}y_{n+2} &= (s_{n+2}x_{n+1} + x_n)y_{n+1} - (t_{n+2}y_{n+1} + y_n)x_{n+1} \\ &= x_n y_{n+1} - x_{n+1}y_n = (-1)^{n+1}. \end{aligned}$$

□

Assim, sendo $x = [a_0; a_1, a_2, \ldots]$ e p_n/q_n e dadas as sequências (p_n) e (q_n) satisfazendo $p_0 = a_0$, $p_1 = a_1a_0 + 1$, $p_{n+2} = a_{n+2}p_{n+1} + p_n$ e $q_0 = 1$, $q_1 = a_1$ e $q_{n+2} = a_{n+2}q_{n+1} + q_n$, sabemos que $p_n/q_n = [a_0; a_1, a_2, \ldots, a_n]$ e que $p_{n+1}q_n - p_n q_{n+1} = (-1)^n$, ou seja, p_n e q_n são coprimos, além de que $q_i > 0$ para todo i. Logo, (p_n) e (q_n) são os numeradores e os denominadores das reduzidas de x, respectivamente.
Definindo α_n como em (×), sabemos que $x = [a_0; a_1, a_2 \ldots, a_{n-1}, \alpha_n]$, de modo que, pela Proposição 2.1, temos

$$x = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}.$$

Disso, segue a

Proposição 2.2. *Temos que*

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{(\alpha_{n+1} + \beta_{n+1})q_n^2},$$

em que

$$\beta_{n+1} = \frac{q_{n-1}}{q_n}.$$

Demonstração. Sabemos que

$$x - \frac{p_n}{q_n} = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - p_n q_{n-1}}{(\alpha_{n+1}q_n + q_{n-1})q_n} = \frac{(-1)^n}{(\alpha_{n+1} + \beta_{n+1})q_n^2}.$$

Podemos concluir que

$$\left| x - \frac{p_n}{q_n} \right| = \frac{1}{(\alpha_{n+1} + \beta_{n+1})q_n^2}.$$

Entretanto, como $\lfloor \alpha_{n+1} \rfloor = a_{n+1}$ e $0 < \beta_{n+1} = \frac{q_{n-1}}{q_n} < 1$, temos $a_{n+1} < \alpha_{n+1} + \beta_{n+1} < a_{n+1} + 2$, de modo que

$$\frac{1}{(a_{n+1} + 2)q_n^2} < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{a_{n+1}q_n^2}.$$

□

Corolário 2.3. *Sendo $x = [a_0; a_1, a_2, \ldots]$ e p_n/q_n sua n-ésima reduzida, temos $\lim_{n\to\infty} \frac{p_n}{q_n} = x$, o que dá sentido à igualdade*

$$[a_0; a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}.$$

Demonstração. Como q_n é uma sequência de inteiros estritamente crescente e $a_n \geq 1$ para $n > 0$, temos então que $\lim_{n\to\infty} \left| x - \frac{p_n}{q_n} \right| = 0$ pela Proposição 2.2. Assim, podemos dizer que

$$[a_0; a_1, a_2, \ldots] = \lim_{n\to\infty} [a_0; a_1, a_2, \ldots, a_n] = \lim_{n\to\infty} \frac{p_n}{q_n} = x.$$

□

Ainda da Proposição 2.2, podemos concluir o seguinte

Teorema 2.4 (Dirichilet)**.** *Dado um número α irracional, a desigualdade*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$$

ocorre para infinitos pares de inteiros (p, q).

Podemos concluir também a seguinte

Proposição 2.5. *Para todo $n \geq 0$, temos que*

$$\frac{p_{2n}}{q_{2n}} \leq \frac{p_{2n+2}}{q_{2n+2}} \leq x \leq \frac{p_{2n+3}}{q_{2n+3}} \leq \frac{p_{2n+1}}{q_{2n+1}}.$$

Demonstração. Como visto acima, $x - \frac{p_n}{q_n} = \frac{(-1)^n}{(\alpha_{n+1}q_n + q_{n-1})q_n}$, que é positivo para n par e negativo par n ímpar. Além disso,

$$\begin{aligned}\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} &= \frac{a_{n+2}p_{n+1} + p_n}{a_{n+2}q_{n+1} + q_n} - \frac{p_n}{q_n} = \frac{a_{n+2}(p_{n+1}q_n - p_nq_{n+1})}{q_n(a_{n+2}q_{n+1} + q_n)} \\ &= \frac{a_{n+2}(-1)^n}{q_nq_{n+2}},\end{aligned}$$

que é positivo para n par e negativo para n ímpar. □

Nós já vimos que todo número real x possui uma representação por frações contínuas. Nas próximas duas proposições, veremos que toda sequência de inteiros positivos $a_0, a_1, a_2, \ldots$ é a representação por frações contínuas de um único número irracional.

Proposição 2.6. *Seja $a_0, a_1, \ldots, a_n$ uma sequência de inteiros positivos, e (p_k/q_k) a sequência de reduzidas da fração contínua $[a_0; a_1, a_2, \ldots, a_n]$. Então o conjunto dos númeos reais cuja representação por frações contínuas começa com $a_0, a_1, \ldots, a_n$ é*

$$\begin{aligned}J(a_0; a_1, a_2, \ldots, a_n) &= \left\{\frac{p_n}{q_n}\right\} \cup \{[a_0; a_1, a_2, \ldots, a_n, \alpha], \alpha > 1\} \\ &= \begin{cases} \left[\frac{p_n}{q_n}, \frac{p_n+p_{n-1}}{q_n+q_{n-1}}\right) & \text{se } n \text{ for par} \\ \left(\frac{p_n+p_{n-1}}{q_n+q_{n-1}}, \frac{p_n}{q_n}\right] & \text{se } n \text{ for ímpar.} \end{cases}\end{aligned}$$

Demonstração. Seja x um real cuja representação por frações contínuas começa com $a_0, a_1, \ldots, a_n$, ou seja, ou $x = [a_0; a_1, a_2, \ldots, a_n]$ ou $x = [a_0; a_1, a_2, \ldots, a_n, \alpha_{n+1}]$, com $\alpha_{n+1} > 1$. Assim, é suficiente descobrir a imagem da função $G\colon (1, +\infty) \to \mathbb{R}$ dada por $G(\alpha) = [a_0; a_1, a_2, \ldots, a_n, \alpha]$. Mas sabemos que $G(\alpha) = \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}} = \frac{p_n}{q_n} + \frac{(-1)^n}{(\alpha q_n + q_{n-1})q_n}$. Assim, G é decrescente quando n é par e crescente quando n é ímpar. Como $\lim\limits_{\alpha\to 1} G(\alpha) = \dfrac{p_n + p_{n-1}}{q_n + q_{n-1}}$ e $\lim\limits_{\alpha\to\infty} G(\alpha) = \dfrac{p_n}{q_n}$, temos então que a imagem de G é

$$G((1, +\infty)) = \begin{cases} \left(\frac{p_n}{q_n}, \frac{p_n+p_{n-1}}{q_n+q_{n-1}}\right) & \text{se } n \text{ for par} \\ \left(\frac{p_n+p_{n-1}}{q_n+q_{n-1}}, \frac{p_n}{q_n}\right) & \text{se } n \text{ for ímpar,} \end{cases}$$

donde o resultado segue. □

Proposição 2.7. *Dada uma sequência de inteiros positivos $a_0, a_1, a_2 \ldots$, existe exatamente um número real x cuja representação por frações contínuas é $[a_0; a_1, a_2 \ldots]$.*

Demonstração. Sendo (p_k/q_k) a sequência de reduzidas da fração contínua $[a_0; a_1, a_2, \ldots]$, sabemos pela proposição 2.5 que $\frac{p_{2n}}{q_{2n}} \leq \frac{p_{2n+2}}{q_{2n+2}} \leq \frac{p_{2n+3}}{q_{2n+3}} \leq \frac{p_{2n+1}}{q_{2n+1}}$. Como $\lim_{k\to\infty} \frac{p_{2k+1}}{q_{2k+1}} - \frac{p_{2k}}{q_{2k}} = 0$, então, considerando os intervalos $I_k = \left[\frac{p_{2k}}{q_{2k}}, \frac{p_{2k+1}}{q_{2k+1}}\right]$, temos $I_k \supset I_{k+1}$ e $|I_k| \to 0$ quando $k \to \infty$, e portanto existe um único x tal que

$$\bigcap_{k\geq 0} I_k = \{x\}.$$

(verifique isso, caso você não conheça esse resultado!) Assim, segue que $\frac{p_{2k}}{q_{2k}} \leq x \leq \frac{p_{2k+1}}{q_{2k+1}}$. Mas $\frac{p_{2k}}{q_{2k}}, \frac{p_{2k+1}}{q_{2k+1}} \in J(a_0; a_1, a_2, \ldots, a_{2k})$, que é um intervalo. Portanto, a representação por frações contínuas de x começa com $a_0, a_1, \ldots, a_{2k}$ pela proposição anterior. Como isso vale para todo k, a representação por frações contínuas de x é $[a_0; a_1, a_2, \ldots]$. Note que x é irracional. □

Os próximos dois teoremas serão úteis na próxima seção, em que mostraremos um método para encontrar soluções da equação de Pell.

Teorema 2.8. *Para todos p, q inteiros, com $q < q_{n+1}$, temos*

$$|q_n x - p_n| \leq |qx - p|,$$

sendo a desigualdade estrita se $0 < q < q_n$.

Demonstração. Se $p/q = p_n/q_n$, o resultado é imediato, já que $\text{mdc}(p_n, q_n) = 1$. Se $p/q \neq p_n/q_n$, temos

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| \geq \frac{1}{qq_n} > \frac{1}{q_n q_{n+1}} = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right|.$$

Isso nos diz que p/q não está entre p_n/q_n e p_{n+1}/q_{n+1}. Como x está nesse intervalo, segue que

$$\left|x - \frac{p}{q}\right| \geq \left|\frac{p_n}{q_n} - \frac{p}{q}\right| \geq \frac{1}{qq_n} \qquad \text{ou} \qquad \left|x - \frac{p}{q}\right| \geq \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p}{q}\right| \geq \frac{1}{qq_{n+1}}.$$

Em ambos os casos,

$$\left|x - \frac{p}{q}\right| \geq \frac{1}{qq_{n+1}}$$
$$\implies |qx - p| \geq \frac{1}{q_{n+1}}.$$

Segue da Proposição 2.2 e de $q_{n+1} = a_{n+1}q_n + q_{n-1}$ que

$$|x - p_n/q_n| = \frac{1}{(a_{n+1}q_n + q_{n-1} + \{\alpha_n\}q_n)q_n} \leq \frac{1}{q_n q_{n+1}},$$

e então

$$|qx - p| \geq \frac{1}{q_{n+1}} \geq |q_n x - p_n|,$$

como desejado. □

Teorema 2.9. *Se $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$, então p/q é uma reduzida de x.*

Demonstração. Tome n de modo que $q_n \leq q < q_{n+1}$ ($q_0 = 1$ por definição, então tal n existe). Se $p/q \neq p_n/q_n$, concluímos, como no teorema anterior, que $|x - p/q| > \frac{1}{qq_{n+1}}$, e que p/q não está entre p_n/q_n e p_{n+1}/q_{n+1}. Isso já nos diz que $q < \frac{q_{n+1}}{2}$, pois caso contrário $|x - p/q| \geq \frac{1}{2q^2}$.
Se p_n/q_n estiver entre x e p/q, temos que $|x - p/q| \geq |p_n/q_n - p/q|$. Caso p_{n+1}/q_{n+1} esteja entre x e p/q, temos que

$$\left|x - \frac{p}{q}\right| \geq \left|\frac{p_{n+1}}{q_{n+1} - \frac{p}{q}}\right| = \left|\frac{p_n}{q_n} - \frac{p}{q}\right| - \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right|.$$

Em ambos os casos,

$$\begin{aligned}\left|x - \frac{p}{q}\right| &\geq \left|\frac{p_n}{q_n} - \frac{p}{q}\right| - \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| \\ &\geq \frac{1}{qq_n} - \frac{1}{q_n q_{n+1}} = \frac{q_{n+1} - q}{qq_n q_{n+1}} \\ &\geq \frac{1}{2qq_n} \quad (\text{pois } q < \frac{q_{n+1}}{2}) \\ &\geq \frac{1}{2q^2},\end{aligned}$$

novamente um absurdo. Portanto, $p/q = p_n/q_n$, como desejado. □

Problemas Propostos

2.1. *Mostre que a fração contínua de um real t é periódica se, e somente se, t é raiz de uma equação do segundo grau de coeficientes inteiros.*

2.2. *Encontre todos os números reais x tais que, para algum n, $\frac{1}{x} = [1, 1, \ldots, 1, x]$, onde aparecem n uns na fração contínua.*

2.3. *Encontre as frações contínuas de $\sqrt{a^2 - 1}$, $\sqrt{a^2 + 1}$, $\sqrt{a^2 - 2}$, $\sqrt{a^2 - a}$, com a natural.*

2.4. *Qual a fração contínua de $\frac{1+\sqrt{5}}{2}$? Encontre também a n-ésima reduzida de $\frac{1+\sqrt{5}}{2}$.*

2.5. *Seja $(a_n)_{n\geq 1}$ a sequência definida por $a_n = n\sqrt{5} - \lfloor n\sqrt{5} \rfloor$. Encontre os valores de $n \leq 2011$ para os quais a_n é máximo ou mínimo.*

3 Equação de Pell

Nesta seção, nosso objeto de estudo são as equações do *tipo Pell*, compostas pela própria equação de Pell $x^2 - Ay^2 = 1$ (lembre-se que A não é quadrado perfeito), e as equações $x^2 - Ay^2 = c$, com $c \in \mathbb{Z}$, e $mx^2 - ny^2 = \pm 1$, com $m, n \in \mathbb{N}$. Além disso, veremos como a representação por frações contínuas auxilia na busca por soluções dessas equações.
A Equação de Pell, em sua essência, emerge como uma poderosa ferramenta destinada à aproximação de raízes de números naturais A maiores que 1, desprovidos de quadrados perfeitos. Observe:

$$X^2 - DY^2 = 1 \Leftrightarrow \sqrt{A} = \sqrt{\frac{X^2 - 1}{Y^2}} \approx X/Y$$

A intuição de que a forma $\sqrt{A} \approx \frac{x}{y}$ poderia ser a melhor aproximação possível para números irracionais foi percebida muito antes do formalismo matemático moderno, com uma nota de cautela deixada por Pitágoras: $\sqrt{D} \neq \frac{x}{y}$ quando D é um número natural maior que 1, livre de quadrados. Além disso, como veremos adiante, a equação $X^2 - AY^2 = \pm 1$ fornece aproximações extremamente boas de $\sqrt{A}$ (erro pequeno com relação ao denominador). Com o mesmo próposito a teoria de frações contínuas foi desenvolvida, isso explica a íntima relação entre ambas. Posteriormente muitas aplicações da equação de Pell foram descobertas principalmente na solução de equações Diofantinas, que são o foco do nosso estudo.

