Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 14

A equação de Pell

1 Equação de Pell

Seja A um inteiro positivo. Estamos interessados na equação $x^2 - Ay^2 = 1$, com x e y inteiros. Se A é um quadrado perfeito, digamos $A = k^2$, temos que $x^2 - Ay^2 = (x - ky)(x + ky) = 1$ admite apenas as soluções triviais $y = 0$, $x = \pm 1$, pois teríamos $x - ky = x + ky = \pm 1$. O caso interessante é quando A não é um quadrado perfeito, e portanto $\sqrt{A}$ é um irracional (de fato, se $\sqrt{A} = \frac{p}{q}$, com $\text{mdc}(p, q) = 1$ e $q > 1$, teríamos $A = \frac{p^2}{q^2}$ o que é um absurdo, pois $\text{mdc}(p, q) = 1 \implies \text{mdc}(p^2, q^2) = 1$, donde p^2/q^2 não pode ser inteiro). Nesse caso, a equação $x^2 - Ay^2 = 1$ é conhecida como uma *equação de Pell*.

As soluções da equação de Pell correspondem a pontos inteiros sobre uma hipérbole. Por exemplo, para a hipérbole $x^2 - 2y^2 = 1$: o ponto $(3, 2)$ é um exemplo de ponto inteiro sobre a hipérbole pois $3^2 - 2 \cdot 2^2 = 1$ mas o ponto $(7, 5)$ está próximo à hipérbole mas não pertence a ela pois $7^2 - 2 \cdot 5^2 = -1 \neq 1$. Como veremos, o próximo ponto de coordenadas inteiras positivas sobre esta hipérbole é $(17, 12)$.

Outro ponto de vista é o de que estamos procurando pontos de uma hipérbole sobre um reticulado. A mesma equação de Pell acma corresponde à hipérbole é $u^2 - v^2 = 1$ e ao reticulado que consiste nos pontos da forma $(a, b\sqrt{2})$, a e b inteiros. As duas figuras correspondentes só diferem por uma transformação linear.

Um terceiro ponto de vista, que será particularmente útil no que segue tem um caráter mais algébrico: sejam $\mathbb{Z}[\sqrt{A}] = \{x + y\sqrt{A}; x, y \in \mathbb{Z}\}$ e $\mathbb{Q}[\sqrt{A}] = \{x + y\sqrt{A}; x, y \in \mathbb{Q}\} \supset \mathbb{Z}[\sqrt{A}]$. Não é difícil ver que $\mathbb{Z}[\sqrt{A}]$ é um anel e $\mathbb{Q}[\sqrt{A}]$ é um corpo. Dado $\gamma = x + y\sqrt{A} \in \mathbb{Q}[\sqrt{A}]$ (com $x, y \in \mathbb{Q}$), podemos definir seu *conjugado* $\hat{\gamma} = x - y\sqrt{A}$, e sua *norma* $N(\gamma) = \gamma\hat{\gamma} = x^2 - Ay^2$.

Uma observação relevante é que, se $x, y, z, w \in \mathbb{Q}$ e $x + y\sqrt{A} = z + w\sqrt{A}$ então $x = z$ e $y = w$. De fato, se $y = w$ então claramente $x = z$, e se $y \neq w$, teríamos $\sqrt{A} = \frac{z-x}{y-w} \in \mathbb{Q}$, absurdo.

As soluções inteiras (x, y) da equação de Pell correspondem a elementos $x + y\sqrt{A} \in \mathbb{Z}[\sqrt{A}]$ (com $x, y \in \mathbb{Z}$) cuja norma $N(x + y\sqrt{A}) = x^2 - Ay^2$ é igual a 1.

Um fato muito importante sobre a norma é que $N\colon \mathbb{Q}[\sqrt{A}] \to \mathbb{Q}$ é uma função multiplicativa, isto é,

$$N\big((x+y\sqrt{A})(u+v\sqrt{A})\big) = N(x+y\sqrt{A})N(u+v\sqrt{A}) \qquad \forall x,y,u,v \in \mathbb{Q}.$$

Isto segue do fato de que, dados $\alpha = x+y\sqrt{A}, \gamma = u+v\sqrt{A} \in \mathbb{Q}[\sqrt{A}]$, $\hat{\alpha\gamma} = \hat{\alpha}\hat{\gamma}$ (o conjugado de $\alpha\gamma = (x+y\sqrt{A})(u+v\sqrt{A}) = (xu+Ayv)+(xv+yu)\sqrt{A}$ é $(xu+Ayv)-(xv+yu)\sqrt{A} = (x-y\sqrt{A})(u-v\sqrt{A}) = \hat{\alpha}\hat{\gamma}$). Com efeito,

$$N(\alpha\gamma) = \alpha\gamma\hat{\alpha\gamma} = \alpha\hat{\alpha}\gamma\hat{\gamma} = N(\alpha)N(\gamma).$$

Alternativamente, podemos provar este fato diretamente:

$$\begin{aligned} N\big((x+y\sqrt{A})(u+v\sqrt{A})\big) &= N((xu+Ayv)+(xv+yu)\sqrt{A}) \\ &= (xu+Ayv)^2 - A(xv+yu)^2 \\ &= x^2u^2 + A^2y^2v^2 - A(x^2v^2+y^2u^2) \\ &= (x^2-Ay^2)(u^2-Av^2). \end{aligned}$$

É fácil ver (a partir da multiplicatividade da norma) que se a equação tem alguma solução (x_1, y_1) com $y_1 \neq 0$ então possui infinitas. Mais geralmente, se $x_1^2 - Ay_1^2 = \pm 1$, temos

$$N((x_1+\sqrt{A}y_1)^n) = (x_1-\sqrt{A}y_1)^n(x_1+\sqrt{A}y_1)^n = (x_1^2-Ay_1^2)^n = (\pm 1)^n.$$

Fazendo a substituição

$$x_n + \sqrt{A}y_n = (x_1+\sqrt{A}y_1)^n = \sum_{i=0}^{n} \binom{n}{i} x_1^{n-i}(\sqrt{A})^i y_1^i$$

onde

$$x_n = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} x_1^{n-2i}A^i y_1^{2i} \qquad \text{e} \qquad y_n = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2i+1} x_1^{n-2i-1}A^i y_1^{2i+1}$$

obtemos $x_n^2 - Ay_n^2 = (\pm 1)^n$ para todo $n \in \mathbb{N}$.

De maneira mais ou menos equivalente, podemos dizer que se (x_1, y_1) é solução então a transformação linear

$$\begin{pmatrix} x_1 & y_1\sqrt{A} \\ y_1\sqrt{A} & x_1 \end{pmatrix}$$

preserva tanto a hipérbole $u^2 - v^2 = 1$ quanto o reticulado que consiste nos pontos da forma $(a, b\sqrt{A})$.

Vejamos agora que a equação de Pell sempre possui solução.

Teorema 1. *A equação $x^2 - Ay^2 = 1$, com A diferente de um quadrado perfeito, possui solução não trivial em inteiros positivos, i.e., com $x + y\sqrt{A} > 1$.*

Demonstração. Como $\sqrt{A}$ é irracional, a desigualdade $|\sqrt{A} - \frac{p}{q}| < \frac{1}{q^2}$ tem infinitas soluções racionais p/q. Note que se $|\sqrt{A} - \frac{p}{q}| < \frac{1}{q^2}$ então

$$|p^2 - Aq^2| = q^2\left|\sqrt{A} - \frac{p}{q}\right|\left|\frac{p}{q} + \sqrt{A}\right| < \left|\frac{p}{q} + \sqrt{A}\right|$$
$$\leq 2\sqrt{A} + \left|\sqrt{A} - \frac{p}{q}\right| \leq 2\sqrt{A} + 1.$$

Considerando infinitos pares de inteiros positivos (p_n, q_n) com $|\sqrt{A} - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$, teremos sempre $|p_n^2 - Aq_n^2| < 2\sqrt{A} + 1$, portanto temos um número finito de possibilidades para o valor (inteiro) de $p_n^2 - Aq_n^2$. Consequentemente, existe um inteiro $k \neq 0$ tal que $p_n^2 - Aq_n^2 = k$ para infinitos valores de n. Obtemos portanto duas sequências crescentes de pares de inteiros positivos $(u_r), (v_r)$, $r \in \mathbb{N}$ tais que $u_r^2 - Av_r^2 = k$ para todo r.

