Y-coordinates of solutions of Pell equations in various sequences

Florian Luca

Debrecen, February 24, 2023

Pell equations

Let d be a positive integer which is not a square. The Pell equation corresponding to d is the equation

$$X^2 - dY^2 = \pm 1 \tag{1}$$

to be solved in positive integers (X, Y).

It is known that (1) always has positive integer solutions. Letting (X_1, Y_1) be the smaller positive integer solution of it, all other solutions are of the form (X_n, Y_n) with

$$X_n + \sqrt{d}Y_n = (X_1 + \sqrt{d}Y_1)^n \quad \text{for all} \quad n \geq 1.$$

Our problem: first attempt

Let $\mathcal{U}$ be your favorite set of positive integers. What can one say about d such that the equation

$$X_n \quad \text{or} \quad Y_n \in \mathcal{U} \quad \text{for some} \quad n? \tag{2}$$

Unfortunately, if one formulates it in this way, the above problem is trivial. Namely, let $u \in \mathcal{U}$. Write

$$u^2 + 1 = dv^2,$$

for some squarefree integer d. Then

$$u^2 - dv^2 = -1,$$

so $u = X_n$ for some $n \geq 1$ corresponding to d. If $u > 1$, we can play the same game with

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

Our problem: second attempt

Since our first attempt seemed to have a trivial answer at least when the X–coordinates are concerned, we try the following potentially more interesting problem:

What can we say about d such that

$$X_n \in \mathcal{U}$$

holds for at least **two** *different values of n?*

That is, we now look for values of the squarefree integer d such that the equation

$$U^2 - dV^2 = \pm 1,$$

has two different positive integer solutions $(U, V) \neq (U', V')$ with $\{U, U'\} \subset \mathcal{U}$.
The next few slides give some examples.

When $\mathcal{U}$ are the base 10-repdigits

Take

$$\mathcal{U} := \left\{ a\left(\frac{10^m - 1}{9}\right); 1 \le a \le 9,\ m \ge 1 \right\}.$$

The elements of $\mathcal{U}$ are base 10 repdigits since

$$a\left(\frac{10^m - 1}{9}\right) = \underbrace{\overline{aa\cdots a}}_{m \text{ times}}.$$

Theorem

*(Dossavi-Yovo, L., Togbé, **2016**). Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = 1.$$

The equation $X_n \in \mathcal{U}$ has at most one solution n except:

(i) $d = 2$ *for which* $n \in \{1, 3\}$;

(ii) $d = 3$ *for which* $n \in \{1, 2\}$.

$$99^2 - 1 = (99 - 1) \times (99 + 1) = 98 \times 100 = 2 \times \square.$$

Appolinaire Dossavi-Yovo

When $\mathcal{U}$ are the Fibonacci numbers

Let $\mathcal{U}$ be the sequence of all Fibonacci numbers given by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 1$.

Theorem

*(L., Togbé, **2016**). Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = \pm 1$$

The equation $X_n \in \mathcal{U}$ has at most one solution n except for $d = 2$ in which case $n \in \{1, 2\}$.

The above result can be reformulated by saying that the only nontrivial solutions of the Diophantine equation

$$(F_n^2 \pm 1)(F_m^2 \pm 1) = \square$$

are $(n, m) = (1, 4),\ (2, 4)$.

Variations: Repdigits in an arbitrary base

Let $g \geq 2$ be an integer and

$$\mathcal{U}_g := \left\{ a \left(\frac{g^m - 1}{g - 1} \right); 1 \leq a \leq g - 1,\ m \geq 1 \right\}.$$

Members of $\mathcal{U}_g$ are called base-g-repdigits.

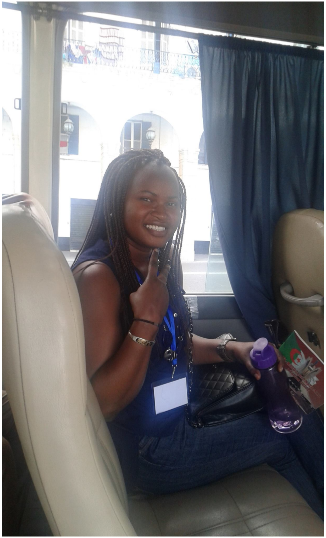
Theorem

(Faye, L. **2016***). Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = 1.$$

If $X_n \in \mathcal{U}$ has two solutions n, then

$$d < \exp\left((10g)^{10^5} \right).$$



Bernadette Faye

Variations: Repdigits in an arbitrary base, II

With the same notations as before, we have.