3.1 A equação $x^2 - Ay^2 = 1$

Estamos interessados nas soluções inteiras de $x^2 - Ay^2 = 1$, com A sendo um inteiro positivo livre de quadrados. Definimos a *norma* no corpo $\mathbb{Q}[\sqrt{A}] \stackrel{\text{def}}{=} \{x + y\sqrt{A} \colon x, y \in \mathbb{Q}\}$ por $N \colon \mathbb{Q}[\sqrt{A}] \to \mathbb{Q}$ por $N(x + y\sqrt{A}) = (x + y\sqrt{A})(x - y\sqrt{A}) = x^2 - Ay^2$, $x, y \in \mathbb{Q}$. Assim, um elemento $\alpha \in \mathbb{Z}[\sqrt{A}] \stackrel{\text{def}}{=} \{x + y\sqrt{A} \colon x, y \in \mathbb{Z}\}$ possui inverso em $\mathbb{Z}[\sqrt{A}]$ se, e somente se, $N(\alpha) = 1$.
Mas qual a vantagem de trabalhar em $\mathbb{Z}[\sqrt{A}]$ ao invés de $\mathbb{Z}$? O principal motivo é o fato da norma N ser multiplicativa, isto é, dados $\alpha, \beta \in \mathbb{Q}[\sqrt{A}]$, vale

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta).$$

(fica a cargo do leitor provar tal propriedade) Deste modo, fica claro que, se encontramos uma solução para $N(\alpha) = 1$, então encontramos infinitas. De fato, $N(\alpha^n) = N(\alpha)^n = 1$ pela multiplicatividade da norma.
Além disso, como

$$x^2 - Ay^2 = 1 \iff N(x + y\sqrt{A}) = (x + y\sqrt{A})(x - y\sqrt{A}) = 1,$$

intuitivamente, para x, y grandes, o número $x - y\sqrt{A}$ deve ser muito pequeno, o que nos fornece uma aproximação boa de $\sqrt{A}$ por racionais. Portanto, a norma é algo natural de se trabalhar.
A seguir, mostramos que a equação de Pell sempre possui solução inteira não trivial.

Teorema 3.1. *A equação $x^2 - Ay^2 = 1$, onde A é um inteiro positivo que não é quadrado perfeito, sempre possui solução não trivial, isto é, com $xy \neq 0$.*

Demonstração. Do teorema 2.4, sabemos que existem infinitos $p, q \in \mathbb{Z}$ satisfazendo

$$\left|\sqrt{A} - \frac{p}{q}\right| < \frac{1}{q^2}, \tag{1}$$

uma vez que $\sqrt{A}$ é irracional. Além disso, podemos supor que p, q são positivos, uma vez que $\sqrt{A}$ é positivo. Disso, podemos concluir que

$$\begin{aligned} |p^2 - q^2 A| = |p + q\sqrt{A}||p - q\sqrt{A}| &= q^2 \left|\sqrt{A} - \frac{p}{q}\right| \left|\sqrt{A} + \frac{p}{q}\right| \\ &\leq \left|\sqrt{A} + \frac{p}{q}\right| = \left|2\sqrt{A} - \left(\sqrt{A} - \frac{p}{q}\right)\right| \\ &\leq 2\sqrt{A} + \left|\sqrt{A} - \frac{p}{q}\right| \leq 2\sqrt{A} + 1. \end{aligned}$$

Sendo (p_n/q_n) uma sequência de racionais satisfazendo (1), temos então $|p_n^2 - Aq_n^2| \leq 2\sqrt{A} + 1$ para todo n. Logo, a igualdade $p_n^2 - Aq_n^2 = k$ ocorre para infinitos n e algum $k \neq 0$, já que $p_n^2 - Aq_n^2$ é

inteiro e portanto pode assumir apenas finitos valores.
Podemos dizer também que existem $0 \leq a, b < k$ tais que $p_n^2 - Aq_n^2 = k$ ocorre para infinitos n, e $p_n \equiv a \pmod{k}$, $q_n \equiv b \pmod{k}$, uma vez que há apenas $|k|^2$ valores para $(p_n, q_n) \pmod{k}$. Vamos assumir que todos os termos de (p_n/q_n) satisfazem $p_n^2 - Aq_n^2 = k$ e $p_n \equiv a \pmod{k}$ e $q_n \equiv b \pmod{k}$ (descartamos os termos que não satisfazem todas essas condições).
Considere dois termos p/q e u/v da sequência (p_n/q_n) com $p + q\sqrt{A} > u + v\sqrt{A} > 0$ (note que, dados $x, y, a, b \in \mathbb{Q}$, a igualdade $x + y\sqrt{A} = a + b\sqrt{A}$ ocorre se, e somente se, $a = x$ e $b = y$, de modo que podemos esolher p/q e u/v com tal propriedade). Então, sendo

$$\begin{aligned} x + y\sqrt{A} = \frac{p + q\sqrt{A}}{u + v\sqrt{A}} &= \frac{(p + q\sqrt{A})(u - v\sqrt{A})}{u^2 - Av^2} = \frac{(p + q\sqrt{A})(u - v\sqrt{A})}{k} \\ &= \frac{pu - Aqv}{k} + \frac{pv - qu}{k}\sqrt{A}, \end{aligned}$$

temos $x + y\sqrt{A} \in \mathbb{Z}[\sqrt{A}]$, pois $pu - Aqv \equiv a^2 - Ab^2 \equiv p^2 - Aq^2 = k \equiv 0 \pmod{k}$, e $pv - qu \equiv ab - ab \equiv 0 \pmod{k}$. Além disso,

$$\begin{aligned} &(x + y\sqrt{A})(u + v\sqrt{A}) = p + q\sqrt{A} \\ \implies &N(x + y\sqrt{A})N(u + v\sqrt{A}) = N(p + q\sqrt{A}) \\ \implies &N(x + y\sqrt{A})k = k \\ \implies &N(x + y\sqrt{A}) = 1. \end{aligned}$$

Para mostrar que $xy \neq 0$, note que, como $p + q\sqrt{A} > u + v\sqrt{A} > 0$, então $x + y\sqrt{A} = \frac{p+q\sqrt{A}}{u+v\sqrt{A}} > 1$. Caso $x = 0$, não obtemos solução da equação $-Ay^2 = 1$; se $y = 0$, teríamos $x = \pm 1$, e então $|x + y\sqrt{A}| = 1$. Assim, $x + y\sqrt{A} > 1 \Rightarrow xy \neq 0$, ou seja, (x, y) é uma solução não trivial da equação $x^2 - Ay^2 = 1$. □

Como visto na prova acima, a condição $xy \neq 0$ para uma solução da equação de Pell é equivalente a $x + y\sqrt{A} > 1$ (supondo x, y inteiros não negativos). Assim, dentre as soluções (x, y) de inteiros positivos (e portanto com $xy \neq 0$) de $x^2 - Ay^2 = 1$, existe uma com x mínimo, e consequentemente y mínimo e também $x + y\sqrt{A}$ mínimo. Chamamos tal par (x, y) de *solução minimal* da equação $x^2 - Ay^2 = 1$. O próximo teorema caracteriza todas as soluções da equação de Pell.

Teorema 3.2. *Seja (x_1, y_1) a solução minimal da equação $x^2 - Ay^2 = 1$, então, para qualquer solução $(x, y) \in \mathbb{N}^2$ de $x^2 - Ay^2 = 1$, existe $n \in \mathbb{N}$ tal que $x + y\sqrt{A} = (x_1 + y_1\sqrt{A})^n$.*

Demonstração. Já sabemos que toda solução $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n$ é solução da equação de Pell pela multiplicatividade da norma. Suponha que $(p, q) \in \mathbb{N}^2$ é uma solução com

$$x_n + y_n\sqrt{A} \leq p + q\sqrt{A} < x_{n+1} + y_{n+1}\sqrt{A}.$$

Então,

$$1 \leq (p + q\sqrt{A})(x_n - y_n\sqrt{A}) = (px_n - qy_nA) + (qx_n - py_n)\sqrt{A} < x_1 + y_1\sqrt{A},$$

já que $x_n \pm y_n\sqrt{A} = (x_1 \pm y_1\sqrt{A})^n$, e então $(x_{n+1} + y_{n+1}\sqrt{A})(x_n - y_n\sqrt{A}) = x_1 + y_1\sqrt{A}$.
Note que, sendo $x, y \in \mathbb{N}$,

$$\begin{aligned} x^2 - y^2A = 1 \implies \frac{x^2}{y^2} = A + \frac{1}{y^2} > A \\ \implies \frac{x}{y} > \sqrt{A}. \end{aligned}$$

Portanto, $\frac{p}{q} \cdot \frac{x_n}{y_n} > A \implies px_n - qy_nA > 0$. Além disso, $p \geq x_n$ e $q \geq y_n$ já que $x_n + y_n\sqrt{A} \leq p + q\sqrt{A}$ são soluções da equação de Pell. Logo,

$$\begin{aligned} \frac{p^2}{q^2} = A + \frac{1}{q^2} \leq A + \frac{1}{y_n^2} = \frac{x_n^2}{y_n^2} \\ \implies \frac{p}{q} \leq \frac{x_n}{y_n} \implies qx_n - py_n \geq 0. \end{aligned}$$

Como $(px_n - qy_nA, qx_n - py_n)$ é uma solução menor do que a minimal (x_1, y_1), devemos ter ou $px_n - qy_nA \leq 0$ ou $qx_n - py_n \leq 0$. Como provamos $px_n - qy_nA > 0$ e $qx_n - py_n \geq 0$, segue que $qx_n - py_n = 0$ e então $px_n - qy_nA = 1$. Ou seja, $(p+q\sqrt{A})(x_n - y_n\sqrt{A}) = 1 \Rightarrow p+q\sqrt{A} = x_n + y_n\sqrt{A}$. Como $\sqrt{A} \notin \mathbb{Q}$, temos

$$\mathbb{Q} \ni p - x_n = \sqrt{A}(y_n - q),$$

e $\sqrt{A} \cdot k \in \mathbb{Q}$, $k \in \mathbb{Z} \Rightarrow k = 0$, segue que $x_n = p$ e $y_n = q$, como desejado. □

3.2 A equação $x^2 - Ay^2 = -1$

Acabamos de mostrar que toda equação $x^2 - Ay^2 = 1$ possui solução não trivial (reforçamos que A nunca é quadrado perfeito). Todavia, a equação $x^2 - Ay^2 = -1$ nem sempre possui solução. Sendo p um divisor primo de A, devemos ter $x^2 \equiv -1 \pmod{p}$. Ou seja, é necessário que p seja 2 ou da forma $4k+1$, $k \in \mathbb{N}$. Essa condição não é suficiente (o teorema 3.5 apresenta uma condição necessária e suficiente). A seguir, apresentamos alguns resultados interessantes na procura por soluções de $x^2 - Ay^2 = -1$.
Caso exista alguma solução, sabemos que existe uma solução minimal, isto é, que minimiza x, y e $x + y\sqrt{A} > 1$, onde $x, y \in \mathbb{N}$. Começamos com a

Proposição 3.3. *Se a equação $x^2 - Ay^2 = -1$ possui solução, seja $(x_0, y_0) \in \mathbb{N}^2$ sua solução minimal. Então, se $(a, b) \in \mathbb{N}^2$ é a solução minimal de $x^2 - Ay^2 = 1$, temos*

$$\left(x_0 + y_0\sqrt{A}\right)^2 = a + b\sqrt{A}, \qquad e \qquad x_0^2 = \frac{a-1}{2}.$$

Demonstração. Note que $(x_0+y_0\sqrt{A})^2$ é solução de $N(\alpha) = 1$. Assim, pelo Teorema 3.2, sabemos que existe $n > 0$ com

$$\left(x_0 + y_0\sqrt{A}\right)^2 = \left(a + b\sqrt{A}\right)^n.$$

Suponha que $n > 1$. Se $n = 2$, teríamos $x_0 + y_0\sqrt{A} = a + b\sqrt{A}$ pois ambos são positivos, um absurdo, pois $N(x_0 + y_0\sqrt{A}) = -1 \neq 1 = N(a + b\sqrt{A})$. Logo, $n > 2$ e

$$\left(\left(x_0 + y_0\sqrt{A}\right)\left(a - b\sqrt{A}\right)\right)^2 = \left(a + b\sqrt{A}\right)^{n-2} > 1$$
$$\Longrightarrow \left(x_0 + y_0\sqrt{A}\right) > \left(x_0 + y_0\sqrt{A}\right)\left(a - b\sqrt{A}\right) > 1 \quad \text{e} \quad N\left(\left(x_0 + y_0\sqrt{A}\right)\left(a - b\sqrt{A}\right)\right) = -1,$$

o que é um absurdo, pois $x_0 + y_0\sqrt{A}$ é, por hipótese, a solução minimal de $N(\alpha) = -1$. Logo, $n = 1$ e $(x_0 + y_0\sqrt{A})^2 = a + b\sqrt{A}$. Como $x_0^2 - Ay_0^2 = -1$, temos que $2x_0^2 + 2x_0y_0\sqrt{A} = a - 1 + b\sqrt{A}$ (apenas somamos as duas igualdades). Portanto $x_0^2 = (a-1)/2$, como desejado. □

Isso já mostra que a condição sobre os fatores primos de A não é suficiente para garantir que $x^2 - Ay^2 = -1$ sempre possui solução. De fato, $35 + 6\sqrt{34}$ é a solução minimal de $x^2 - 34y^2 = 1$, mas $\frac{35-1}{2} = 17$ não é quadrado perfeito, e então $x^2 - 34y^2 = -1$ não possui solução, apesar de seu fator primo ímpar, o 17, ser $4 \cdot 4 + 1$. Provemos agora um caso particular importante.