Como há apenas $|k|^2$ possibilidades para os pares $(u_r \bmod k, v_r \bmod k)$, existem inteiros a e b e infinitos valores de r tais que $u_r \equiv a \pmod{k}$ e $v_r \equiv b \pmod{k}$. Tomamos então $r < s$ com as propriedades acima. Seja

$$x + y\sqrt{A} = \frac{u_s + v_s\sqrt{A}}{u_r + v_r\sqrt{A}} = \frac{(u_s + v_s\sqrt{A})(u_r - v_r\sqrt{A})}{u_r^2 - Av_r^2}$$
$$= \frac{u_s u_r - Av_s v_r}{k} + \left(\frac{u_r v_s - u_s v_r}{k}\right)\sqrt{A}.$$

Temos $u_s u_r - Av_s v_r \equiv u_r^2 - Av_r^2 = k \equiv 0 \pmod{k}$ e $u_r v_s - u_s v_r \equiv ab - ab = 0 \pmod{k}$ e portanto $x = \frac{u_s u_r - Av_s v_r}{k}$ e $y = \frac{u_r v_s - u_s v_r}{k}$ são inteiros. Por outro lado, $(x + y\sqrt{A})(u_r + v_r\sqrt{A}) = u_s + v_s\sqrt{A}$, donde $N(x + y\sqrt{A})N(u_r + v_r\sqrt{A}) = N(u_s + v_s\sqrt{A})$. Como $N(u_r + v_r\sqrt{A}) = N(u_s + v_s\sqrt{A}) = k$, segue que $N(x + y\sqrt{A}) = x^2 - Ay^2 = 1$. Além disso, como $s > r$, $u_s + v_s\sqrt{A} > u_r + v_r\sqrt{A}$, donde $x + y\sqrt{A} = \frac{u_s + v_s\sqrt{A}}{u_r + v_r\sqrt{A}} > 1$. □

Dentre todas as soluções $(x, y) \in \mathbb{N}^2$ da equação de Pell $x^2 - y^2A = 1$ com $x + y\sqrt{A} > 1$, existe uma *solução mínima* ou *fundamental*, i.e., com x e portanto y e $x + y\sqrt{A}$ mínimos. Denote por (x_1, y_1) esta solução mínima. Se, como antes, definimos $(x_n, y_n) \in \mathbb{N}^2$ pela relação $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n$, temos que (x_n, y_n), $n \geq 1$, são todas as soluções inteiras positivas da equação de Pell: de fato, já vimos que (x_n, y_n) são soluções, e se (x', y') é uma outra solução, então como $x_1 + y_1\sqrt{A} > 1$ existe $n \geq 1$ tal que

$$(x_1 + y_1\sqrt{A})^n \leq x' + y'\sqrt{A} < (x_1 + y_1\sqrt{A})^{n+1}.$$

Multiplicando por $x_n - y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^{-n} > 0$, obtemos

$$1 \leq (x' + y'\sqrt{A})(x_n - y_n\sqrt{A}) = (x'x_n - y'y_nA) + (y'x_n - x'y_n)\sqrt{A}$$
$$< x_1 + y_1\sqrt{A}.$$

Como $N\big((x' + y'\sqrt{A})(x_n - y_n\sqrt{A})\big) = N(x' + y'\sqrt{A})N(x_n - y_n\sqrt{A}) = 1$, temos que $(x'x_n - y'y_nA, y'x_n - x'y_n)$ também é uma solução da equação de Pell,

menor que a solução mínima. Temos que $x'x_n - y'y_nA \geq 0$, pois caso contrário $x'x_n - y'y_nA < 0 \iff \frac{x'}{y'}\frac{x_n}{y_n} < A$, porém

$$x_n^2 - y_n^2A = 1 \implies \left(\frac{x_n}{y_n}\right)^2 = A + \frac{1}{y_n^2} > A \implies \frac{x_n}{y_n} > \sqrt{A}$$

e analogamente $\frac{x'}{y'} > \sqrt{A}$, o que contradiz $\frac{x'}{y'}\frac{x_n}{y_n} < A$. Da mesma forma, $y'x_n - x'y_n \geq 0$ pois caso contrário

$$\begin{aligned}\frac{x_n}{y_n} < \frac{x'}{y'} &\implies A + \frac{1}{y_n^2} = \left(\frac{x_n}{y_n}\right)^2 < \left(\frac{x'}{y'}\right)^2 = A + \frac{1}{y'^2} \\ &\implies y' < y_n \implies x' < x_n\end{aligned}$$

o que contradiz o fato de $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n \leq x' + y'\sqrt{A}$. Resumindo, temos que $(x'x_n - y'y_nA, y'x_n - x'y_n) \in \mathbb{N}^2$ é uma solução menor do que a solução mínima, logo $x'x_n - y'y_nA = 1$ e $y'x_n - x'y_n = 0$, ou seja, $(x' + y'\sqrt{A})(x_1 - y_1\sqrt{A})^{-n} = 1 \iff x' + y'\sqrt{A} = x_n + y_n\sqrt{A}$, donde $(x', y') = (x_n, y_n)$, como queríamos.

Assim, as soluções com x e y inteiros positivos podem ser enumeradas por (x_n, y_n), $n \geq 0$ de modo que, para todo n, $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n$ e portanto

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

Observe que as sequências (x_n) e (y_n) acima satisfazem a recorrência $u_{n+2} = 2x_1u_{n+1} - u_n$, $\forall n \geq 1$.

A conjectura de Catalan afirma que as únicas potências perfeitas consecutivas são 8 e 9 e foi resolvida completamente em 2003 por Mihăilescu. Vejamos uma aplicação da equação de Pell em um caso particular.

Teorema 2 (Ko Chao). *Seja p um número primo com $p \geq 5$, então a equação*

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

não possui solução com x e y inteiros não nulos.

Demonstração. Suponhamos por contradição que a equação possui solução inteira não nula e sem perda de generalidade podemos supor $x > 0$ e $y > 0$.

No caso em que x é par e y é ímpar, fazendo $y^p = x^2 - 1 = (x-1)(x+1)$, como $\text{mdc}(x+1, x-1) = 1$, segue que $x-1$ e $x+1$ são potências p-ésimas, ou seja, existem inteiros s e t tais que $x - 1 = s^p$ e $x + 1 = t^p \implies t^p - s^p = 2$ com $s, t \in \mathbb{Z}$ e $p \geq 5$. Com isto a única solução é $t = 1$ e $s = -1$, mas isso implica que $x = 0$, o que foi descartado nas hipóteses.

Agora, no caso em que x é ímpar e y é par, temos que $x+1$ e $x-1$ são pares e $\text{mdc}(x+1, x-1) = 2$. Daqui podemos dividir o problema em dois subcasos: No caso em que $\frac{x-1}{2}$ é ímpar, existem inteiros w e z tais que

$$\frac{x-1}{2} = w^p, \quad \frac{x+1}{2} = 2^{p-2}z^p \quad \text{e} \quad y = 2wz \quad \text{com} \quad \text{mdc}(w, 2z) = 1.$$

Assim

$$w^p = \frac{x+1}{2} - 1 = 2^{p-2}z^p - 1 \geq (2^{p-2}-1)z^p,$$

isto é,

$$\left(\frac{w}{z}\right)^p \geq 2^{p-2} - 1 > 1,$$

portanto $w > z$.