Theorem

(Gómez, L., Zottor, **2020***). Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = 1.$$

Assume $n_1 < n_2$ are such that

$$X_{n_i} = a_i \left(\frac{g^{m_i} - 1}{g - 1} \right), \quad 1 \le a_i \le g - 1, \quad i = 1, 2. \tag{3}$$

Then putting $B = \max\{m_1, m_2, n_1, n_2\}$ we have

$$B < 6 \times 10^{27} (\log(2g))^6.$$

Numerical corollary

Corollary

Let $g \in [2, 100]$*. All integer positive solutions of equation* (3) *have* $1 \le n_1 < n_2 \le 5$ *and* d *in the set:*

$$\{2, 3, 5, 8, 10, 15, 17, 24, 26, 35, 37, 48, 50, 63, 65, 80, 101, 120, 122, 143, 170, 195, 226, 255, 257, 325, 399, 401, 485, 528, 677, 728, 842, 1023, 1224, 1226, 1370, 1601, 1682, 1935, 2117, 3248, 3250, 3968, 4095\}.$$

We do not list the corresponding a_1, a_2, m_1, m_2 for each d, g since these are easy to obtain.

Carlos Alexis Gómez

Faith Zottor

How about for the Tribonacci sequence

Let $\mathcal{U}$ be the sequence of Tribonacci numbers given by $T_1 = T_2 = 1,\ T_3 = 2$ and $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ for all $n \geq 1$.

Theorem

(L., Montejano, Szalay, Togbé, **2016***). Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = \pm 1. \tag{4}$$

The equation $X_n = T_m$ has at most one solution (n, m) except:

(i) $(n, m) = (1, 3)$ *and* $(2, 5)$ *in the* $+$ *case* $(d = 3)$*;*

(ii) $(n, m) = (1, 1),\ (1, 2),\ (3, 5)$ *in the* $-$ *case* $(d = 2)$*.*

The ALFA team.

A general result

Up to the numerics, all of the above results follow from a theorem of Bennett and Pintér **2015**. Let us explain.

Theorem

Let $\mathbf{u} := \{u_n\}_{n\geq 0}$ *and* $\mathbf{v} := \{v_n\}_{n\geq 0}$ *be linearly recurrent sequences of integers and that the formulas*

$$u_n = P_1\alpha_1^n + \cdots + P_r\alpha_r^n \qquad v_n = Q_1\beta_1^n + \cdots + Q_s\beta_s^n$$

hold for all $n \geq 0$*. Further assume*

$$|\alpha_1| > \max\{|\alpha_2|, \ldots, |\alpha_r|\} \qquad \textit{and} \qquad |\beta_1| > \max\{|\beta_2|, \ldots, |\beta_s|\}.$$

Let

$$M := \max\{r, s, \log|\beta_1|, 3, h(P_i), h(Q_j) : 1 \leq i \leq r,\ 1 \leq j \leq s\}.$$

There exists an effectively computable constant C *such that if*

$$\log|\alpha_1| > CM^2 \log^3 M, \tag{5}$$

then there is at most one pair of positive integers (n, m) *such that* $u_n = v_m$ *and* $P_1\alpha_1^n \neq Q_1\beta_1^m$*.*

In particular, say we want $X_n = v_m$. Then putting

$$\alpha = X_1 + \sqrt{d}Y_1 \qquad and \qquad \alpha_2 = X_1 - \sqrt{d}Y_1,$$

we have

$$\frac{\alpha_1^n + \alpha_2^n}{2} = Q_1\beta_1^n + \cdots + Q_s\beta_s^n.$$

So, $P_1 = P_2 = 1/2$ and $Q_1, \ldots, Q_s$ are known. Thus, M depends only on **v**. Assuming also that $\alpha_1^n/2 \neq Q_1\beta_1^m$, we get that if α_1 is large enough (so, d is large enough), there is at most one solution (n, m) to the equation

$$X_n = v_m.$$

The condition that $\alpha_1^n/2 \neq Q_1\beta_1^m$ is easy to satisfy:

- when β_1 is an integer for example, (rep-digits, base g-repdigits, etc.).
- when β_1 is a unit but $2Q_1$ is not (the Fibonacci sequence for which $2Q_1 = 2/\sqrt{5}$, also the Tribonacci sequence, etc.).