Proposição 3.4. *Se $A = p$ é um primo, $x^2 - py^2 = -1$ possui solução se, e somente se, p é da forma $4k+1$.*

Demonstração. Se a equação possui solução, é trivial que $p \equiv 1 \pmod{4}$. Suponha que $p \equiv 1 \pmod{4}$.
Seja (x, y) a solução minimal de $x^2 - py^2 = 1$. Então,

$$1 = x^2 - py^2 \equiv x^2 - y^2 \pmod{4},$$

e isso nos dá x ímpar e y par. Suponha $x = 2t + 1$, $y = 2s$. Então

$$(x+1)(x-1) = py^2$$
$$\Longrightarrow 4(t+1)t = 4ps^2$$
$$\Longrightarrow (t+1)t = ps^2.$$

Como $t+1$ e t são coprimos, existem $a, b \in \mathbb{N}$ com $s^2 = a^2b^2$, $a^2|t$ e $b^2|t+1$, uma vez que $s^2|(t+1)t$. Seja $t = a^2k$, $t+1 = b^2\ell$. Segue que $b^2\ell - a^2k = 1$ e

$$a^2b^2k\ell = ps^2 \implies k\ell = p.$$

Temos então $k = p$ ou $k = 1$. Se $k = p$, teríamos $\ell = 1$ e $b^2 - a^2p = 1$. Mas $ab = s = y/2$, e então $y > a > 0$, absurdo, pois (x, y) é por definição a solução mínima de $u^2 - pv^2 = 1$. Logo, temos $k = 1$ e $\ell = p$, o que nos dá

$$b^2p - a^2 = 1 \implies a^2 - pb^2 = -1,$$

uma solução de $u^2 - pv^2 = -1$, como desejado. □

Vimos que, se $x^2 - Ay^2 = -1$ possui solução, os fatores primos de A são 2 ou da forma $4k+1$. Além disso, se A for par, não é possível que A seja múltiplo de 4, uma vez que $x^2 \equiv -1 \pmod 4$ não possui solução. Disso, segue que $A \equiv 1, 2 \pmod 4$.
Para finalizar, temos o seguinte

Teorema 3.5. *Suponha que $A \equiv 1, 2 \pmod 4$ é um inteiro não quadrado perfeito. Seja (x_0, y_0) a solução minimal de $x^2 - Ay^2 = 1$. Então, a equação $x^2 - Ay^2 = -1$ possui solução se, e somente se, $x_0 \equiv -1 \pmod{2A}$.*

Demonstração. Se a $x^2 - Ay^2 = -1$ possui solução, segue da Proposição 3.3 que sua solução minimal (a, b) satisfaz

$$(a + b\sqrt{A})^2 = x_0 + y_0\sqrt{A} \implies x_0 = a^2 + Ab^2.$$

Portanto,

$$x_0 = a^2 + Ab^2 = (a^2 - Ab^2) + 2Ab^2 \equiv -1 \pmod{2A}.$$

Ainda precisamos mostrar a recíproca. Suponha então $x_0 \equiv -1 \pmod{2A}$. Já sabemos que x_0 é ímpar e y_0 é par. Então escreva $x_0 = 2At - 1$ e $y_0 = 2s$. Conclui-se que

$$\begin{aligned}(x_0 + 1)(x_0 - 1) &= Ay_0^2 \\ \implies 4At(At - 1) &= 4As^2 \\ \implies t(At - 1) &= s^2.\end{aligned}$$

Como t e $At - 1$ são coprimos, segue que $t = M^2$ e $At - 1 = N^2 \implies N^2 - AM^2 = -1$, como desejado. □

Esse teorema, apesar de fornecer uma condição necessária e suficiente para que $x^2 - Ay^2 = -1$ possua solução, pode não ser de grande utilidade, já que depende da solução minimal de $x^2 - Ay^2 = 1$, e nem sempre é fácil determinar $x_0 \pmod{2A}$.

3.3 A equação $x^2 - Ay^2 = c$

Como no caso $c = -1$, sabemos que c precisa ser resíduo quadrático módulo qualquer divisor de A, já que $x^2 - Ay^2 \equiv x^2 \equiv c \pmod A$. Da mesma forma, essa condição não é suficiente. Os próximos resultados, porém, auxiliam na busca por soluções.

Teorema 3.6. *Seja $\alpha = x_0 + y_0\sqrt{A}$ a solução minimal de $x^2 - Ay^2 = 1$. Se $(x, y) \in \mathbb{N}^2$ é solução de $x^2 - Ay^2 = c$, existem $u, v \in \mathbb{N}$ tais que $u + v\sqrt{A} < \alpha\sqrt{|c|}$ e $x + y\sqrt{A} = (u + v\sqrt{A})\alpha^k$ para algum $k \in \mathbb{N}$.*

Demonstração. Caso $x + y\sqrt{A} < \alpha\sqrt{|c|}$, basta escolher $(u, v) = (x, y)$ e $k = 0$. Caso contrário, temos $x + y\sqrt{A} \geq \alpha\sqrt{|c|}$. Tome $\ell \in \mathbb{Z}$ tal que $\sqrt{|c|} \leq (x + y\sqrt{A})\alpha^\ell < \alpha\sqrt{|c|}$. É claro que $\ell < 0$ e que $N((x + y\sqrt{A})\alpha^\ell) = c$. Sendo $u + v\sqrt{A} = (x + y\sqrt{A})\alpha^\ell$, com $u, v \in \mathbb{Z}$, já temos $x + y\sqrt{A} = (u + v\sqrt{A})\alpha^{-\ell}$, com $-\ell \in \mathbb{N}$. Basta mostrar que $u, v \in \mathbb{N}$.
Como $N(u + v\sqrt{A}) = c$, temos

$$\begin{aligned}|u - v\sqrt{A}|\sqrt{|c|} \leq |u - v\sqrt{A}||u + v\sqrt{A}| &= |c| \\ \implies |u - v\sqrt{A}| \leq \sqrt{|c|} &\leq u + v\sqrt{A}.\end{aligned}$$

Portanto,

$$\begin{aligned}u - v\sqrt{A} \leq u + v\sqrt{A} &\implies v \geq 0 \\ -u + v\sqrt{A} \leq u + v\sqrt{A} &\implies u \geq 0.\end{aligned}$$

□

O teorema acima nos diz que pode haver diversas "soluções minimais", já que as soluções pequenas estão gerando todas as soluções.

Teorema 3.7. *Seja $\alpha = x_0 + y_0\sqrt{A}$ a solução minimal de $x^2 - Ay^2 = 1$. Se $(x, y) \in \mathbb{N}^2$ é solução de $x^2 - Ay^2 = c$, existem $u, v \geq 0$ inteiros tais que $u + v\sqrt{A} \leq \sqrt{\alpha|c|}$ e $x + y\sqrt{A} = (u + v\sqrt{A})\alpha^k$ ou $x + y\sqrt{A} = |u - v\sqrt{A}|\alpha^k$, com $k \in \mathbb{N}$.*

Demonstração. A demonstração é similar à do Teorema 3.6, e é deixada como exercício. □

Definimos $\alpha = x_0 + y_0\sqrt{A}$ como a solução minimal de $x^2 - Ay^2 = 1$. Os Teoremas 3.6 e 3.7 nos dizem que todas as soluções de $x^2 - Ay^2 = c$, caso existam, são o produto de alguma solução $u + v\sqrt{A} \leq \alpha\sqrt{|c|}$ (de módulo pequeno) com alguma potência de α.
Assim, vamos dizer que duas soluções $u+v\sqrt{A}$, $u'+v'\sqrt{A}$ são *associadas* se existe $k \in \mathbb{Z}$ satisfazendo $u + v\sqrt{A} = (u' + v'\sqrt{A})\alpha^k$. Uma condição necessária e suficiente para que duas soluções $u + v\sqrt{A}$ e $u' + v'\sqrt{A}$ sejam associadas é

$$\frac{u + v\sqrt{A}}{u' + v'\sqrt{A}} \in \mathbb{Z}[\sqrt{A}] \iff \frac{uu' - vv'A}{c}, \frac{u'v - uv'}{c} \in \mathbb{Z}.$$

Caso duas soluções β e γ sejam associadas, o resultado é trivial. Caso $\beta/\gamma \in \mathbb{Z}[\sqrt{A}]$, temos

$$N(\beta\gamma^{-1}) = N(\beta)N(\gamma^{-1}) = N(\beta)N(\gamma)^{-1} = c \cdot c^{-1} = 1,$$

e então $b\gamma^{-1}$ é solução de $x^2 - Ay^2 = 1$, de modo que, pelo Teorema 3.2, existe $k \in \mathbb{Z}$ com $\beta\gamma^{-1} = \alpha^k \implies \beta = \gamma\alpha^k$, ou seja, β e γ são soluções associadas.
Portanto, podemos dividir o conjunto de soluções de $x^2 - Ay^2 = c$ em classes de elementos associados. Os teoremas 3.6 e 3.7 mostram que toda solução de $x^2 - Ay^2 = c$ é associada a uma solução $u + v\sqrt{A} < \alpha\sqrt{|c|}$ $(u, v \in \mathbb{N})$, e que portanto existem finitas classes. No caso $c = 1$ obtemos apenas uma classe, como mostramos no teorema 3.2. Para $c = -1$ também obtemos apenas uma classe, já que, sendo (x_1, y_1) a solução minimal de $x^2 - Ay^2 = 1$ e (x_{-1}, y_{-1}) a solução minimal de $x^2 - Ay^2 = -1$, e, dada qualquer solução (u, v) dessa última equação, sabemos que existe $n \in \mathbb{Z}$ de modo que

$$(u + v\sqrt{A})^2 = (x_1 + y_1\sqrt{A})^n = (x_{-1} + y_{-1}\sqrt{A})^{2n} \implies (u + v\sqrt{A}) = \pm(x_{-1} + y_{-1}\sqrt{A})^n,$$

e portanto todas as soluções de $x^2 - Ay^2 = -1$ são associadas (e então há apenas uma classe de soluções nesse caso).
Seja K uma classe de soluções associadas. Vamos definir a solução minimal $u+v\sqrt{A}$ deste conjunto. Escolha v como o menor inteiro não negativo que ocorre em K. Então sabemos que $|u|$ está determinado. Caso $\pm u + v\sqrt{A} \in K$, escolha $u \geq 0$. Caso contrário, u está bem determinado.
A seguir, enunciamos dois teoremas cujas demonstrações podem ser encontradas em [1].

Teorema 3.8. *Seja K uma classe de soluções associadas da equação $x^2 - Ay^2 = c$, e $u + v\sqrt{A}$ a solução minimal de K. Se $c > 0$ e $x_1 + y_1\sqrt{A}$ é solução minimal da equação de Pell, valem as desigualdades*

$$0 \leq v \leq \frac{y_1}{\sqrt{2(x_1 + 1)}}\sqrt{c} \tag{2.8.1}$$

$$0 < |u| \leq \sqrt{\frac{c}{2}(x_1 + 1)}. \tag{2.8.2}$$

Teorema 3.9. *Seja K uma classe de soluções associadas da equação $x^2 - Ay^2 = c$, e $u + v\sqrt{A}$ a solução minimal de K. Se $c < 0$ e $x_1 + y_1\sqrt{A}$ é solução minimal da equação de Pell, valem as desigualdades*

$$0 < v \leq \frac{y_1}{\sqrt{2(x_1 - 1)}}\sqrt{-c} \tag{2.9.1}$$

$$0 \leq |u| \leq \sqrt{\frac{-c}{2}(x_1 - 1)}. \tag{2.9.2}$$

Provemos agora que o número de classes da equação $x^2 - Ay^2 = \pm p$, com p primo, é no máximo dois (o sinal de p é previamente escolhido).

Proposição 3.10. *A equação*

$$x^2 - Ay^2 = \pm p,$$

onde p é um número primo, possui no máximo uma solução $u+v\sqrt{A}$, com $u \geq 0$ e u e v satisfazendo (2.8.1) e (2.8.2) ou (2.9.1) e (2.9.2).

Demonstração. Sejam $u + v\sqrt{A}$, $r + s\sqrt{A}$ duas soluções satisfazendo (2.8.1) e (2.8.2) ou (2.9.1) e (2.9.2). Note que

$$\begin{aligned} u^2 - Av^2 = \pm p &\implies u^2s^2 - Av^2s^2 = \pm ps^2 \\ r^2 - As^2 = \pm p &\implies r^2v^2 - As^2v^2 = \pm pv^2 \\ \implies u^2s^2 - r^2v^2 &= \pm p(s^2 - v^2). \end{aligned}$$

Assim, obtemos $us \equiv \pm rv \pmod p$ (este sinal $\pm$ *não depende* do sinal de p). Agora, note que

$$\begin{aligned} (u^2 - Av^2)(r^2 - As^2) &= u^2r^2 + A^2v^2s^2 - A(u^2s^2 - r^2v^2) \\ &= (ur \mp Avs)^2 - A(us \mp rv)^2. \end{aligned}$$

Se escolhermos o sinal na equação acima de modo que $p|us \mp rv$, teremos $uv^{-1} \equiv \pm rs^{-1} \pmod p$. Como $A \equiv (uv^{-1})^2 \equiv \pm(uv^{-1})(rs^{-1}) \pmod p$, e então $ur \mp Avs \equiv ur \mp (\pm(uv^{-1})(rs^{-1}))vs \equiv 0 \pmod p$, ou seja, $p|us \mp rv \Rightarrow p|ur \mp Avs$. Por outro lado,

$$(ur \mp Avs)^2 - A(us \mp rv)^2 = (u^2 - Av^2)(r^2 - As^2) = p^2,$$

de modo que

$$\left(\frac{ur \mp Avs}{p}\right)^2 - A\left(\frac{us \mp rv}{p}\right)^2 = 1,$$

e ambos os números dos parênteses são inteiros. Logo, se $x_1 + y_1\sqrt{A}$ é a solução minimal de $x^2 - Ay^2 = 1$, temos

$$|us \mp rv| \geq py_1 \qquad \text{ou} \qquad us \mp rv = 0.$$

Uma rápida verificação nos diz que, no segundo caso, $u = r$ e $v = s$, que é o queremos mostrar. Porém, caso o primeiro caso ocorra, sabemos que

$$\begin{aligned} 0 \leq v \leq \frac{y_1}{\sqrt{2(x_1 \pm 1)}}\sqrt{p}, &\qquad 0 \leq s \leq \frac{y_1}{\sqrt{2(x_1 \pm 1)}}\sqrt{p} \\ 0 \leq u \leq \sqrt{\frac{p}{2}(x_1 \pm 1)}, &\qquad 0 \leq r \leq \sqrt{\frac{p}{2}(x_1 \pm 1)}, \end{aligned}$$

de acordo com o sinal de p em $x^2 - Ay^2 = \pm p$. Daí segue que

$$0 \leq us \leq \frac{py_1}{2}, \qquad 0 \leq rv \leq \frac{py_1}{2},$$

e então

$$|us \mp rv| \leq py_1 \implies |us \mp rv| = py_1.$$

Caso a igualdade ocorra, devemos ter $u = \sqrt{\frac{p}{2}(x_1 \pm 1)} = r$, e da mesma forma $v = s$, como desejado. □

3.4 A equação $mx^2 - ny^2 = \pm 1$

Consideremos as equações

$$mx^2 - ny^2 = \pm 1 \tag{$*$}$$

e

$$x^2 - mny^2 = 1. \tag{$*$}$$

(na primeira equação, o sinal é previamente escolhido. Assumimos sempre que $m, n > 1$ e que mn não é quadrado perfeito)
Assim como na equação de Pell, vamos mostrar que, se $mx^2 - ny^2 = \pm 1$ possui solução, existe uma solução minimal que gera todas as outras soluções. Para mais detalhes, ver [2].
A partir de agora, vamos considerar soluções de ($*$) com x, y inteiros não negativos. Portanto,

caso haja alguma solução, existe uma solução com x mínimo, e portanto y e $\sqrt{m}x + \sqrt{n}y$ mínimos também. Assim como nas subseções anteriores, temos que $\sqrt{m}x + \sqrt{n}y$ é solução de $(\ast)$ se

$$(\sqrt{m}x + \sqrt{n}y)(\sqrt{m}x - \sqrt{n}y) = mx^2 - ny^2 = \pm 1.$$

Sendo $\sqrt{m}x + \sqrt{n}y$ uma solução de $(\ast)$ e $r + s\sqrt{mn}$ uma solução de $(*)$, temos que

$$(\sqrt{m}x + \sqrt{n}y)(r + s\sqrt{mn}) = \sqrt{m}(xr + nys) + \sqrt{n}(mxs + yr)$$

também é solução de $(\ast)$. A verificação é deixada para o leitor.
Além disso, dadas duas soluções $\sqrt{m}x + \sqrt{n}y$, $\sqrt{m}u + \sqrt{n}v$ de $(\ast)$, o produto

$$(\sqrt{m}x + \sqrt{n}y)(\sqrt{m}u + \sqrt{n}v) = (mxu + nyv) + (xv + uy)\sqrt{mn}$$

é solução de $(*)$. Novamente, a verificação é deixada para o leitor.
Em particular, uma solução $\sqrt{m}x + \sqrt{n}y$ de $(\ast)$ produz a solução

$$(mx^2 + ny^2) + 2xy\sqrt{mn}$$

de $(*)$.
Por último, vejamos que $\sqrt{m}x + \sqrt{n}y = \sqrt{m}a + \sqrt{n}b \implies x = a, y = b$. Essa igualdade, caso $x \neq a \iff y \neq b$ é equivalente a

$$\mathbb{Q} \ni \frac{x-a}{b-y} = \sqrt{\frac{n}{m}}.$$

Então existem inteiros r, s tais que $n/m = (r/s)^2 \implies mn = (mr/s)^2$, e então mn seria o quadrado de um inteiro, aburdo.
Agora, provemos a

Proposição 3.11. *Seja $\sqrt{m}x + \sqrt{n}y$ uma solução de $(\ast)$ e $u + v\sqrt{mn}$ uma solução de $(*)$. Se*

$$(\sqrt{m}x + \sqrt{n}y)^2 = (u + v\sqrt{mn})^2,$$

então $m = 1$ ou $n = 1$.