Por outro lado

$$w^{2p} = \left(\frac{x-1}{2}\right)^2 = \frac{x^2+6x+9-8(x+1)}{4} = \left(\frac{x+3}{2}\right)^2 - (2z)^p.$$

Assim obtemos a equação $(w^2)^p + (2z)^p = (\frac{x+3}{2})^2$. Como

$$\begin{aligned}\frac{(w^2)^p + (2z)^p}{w^2+2z} &= (w^2)^{p-1} - (w^2)^{p-2}(2z) + (w^2)^{p-3}(2z)^2 - \cdots + (2z)^{p-1} \\ &\equiv p(w^2)^{p-1} \pmod{w^2+2z}\end{aligned}$$

e $\text{mdc}(w, 2z) = 1$ temos

$$\text{mdc}\left(w^2+2z, \frac{(w^2)^p+(2z)^p}{w^2+2z}\right) = \text{mdc}(w^2+2z, p(w^2)^{p-1}) \mid p,$$

logo se $p \nmid \frac{x+3}{2}$ temos que w^2+2z é um quadrado. Mas $w^2 < w^2+2z < w^2+2w < (w+1)^2$ assim w^2+2z não pode ser um quadrado, logo $p \mid \frac{x+3}{2}$ e além disso do fato que $p > 3$ segue que $p \nmid x$.

De forma similar, no caso que $\frac{x+1}{2} = w^p$ e $\frac{x-1}{2} = 2^{p-2}z^p$, usando a equação $(w^2)^p - (2z)^p = (\frac{x-3}{2})^2$, concluímos analogamente que $p \mid \frac{x-3}{2}$ e portanto $p \nmid x$.

Voltando à equação original temos que $x^2 = y^p + 1^p$. Como $p \nmid x$ e (como antes) $\text{mdc}\left(y+1, \frac{y^p+1}{y+1}\right) \mid p$ temos que $y+1 = s^2$. Logo $(s,1)$ e $(x, y^{\frac{p-1}{2}})$ são soluções da equação de Pell

$$u^2 - yv^2 = 1.$$

Observe que $(s,1)$ é uma solução fundamental pela minimalidade da segunda coordenada, donde existe um natural $m \in \mathbb{N}$ tal que

$$x + y^{\frac{p-1}{2}}\sqrt{y} = (s+\sqrt{y})^m.$$

Desenvolvendo a anterior identidade obtemos

$$\begin{aligned}x &= s^m + \binom{m}{2}s^{m-2}y + \binom{m}{4}s^{m-4}y^2 + \cdots \\ y^{\frac{p-1}{2}} &= ms^{m-1} + \binom{m}{3}s^{m-3}y + \binom{m}{5}s^{m-5}y^2 + \cdots\end{aligned}$$

Desta segunda equação temos que y divide o termo ms^{m-1}, ou seja, $ms^{m-1} \equiv 0 \pmod{y}$. Como y é par e s é ímpar segue que m é par. Novamente usando a segunda equação, como s em cada somando à direita está elevado a uma potência ímpar, temos que $s \mid y^{\frac{p-1}{2}}$. Mas $y+1 = s^2$, assim $y \equiv -1 \pmod{s}$ e elevando a $\frac{p-1}{2}$ obtemos

$$0 \equiv y^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{s},$$

mas isto implica que $s = 1$ e neste caso $y = 0$. Portanto a única solução de $x^2 = y^p + 1$ é $x = \pm 1$ e $y = 0$. □

1.1 Solução Inicial da Equação de Pell

Na prova da existência de soluções da equação de Pell, não mostramos um procedimento para encontrar explicitamente uma solução, que é o que faremos nesta seção.

Para determinar uma solução da equação $x^2 - Ay^2 = 1$, vamos considerar a fração contínua de $\sqrt{A}$. Isso é natural, pois, se x e y são inteiros positivos tais que $x^2 - Ay^2 = \pm 1$, temos

$$\left|\frac{x}{y} - \sqrt{A}\right| \left|\frac{x}{y} + \sqrt{A}\right| = \frac{1}{y^2}\left|x^2 - Ay^2\right| = \frac{1}{y^2}, \text{ donde}$$

$$\left|\frac{x}{y} - \sqrt{A}\right| = \frac{1}{|\ \frac{x}{y} + \sqrt{A}\ |\ y^2} < \frac{1}{y^2}.$$

Mais ainda, temos $|\frac{x}{y} + \sqrt{A}| > 2$. De fato, $|\ \frac{x}{y} + \sqrt{A}\ | \geq 2\sqrt{A} - |\ \frac{x}{y} - \sqrt{A}\ | > 2\sqrt{A} - \frac{1}{y^2}$. Se $A \geq 3$, segue que $|\ \frac{x}{y} + \sqrt{A}\ | > 2\sqrt{A} - \frac{1}{y^2} \geq 2\sqrt{A} - 1 \geq 2\sqrt{3} - 1 > 2$, e, se A=2, $y \geq 2$, donde $|\ \frac{x}{y} + \sqrt{A}\ | > 2\sqrt{A} - \frac{1}{y^2} \geq 2\sqrt{A} - \frac{1}{4} = 2\sqrt{2} - \frac{1}{4} > 2$. Portanto,

$$\left|\frac{x}{y} - \sqrt{A}\right| = \frac{1}{|\ \frac{x}{y} + \sqrt{A}\ |\ y^2} < \frac{1}{2y^2},$$

e logo $\frac{x}{y}$ é uma reduzida $\frac{p_n}{q_n}$ da fração contínua de $\sqrt{A}$.

Mais precisamente, vamos considerar a fração contínua de $\sqrt{A} + \lfloor\sqrt{A}\rfloor = [a_0; a_1, a_2, \ldots]$ (a qual difere da fração contínua de $\sqrt{A}$ apenas pelo primeiro termo $a_0 = 2\lfloor\sqrt{A}\rfloor$, que na fração contínua de $\sqrt{A}$ é igual a $\lfloor\sqrt{A}\rfloor = a_0/2$).

Vamos mostrar que existem duas sequências de inteiros positivos b_i e c_i de modo que

$$0 < \frac{\sqrt{A} - c_i}{b_i} < 1 \quad \text{e} \quad \frac{\sqrt{A} + c_i}{b_i} = [a_i; a_{i+1}, a_{i+2} \ldots] \qquad (*)$$

para todo $i \geq 0$. Começamos definindo $b_0 = 1$ e $c_0 = \lfloor\sqrt{A}\rfloor$. Note que $0 < \sqrt{A} - \lfloor\sqrt{A}\rfloor = \frac{\sqrt{A} - c_0}{b_0} =< 1$. Em geral, definimos recursivamente $c_{i+1} = a_i b_i - c_i$ e $b_{i+1} = (A - c_{i+1}^2)/b_i$.

Mostremos inicialmente por indução que b_i e c_i são inteiros com $b_i \neq 0$ e tais que $b_i \mid A - c_i^2$ para todo i. Isto é claramente verdade para $i = 0$. Por hipótese de indução, temos que b_i e c_i são inteiros, logo $c_{i+1} = a_i b_i - c_i$ também será inteiro e $A - c_{i+1}^2 \neq 0$ já que A não é quadrado perfeito. Além disso,

$$A - c_{i+1}^2 = A - (a_i b_i - c_i)^2 = A - c_i^2 - b_i(a_i^2 b_i - 2a_i c_i)$$

será múltiplo de b_i já que $b_i \mid A - c_i^2$ por hipótese de indução. Assim $b_{i+1} = (A - c_{i+1}^2)/b_i$ será um inteiro não nulo tal que $b_{i+1} \mid A - c_{i+1}^2$.