Demonstração. Se tal igualdade ocorre, temos que

$$\Big((\sqrt{m}x + \sqrt{n}y)(u - v\sqrt{mn})\Big)^2 = \Big((u + v\sqrt{mn})(u - v\sqrt{mn})\Big)^2 = 1.$$

Sendo $(\sqrt{m}x + \sqrt{n}y)(u - v\sqrt{mn}) = \sqrt{m}r + \sqrt{n}s$ uma solução de $(\ast)$, obtemos

$$(\sqrt{m}r + \sqrt{n}s)^2 = 1 \implies (mr^2 + ns^2) + 2rs\sqrt{mn} = 1.$$

Como $\sqrt{mn}$ é irracional, devemos ter $s = 0$ ou $r = 0$, e isso nos dá $m = 1$ ou $n = 1$. □

Disso segue o

Teorema 3.12. *Se $\sqrt{m}x + \sqrt{n}y$ uma solução de $(\ast)$ e $r + s\sqrt{mn}$ a solução minimal de $(*)$, existe $k \geq 0$ inteiro tal que*

$$(\sqrt{m}x + \sqrt{n}y)^2 = (r + s\sqrt{mn})^{2k+1}.$$

Demonstração. Como $(\sqrt{m}x + \sqrt{n}y)^2$ é solução de $(*)$, existe t tal que

$$(\sqrt{m}x + \sqrt{n}y)^2 = (r + s\sqrt{mn})^t.$$

Mas a proposição 3.11 nos diz que t não pode ser par, pois $m, n > 1$. Então $t = 2k + 1$ para algum $k \geq 0$ inteiro, como desejado. □

Teorema 3.13. *Seja $\sqrt{m}u + \sqrt{n}v$ a solução minimal de $(\ast)$ e $r + s\sqrt{mn}$ a solução minimal de $(*)$. Então,*

$$(\sqrt{m}u + \sqrt{n}v)^2 = r + s\sqrt{mn}.$$

Demonstração. Basta mostrar que tal equação possui solução, já que, como

$$(\sqrt{m}u + \sqrt{n}v)^2 = (r + s\sqrt{mn})^{2k+1}$$

pelo teorema 3.12, e esse é o menor valor positivo de $(\sqrt{m}x + \sqrt{n}y)^2$ para uma solução de $(*)$, devemos ter $k = 0$.
Mostremos então que

$$(\sqrt{m}x + \sqrt{n}y)^2 = r + s\sqrt{mn}$$

possui solução com x, y inteiros positivos. Como

$$\begin{aligned}&(\sqrt{m}x + \sqrt{n}y)^2 = (r + s\sqrt{mn})^{2k+1}\\ \implies &\left((\sqrt{m}x + \sqrt{n}y)(r - s\sqrt{mn})^k\right)^2 = (r + s\sqrt{mn})^{2k+1}(r - s\sqrt{mn})^{2k} = r + s\sqrt{mn},\end{aligned}$$

sendo $(\sqrt{m}x+\sqrt{n}y)(r-s\sqrt{mn})^k = \sqrt{m}a+\sqrt{n}b$, basta que $ab > 0$, já que, se ambos forem negativos, podemos trocá-los por $-a$ e $-b$.
Mas

$$(\sqrt{m}a + \sqrt{n}b)^2 = (ma^2 + nb^2) + 2ab\sqrt{mn} = r + s\sqrt{mn},$$

segue que $2ab = s > 0 \implies ab > 0$, como desejado. □

Como $\sqrt{m}x + \sqrt{n}y = \sqrt{m}a + \sqrt{n}b \implies x = a, y = b$, a solução minimal é a única que satisfaz tal propriedade, isto é, se

$$(\sqrt{m}u + \sqrt{n}v)^2 = r + s\sqrt{mn},$$

com $u, v > 0$, então $\sqrt{m}u + \sqrt{n}v$ é a solução minimal de $(*)$.
Provemos agora o mais importante

Teorema 3.14. *Se a equação $(*)$ possui solução, então, sendo $\sqrt{m}u + \sqrt{n}v$ sua solução minimal, todas as soluções de $(*)$ são dadas pela fórmula*

$$\sqrt{m}u_k + \sqrt{n}v_k = (\sqrt{m}u + \sqrt{n}v)^{2k+1}.$$

Demonstração. É trivial que todos os números acima são soluções de $(*)$. Mostremos que não existem outras soluções. Assuma que $\sqrt{m}p + \sqrt{n}q$, com $p, q > 0$, é uma solução tal que, para algum $k \geq 0$

$$(\sqrt{m}u + \sqrt{n}v)^{2k+1} < \sqrt{m}p + \sqrt{n}q < (\sqrt{m}u + \sqrt{n}v)^{2k+3}.$$

Então,

$$1 < (\pm\sqrt{m}p \pm \sqrt{n}q)(\sqrt{m}u - \sqrt{n}v)^{2k+1} < (\sqrt{m}u + \sqrt{n}v)^2,$$

de acordo com o sinal escolhido em $(*)$. Mas $(\pm\sqrt{m}p \pm \sqrt{n}q)(\sqrt{m}u - \sqrt{n}v)^{2k+1} = a + b\sqrt{mn}$ e $(\sqrt{m}u + \sqrt{n}v)^2 = r + s\sqrt{mn}$ são soluções de $(*)$, sendo esta a minimal pelo teorema 3.13. Logo,

$$1 < a + b\sqrt{mn} < r + s\sqrt{mn}. \qquad (\bigcirc)$$

Como $0 < a - b\sqrt{mn} < 1$, pois $a - b\sqrt{mn} = (a + b\sqrt{mn})^{-1}$, segue que, somando essas desigualdades, $2a > 1 \Rightarrow a > 0$, e que $(a + b\sqrt{mn}) - (a - b\sqrt{mn}) > 0 \Rightarrow 2\sqrt{mn}b > 0 \Rightarrow b > 0$. Mas isso diz que $a + b\sqrt{mn}$ é uma solução positiva de $(*)$, e portanto $a + b\sqrt{mn} \geq r + s\sqrt{mn}$, o que contradiz $(\bigcirc)$. Logo, não existe solução diferente das indicadas no enunciado do teorema. □

Finalizamos esta subseção com o seguinte

Teorema 3.15. *Se m e n forem ambos inteiros não quadrados perfeitos, a equação $(*)$ não possui solução caso $x^2 - mny^2 = -1$ possua solução.*

Demonstração. O teorema 3.5 nos diz que a solução minimal de $x^2 - y^2mn = -1$ satisfaz

$$(u + v\sqrt{mn})^2 = r + s\sqrt{mn},$$

onde $r + s\sqrt{mn}$ é a solução minimal de $(*)$. Por outro lado, o teorema 3.13 diz que a solução minimal de $(*)$ satisfaz

$$(\sqrt{m}a + \sqrt{n}b)^2 = r + s\sqrt{mn}.$$

Fica a cargo do leitor encontrar um absurdo assumindo que ambas as equações possuem solução, e então que ambas as igualdades acima ocorrem. □

3.5 A solução minimal de Equação de Pell

Até agora, toda a teoria sobre equações do tipo Pell que desenvolvemos estão diretamente relacionadas com a Equação de Pell, e em especial com sua solução minimal. O objetivo desta subseção é apresentar um método eficiente para encontrar tal solução.
Começamos com a seguinte

Proposição 3.16. *Se $u^2 - Av^2 = \pm 1$, com $u, v > 0$, então $\frac{u}{v}$ é uma reduzida da fração contínua de $\sqrt{A}$.*

Demonstração. Se $u^2 - Av^2 = \pm 1$, então

$$\left|\frac{u}{v} - \sqrt{A}\right|\left|\frac{u}{v} + \sqrt{A}\right| = \frac{1}{v^2}|u^2 - Av^2| = \frac{1}{v^2}.$$

Mas também temos que

$$\left|\frac{u}{v} + \sqrt{A}\right| = \left|(\sqrt{A} - \frac{u}{v}) - 2\sqrt{A}\right| \geq 2\sqrt{A} - \left|\frac{u}{v} - \sqrt{A}\right| \geq 2\sqrt{A} - \frac{1}{v^2}.$$

Fica a cargo do leitor verificar que $2\sqrt{A} - \frac{1}{v^2} > 2$, e portanto

$$\left|\frac{u}{v} - \sqrt{A}\right|\left|\frac{u}{v} + \sqrt{A}\right| = \frac{1}{v^2} \Longrightarrow \left|\sqrt{A} - \frac{u}{v}\right| < \frac{1}{2v^2},$$

e segue do Teorema 2.9 que $\frac{u}{v}$ é uma reduzida de $\sqrt{A}$. □

Agora estamos prontos para o

Teorema 3.17. *Seja A um inteiro positivo que não é quadrado perfeito. Sendo*

$$\sqrt{A} = [a_0; \overline{a_1, a_2, \ldots, a_t}]$$

a representação por frações contínuas de $\sqrt{A}$, de período $a_1, a_2, \ldots, a_t$, temos que $a_t = 2a_0$.
Se t for par, a solução minimal da Equação de Pell é (p_{t-1}, q_{t-1}) (p_{t-1}/q_{t-1} é a $(t-1)$-ésima reduzida de $\sqrt{A}$), e a equação $x^2 - Ay^2 = -1$ não possui solução. Se t for ímpar, a solução minimal da Equação de Pell é (p_{2t-1}, q_{2t-1}), e (p_{t-1}, q_{t-1}) é solução de $x^2 - Ay^2 = -1$.

Demonstração. Ao invés de considerarmos a fração contínua de $\sqrt{A}$, vamos considerar a fração contínua de $\sqrt{A} + \lfloor\sqrt{A}\rfloor$, pois os a_i's continuam os mesmos para $i \geq 1$, e $a_0 = \lfloor\sqrt{A}\rfloor$ passa a ser $a_0 = 2\lfloor\sqrt{A}\rfloor$. Agora, queremos que $a_0 = a_t$.
Vamos encontrar duas sequências de inteiros $(b_k)_{k\geq 0}$ e $(c_k)_{k\geq 0}$ para as quais

$$0 < \frac{\sqrt{A} - c_k}{b_k} < 1 \quad \text{e} \quad \frac{\sqrt{A} + c_k}{b_k} = [a_k; a_{k+1}, a_{k+2}, \ldots] \qquad (*)$$

Para todo $k \geq 0$. Tomemos $b_0 = 1$, $c_0 = \lfloor\sqrt{A}\rfloor$, e esse par claramente satisfaz as duas condições acima.
Para $k \geq 1$, defina

$$c_k = a_{k-1}b_{k-1} - c_{k-1} \quad \text{e} \quad b_k = \frac{A - c_k^2}{b_{k-1}},$$

Primeiro, vamos mostrar por indução que b_k e c_k são inteiros. Para b_k ser inteiro, devemos ter $b_k | A - c_{k+1}^2 \Longleftrightarrow b_k | A - c_k^2$, já que $c_k^2 \equiv c_{k+1}^2 \pmod{b_k}$ (assumindo que eles sejam inteiros). Portanto, assumindo que b_{k-1} e c_{k-1} são inteiros por hipóetese de indução e que $b_{k-1} | A - c_{k-1}^2$ (a base $k = 0$ já está provada), temos $c_k = a_{k-1}b_{k-1} - c_{k-1}$ é inteiro, e que

$$b_k = \frac{A - c_k^2}{b_{k-1}}$$

é inteiro, e que $c_{k-1}^2 \equiv c_k^2 \pmod{b_{k-1}}$ já que ambos são inteiros. Como $A \neq c_k^2$, temos que $b_k \neq 0$ é inteiro, pois $b_{k-1} | A - c_{k-1}^2 \Longrightarrow b_{k-1} | A - c_k^2$. Logo $b_k | A - c_k^2$, o que completa a indução. É trivial verificar que essas sequências satisfazem a segunda condição dada em $(*)$.
Provemos que elas satisfazem a primeira também. Para isso, vamos mostrar por indução que $0 <$

$c_k < \sqrt{A}$ e que $b_k > 0$. O caso base $k = 0$ segue diretamente da definição de b_0 e c_0. Suponha que $b_{k-1} > 0$ e que $0 < c_{k-1} < \sqrt{A}$. Então, temos que

$$a_{k-1} < \frac{\sqrt{A} + c_{k-1}}{b_{k-1}} = [a_{k-1}; a_k, \ldots] < a_{k-1} + 1,$$

e então $c_k = a_{k-1}b_{k-1} - c_{k-1} < \sqrt{A} < b_{k-1} + c_k$. Caso $c_k \leq 0$, teríamos, dessa última desigualdade, que $b_{k-1} > \sqrt{A} > c_{k-1}$, e então $c_k = a_{k-1}b_{k-1} - c_{k-1} > b_{k-1} - c_{k-1} > 0$, um absurdo. Logo, $c_k > 0$, e isso diz que

$$b_k = \frac{A - c_k^2}{b_{k-1}} > 0,$$

completando a hipótese de indução.
Portanto, segue que

$$\begin{aligned}\frac{\sqrt{A} - c_k}{b_k} &= \frac{\sqrt{A} - c_k}{\frac{A - c_k^2}{b_{k-1}}} \\ &= \frac{b_{k-1}}{\sqrt{A} + c_k} = \frac{1}{a_{k-1} + \frac{\sqrt{A} - c_{k-1}}{b_{k-1}}},\end{aligned}$$

e então, como $a_{k-1} + \frac{\sqrt{A} - c_{k-1}}{b_{k-1}} > 1$, temos

$$0 < \frac{\sqrt{A} - c_k}{b_k} < 1.$$

Note que, sabendo os valores de b_k e c_k, os valores de b_{k-1} e c_{k-1} estão bem determinados, pois $b_{k-1} = \frac{A - c_k^2}{b_k}$, e $c_{k-1} = a_{k-1}b_{k-1} - c_k$, além de que

$$a_{k-1} = \left\lfloor a_{k-1} + \frac{\sqrt{A} - c_{k-1}}{b_{k-1}} \right\rfloor = \left\lfloor \frac{\sqrt{A} + c_k}{b_{k-1}} \right\rfloor.$$