Desta forma, temos

$$\frac{\sqrt{A} + c_i}{b_i} = a_i + \frac{\sqrt{A} - c_{i+1}}{b_i} = a_i + \frac{b_{i+1}}{\sqrt{A} + c_{i+1}} = a_i + \frac{1}{\frac{\sqrt{A} + c_{i+1}}{b_{i+1}}}.$$

de modo que $(*)$ será válida para todo i. Vamos provar agora que b_i e c_i são positivos. Para isto, vamos provar por indução que $b_i > 0$ e $0 < c_i < \sqrt{A}$, o que é verdadeiro para $i = 0$ pois $c_0 = \lfloor \sqrt{A} \rfloor$ e A não é quadrado perfeito. Além disso, pela definição de a_i temos

$$a_i < \frac{\sqrt{A} + c_i}{b_i} = [a_i; a_{i+1}, a_{i+2} \ldots] < a_i + 1$$

donde obtemos $a_i b_i < \sqrt{A} + c_i < a_i b_i + b_i$ (já que $b_i > 0$ por hipótese de indução) e portanto

$$c_{i+1} = a_i b_i - c_i < \sqrt{A} < a_i b_i - c_i + b_i = c_{i+1} + b_i$$

e assim $c_{i+1} < \sqrt{A}$, o que implica $b_{i+1} = (A - c_{i+1}^2)/b_i > 0$ também. Agora suponha por absurdo que $c_{i+1} \leq 0$. Neste caso teríamos $b_i > \sqrt{A} - c_{i+1} \geq \sqrt{A}$, mas como $\sqrt{A} > c_i$ por hipótese de indução, teríamos $b_i > c_i$, donde $c_{i+1} = a_i b_i - c_i \geq b_i - c_i > 0$, o que é uma contradição. Portanto $c_{i+1} > 0$, completando a indução.

Finalmente, temos

$$\frac{\sqrt{A} - c_{i+1}}{b_{i+1}} = \frac{\sqrt{A} - c_{i+1}}{(A - c_{i+1}^2)/b_i} = \frac{b_i}{\sqrt{A} + c_{i+1}} =$$

$$= \frac{b_i}{\sqrt{A} + a_i b_i - c_i} = \frac{1}{a_i + (\sqrt{A} - c_i)/b_i} \in (0, 1),$$

pois $a_i \geq 1$ e $(\sqrt{A} - c_i)/b_i > 0$.

Como $0 < c_i < \sqrt{A}$ e $b_i \mid A - c_i^2$, temos que as sequências $\{c_i\}$ e $\{b_i\}$ só assumem um número finito de valores. Além disso, podemos recuperar os valores de b_i e c_i a partir dos de b_{i+1} e c_{i+1}, para todo $i \geq 0$. De fato, $b_i = (A - c_{i+1}^2)/b_{i+1}$. Além disso, como $0 < \frac{\sqrt{A} - c_i}{b_i} < 1$, temos

$$a_i = \lfloor a_i + \frac{\sqrt{A} - c_i}{b_i} \rfloor = \lfloor \frac{\sqrt{A} + c_{i+1}}{b_i} \rfloor.$$

Finalmente, temos $c_i = a_i b_i - c_{i+1}$. Portanto estas sequências, assim como a fração contínua $\sqrt{A} + \lfloor \sqrt{A} \rfloor = [a_0; a_1, a_2, \ldots]$, são *periódicas puras*, digamos de período k. Em particular $b_k = 1$ e $c_k = a_0$.

Lembramos que como $a_0 = 2\lfloor \sqrt{A} \rfloor$, temos que a expansão em fração contínua de $\sqrt{A}$ é $[a_0/2; a_1, a_2, \ldots]$. Logo, para $i \geq 1$, denotando por p_i/q_i a i-ésima convergente desta fração contínua, temos

$$\sqrt{A} = \frac{\frac{\sqrt{A} + c_{i+1}}{b_{i+1}} p_i + p_{i-1}}{\frac{\sqrt{A} + c_{i+1}}{b_{i+1}} q_i + q_{i-1}},$$

e portanto

$$A q_i + c_{i+1} \sqrt{A} q_i + \sqrt{A} b_{i+1} q_{i-1} = \sqrt{A} p_i + c_{i+1} p_i + b_{i+1} p_{i-1}.$$

Separando parte racional da parte irracional obtemos as equações

$$Aq_i = c_{i+1}p_i + b_{i+1}p_{i-1} \qquad \text{e} \qquad p_i = c_{i+1}q_i + b_{i+1}q_{i-1}.$$

Isolando c_{i+1} nas equações anteriores e igualando obtemos

$$\begin{aligned} &\frac{Aq_i - b_{i+1}p_{i-1}}{p_i} = \frac{p_i - b_{i+1}q_{i-1}}{q_i} \\ \iff &Aq_i^2 - b_{i+1}p_{i-1}q_i = p_i^2 - b_{i+1}q_{i-1}p_i \\ \iff &p_i^2 - Aq_i^2 = b_{i+1}(p_iq_{i-1} - p_{i-1}q_i) \\ \iff &p_i^2 - Aq_i^2 = (-1)^{i+1}b_{i+1} \end{aligned}$$

donde obtemos uma solução da equação $x^2 - Ay^2 = (-1)^{i+1}b_{i+1}$. Se k é o período teremos que $b_k = 1$ e portanto a equação $x^2 - Ay^2 = -1$ tem solução se k é ímpar, enquanto que $x^2 - Ay^2 = 1$ sempre tem solução (tomando $i+1 = 2k$).

Por outro lado, se x e y são inteiros positivos tais que $x^2 - Ay^2 = \pm 1$, vimos que $\frac{x}{y}$ é uma reduzida $\frac{p_n}{q_n}$ da fração contínua de $\sqrt{A}$. Como $p_n^2 - Aq_n^2 = (-1)^{n+1}b_{n+1}$, segue que $b_{n+1} = 1$, mas, como $0 < \sqrt{A} - c_{n+1} = \frac{\sqrt{A}-c_{n+1}}{b_{n+1}} < 1$, segue que $c_{n+1} = \lfloor \sqrt{A} \rfloor$, donde $[a_{n+1}; a_{n+2}, a_{n+3} \ldots] = \frac{\sqrt{A}+c_{n+1}}{b_{n+1}} = \sqrt{A} + \lfloor \sqrt{A} + \rfloor$, e portanto $n+1$ é necessariamente múltiplo de período k.

Por exemplo, se queremos encontrar uma solução da equação $x^2 - 21y^2 = 1$, como

$$4 + \sqrt{21} = [\overline{8; 1, 1, 2, 1, 1}] \qquad \text{e} \qquad \frac{p_5}{q_5} = \frac{55}{12},$$

(a barra denota o período) temos que $55^2 - 21 \times 12^2 = 3025 - 3024 = 1$.

1.2 A Equação $x^2 - Ay^2 = -1$

Suponha, como sempre, que A não é quadrado perfeito. Na seção anterior mostramos que a equação de Pell sempre possui solução. Em contrapartida, a equação $x^2 - Ay^2 = -1$ nem sempre possui solução, de fato se p é um divisor primo de A temos que $x^2 - Ay^2 \equiv x^2 \equiv -1 \pmod{p}$, assim uma condição necessária para a existência de solução é que todo divisor primo de A seja 2 ou da forma $4k+1$. Porém, esta condição ainda não é suficiente. O seguinte teorema dá uma relação entre as soluções fundamentais da equações $x^2 - Ay^2 = 1$ e $x^2 - Ay^2 = -1$ (como antes, a solução fundamental de $x^2 - Ay^2 = -1$, quando esta equação tem solução inteira, é o menor número da forma $a + b\sqrt{A}$ com a e b inteiros positivos tais que $a^2 - Ab^2 = -1$).

Proposição 3. *Suponha que a equação $x^2 - Ay^2 = -1$ admita solução inteira e seja $a + b\sqrt{A}$ sua solução fundamental. Seja $c + d\sqrt{A}$ a solução fundamental da equação $x^2 - Ay^2 = 1$. Então*

$$(a + b\sqrt{A})^2 = c + d\sqrt{A}, \quad a^2 = \frac{c-1}{2}.$$

Demonstração. Observemos que $(a+b\sqrt{A})^2$ é solução da equação $x^2-Ay^2=1$. Suponhamos por contradição que não é a solução fundamental, isto é suponhamos que

$$(a+b\sqrt{A})^2 > c+d\sqrt{A} > 1$$

Como $(a+b\sqrt{A})(a-b\sqrt{A}) = -1 < 0$ temos que $1 > -a+b\sqrt{A} > 0$, de fato $-a+b\sqrt{A}$ é a maior solução positiva que tem x negativo e y positivo. Multiplicando a desigualdade anterior por $-a+b\sqrt{A}$, obtemos

$$\begin{aligned}(a+b\sqrt{A}) &> (c+d\sqrt{A})(-a+b\sqrt{A}) = (-ac+bdA)+(cb-ad)\sqrt{A}\\ &> -a+b\sqrt{A} > 0.\end{aligned}$$

Temos que $(-ac+bdA, cb-ad)$ é solução de $x^2-Ay^2=-1$. Observemos que $-ac+bdA$, $cb-ad$ não podem ser simultaneamente positivos, porque isto contradiz a escolha da solução fundamental. Também não podemos ter que $-ac+bdA<0$, $cb-ad>0$ porque $-a+b\sqrt{A}$ é a maior solução positiva de $x^2-Ay^2=-1$ com x negativo e y positivo. Por último, no caso $-ac+bdA>0$, $cb-ad<0$, isto é, $bdA>ac$, $ad>cb$, multiplicando a primeira desigualdade por d e a segunda por c obtemos $bd^2A>acd>c^2b$, assim $0>b(c^2-Ad^2)=b$, o que também é contraditório. Assim concluímos que $(a+b\sqrt{A})^2=c+d\sqrt{A}$. Como $a^2-Ab^2=-1$, somando as igualdades temos $c-1=2a^2$ logo $a^2=(c-1)/2$. □

Vejamos agora que a condição sobre os fatores primos de A não é suficiente para garantir a existência de solução. Por exemplo, $x^2-34y^2=-1$ não possui solução inteira. De fato, a solução fundamental de $x^2-34y^2=1$ é $35+6\sqrt{34}$, mas $\frac{35-1}{2}=17$ não é quadrado, logo, pelo teorema anterior, $x^2-34y^2=-1$ não possui soluções.

No caso em que A é um primo da forma $4k+1$, a equação $x^2-Ay^2=-1$ sempre possui solução. Mais geralmente, temos o seguinte resultado, devido a Dirichlet.

Proposição 4 (Dirichlet). *Seja A produto de no máximo três primos distintos da forma $4k+1$ tais que $\left(\frac{p}{q}\right)=-1$ para todo $p\neq q$ divisores primos de A. Então a equação $x^2-Ay^2=-1$ possui solução.*

Demonstração. Seja $x_0+\sqrt{A}y_0$ a solução fundamental de $x^2-Ay^2=1$. Como

$$1 = x_0^2 - Ay_0^2 \equiv x_0^2 - y_0^2 \pmod 4,$$

então x_0 é ímpar e y_0 é par. Além disso, do fato de que $(x_0-1)(x_0+1)=Ay_0^2$ e x_0+1 e x_0-1 só tem fator comum 2, segue que existem inteiros s e t primos relativos e inteiros a,b com $A=ab$ tais que

$$y_0 = 2st, \qquad x_0-1 = 2as^2 \qquad \text{e} \qquad x_0+1 = 2bt^2$$

e assim $as^2-bt^2=-1$. Basta portanto mostrar que $a=1$ (de modo que $b=A$). Para isto, observemos que $a\neq A$ porque caso contrário $b=1$ e (t,s) seria uma solução menor do que a solução mínima (x_0,y_0) de $x^2-Ay^2=1$. Por outro lado, se $1<a<A$ temos dois possíveis casos:

1. a é primo, neste caso tomamos um divisor primo p de b e temos que $as^2 \equiv -1 \pmod{p}$. Logo $\left(\frac{-a}{p}\right) = 1$, mas p é da forma $4k+1$ e portanto isto implica $\left(\frac{a}{p}\right) = 1$, o que contradiz a hipótese do teorema.

2. a é produto de dois primos e b é primo, neste caso se p é um divisor primo de a temos que $bt^2 \equiv 1 \pmod{p}$, assim $\left(\frac{b}{p}\right) = 1$, o que de novo contradiz a hipótese do teorema.

□

O resultado anterior foi generalizado por Richaud, Tano e outros. O seguinte teorema contém essencialmente todos estes resultados.

Teorema 5 (Nagell-Trotter). *Sejam $p_1, \ldots, p_n$ números primos distintos congruentes a 1 módulo 4 e $A = p_1 p_2 \ldots p_n$.*

- *Se n é ímpar e* não *existem índices diferentes i, j, k tais que $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_j}{p_k}\right) = 1$, então $x^2 - Ay^2 = -1$ possui solução.*
- *Se n é par, $\left(\frac{p_1}{p_2}\right) = -1$, $\left(\frac{p_1}{p_j}\right) = 1, \forall j > 2$ e* não *existem índices diferentes $i, j, k \geq 2$ tais que $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_j}{p_k}\right) = 1$, então $x^2 - Ay^2 = -1$ possui solução.*
- *Se $\left(\frac{p_1}{p_j}\right) = -1, \forall j \geq 2$, e* não *existem índices diferentes $i, j, k \geq 2$ tais que $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_j}{p_k}\right) = -1$, então $x^2 - Ay^2 = -1$ possui solução.*

Demonstração. Ver [3] ou [2]. □

1.3 Soluções da Equação $x^2 - Ay^2 = c$

Novamente assumimos que A não é quadrado perfeito. Seja $(x_1, y_1) \in (\mathbb{N}_{>0})^2$ a solução mínima de $x^2 - Ay^2 = 1$. Dado $c \in \mathbb{Z}$ não nulo, se existe alguma solução de $x^2 - Ay^2 = c$ com $(x, y) \in \mathbb{N}^2$, então existem infinitas: de fato, se $u + v\sqrt{A} = (x + y\sqrt{A})(x_1 + y_1\sqrt{A})^n$ com $n \in \mathbb{Z}$, então $u^2 - Av^2 = c$.

Por outro lado, nem sempre existe uma tal solução. Uma condição necessária para a existência de soluções é a seguinte: se p é um divisor primo de A, temos $x^2 \equiv c \pmod{p}$, assim para que exista solução c deve ser resíduo quadrático módulo p para todo divisor primo p de A. Infelizmente esta condição não é suficiente, por exemplo a equação $x^2 - 7y^2 = 11$ não possui solução já que olhando módulo 4

$$x^2 + y^2 \equiv x^2 - 7y^2 = 11 \equiv -1 \pmod{4},$$

o que é impossível. Entretanto $\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = 1$.

As seguintes proposições ajudam a reduzir o trabalho necessário para decidir se $x^2 - Ay^2 = c$ tem alguma solução $(x, y) \in \mathbb{N}^2$.