Portanto, como $0 < c_k < \sqrt{A}$ e $b_k | A - c_k^2$, concluímos que b_k e c_k assumem um número finito de valores, e então essas sequências são puramente periódicas (e de mesmo período), isto é, existe t tal que $c_{n+t} = c_n$ e $b_{n+t} = b_n$ para todo $n \geq 0$. Em particular, tomando t como o menor número satisfazendo isso, obtemos que $\sqrt{A} + \lfloor \sqrt{A} \rfloor = [a_0; \overline{a_1, a_2, \ldots, a_t}]$, e então $c_t = c_0 = a_0$ e $b_t = b_0 = 1$, e daí $a_t = a_0$, como queríamos.
Defina $\alpha_k = \frac{\sqrt{A} + c_k}{b_k} = [a_k; a_{k+1}, \ldots]$.
Para $k \geq 1$, note que, como $\sqrt{A} = [a_0/2; a_1, a_2, \ldots, a_k, \alpha_{k+1}]$, obtemos, pela Proposição 2.1, que

$$\sqrt{A} = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}} = \frac{\frac{\sqrt{A} + c_{k+1}}{b_{k+1}}p_k + p_{k-1}}{\frac{\sqrt{A} + c_{k+1}}{b_{k+1}}q_k + q_{k-1}}.$$

Expandindo, obtemos

$$Aq_k + \sqrt{A}(c_{k+1}q_k + b_{k+1}q_{k-1}) = c_{k+1}p_k + b_{k+1}p_{k-1} + \sqrt{A}p_k.$$

Portanto, segue que

$$Aq_k = c_{k+1}p_k + b_{k+1}p_{k-1} \quad \text{e} \quad p_k = c_{k+1}q_k + b_{k+1}q_{k-1}.$$

Isolando c_{k+1} nas equações acima, obtemos

$$\frac{Aq_k - b_{k+1}p_{k-1}}{p_k} = c_{k+1} = \frac{p_k - b_{k+1}q_{k-1}}{q_k}.$$

Logo,

$$\begin{aligned}&Aq_k^2 - b_{k+1}p_{k-1}q_k = p_k^2 - b_{k+1}p_kq_{k-1} \\ \implies &p_k^2 - Aq_k^2 = b_{k+1}(p_kq_{k-1} - p_{k-1}q_k) = (-1)^{k+1}b_{k+1},\end{aligned}$$

onde a última igualdade ocorre pela Proposição 2.1.
Logo, obtemos que $p_{t-1}^2 - Aq_{t-1}^2 = (-1)^t$, e portanto (p_{t-1}, q_{t-1}) é solução da Equação de Pell quando t for par, e, quando t for ímpar, (p_{t-1}, q_{t-1}) é solução de $x^2 - Ay^2 = -1$.
Caso u e v sejam inteiros positivos satisfazendo $u^2 - Av^2 = \pm 1$, vimos na Proposição 3.16 que $u/v = p_m/q_m$ para algum $m \geq 0$. Como $p_m^2 - Aq_m^2 = (-1)^{m+1}b_{m+1}$, devemos ter $b_{m+1} = 1$ e então $0 < \sqrt{A} - c_{m+1} < 1$, de modo que $c_{m+1} = \lfloor \sqrt{A} \rfloor$, donde segue que $t | m+1$. Portanto, no caso t par, a solução minimal da equação é (p_{t-1}, q_{t-1}), e no caso t ímpar teremos como solução minimal (p_{2t-1}, q_{2t-1}). Além disso, se t for par, e como $t | m+1$, segue que $m+1$ é par e que $u^2 - Av^2 = \pm 1 \implies u^2 - Av^2 = p_m - Aq_m^2 = (-1)^{m+1} = 1$, e portanto a equação $x^2 - Ay^2 = -1$ não possui solução. □

Para mostrar a eficiência deste método, vamos encontrar a solução minimal de $x^2 - 41y^2 = 1$. Como a fração contínua de $\sqrt{41} = [6; \overline{2, 2, 12}]$ possui período 3, a solução minimal desta equação será (p_5, q_5). Então,

$$\frac{p_5}{q_5} = 6 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{12 + \cfrac{1}{2 + \frac{1}{2}}}}} = \frac{2049}{320}.$$

Portanto, a solução minimal é $(2049, 320)$, e claramente seria muito demorado encontrá-la tentando valores de y ou x.

3.6 A sequência das soluções da Equação de Pell

Seja (x_1, y_1) a solução minimal da equação $x^2 - Ay^2 = 1$. O Teorema 3.2 nos diz que todas as soluções dessa equação assumem a forma

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

Assim, podemos encontrar relações recorrentes a partir desta equação:

$$\begin{aligned} x_{m+n} + y_{m+n}\sqrt{A} = (x_1 + y_1\sqrt{A})^{m+n} &= (x_m + y_m\sqrt{A})(x_n + y_n\sqrt{A}) \\ &= (x_m x_n + A y_m y_n) + \sqrt{A}(x_m y_n + x_n y_m), \end{aligned}$$

e então

$$x_{m+n} = x_m x_n + A y_m y_n \qquad \text{e} \qquad y_{m+n} = x_m y_n + x_n y_m.$$

Em particular,

$$x_{n+1} = x_n x_1 + A y_n y_1 \qquad \text{e} \qquad y_{n+1} = x_1 y_n + x_n y_1. \tag{2}$$

Outra fórmula que podemos encontrar é

$$\begin{aligned} x_n + y_n\sqrt{A} &= (x_1 + y_1\sqrt{A})^n \\ \implies x_n - y_n\sqrt{A} &= (x_1 - y_1\sqrt{A})^n. \end{aligned}$$

Somando e subtraindo essas equações, obtemos

$$x_n = \frac{1}{2}\left((x_1 + y_1\sqrt{A})^n + (x_1 - y_1\sqrt{A})^n\right) \quad \text{e} \quad y_n = \frac{1}{2\sqrt{A}}\left((x_1 + y_1\sqrt{A})^n - (x_1 - y_1\sqrt{A})^n\right). \tag{1}$$

Com isso, as sequências (x_n) e (y_n) satisfazem a recorrência de segunda ordem

$$a_{n+2} - 2x_1 a_{n+1} + a_n = 0$$

Podemos escrever isso na seguinte forma matricial:

$$\begin{pmatrix} a_{n+2} & a_{n+1} \\ a_{n+1} & a_n \end{pmatrix} = \begin{pmatrix} a_{n+1} & a_n \\ a_n & a_{n-1} \end{pmatrix} \begin{pmatrix} 2x_1 & 1 \\ -1 & 0 \end{pmatrix}.$$

Sendo

$$M_n = \begin{pmatrix} a_{n+1} & a_n \\ a_n & a_{n-1} \end{pmatrix},$$

Concluímos que

$$M_n = M_1 \begin{pmatrix} 2x_1 & 1 \\ -1 & 0 \end{pmatrix}^{n-1}$$

Note que $x_0 = 1$ e $y_0 = 0$, a solução trivial da equação de Pell. Vamos mostrar que, nos casos $a_n = x_n$ e $a_n = y_n$, a matriz M_1 é inversível. Basta que

$$\begin{aligned} & x_2x_0 \neq x_1^2 \qquad \text{e} \qquad y_2y_0 \neq y_1^2 \\ \iff & 2x_1^2 - 1 \neq x_1^2 \qquad \text{e} \qquad y_1^2 \neq 0, \end{aligned}$$

e ambas as verificações são triviais, já que $x_1, y_1 > 1$. Assim, prosseguimos assumindo que M_1 é inversível.

$$\begin{aligned} M_1^{-1}M_n &= \begin{pmatrix} 2x_1 & 1 \\ -1 & 0 \end{pmatrix}^{n-1}, \quad M_r = M_1 \begin{pmatrix} 2x_1 & 1 \\ -1 & 0 \end{pmatrix}^{r-1} \\ \implies M_rM_1^{-1}M_n &= M_1 \begin{pmatrix} 2x_1 & 1 \\ -1 & 0 \end{pmatrix}^{n+r-2} = M_{n+r-1}. \end{aligned}$$

Além disso, note que

$$M_1M_1^{-1} = I \implies (M_1M_1^{-1})^t = (M_1^{-1})^tM_1^t = (M_1^{-1})^tM_1 = I = M_1^{-1}M_1 \implies (M_1^{-1})^t = M_1^{-1},$$

e portanto podemos escrever

$$M_1^{-1} = \begin{pmatrix} b_2 & b_1 \\ b_1 & b_0 \end{pmatrix},$$

onde $b_0, b_1, b_2 \in \mathbb{Q}$. Logo,

$$\begin{aligned} & M_rM_1^{-1}M_n = M_{n+r-1} \\ \implies & \begin{pmatrix} a_{r+1} & a_r \\ a_r & a_{r-1} \end{pmatrix} \begin{pmatrix} b_2 & b_1 \\ b_1 & b_0 \end{pmatrix} \begin{pmatrix} a_{n+1} & a_n \\ a_n & a_{n-1} \end{pmatrix} = \begin{pmatrix} a_{n+r} & a_{n+r-1} \\ a_{n+r-1} & a_{n+r-2} \end{pmatrix}. \end{aligned}$$

Uma simples conta nos diz que

$$a_{n+r} = a_{n+1}a_{r+1}b_2 + a_{n+1}a_rb_1 + a_na_{r+1}b_1 + a_na_rb_0.$$

Isso nos permite encontrar termos da sequência em função de termos anteriores com maior facilidade, já que b_0, b_1 e b_2 são constantes conhecidas e fáceis de calcular. Além disso, podemos ver que

$$|M_n| = |M_1| \begin{vmatrix} 2x_1 & 1 \\ -1 & 0 \end{vmatrix} = |M_1| \implies a_n^2 - a_{n+1}a_{n+1} = c \quad \forall n \geq 1,$$

para alguma constante c. Para casos particulares, podemos encontrar outras fórmulas e refinar as vistas acima. Como exemplo, vejamos algumas propriedades da sequência (x_n) quando $A = 2$.
A solução minimal de $x^2 - 2y^2 = 1$ é $x_1 = 3$, $y_2 = 2$. Então, sabemos que a sequência x_n satisfaz $x_{n+2} = 6x_{n+1} - x_n$. Sabemos também que a equação $x^2 - 2y^2 = -1$ tem como solução minimal $(1, 1)$, e então todas as soluções de $x^2 - 2y^2 = \pm 1$ podem ser escritas na forma

$$a_n + b_n\sqrt{2} = (1 + \sqrt{2})^n,$$

sendo $a_{2n} = x_n$. Olhemos para a sequência (b_n). Concluímos que (b_n) satisfaz a recorrência $b_{n+2} = 2b_{n+1} + b_n$, sendo $b_0 = 0, b_1 = 1$. Logo, definindo

$$M_n = \begin{pmatrix} b_{n+1} & b_n \\ b_n & b_{n-1} \end{pmatrix},$$

temos que

$$M_{n+1} = M_n \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix},$$

de modo que

$$M_n = M_1 \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^n,$$

pois $M_1 = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$. Com isso, as contas feitas anteriormente tornam-se muito mais fáceis, já que teremos

$$M_n M_r = M_{n+r},$$

e disso segue que

$$b_{n+r} = b_{n+1}b_r + b_n b_{r-1}.$$

Além disso, temos que

$$|M_n| = \begin{vmatrix} 2 & 1 \\ 1 & 0 \end{vmatrix}^n = (-1)^n \implies b_{n+1}b_{n-1} - b_n^2 = (-1)^n.$$

Com essas fórmulas, podemos demonstrar a seguinte

Proposição 3.18. *Sendo (b_n) a sequência dada por $b_0 = 0$, $b_1 = 1$ e $b_{n+2} = 2b_{n+1} + b_n$, temos as seguintes propriedades:*

(i) $b_n^2 - b_{n-1}^2 = 2b_n b_{n-1} + (-1)^{n+1}$

(ii) $b_n^2 - b_{n+r}b_{n-r} = (-1)^{n-r}b_r$

Demonstração. Para a primeira, basta ver que $b_n^2 + (-1)^n = b_{n+1}b_{n-1} = 2b_n b_{n-1} + b_{n-1}^2$, donde o resultado segue. Para a segunda, note que

$$b_n = b_r b_{n-r+1} + b_{r-1}b_{n-r},$$

e

$$\begin{aligned} b_{n+r} &= b_{2r}b_{n-r+1} + b_{2r-1}b_{n-r} \\ &= (b_{r+1}b_r + b_r b_{r-1})b_{n-r+1} + (b_r^2 + b_{r-1}^2)b_{n-r} \\ &= 2(b_r^2 + b_r b_{r-1})b_{n-r+1} + (b_r^2 + b_{r-1}^2)b_{n-r}. \end{aligned}$$

Assim,

$$b_n^2 - b_{n+r}b_{n-r} = (b_r b_{n-r+1} + b_{r-1}b_{n-r})^2 - (2(b_r^2 + b_r b_{r-1})b_{n-r+1} + (b_r^2 + b_{r-1}^2)b_{n-r})b_{n-r}.$$

Expandindo e cancelando termos iguais, obtemos

$$\begin{aligned} b_n^2 - b_{n+r}b_{n-r} &= b_r^2 b_{n-r+1}^2 - 2b_r^2 b_{n-r+1}b_{n-r} - b_r^2 b_{n-r}^2 \\ &= b_r^2(b_{n-r+1}^2 - 2b_{n-r+1}b_{n-r} - b_{n-r}^2) \\ &= b_r^2(b_{n-r+1}b_{n-r-1} - b_{n-r}^2) \\ &= b_r^2(-1)^{n-r}, \end{aligned}$$

como desejado. □

Agora, provemos a seguinte proposição, que relaciona a sequência b_n e a sequência x_n.

Proposição 3.19. *Sendo (b_n) a sequência dada por $b_0 = 0$, $b_1 = 1$ e $b_{n+2} = 2b_{n+1} + b_n$, e (x_n) a sequência dada por $x_0 = 1$, $x_1 = 3$ e $x_{n+2} = 6x_{n+1} - x_n$, vale, para todo $n \geq 0$, que*

$$x_n = (2b_n)^2 + (-1)^n.$$

Demonstração. A prova é por indução. Os casos $n = 0, 1$ são triviais. Assuma que o resultado valha para $n-2, n-1$. Queremos então que

$$\begin{aligned} &(2b_n)^2 + (-1)^n = 6(2b_{n-1})^2 - 6(-1)^n - (2b_{n-2})^2 - (-1)^n \\ \iff &4(b_n^2 - 6b_{n-1}^2 + b_{n-2}^2) = 8(-1)^{n-1} \\ \iff &(2b_{n-1} + b_{n-2})^2 - 6b_{n-1}^2 + b_{n-2}^2 = 2(-1)^{n-1} \\ \iff &2b_{n-2}^2 + 4b_{n-1}b_{n-2} - 2b_{n-1}^2 = 2(-1)^{n-1} \\ \iff &b_{n-2}(2b_{n-1} + b_{n-2}) - b_{n-1}^2 = (-1)^{n-1} \\ \iff &b_n b_{n-2} - b_{n-1}^2 = (-1)^{n-1}, \end{aligned}$$

o que é verdade. Assim, a indução está completa. □

Portanto, concluímos que as sequências formadas por soluções de equações de Pell possuem características interessantes e que, com um pouco de criatividade, podem ser encontradas. O objetivo desta subseção era mostrar isso ao leitor.

4 Problemas Resolvidos

Nesta seção, diversos problemas com aplicações e ideias úteis envolvendo as equações tipo Pell são resolvidos.
Às vezes, quando trabalhando com equações diofantinas quadráticas, completar quadrados para obtermos apenas termos de grau 2 pode fazer aparecer equações de Pell, como no exemplo abaixo.

Exemplo 4.1. *Mostre que a soma dos n primeiros inteiros é um quadrado perfeito para infinitos n.*

Solução. Queremos que

$$1+2+\cdots+n=\frac{n(n+1)}{2}=m^2$$

para algum inteiro m. Então,

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

Olhando para as soluções de $x^2-2y^2=1$, é imediato verificar que todas as soluções possuem x ímpar e y par analisando módulo 4. Como sabemos que existem infinitas soluções para tal equação, concluímos que existem infinitos n que satisfazem a condição do enunciado, como desejado. □

Exemplo 4.2. *Mostre que existem infinitos inteiros n tais que n^2+1 possui dois divisores cuja diferença é n.*

Solução. Queremos encontrar infinitos n tais que existe algum d satisfazendo $d|n^2+1$ e $d+n|n^2+1$. Como d e n devem ser coprimos (verifique!), essas duas condições são equivalentes a $d(d+n)|n^2+1$. Em outras palavras, temos que

$$n^2+1=kd(d+n) \iff n^2+1=kd^2+kdn.$$

Novamente, tentemos completar quadrados de modo a obter apenas termos de grau 2:

$$n^2+1=k(d^2+dn) \iff k(2d+n)^2-(k+4)n^2=4.$$

Queremos que a equação $kx^2-(k+4)y^2=4$ possua infinitas soluções com $x-y$ par. Vamos supor que n é par, e agora queremos apenas infinitas soluções para $kx^2-(k+4)y^2=1$ (a escolha de n par é natural, já que ficamos com um tipo de equação com a qual conhecemos, pois a estudamos na subseção 3.4). Mas sabemos que se tal equação possui uma solução, então ela possui infinitas. Ou seja, basta encontrarmos um valor de k de modo que tal equação tenha solução. Mas $k=1$ imediatamente nos garante isso, pois ficamos com a Pell $x^2-5y^2=1$. Daí, para cada solução dessa equação, temos $n=2y$ e $d=x-y$, e isso nos garante infinitas soluções de nossa equação.
É claro que era possível assumirmos $k=1$ desde o começo, querendo resolver a equação $n^2+1=d(d+n)$. Entretanto, poderia ser o caso de essa equação não ter solução, pois escolhemos o valor de k sem muitos fundamentos. Ao manter a generalidade, fica muito mais fácil de ver que $k=1$ é uma ótima opção. □

Exemplo 4.3. *Mostre que a equação*

$$c(ac+1)^2=(5c+2b)(2c+b)$$

possui infinitas soluções com a,b,c inteiros positivos.

Solução. Note que $\mathrm{mdc}(5c+2b,2c+b)=\mathrm{mdc}(c,2c+b)=\mathrm{mdc}(c,b)=d$. Escreva $b=d\beta$ e $c=d\gamma$. Nossa equação torna-se

$$d\gamma(ad\gamma+1)^2=d^2(5\gamma+2\beta)(2\gamma+\beta) \iff \gamma(ad\gamma+1)^2=d(5\gamma+2\beta)(2\gamma+\beta).$$

Se γ for ímpar, é imediato que $\gamma|d$ (lembre-se que $\mathrm{mdc}(\beta,\gamma)=1$). Caso γ seja par, concluímos que $\gamma|2d$.
Note que resolver esta equação deve ser algo bastante trabalhoso, já que existem muitas variáveis. Ou seja, o nosso grau de liberdade é alto. Assim, podemos impor algumas condições sobre nossas variáveis, de modo que a equação torne-se mais simples de resolver. Neste caso, vamos assumir que $\gamma|d$ já que, em qualquer caso, sabemos que $\gamma|d$ e $\gamma|2d$. Ficamos com

$$(a\gamma^2+1)^2=(5\gamma+2\beta)(2\gamma+\beta).$$

Mas já sabemos que $\text{mdc}(5\gamma+2\beta, 2\gamma+\beta) = 1$, e disso segue que ambos devem ser quadrados perfeitos. Então, queremos resolver o sistema $5\gamma + 2\beta = x^2$ e $2\gamma + \beta = y^2$. Caso isso ocorra, devemos ter que $x^2 - 2y^2 = \gamma$. Além disso, é necessário que $xy \equiv 1 \pmod{\gamma^2}$, pois queremos que $a = \frac{xy-1}{\gamma^2}$ seja inteiro. Uma boa forma de lidarmos com essas condições é tomar $\gamma = 1$, pois certamente teremos $a = xy - 1$ inteiro, e nossa equação torna-se

$$(a+1)^2 = (2\beta+5)(\beta+2).$$

Além disso, nosso sistema se reduz a $2\beta+5 = x^2$ e $\beta+2 = y^2$, e então $\beta = x^2 - y^2 - 3$ e $x^2 - 2y^2 = 1$. Como existem infinitos x, y satisfazendo $x^2 - 2y^2 = 1$, obtemos infinitos valores de a e β, como desejado. □

Exemplo 4.4. *Seja S o conjunto de todos os inteiros positivos n tais que n^4 possui algum divisor no conjunto $n^2+1, n^2+2, \ldots, n^2+2n$. Mostre que existem infinitos inteiros n em S que são das formas $7m$, $7m+1$, $7m+2$, $7m+5$, $7m+6$, enquanto não há elementos n em S da forma $7m+3$, $7m+4$.*

Solução. Suponha que $n^2 + i | n^4$ para algum $i \in \{1, 2, \ldots, 2n\}$. Como $n^2 \equiv -i \pmod{n^2+i} \implies n^4 \equiv i^2 \pmod{n^2+i}$, temos que $n^2 + i | i^2$. Segue que

$$i^2 = d(n^2+i), d \in \mathbb{N}.$$

Além disso, $i \leq 2n \implies i^2 \leq 4n^2$. Isso nos diz que $d < 4$. Além disso, se $d = 1$, teríamos $i(i-1) = n^2$. Então i e $i-1$ seriam quadrados perfeitos (ou $i = 0$, o que não ocorre pois $i \geq 1$), o que só ocorre se $i = 1$. Mas isso nos diria que $n^2 = i(i-1) = 0$, o que é impossível pois $n > 0$. Logo, $d = 2$ ou $d = 3$. Em particular, d é primo, e então $d | i^2 \implies d | i$. Escrevamos $i = dj$:

$$dj^2 = n^2 + dj.$$

Logo, $d | n$. Escrevendo $n = dm$, obtemos

$$j^2 = dm^2 + j \iff j^2 - j = dm^2.$$

Aplicando a ideia apresentada no exemplo 4.1, completamos quadrados de modo a obter apenas termos de grau 2:

$$j^2 - j = dm^2 \iff (2j-1)^2 - d(2m)^2 = 1.$$

Portanto, todos os n satisfazendo a condição do enunciado derivam de soluções das equações de Pell $x^2 - 2y^2 = 1$ e $x^2 - 3y^2 = 1$. Assim, dividimos agora em dois casos.

Caso 1. $d = 2$.

Estamos interessados nas soluções de $x^2 - 2y^2 = 1$, onde x é ímpar e y é par. Analisando módulo 4 verificamos que toda solução dessa Pell satisfaz x ímpar e y par. Portanto, queremos analisar as soluções módulo 7. Como a solução minimal é $(x, y) = (3, 2)$ e a próxima solução é $x + y\sqrt{2} = (3+2\sqrt{2})^2 = 17 + 12\sqrt{2}$, queremos analisar a seguinte recorrência módulo 7:

$$y_1 = 2, y_2 = 12 \text{ e } y_{n+2} = 6y_{n+1} - y_n, n \geq 1.$$

Como $n = 2m = y_i$ para algum i, precisamos verificar os valores de y_i módulo 7. Então, basta ver qual será o período desta sequência módulo 7:

$$y_1 = 2, y_2 = 5, y_3 = 0, y_4 = 2, y_5 = 5, \ldots$$

Portanto, isso nos fornece infinitos n nas formas $7k$, $7k+2$ e $7k+5$.

Caso 2. $d = 3$.

Agora, estamos interessados nas soluções de $x^2 - 3y^2 = 1$, com x ímpar e y par. Analisando módulo 4, $x^2 + y^2 \equiv 1 \pmod 4$, e então exatamente um entre x e y é par. Logo, basta garantirmos que y é par. Como a solução minimal é $(x, y) = (2, 1)$ e a próxima solução é $x + y\sqrt{3} = (2+\sqrt{3})^2 = 7 + 4\sqrt{3}$, queremos analisar e seguinte recorrência:

$$y_1 = 1, y_2 = 4 \text{ e } y_{n+2} = 4y_{n+1} - y_n, n \geq 1.$$

É imediato que $y_{n+2} \equiv y_n \pmod 2$. Como y_1 é ímpar e y_2 é par, estamos interessados apenas nas soluções y_{2i}. Sabemos que

$$y_{2i} = \frac{(2+\sqrt{3})^{2i} - (2-\sqrt{3})^{2i}}{2\sqrt{3}} = \frac{(7+4\sqrt{3})^{i} - (7-4\sqrt{3})^{i}}{2\sqrt{3}}.$$

Como $y_2 = 4$ e $y_4 = 56$, a sequência dos y_{2i} satisfaz

$$y_{2(n+2)} = 14y_{2(n+1)} - y_{2n}.$$

Nesse caso, note que $n = 3m = \frac{3}{2}y_{2i}$ para algum i. Portanto, $n \equiv -2y_{2i} \pmod 7$. Como $y_{2(i+2)} \equiv -y_{2i} \pmod 7$, analisando essa sequência módulo 7, temos

$$y_2 = 4, y_4 = 0, y_6 = 3, y_8 = 0, \ldots$$

Portanto, $n \equiv -2 \cdot 4, -2 \cdot 0, -2 \cdot 3 \pmod 7$, ou seja, $d = 3$ nos dá infinitos n da forma $7k, 7k+1$ e $7k+6$.
Juntando os dois casos analisados, obtemos infinitos n nas formas $7k, 7k+1, 7k+2, 7k+5$ e $7k+6$, enquanto nenhuma solução encontrada é da forma $7k+3$ ou $7k+4$. Como as soluções que encontramos são, na verdade, todas as soluções, concluímos o problema. □

Exemplo 4.5. *Sejam m, k inteiros positivos, e m não é quadrado perfeito. Mostre que existem infinitos inteiros (x, y) que são soluções de $x^2 - my^2 = 1$ e $k|y$.*

Solução. De fato, a equação $x^2 - mk^2y^2 = 1$ possui infinitas soluções, já que mk^2 não é quadrado perfeito. Entretanto, apresentamos outra maneira de provar isso, que é mais interessante.
Sabemos que a sequência $\{y_n\}_{n\geq 1}$ das soluções de $x^2 - my^2 = 1$ satisfaz a recorrência $y_{n+2} = 2x_1y_{n+1} - y_n$, onde (x_1, y_1) é a solução minimal. Além disso, temos uma fórmula geral para y_n:

$$y_n = \frac{1}{2\sqrt{m}}\Big(\big(x_1 + y_1\sqrt{m}\big)^n - \big(x_1 - y_1\sqrt{m}\big)^n\Big).$$

Assim, podemos definir $y_0 = 0$, e a recorrência continua sendo satisfeita. Ainda mais, se analisarmos a sequência $\{y_n\}_{n\geq 0}$ módulo k, sabemos que ela é eventualmente periódica, já que a quantidade de pares $(a, b) \pmod k$ é finita, e então existem $p > q$ tais que $(y_p, y_{p+1}) = (y_q, y_{q+1})$ módulo k, e então, sendo $p - q = T > 0$, temos que $y_n \equiv y_{n+T} \pmod k$ para todo $n \geq q$. Entretanto, note que $(y_p, y_{p+1}) = (y_q, y_{q+1})$ módulo k implica que $(y_{p-1}, y_p) = (y_{q-1}, y_q)$ módulo k, pois, dados os restos de y_n, y_{n+1} módulo k, o resto de y_{n-1} está determinado. Isso nos diz que podemos supor $q = 0$, e então $y_n \equiv y_{n+T} \pmod k$ para todo $n \geq q = 0$, de modo que $y_{Tr} \equiv y_0 = 0 \pmod k$. Assim, provamos que todas as sequências definidas pela relação de recorrência $a_{n+2} = ra_{n+1} \pm a_n$ são *puramente periódicas* módulo k para todo k inteiro, isto é, existe $T > 0$ tal que $a_n \equiv a_{n+T} \pmod k$ para todo n natural. □

Exemplo 4.6. *Encontre todos os pares de inteiros positivos (x, y) satisfazendo a equação $x^2 + y^2 - 5xy + 5 = 0$.*

Solução. Analisando a equação dada como uma quadrática em x, o discriminante deve ser quadrado perfeito, ou seja,

$$25y^2 - 4(y^2 + 5) = T^2 \Leftrightarrow T^2 - 21y^2 = -20.$$

A solução minimal de $X^2 - 21Y^2 = 1$ é $(55, 12)$ (use o método das frações contínuas!). Assim, basta encontrar todas as soluções de $u^2 - 21v^2 = -20$ com $u + v\sqrt{21} < (55 + 12\sqrt{21})\sqrt{20}$ pelo Teorema 3.6. Isso é deixado como exercício (para facilitar na procura, vale à pena analisar módulo 20 e 21 por exemplo, já que $u^2 + v^2 \equiv 1 \pmod{20}$ e $u^2 \equiv 1 \pmod{21}$. Como $u > 55\sqrt{20} \Longrightarrow v > 12\sqrt{20}$, basta analisar todos os $u < 55\sqrt{20}$ com $u^2 \equiv 1 \pmod{21}$). □

Exemplo 4.7. *Encontre todos os primos p tais que $n\sqrt{p}\{n\sqrt{p}\} > 1$ para todo n inteiro positivo, onde $\{x\}$ é a parte fracionária de x.*

Solução. Escrevendo $\{n\sqrt{p}\} = n\sqrt{p} - \lfloor n\sqrt{p}\rfloor$, nossa desigualdade torna-se

$$n\sqrt{p}\Big(n\sqrt{p} - \lfloor n\sqrt{p}\rfloor\Big) > 1 \Longleftrightarrow n\sqrt{p} - \lfloor n\sqrt{p}\rfloor > \frac{1}{n\sqrt{p}}.$$

Suponha que tal desigualdade não ocorra para algum n. Temos então

$$0 < n\sqrt{p} - \lfloor n\sqrt{p}\rfloor \leq \frac{1}{n\sqrt{p}} \Longleftrightarrow 0 < n^2p - \lfloor n\sqrt{p}\rfloor^2 \leq \frac{n\sqrt{p} + \lfloor n\sqrt{p}\rfloor}{n\sqrt{p}} < 2.$$

Como $n^2p - \lfloor n\sqrt{p}\rfloor^2$ é inteiro, devemos ter $n^2p - \lfloor n\sqrt{p}\rfloor^2 = 1$. Pela Proposição 3.4, sabemos que $x^2 - py^2 = -1$ só possui solução se p é da forma $4k+1$. Logo, segue que a condição inicial é satisfeita se, e só se, p é da forma $4k + 3$, com $k \geq 0$ inteiro. □

Exemplo 4.8. *Encontre o maior real c tal que, para todo n natural, vale a desigualdade*

$$\{n\sqrt{2}\} \geq \frac{c}{n},$$

e determine todos os naturais n para os quais a igualdade ocorre.