Proposição 6. *Seja $\alpha = x_1 + y_1\sqrt{A} > 1$ onde (x_1, y_1) é a solução mínima de $x^2 - Ay^2 = 1$. Dado $c \in \mathbb{N}$ não nulo, se existem $x, y \in \mathbb{N}$ com $x^2 - Ay^2 = c$, então existem $r \in \mathbb{N}$ e $u, v \in \mathbb{N}$ com $u + v\sqrt{A} < \alpha\sqrt{|c|}$ e $u^2 - Av^2 = c$ tais que $x + y\sqrt{A} = (u + v\sqrt{A})\alpha^r$.*

Demonstração. Se $x + y\sqrt{A} < \alpha\sqrt{|c|}$, podemos tomar $(u, v) = (x, y)$ e $r = 0$. Suponhamos então que $x + y\sqrt{A} \geq \alpha\sqrt{|c|}$. Seja $\beta = x + y\sqrt{A} > 0$ com $N(\beta) = x^2 - Ay^2 = c$. Então $N(\beta \cdot \alpha^k) = c$ para todo $k \in \mathbb{Z}$. Podemos escolher um $k \in \mathbb{Z}$ tal que $\sqrt{|c|} \leq \beta \cdot \alpha^k < \alpha\sqrt{|c|}$. Definimos $\gamma = \beta \cdot \alpha^k$. Temos que $\gamma = u + v\sqrt{A}$ com $u, v \in \mathbb{Z}$ e logo $x + y\sqrt{A} = \beta = \gamma\alpha^r = (u + v\sqrt{A})\alpha^r$, com $r = -k$. Como $x + y\sqrt{A} \geq \alpha\sqrt{|c|} \geq u + v\sqrt{A}$, segue que $r \geq 0$, donde $r \in \mathbb{N}$.

Finalmente, vamos verificar que u, v são naturais: temos $c = N(\gamma) = u^2 - Av^2 = (u + v\sqrt{A})(u - v\sqrt{A})$, donde

$$|u - v\sqrt{A}| = \frac{|c|}{u + v\sqrt{A}} \leq \frac{|c|}{\sqrt{|c|}} = \sqrt{|c|} \leq u + v\sqrt{A}.$$

Temos assim $u - v\sqrt{A} \leq u + v\sqrt{A}$, donde $v \geq 0$ e simultaneamente $-u + v\sqrt{A} \leq u + v\sqrt{A}$, e logo $u \geq 0$. □

Proposição 7. *Seja $\alpha = x_1 + y_1\sqrt{A} > 1$ onde (x_1, y_1) é a solução mínima de $x^2 - Ay^2 = 1$. Dado $c \in \mathbb{Z}$ não nulo, se existem $x, y \in \mathbb{N}$ com $x^2 - Ay^2 = c$, então existem $u, v \in \mathbb{N}$ com $u + v\sqrt{A} \leq \sqrt{\alpha|c|}$ e $u^2 - Av^2 = c$ (em particular, para esta solução $0 \leq u \leq \sqrt{\alpha|c|}$ e $0 \leq v \leq \sqrt{\alpha|c|/A}$).*

Além disso, dados $x, y \in \mathbb{N}$ com $x^2 - Ay^2 = c$, existem $r \in \mathbb{N}$ e $u, v \in \mathbb{N}$ com $u + v\sqrt{A} \leq \sqrt{\alpha|c|}$ e $u^2 - Av^2 = c$ tais que $x + y\sqrt{A} = (u + v\sqrt{A})\alpha^r$ ou $x + y\sqrt{A} =\mid u - v\sqrt{A} \mid \alpha^{r+1}$.

Demonstração. Se $x + y\sqrt{A} < \sqrt{\alpha|c|}$, podemos tomar $(u, v) = (x, y)$ e $r = 0$. Suponhamos então que $x + y\sqrt{A} \geq \sqrt{\alpha|c|}$.

Se $\gamma = r + s\sqrt{A}$ com $r, s \in \mathbb{Q}$ lembramos que $\hat{\gamma} = r - s\sqrt{A}$, e $N(\gamma) = N(\hat{\gamma}) = \gamma \cdot \hat{\gamma} = r^2 - As^2$.

Seja $\beta = x + y\sqrt{A} > 0$ com $N(\beta) = x^2 - Ay^2 = c$. Então $N(\beta \cdot \alpha^k) = c$ para todo $k \in \mathbb{Z}$. Podemos escolher um $k \in \mathbb{Z}$ tal que $\sqrt{|c|} \leq \beta \cdot \alpha^k < \alpha\sqrt{|c|}$. No caso que $\sqrt{|c|} \leq \beta \cdot \alpha^k \leq \sqrt{\alpha|c|}$ definimos $\gamma = \beta \cdot \alpha^k$ e no caso que $\sqrt{\alpha|c|} < \beta \cdot \alpha^k \leq \alpha\sqrt{|c|}$, podemos definir $\gamma = \alpha \cdot |c|/(\beta \cdot \alpha^k) =\mid \hat{\beta} \mid \alpha^{1-k}$; assim $N(\gamma) = N(\beta) = N(\hat{\beta}) = c$ e $\sqrt{|c|} < \gamma \leq \sqrt{\alpha|c|}$. Logo, sem perda de generalidade, podemos supor que $\sqrt{|c|} \leq \gamma \leq \sqrt{\alpha|c|}$. No primeiro caso temos $\beta = \gamma\alpha^r = (u + v\sqrt{A})\alpha^r$, com $r = -k \in \mathbb{Z}$, e, como $\beta = x + y\sqrt{A} \geq \sqrt{\alpha|c|} \geq \gamma$, temos $r \in \mathbb{N}$. No segundo caso, temos $\beta = |\beta| =\mid \hat{\gamma} \mid \alpha^{r+1} =\mid u - v\sqrt{A} \mid \alpha^{r+1}$, com $r = k - 2 \in \mathbb{Z}$, e, como $\beta = x + y\sqrt{A} \geq \sqrt{\alpha|c|} > \sqrt{|c|} \geq |c|/\gamma = |\hat{\gamma}|$, temos $r + 1 > 0$, donde $r \in \mathbb{N}$.

Temos que $\gamma = u + v\sqrt{A}$ com $u, v \in \mathbb{Z}$. Ainda precisamos verificar que u, v são naturais, mas

$$c = N(\gamma) = u^2 - Av^2 = (u + v\sqrt{A})(u - v\sqrt{A}).$$

Temos então

$$|u - v\sqrt{A}| = \frac{|c|}{u + v\sqrt{A}} \leq \frac{|c|}{\sqrt{|c|}} = \sqrt{|c|} \leq u + v\sqrt{A}.$$

Temos assim $u - v\sqrt{A} \leq u + v\sqrt{A}$, donde $v \geq 0$ e simultaneamente $-u + v\sqrt{A} \leq u + v\sqrt{A}$, e logo $u \geq 0$. □

1.4 Soluções da Equação $mx^2 - ny^2 = \pm 1$

Suponha que mn não seja quadrado perfeito. Vejamos que se $mx_0^2 - ny_0^2 = \pm 1$ possui uma solução (x_0, y_0) então possui infinitas soluções. Temos

$$(\sqrt{m}x_0 + \sqrt{n}y_0)(\sqrt{m}x_0 - \sqrt{n}y_0) = \pm 1.$$

Como mn não é um quadrado perfeito, a equação de Pell $X^2 - mnY^2 = 1$ possui infinitas soluções; se (z, w) é uma delas, temos

$$(z + \sqrt{mn}w)(z - \sqrt{mn}w) = 1.$$

Multiplicando estas duas equações obtemos

$$(\sqrt{m}x_0 + \sqrt{n}y_0)(z + \sqrt{mn}w)(z - \sqrt{mn}w)(\sqrt{m}x_0 - \sqrt{n}y_0) = \pm 1,$$

que é equivalente a

$$\begin{aligned}&(\sqrt{m}(zx_0 + ny_0w) + \sqrt{n}(y_0z + mx_0w))\\ &\times (\sqrt{m}(zx_0 + ny_0w) - \sqrt{n}(y_0z + mx_0w)) = \pm 1\end{aligned}$$

portanto $x' = zx_0 + ny_0w$ e $y' = y_0z + mx_0w$ geram uma nova solução da equação $mx^2 - ny^2 = \pm 1$.