Solução. Queremos encontrar $\inf_{n\in\mathbb{N}} \left\{n\{n\sqrt{2}\}\right\}$. Para isso, note que

$$n\{n\sqrt{2}\} = n(n\sqrt{2} - \lfloor n\sqrt{2}\rfloor).$$

Assim, para que tal valor seja pequeno, é necessário que $n\sqrt{2} - \lfloor n\sqrt{2}\rfloor$ seja pequeno. Sabemos que a Equação de Pell nos dá boas aproximações da raiz quadrada de um natural por racionais, de modo que torna-se claro encontrar valores de n utilizando Pell. Tome n de modo que $2n^2 - \lfloor n\sqrt{2}\rfloor^2 = 1$, e sabemos que existem infinitos n com essa propriedade, já que a equação $x^2 - 2y^2 = -1$ possui infinitas soluções. Logo, temos que

$$n\{n\sqrt{2}\} = n(n\sqrt{2} - \lfloor n\sqrt{2}\rfloor) = \frac{n}{n\sqrt{2} + \lfloor n\sqrt{2}\rfloor} > \frac{n}{2n\sqrt{2}} = \frac{1}{2\sqrt{2}}.$$

De fato, isso é o melhor que podemos fazer, já que, se $2n^2 - \lfloor n\sqrt{2}\rfloor^2 = t \geq 1$, temos

$$n\{n\sqrt{2}\} = n(n\sqrt{2} - \lfloor n\sqrt{2}\rfloor) = \frac{tn}{n\sqrt{2} + \lfloor n\sqrt{2}\rfloor} > \frac{n}{2n\sqrt{2}} = \frac{1}{2\sqrt{2}}.$$

Como

$$\lim_{n\to\infty} \frac{n}{n\sqrt{2} + \lfloor n\sqrt{2}\rfloor} = \frac{1}{2\sqrt{2}},$$

Segue que $c = \frac{1}{2\sqrt{2}}$ é a melhor cota possível, pois ela é verdadeira para todo n, e existe uma sequência infinita de naturais tal que $n\{n\sqrt{2}\}$ tende para c por cima (tal sequência é dada pela equação $x^2 - 2y^2 = -1$). □

Exemplo 4.9. *Seja n um natural, e suponha que $m = 2\sqrt{28n^2+1} + 2$ é inteiro. Mostre que m é um quadrado perfeito.*

Solução 1. Esta solução mostra como, às vezes, é necessário calcular termos iniciais de sequências para encontrar padrões, e então provar resultados mais gerais.
Primeiro, note que

$$m = 2\sqrt{28n^2+1} + 2 \iff (m-2)^2 - 7(4n)^2 = 4.$$

Portanto, estamos interessados nas soluções de

$$x^2 - 7y^2 = 4,$$

com y múltiplo de 4.
Note que a solução minimal de $x^2 - 7y^2 = 1$ é $(8, 3)$, e que existe apenas uma classe de soluções para $x^2 - 7y^2 = 4$, tendo como solução minimal $(16, 6)$ (o leitor pode verificar isso com o auxílio do Teorema 3.6).
Portanto, todas as soluções serão dadas pela fórmula

$$x_i + y_i\sqrt{7} = \left(16 + 6\sqrt{7}\right)\left(8 + 3\sqrt{7}\right)^{i-1} = 2(8 + 3\sqrt{7})^i.$$

Fica como exercício verificar que y_i é múltiplo de 4 apenas quando i é par. Olhemos para a sequência $\{x_{2i}\}$. Queremos mostrar que $x_{2i} + 2$ é quadrado perfeito. Portanto, segue da fórmula encontrada para as soluções de $x^2 - 7y^2 = 4$ que a sequência $\{x_{2i}\}$ satisfaz a recorrência

$$x_{2(i+1)} = 254x_{2i} - x_{2(i-1)},$$

sendo $x_0 = 2$, $x_2 = 254$. Queremos que $z_i = x_{2i} + 2$ seja quadrado perfeito. Note que

$$z_{i+1} = 254z_i - z_{i-1} - 504.$$

Calculemos alguns termos iniciais da sequência $\{z_i\}$:

$$z_0 = 4 = 2^2, z_1 = 256 = 16^2, z_2 = 254^2, z_3 = 4048^2.$$

Olhemos para a sequência $t_i = \sqrt{z_i}$. Temos que $t_0 = 2, t_1 = 16, t_2 = 254, t_3 = 4048$. Com um pouco de atenção, podemos conjecturar o seguinte padrão:

$$254 = 16 \cdot 16 - 2, \quad 4048 = 16 \cdot 254 - 16.$$

Provemos, então, por indução, que

$$t_{i+2} = 16t_{i+1} - t_i$$

para todo $i \geq 0$. Como $z_i > 0$ para todo i (uma simples indução nos garante isso), então basta que

$$z_{i+2} = 256z_{i+1} + z_i - 32t_{i+1}t_i \iff 254z_{i+1} - z_1 - 504 = 256z_{i+1} + z_i - 32t_{i+1}t_i.$$

Simplificando, basta que

$$16t_{i+1}t_i = z_{i+1} + z_i + 252 \iff t_i^2 - 16t_{i+1} \cdot t_i + z_{i+1} + 252 = 0.$$

Suponha que isso valha para i, e provemos para $i+1$. Queremos que

$$t_{i+2}^2 - 16t_{i+1} \cdot t_{i+2} + z_{i+1} + 252 = 0.$$

Portanto, olhando para a equação quadrática $x^2 - 16t_{i+1}x + z_{i+1} + 252 = 0$, sabemos que uma de suas raízes é t_i, e queremos que a outra seja t_{i+2}. Seja α a outra raiz. Note que

$$\alpha + t_i = 16t_{i+1} \qquad \text{e} \qquad \alpha t_i = z_{i+1} + 252.$$

Elevando a primeira equação ao quadrado, temos

$$\alpha^2 + z_i + 2\alpha t_i = 256z_{i+1} \iff \alpha^2 = 254z_{i+1} - z_i - 504 = z_{i+2}.$$

Logo, $\alpha = \pm t_{i+2}$. Como $\alpha = \frac{z_{i+1}+252}{t_i} > 0$, segue que $\alpha = t_{i+2}$. Isso nos mostra que

$$t_{i+2} = 16t_{i+1} - t_i.$$

Como os termos iniciais de t_i são inteiros positivos, todos os termos subsequentes também serão inteiros, e isso garante que z_i é quadrado perfeito, como desejado. □

Solução 2. Seja $r = \sqrt{28n^2 + 1}$, que é inteiro, e então $r^2 - 7(2n)^2 = 1$. Estamos interessados nas soluções de

$$x^2 - 7y^2 = 1$$

com y par, e queremos que $2x+2$ seja quadrado perfeito nesse caso. Como $(8, 3)$ é a solução minimal, segue que

$$x_i + y_i\sqrt{7} = (8 + 3\sqrt{7})^i$$

nos fornece todas as soluções da Pell. Sabemos que $\{y_i\}$ satisfaz a recorrência $y_{i+2} = 16y_{i+1} - y_i$, pois $x_1 = 8$, e então, como $y_0 = 0, y_1 = 3$, segue y_i é par apenas quando i é par. Disso, segue que

$$r = \frac{(8 + 3\sqrt{7})^{2k} + (8 - 3\sqrt{7})^{2k}}{2} \iff 2r+2 = (8+3\sqrt{7})^{2k}+(8-3\sqrt{7})^{2k}+2 = \left((8+3\sqrt{7})^k+(8-3\sqrt{7})^k\right)^2.$$

Claramente $(8 + 3\sqrt{7})^k + (8 - 3\sqrt{7})^k \in \mathbb{Z}$, o que termina o problema. □

Exemplo 4.10. *Seja a um inteiro positivo que não é quadrado perfeito. Seja A o conjunto dos inteiros positivos k tais que*

$$k = \frac{x^2 - a}{x^2 - y^2} \tag{1}$$

para inteiros não negativos, com $x > \sqrt{a}$. Seja B o conjunto dos inteiros positivos k tais que (1) ocorre para inteiros não negativos x, y com $x < \sqrt{a}$. Mostre que $A = B$.

Solução 1. Reescrevendo a relação (1), obtemos

$$ky^2 - (k-1)x^2 = a \iff (ky)^2 - k(k-1)x^2 = ak.$$

Vamos supor que tal equação possui solução, e então mostrar que $k \in B$ e $k \in A$.
Analisemos a equação $X^2 - k(k-1)Y^2 = ak$. Como $k > 1$ pois a não é quadrado perfeito, $k(k-1) > 0$ não é quadrado perfeito. Portanto, tudo o que sabemos sobre Pell torna-se válido aqui. Olhemos

para a solução minimal de $X^2 - k(k-1)Y^2 = 1$. É imeditado que $(2k-1) + 2\sqrt{k(k-1)}$ é solução, e que não há solução com $Y = 1$. Logo, a solução minimal é $(2k-1, 2)$.
A condição do problema é equivalente a mostrar que, se $(ky)^2 - k(k-1)x^2 = ak$ posssui solução, então existe uma solução com $x < \sqrt{a}$ e uma com $x > \sqrt{a}$. Caso $x < \sqrt{a}$, isso nos diz que $x < y < \sqrt{a}$. Caso $x > \sqrt{a}$, isso nos diz que $x > y > \sqrt{a}$.
Assim, estamos interessados em soluções pequenas da Pell, pois, a partir delas, encontramos soluções com x, y grandes. Tome a solução (ky, x) da equação de Pell. Pelo Teorema 3.7, existe uma solução $u + v\sqrt{k(k-1)} \leq \sqrt{(2k-1+2\sqrt{k(k-1)}) \cdot ak}$ tal que $ky + x\sqrt{k(k-1)} = (u + v\sqrt{k(k-1)})(2k - 1 + 2\sqrt{k(k-1)})^r$ ou $ky + x\sqrt{k(k-1)} = |u - v\sqrt{k(k-1)}|(2k-1+2\sqrt{k(k-1)})^r$. Vamos mostrar que $u < k\sqrt{a}$ e $v < \sqrt{a}$, além de que u é múltiplo de k.
Fica cargo do leitor verificar que, se (p, q) é solução para $p^2 - k(k-1)q^2 = ak$, então $p > k\sqrt{a} \iff q > \sqrt{a}$. Assim, como

$$u+v\sqrt{a} \leq \sqrt{(2k-1+2\sqrt{k(k-1)}) \cdot ak} = \sqrt{a}\sqrt{k^2 + 2k\sqrt{k(k-1)} + (k^2-k)} = \sqrt{a}(k+\sqrt{k(k-1)}),$$

não podemos ter $u > k\sqrt{a}$ nem $v > \sqrt{a}$.
Ainda falta mostrar que k divide u. Como (ky, x) era a solução original, basta ver se a solução

$$(ky + x\sqrt{k(k-1)})(2k - 1 - 2\sqrt{k(k-1)}) = y_1 + x_1\sqrt{k(k-1)}$$

satisfaz $k|y_1$, já que $(u + v\sqrt{k(k-1)}) = (ky + x\sqrt{k(k-1)})(2k - 1 - 2\sqrt{k(k-1)})^r$, ou $|u - v\sqrt{k(k-1)}| = (ky + x\sqrt{k(k-1)})(2k - 1 - 2\sqrt{k(k-1)})^r$. Mas

$$(ky + x\sqrt{k(k-1)})(2k - 1 - 2\sqrt{k(k-1)}) = yk(2k-1) - 2xk(k-1) + (x(2k-1) - 2ky)\sqrt{k(k-1)},$$

e segue que $k|y_1$, e portanto, com várias aplicações desse processo, concluímos que $k|u$.
Assim, escrevemos $u = k \cdot b$, e temos $b < \sqrt{a}$:

$$(kb)^2 - k(k-1)v^2 = ak \iff k = \frac{v^2 - a}{v^2 - b^2}.$$

Como $0 \leq b, v < \sqrt{a}$, temos que $k \in B$. Entretanto, tomando a solução (kb, v) da Pell $x^2 - k(k-1)y^2 = ak$, sabemos que podemos encontrar soluções de módulo arbitrariamente grande, já que todas as soluções

$$kt_i + s_i\sqrt{k(k-1)} = \left(kb + v\sqrt{k(k-1)}\right)\left(2k - 1 + 2\sqrt{k(k-1)}\right)^i$$

nos fornecem soluções de (1) (a prova de que $t_i \in \mathbb{N}$ é análoga à prova de que k divide u). Assim, tomando i de modo que $t_i, s_i > \sqrt{a}$, concluímos que $k \in A$. Logo, se (1) possui solução, concluímos que $k \in A, B$, de modo que $A = B$. □

Solução 2. Apresentamos outra solução, em que são necessários menos conhecimentos sobre equação de Pell, mas envolvem mais espertise algébrica. Novamente, trabalhamos com a equação

$$(ky)^2 - k(k-1)x^2 = ak,$$

e vamos construir soluções onde $x < \sqrt{a}$ e $x > \sqrt{a}$. Novamente, observamos que $(2k-1, 2)$ é solução de $X^2 - k(k-1)Y^2 = 1$, já que é a partir dela e que conseguimos mais soluções para $X^2 - k(k-1)Y^2 = ak$.
Como na Solução 1, a partir da solução (ky, x) de $X^2 - k(k-1)Y^2 = ak$ obtemos as soluções $\big(yk(2k-1) \pm 2xk(k-1), x(2k-1) \pm 2yk\big)$ multiplicando por $2k - 1 \pm 2\sqrt{k(k-1)}$. A partir de agora, $(x_0, y_0) \to (x_1, y_1)$ indica que, a partir da solução (x_0, y_0), obtemos a solução (x_1, y_1) multiplicando por $2k - 1 \pm 2\sqrt{k(k-1)}$. Portanto,

$$(ky, x) \to \big(yk(2k-1) \pm 2xk(k-1), x(2k-1) \pm 2yk\big).$$

É trivial que, se $k|x_0$, então $k|x_1$. Então, como $x(2k-1) + 2yk > x$, geramos soluções (u, v) com v aribitrariamente grande e $k|u$, e isso garante que, se $k \in A \cup B$, então $k \in A$, e então $A \subseteq B$.
Basta então que encontremos soluções com (u, v) onde v é pequeno. A principal observação é a seguinte: se (u, v) é uma solução, então $(\pm u, \pm v)$ também é solução, e então precisamos nos preocupar apenas com o módulo de v.
Assim, suponha que temos uma solução (kx_0, y_0) onde $|y_0| > \sqrt{a}$. Isso nos diz que $|y_0| > |x_0| > \sqrt{a}$. Vamos mostrar que, se $(kx_0, y_0) \to (kx_1, y_1)$, onde o sinal negativo foi escolhido, então $|x_1| < |x_0|$.

Caso $|x_1| < \sqrt{a}$, temos também que $|y_1| < \sqrt{a}$ e então encontramos a solução desejada. Caso $|x_1| > \sqrt{a}$, então $|y_1| > \sqrt{a}$ e podemos aplicar o mesmo processo novamente e encontrar uma solução (x_2, y_2) com $|x_2| < |x_1|$.
Finalmente, provemos que $|x_1| < |x_0|$. Como $|x_1| = \big||x_0|(2k-1) - 2(k-1)|y_0|\big|$, basta que

$$\big||x_0|(2k-1) - 2(k-1)|y_0|\big| < |x_0|.$$

Como

$$|x_0|(2k-1) - 2(k-1)|y_0| < |x_0| \iff |x_0| < |y_0|,$$

o que é verdade por hipótese, basta que

$$2(k-1)|y_0| - (2k-1)|x_0| < |x_0| \iff \frac{|x_0|}{|y_0|} > \frac{k-1}{k}.$$

De fato, note que

$$(kx_0)^2 - k(k-1)y_0^2 = a > 0 \Longrightarrow \frac{x_0^2}{y_0^2} > \frac{k-1}{k}.$$

Como $\frac{|x_0|}{|y_0|} < 1$, então

$$\frac{|x_0|}{|y_0|} > \frac{x_0^2}{y_0^2} > \frac{k-1}{k},$$

como desejado.
Portanto, se $k \in A \cup B$, provamos que $k \in B$ e então $B \subseteq A$. Como $A \subseteq B$ já foi demonstrado, temos $A = B$. □

Exemplo 4.11. *Determine todos os inteiros (x, y) tais que $(xy+1)(xy+x+2)$ é quadrado perfeito.*

Solução. Começamos calculando $\text{mdc}(xy+1, xy+x+2)$:

$$\text{mdc}(xy+1, xy+x+2) = \text{mdc}(xy+1, x+1) = \text{mdc}(-y+1, x+1) = d.$$

Logo, sendo $x = d\alpha - 1$ e $y = d\beta + 1$ com $\text{mdc}(\alpha, \beta) = 1$ e $\alpha, \beta > 0$, queremos que

$$\big((d\alpha-1)(d\beta+1)+1\big)\big((d\alpha-1)(d\beta+1)+(d\alpha-1)+2\big) = d^2\big(d\alpha\beta+\alpha-\beta\big)\big(d\alpha\beta+2\alpha-\beta\big)$$

seja quadrado perfeito. Para isso, queremos que

$$d\alpha\beta + \alpha - \beta = p^2 \qquad \text{e} \qquad d\alpha\beta + 2\alpha - \beta = q^2,$$

onde $p, q \in \mathbb{N}$. Mas isso só ocorre se

$$d\alpha\beta + \alpha - \beta = p^2 \qquad \text{e} \qquad \alpha = q^2 - p^2.$$

Substituindo $\alpha = q^2 - p^2$ na primeira equação reduzimos a resolver

$$q^2(d\beta+1) - p^2(d\beta+2) = \beta.$$

Multiplicando por $d\beta + 1$, queremos que

$$\big(q(d\beta+1)\big)^2 - p^2(d\beta+1)(d\beta+2) = \beta(d\beta+1). \tag{1}$$

Seja $d\beta + 1 = t$. Em suma, sabemos que $t \equiv 1 \pmod{\beta}$ e $t > 1$. Procuramos por soluções de $x^2 - t(t+1)y^2 = \beta t$. Como $(2t+1, 2)$ é solução de $x^2 - t(t+1)y^2 = 1$, temos que, se (qt, p) é solução de (1), então $\big(|(2t+1)qt - 2pt(t+1)|, |2qt - p(t+2)|\big)$ também é solução.
Suponha que tal par (x, y) exista, e tome-o de modo que q seja mínimo. Isso nos diria que $|(2t+1)qt - 2pt(t+1)| \geq qt$. Como $\alpha = q^2 - p^2 > 0$, sabemos que $q > p$. Assim, se $(2t+1)qt - 2pt(t+1) < 0$, teríamos

$$2pt(t+1) - (2t+1)qt \geq qt \iff p \geq q,$$

o que é absurdo. Caso $(2t+1)qt - 2pt(t+1) \geq 0$, teríamos

$$(2t+1)qt - 2pt(t+1) \geq qt \iff qt \geq p(t+1)$$

Mas

$$\beta t = (qt)^2 - p^2t(t+1) \geq p(qt(t+1) - pt(t+1)) = p(q-p)t(t+1) > \beta t,$$

um absurdo. Logo, não há soluções com $x, y > 0$. □

Exemplo 4.12. *Encontre todos os pares de inteiros positivos (a, b) que satisfazem*

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

Solução. Dividamos o problema em dois casos.
Caso 1: a é par.
Escrevemos $a = 2k$ com $k \geq 1$ e obtemos

$$(3^k + 1)(3^k - 1) = 2b^2.$$

Assim, como 4 divide o lado esquerdo, segue que b é par, e então escrevemos $b = 2\ell$ para obter

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

Como $(3^k + 1)/2$ e $(3^k - 1)/2$ são coprimos (verifique!), temos que

$$3^k + 1 = 2x^2 \quad \text{e} \quad 3^k - 1 = 4y^2 \tag{1}$$

ou

$$3^k + 1 = 4x^2 \quad \text{e} \quad 3^k - 1 = 2y^2 \tag{2}$$

Para (1), como $4|3^k - 1$, temos que k é par (verifique!), e daí teríamos

$$(3^{k/2} + 2y)(3^{k/2} - 2y) = 1,$$

o que é um absurdo, pois $3^{k/2} \pm 2y \in \mathbb{Z}$ e $3^{k/2} + 2y > 1$. Para (2), teríamos, pela primeira equação, que

$$3^k = (2x + 1)(2x - 1),$$

e então $2x + 1 = z + 2$ e $2x - 1 = z$ são potências de 3. Como 3 não pode dividir z e $z + 2$, devemos ter $z = 1$ e então $x = 1$. Disso segue que $k = 1$, e então $(a, b) = (2, 2)$.
Caso 2: a é ímpar.
Escrevemos $a = 2k + 1$, com $k \geq 0$. Assim, queremos que

$$3^{2k+1} = 2b^2 + 1 \iff 3(3^k)^2 - 2b^2 = 1.$$

Assim, olhemos para as soluções de

$$3x^2 - 2y^2 = 1,$$

com x e y inteiros positivos. Como $(1, 1)$ é solução dessa equação, ele deve ser a minimal. Pelo Teorema 3.14, todas as soluções assumem a forma

$$\sqrt{3}x_i + \sqrt{2}y_i = (\sqrt{3} + \sqrt{2})^{2i+1}.$$

Queremos todos os i para os quais x_i é potência de 3. Podemos imitar o que foi feito na seção 3.6 e obter uma fórmula fechada para x_i:

$$\begin{aligned}
&\sqrt{3}x_i + \sqrt{2}y_i = (\sqrt{3} + \sqrt{2})^{2i+1} \\
\implies &\sqrt{3}x_i - \sqrt{2}y_i = (\sqrt{3} - \sqrt{2})^{2i+1} \\
\implies &x_i = \frac{(\sqrt{3} + \sqrt{2})^{2i+1} + (\sqrt{3} - \sqrt{2})^{2i+1}}{2\sqrt{3}}.
\end{aligned}$$

Expandindo os binomiais, temos

$$\begin{aligned}
x_i &= \frac{\sum_{j=0}^{2i+1} \binom{2i+1}{j} \sqrt{3}^j \sqrt{2}^{2i+1-j} + \sum_{j=0}^{2i+1} \binom{2i+1}{j} \sqrt{3}^j (-\sqrt{2})^{2i+1-j}}{2\sqrt{3}} \\
&= \frac{1}{2\sqrt{3}} \sum_{j \geq 0} \binom{2i+1}{2j+1} \sqrt{3} \cdot 3^j \cdot 2^{i-j+1} \\
&= \sum_{j \geq 0} \binom{2i+1}{2j+1} 3^j \cdot 2^{i-j}.
\end{aligned}$$

Assim, reduzimos a encontrar todos os inteiros $i \geq 0$ para os quais

$$\sum_{j\geq 0} \binom{2i+1}{2j+1} 3^j \cdot 2^{i-j}$$

é uma potência de 3. É trivial verificar que isso ocorre para $i = 0$ e $i = 1$, que nos dão as soluções $(a, b) = (1, 1)$ e $(a, b) = (5, 11)$. Agora, suponha $i \geq 2$, ou seja, $2i + 1 \geq 5$:

$$\sum_{j\geq 0} \binom{2i+1}{2j+1} 3^j \cdot 2^{i-j} = (2i+1)2^i + \binom{2i+1}{3} 3 \cdot 2^{i-1} + \sum_{j\geq 2} \binom{2i+1}{2j+1} 3^j \cdot 2^{i-j}. \qquad (*)$$

Então, fica claro que $3|2i + 1$. Assim, note que

$$\begin{aligned} \nu_3\left(\binom{2i+1}{2j+1} 3^j \cdot 2^{i-j}\right) &= \nu_3\left(\frac{2i+1}{2j+1}\binom{2i}{2j} 3^j \cdot 2^{i-j}\right) \\ &\geq \nu_3(2i+1) + j - \nu_3(2j+1) \geq \nu_3(2i+1) + 2, \end{aligned}$$

onde a última desigualdade $j - \nu_3(2j + 1) \geq 2$ ocorre para $j \geq 2$, pois $\nu_3(2j + 1) \leq \log_3(2j + 1)$, e $j - \log_3(2j + 1) \geq 2$ para $j \geq 4$, e para $j = 2, 3$, temos $\nu_3(2j + 1) = 0$, donde o resultado segue. Como estamos assumindo que $i \geq 2$, concluímos que

$$\sum_{j\geq 2} \binom{2i+1}{2j+1} 3^j \cdot 2^{i-j} \neq 0,$$

e então, para que x_i seja potência de 3, devemos ter

$$\begin{aligned} & 3^{\nu_3(2i+1)+2} | (2i+1)2^i + \binom{2i+1}{3} 3 \cdot 2^{i-1} \\ \iff & 9 | 2^i + 2i(2i-1)2^{i-2} \\ \iff & 9 | 2i^2 - i + 2. \end{aligned}$$

Como $3|2i + 1 \implies 3|i - 1$, temos que $i = 3r + 1$, para algum r inteiro. Então,

$$\begin{aligned} & 9 | 2i^2 - i + 2 \\ \iff & 9 | 2(6r+1) - 3r + 1 = 9r + 3, \end{aligned}$$

o que nunca ocorre. Logo, para $i \geq 2$, não é possível que x_i seja potência de 3, e isso termina problema.

Note que, no caso a par, poderíamos ter deduzido que $x^2 - 2y^2 = 1$ ou $y^2 - 2x^2 = -1$ em (1) ou (2), e torna-se natural olhar para essa equação, que diz que x e y são soluções de uma equação de Pell. Entretanto, é sempre bom ter em mente que devemos tentar artifícios mais simples antes de partir para técnicas mais avançadas, como analisar módulo algum primo esperto, etc.. Para o caso a ímpar, o leitor pode verificar que não é trivial mostrar que $a \leq 5$ ou alguma cota superior boa com técnicas elementares. Portanto, torna-se necessário o uso de artifícios mais avançados. □

Observação 4.13. *Para resultados mais gerais e similares aos vistos no problema acima, recomendamos ao leitor consultar [2]. Ademais, para outra solução desse problema, consulte [5].*

Problemas Propostos

4.1. *Encontre todos os inteiros positivos n tais que $(2^n - 1)(3^n - 1)$ é um quadrado perfeito.*

4.2. *Existem inteiros $a, b > 1$ tais que $ab + 1$ e $ab^3 + 1$ são ambos quadrados perfeitos?*

4.3. *Prove que $\frac{1^2+2^2+\ldots+n^2}{n}$ é quadrado perfeito para infinitos inteiros potivos n.*

4.4. *Mostre que existem infinitos inteiros x, y, z, t com $mdc(x, y, z, t) = 1$ e*

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

4.5. *Mostre que existem infinitas triplas (x, y, z) de inteiros satisfazendo*

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

4.6. *Mostre que $\lfloor n\sqrt{2} \rfloor$ é quadrado perfeito para infinitos n. Mostre o mesmo para $\lfloor n\sqrt{5} \rfloor$.*

4.7. *Mostre que existem infinitos inteiros positivos x, y com*

$$2x^2 - 3x - 3y^2 - y + 1 = 0.$$

4.8. *Seja $c > 0$ um real. Mostre que o maior divisor primo de $n^2 + 1$ é menor que $c \cdot n$ para infinitos inteiros n.*

4.9. *Resolva, nos inteiros não negativos,*

$$2^x - 5^y = 3.$$

4.10. *Encontre todos os pares $(m, n) \in \mathbb{N}$ tais que*

$$7^n = m^2 + m + 1.$$

4.11. *Resolva, nos inteiros não negativos, $2^x + 7^y = 9^z$.*

4.12. *Seja $x, y, z \in \mathbb{N}$ tais que $z^2 = \frac{x^2+1}{y^2} + 4$. Mostre que $z = 3$.*

4.13. *Mostre que existem infinitos pares (x, y) de inteiros tais que $2^{x^2} + 2^{y^2} + 1$ é quadrado perfeito.*

4.14. *Mostre que $x^3 + y^3 + z^3 + t^3 = 1999$ possui infinitas soluções inteiras positivas.*

4.15. *Mostre que $mdc(n, \lfloor n\sqrt{2} \rfloor) < \sqrt[4]{8}\sqrt{n}$ para $n \in \mathbb{N}$, mas que existem infinitos $n \in \mathbb{N}$ tais que $mdc(n, \lfloor n\sqrt{2} \rfloor) > \sqrt[4]{7.99}\sqrt{n}$.*

4.16. *Encontre a maior potência de 2 que divide $\lfloor (1 + \sqrt{3})^{2n+1} \rfloor$.*

4.17. *Resolva, nos inteiros positivos,*

$$n^2 - 2 = 7^m.$$

Referências

[1] Trygve Nagell. *Introduction to Number Theory*. Wiley, 1951.

[2] D. T. Walker. "On the Diophantine Equation mX2-nY2=±1". In: *The American Mathematical Monthly* 74.5 (1967), pp. 504–513. DOI: 10.1080/00029890.1967.11999992. eprint: https://doi.org/10.1080/00029890.1967.11999992. URL: https://doi.org/10.1080/00029890.1967.11999992.

[3] Samuel Feitosa. *Equação de Pell - Teoria dos Números, Aula 15*. POTI, 2012.

[4] Fabio Brochero; et al. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. IMPA, 2013.

[5] Rafael Filipe. *Equação de Pell Generalizada*. Semana Olímpica, 2020. URL: https://www.obm.org.br/content/uploads/2020/02/23_SO_Rafael_Filipe_Equacao_de_Pell_Generalizada_Nivel_3_compressed.pdf.