Reciprocamente, para toda solução (a, b) de $mx^2 - ny^2 = \pm 1$,

$$\begin{aligned}1 &= (ma^2 - nb^2)^2 = (\sqrt{m}a + \sqrt{n}b)^2(\sqrt{m}a - \sqrt{n}b)^2\\ &= (ma^2 + nb^2 + 2\sqrt{mn}ab)(ma^2 + nb^2 - 2\sqrt{mn}ab)\\ &= (2ma^2 \mp 1)^2 - mn(2ab)^2.\end{aligned}$$

Assim $(2ma^2 \mp 1, 2ab)$ é solução da equação $x^2 - mny^2 = 1$. Por outra parte, fixando $A = mn$, o seguinte resultado mostra que nem para todo valor de m e n a equação $mx^2 - ny^2 = 1$ possui solução.

Teorema 8. *Seja $A \in \mathbb{Z}$ livre de quadrados.*

- *Se A é par, então x_1 é ímpar, e existe um único par de inteiros positivos (m, n), com $A = mn$ e $(m, n) \neq (1, A)$, tal que a equação $mx^2 - ny^2 = 1$ possui solução. Além disso, a equação $m'x^2 - n'y^2 = 2$, com m', n' inteiros positivos tais que $A = m'n'$ possui solução apenas para $(m', n') = (2, A/2)$ e para $(m', n') = (m/2, 2n)$, caso m seja par ou $(m', n') = (2m, n/2)$, caso m seja ímpar (o que implica n par).*

- *Se A e x_1 são ímpares, então existe um único par de inteiros positivos (m, n), com $A = mn$ e $(m, n) \neq (1, A)$, tal que a equação $mx^2 - ny^2 = 1$ possui solução. Além disso, a equação $m'x^2 - n'y^2 = 2$, com m', n' inteiros positivos tais que $A = m'n'$ não possui solução.*

- *Se A é ímpar e x_1 é par, então não existe nenhum par de inteiros positivos (m, n), com $A = mn$ e $(m, n) \neq (1, A)$, tal que a equação $mx^2 - ny^2 = 1$ possui solução, mas existe um único par de inteiros positivos (m, n), com $A = mn$, tal que a equação $mx^2 - ny^2 = 2$ possui solução.*

Demonstração. Seja (x_1, y_1) solução fundamental de $x^2 - Ay^2 = 1$. Temos então $(x_1 - 1)(x_1 + 1) = x_1^2 - 1 = Ay_1^2$. Observemos que $\mathrm{mdc}(x_1 - 1, x_1 + 1) = \mathrm{mdc}(x_1 - 1, 2) = d$, onde $d = 1$ (se x_1 é par) ou $d = 2$ (se x_1 é ímpar). Segue que $\frac{x_1-1}{d}$ e $\frac{x_1+1}{d}$ são primos relativos, e $d^2 \mid Ay_1^2$. Mas A é livre de quadrados, donde concluímos que $d \mid y_1$.

Definamos $m = \mathrm{mdc}(\frac{x_1+1}{d}, A)$ e $n = \mathrm{mdc}(\frac{x_1-1}{d}, A)$, e assim m e n satisfazem $A = mn$ e

$$\frac{x_1 + 1}{dm}\frac{x_1 - 1}{dn} = \left(\frac{y_1}{d}\right)^2,$$

logo existem s, t primos relativos tais que $y_1 = dst$ e

$$\frac{x_1 + 1}{d} = ms^2 \qquad \text{e} \qquad \frac{x_1 - 1}{d} = nt^2,$$

donde subtraindo as equações obtemos $\frac{2}{d} = ms^2 - nt^2$, o que garante a existência de m e n como no enenciado. Além disso, no caso em que $d = 2$ (que equivale a termos x_1 ímpar), temos $\frac{2}{d}=1$), e o par (m, n) é diferente de $(1, A)$ já que $t < y_1$ e (x_1, y_1) é a solução fundamental de $x^2 - Ay^2 = 1$.

Na outra direção, suponhamos que existam (m', n') e (a, b) tais que $A = m'n'$ e $m'a^2 - n'b^2 = e$ com $e = 1$ ou $e = 2$.

Vamos considerar inicialmente o caso em que $e = 1$. O par $(2m'a^2 - 1, 2ab)$ é solução de $x^2 - Ay^2 = 1$, isto é,

$$(\sqrt{m'}a + \sqrt{n'}b)^2 = (2m'a^2 - 1) + 2ab\sqrt{A} = (x_1 + y_1\sqrt{A})^k = x_k + y_k\sqrt{A}$$

para algum inteiro $k \in \mathbb{N}$. Se k é par, vemos que $\sqrt{m'}a + \sqrt{n'}b = x_{k/2} + y_{k/2}\sqrt{A}$, e a única possibilidade é $m' = 1$ e $n' = A$. No caso k ímpar, temos (como consequência da recorrência $x_{r+2} = 2x_1x_{r+1} - x_r, \forall r \geq 0$) $x_1 \equiv x_k = 2m'a^2 - 1 \equiv 1 \pmod 2$. Além disso, do fato que

$$x_k = \sum_{j=0}^{(k-1)/2} \binom{k}{2j} x_1^{k-2j} A^j y_1^{2j} \equiv x_1^k \pmod A$$

temos que

$$\begin{aligned} m \;\Big|\; \mathrm{mdc}\Big(x_1 + 1, A\Big) \;\Big|\; \mathrm{mdc}\Big(x_1^k + 1, A\Big) &= \mathrm{mdc}\Big(x_k + 1, A\Big) \\ &= \mathrm{mdc}(2a^2m', A) \;\Big|\; 2m' \end{aligned}$$

e

$$\begin{aligned} n \;\Big|\; \mathrm{mdc}\Big(x_1 - 1, A\Big) \;\Big|\; \mathrm{mdc}\Big(x_1^k - 1, A\Big) &= \mathrm{mdc}\Big(x_k - 1, A\Big) \\ &= \mathrm{mdc}(2b^2n', A) \;\Big|\; 2n', \end{aligned}$$

onde as últimas afirmações seguem do fato de que $m'(a^2m') - Ab^2 = m'$ e $Aa^2 - n'(n'b^2) = n'$.

Quando A é ímpar, m e n são ímpares, donde $m \mid m'$, e $n \mid n'$, e como $A = mn \mid m'n' = A$ devemos ter $m = m'$ e $n = n'$.

No caso $e = 2$ temos que $(m'a^2-1, ab)$ é solução de $x^2-Ay^2 = 1$. De fato, se $m'n' = A$ e $m'a^2-n'b^2 = 2$, temos $m'a^2-1+ab\sqrt{A} = (a\sqrt{m'}+b\sqrt{n'})^2/2 = (x_1+y_1\sqrt{A})^k = x_k+y_k\sqrt{A}$, para algum $k \in \mathbb{N}$. Se k é par, vemos que $\sqrt{m'}a+\sqrt{n'}b = x_{k/2}\sqrt{2}+y_{k/2}\sqrt{2A}$, e a única possibilidade é $m' = 2$ e $n' = A/2$ (e logo A é par). No caso k ímpar, temos, como antes, $m \mid \mathrm{mdc}(x_k+1, A) = \mathrm{mdc}(m'a^2, A) \mid 2m'$ e $n \mid \mathrm{mdc}(x_k-1, A) \mid \mathrm{mdc}(n'b^2, A) \mid 2n'$.

Se $e = 2$ e $A = m'n'$ é ímpar, temos m' e n' ímpares, e, como $m'a^2-n'b^2 = 2$, temos a e b ímpares, pois, caso contrário, como eles têm a mesma paridade, seriam ambos pares, e teríamos $4 \mid 2$, absurdo. Assim, nesse caso, $x_1 \equiv x_k = m'a^2-1 \equiv 0 \pmod 2$.

Se $m'a^2-n'b^2 = 2$ e $\tilde{m}a^2-\tilde{n}b^2 = 2$ com m' e $\tilde{m}$ distintos de 2 e $m'n' = \tilde{m}\tilde{n} = A$, temos $m'a^2-1+ab\sqrt{A} = (a\sqrt{m'}+b\sqrt{n'})^2/2 = (x_1+y_1\sqrt{A})^k$ e $\tilde{m}a^2-1+ab\sqrt{A} = (a\sqrt{\tilde{m}}+b\sqrt{\tilde{n}})^2/2 = (x_1+y_1\sqrt{A})^r$, com k e r ímpares. Assim, teremos $a\sqrt{\tilde{m}}+b\sqrt{\tilde{n}} = (a\sqrt{m'}+b\sqrt{n'})(x_1+y_1\sqrt{A})^t$, onde $t = \frac{r-k}{2} \in \mathbb{Z}$, e portanto $\tilde{m} = m'$ e $\tilde{n} = n'$.

No caso em que A é par (e portanto x_1 é ímpar), os argumentos acima mostram que $m \mid 2m'$ e $n \mid 2n'$. Nesse caso, as soluções de $mx^2-ny^2 = 1$ e $mx^2-ny^2 = 2$ estão relacionadas da seguinte forma: se $mx^2-ny^2 = 1$ e m é par, então $(m/2)(2x)^2-2ny^2 = 2$, e, se n é par, então $2mx^2-(n/2)(2y)^2 = 2$; se $mx^2-ny^2 = 2$ e m é par, então $(m/2)x^2-2n(y/2)^2 = 1$, e, se n é par, então $2m(x/2)^2-(n/2)y^2 = 2$. □

Corolário 9. *Dedos inteiros positivos livres de quadrados m e n com $\mathrm{mdc}(m, n) = 1$ e $m \neq 1$, a equação $mx^2-ny^2 = 1$ possui uma solução se, e só se, dada a solução fundamental (x_1, y_1) de $x^2-mny^2 = 1$, o sistema de equações*

$$\begin{aligned} 2mx^2-1 &= x_1 \\ 2xy &= y_1 \end{aligned}$$

tem solução inteira.

Demonstração. Vimos acima que, se a equação possui solução, x_1 deve ser ímpar e existem s, t primos relativos tais que $y_1 = 2st$ e $\frac{x_1+1}{2} = ms^2$, o que prova que o sistema do enunciado tem a solução inteira $(x, y) = (s, t)$. Reciprocamente, como $x_1^2-1 = Ay_1^2$, de $2mx^2-1 = x_1$ segue que $x_1+1 = 2mx^2$, donde $x_1-1 = \frac{x_1^2-1}{x_1+1} = 2\frac{A}{m}(\frac{y_1}{2x})^2 = 2n(\frac{y_1}{2x})^2 = 2ny^2$, e logo $mx^2-ny^2 = \frac{1}{2}((x_1+1)-(x_1-1)) = 1$. □

Exemplo 10 (OIbM1989). *Demonstrar que existe uma infinidade de pares (x, y) de números naturais tais que*

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

Solução: Completando quadrados e fatorando temos que a equação original é equivalente a

$$3(4x-3)^2-2(6y+1)^2 = 1.$$

Substituindo $z = 4x - 3$ e $w = 6y + 1$, o problema inicial se transforma em encontrar infinitas soluções da equação

$$3z^2 - 2w^2 = 1 \quad \text{com} \quad z \equiv 1 \pmod 4 \qquad \text{e} \qquad w \equiv 1 \pmod 6.$$

Para isto, consideremos a equação de Pell auxiliar $s^2 - 6t^2 = 1$, que possui solução mínima $(5, 2)$, assim todas as soluções positivas são dadas por

$$s_n + \sqrt{6}t_n = (5 + 2\sqrt{6})^n = (5 + 2\sqrt{6})(s_{n-1} + \sqrt{6}t_{n-1}),$$

ou seja,

$$s_n = 5s_{n-1} + 12t_{n-1} \qquad \text{e} \qquad t_n = 2s_{n-1} + 5t_{n-1}.$$

A partir de uma solução de $s^2 - 6t^2 = 1$ obtemos uma solução de $3z^2 - 2w^2 = 1$ da seguinte forma

$$\sqrt{3}z_n + \sqrt{2}w_n = (\sqrt{3} + \sqrt{2})(s_n + \sqrt{6}t_n),$$

ou seja,

$$z_n = s_n + 2t_n \qquad \text{e} \qquad w_n = s_n + 3t_n.$$

Assim, só nos falta mostrar que existem infinitos pares (z_n, w_n) tais que $z_n \equiv 1 \pmod 4$ e $w_n \equiv 1 \pmod 6$. Vamos provar por indução que para todo n par

$$s_n \equiv 1 \pmod{12} \qquad \text{e} \qquad t_n \equiv 0 \pmod 2$$

donde concluiremos que, para todo n par,

$$z_n \equiv 1 \pmod 4 \qquad \text{e} \qquad w_n \equiv 1 \pmod 6$$

Temos que $s_2 = 49$ e $t_2 = 20$ cumprem as condições pedidas. Agora se $n \geq 2$ é par temos, por hipótese de indução,

$$s_{n+2} \equiv 5s_{n+1} \equiv 5^2 s_n \equiv s_n \pmod{12}$$
$$t_{n+2} \equiv 5t_{n+1} \equiv 5^2 t_n \equiv t_n \pmod 2$$

o que encerra a prova. □

Problemas Propostos

Problema 11. *Demonstrar que $\lfloor (1 + \sqrt{3})^{2n-1} \rfloor$ é divisível por 2^n.*

Problema 12. *Encontrar todos os triângulos retângulos com lados inteiros tais que a diferença entre os catetos é 1.*

Problema 13. *Demonstrar que a equação $7x^2 - 13y^2 = 1$ não tem soluções inteiras.*

Problema 14. *Seja p um primo. Demonstrar que a equação $x(x+1) = p^2 y(y+1)$ não tem soluções inteiras positivas. A equação pode ter soluções inteiras?*

Problema 15. *Demonstrar que* $2x^2 - 219y^2 = -1$ *não tem soluções inteiras, mas* $2x^2 - 219y^2 \equiv -1 \pmod{m}$ *tem soluções para todo inteiro positivo* m*.*

Sugestão: *Considere a "nova solução"* $x_1 = |293x - 3066y|$, $y_1 = -28x + 293y$*.*

Problema 16. *(OBM2010) Encontre todos os pares* (a, b) *de inteiros positivos tais que*

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

Dicas e Soluções

Em breve.

Referências

[1] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.

[2] T. Nagell, *On a special class of Diophantine equation of the second degree*, Ark. Mat. 3 (1954), 51–65.

[3] H. F. Trotter, *On the norms of units in quadratic fields*, Proc. Amer Math. Soc. 22 (1969), 198–201.