What about computing the solutions?

In all cases, one can use two linear forms in logarithms and a clever linear combination of them. Here is at work for the example $X_n = F_m$. Say $s = 2$,

$$(\beta_1, \beta_2) = \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2} \right), \quad \alpha_1 = X_1 + \sqrt{d} Y_1.$$

Then with $\alpha_2 = \pm \alpha_1^{-1}$, the equation $X_n = F_m$ is equivalent to

$$\frac{\alpha_1^n + \alpha_2^n}{2} = \frac{\beta_1^m - \beta_2^m}{\sqrt{5}}.$$

This implies

$$n \log \alpha_1 - \log(2/\sqrt{5}) - m \log \beta_1 = O\left(\min\left\{ \frac{1}{\alpha_1^n}, \frac{1}{\beta_1^m} \right\} \right).$$

Linear forms in logs give $n \ll \log m$ and $m \ll \log \alpha_1 \log m$. Unfortunately we don't know α_1.

But say we have another such relation $X_{n'} = F_{m'}$ with $n < n'$. Then also

$$n' \log \alpha_1 - \log(2/\sqrt{5}) - m' \log \beta_1 = O\left(\min\left\{\frac{1}{\alpha_1^{n'}}, \frac{1}{\beta_1^{m'}}\right\}\right).$$

Then we do linear algebra and assuming $n < n'$, we get

$$(n'm - m'n) \log \beta_1 - (n' - n) \log(2/\sqrt{5}) = O\left(\frac{m'}{\beta_1^{m}}\right).$$

This gives $m \ll \log m'$. Since $m \gg \log \alpha_1$, we get that $\log \alpha_1 \ll \log m'$. Thus, $m' \ll (\log \alpha_1) \log m' \ll (\log m')^2$, so everything is bounded.

The proof of the result on

$$X_{n_i} = a_i \left(\frac{g^{m_i} - 1}{g - 1} \right) \qquad i = 1, 2,$$

is more technical. There the “small linear form” is

$$\left| (n_2 m_1 - n_1 m_2) \log g + n_2 \log \left(\frac{2a_1}{g-1} \right) - n_1 \left(\frac{2a_2}{g-1} \right) \right| = O\left(\frac{n_2}{g^{m_1}} \right)$$

and one has to distinguish among the cases when

$$g, \quad \frac{2a_1}{g-1}, \quad \frac{2a_2}{g-1}$$

are multiplicatively independent or not.

Anyway, this program ended up being very fruitful. The next few slides show results obtained using it.

With sums of two Fibonacci numbers

Let $2\mathcal{F} = \mathcal{F} + \mathcal{F}$ be the set of numbers which can be written as a sum of two Fibonacci numbers.

Theorem

*(C. A. Gómez Ruiz, L., **2018**). Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = \pm 1. \qquad (6)$$

The equation $X_n \in 2\mathcal{F}$ has at most one solution n except for $d \in \{2, 3, 5, 11, 30\}$.

Is it true that for every $k \geq 3$ there are only finitely many d such that $X_n \in k\mathcal{F}$ has more than one solution n? Here

$$k\mathcal{F} = \mathcal{F} + \mathcal{F} + \cdots + \mathcal{F}.$$

We have no idea. If we replace $k\mathcal{F}$ by having at most k ones in their binary expansion the answer is NO.

With products of two Fibonacci numbers

Let $\mathcal{F}^2 = \mathcal{F} \cdot \mathcal{F}$ be the sequence of numbers which are products of two Fibonacci numbers.

Theorem

*(L., Montejano, Szalay, Togbé, **2018**). Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = \pm 1. \tag{7}$$

The equation $X_n \in \mathcal{F}^2$ has at most one solution n except for $d \in \{2, 3, 5\}$.

With generalized k-Fibonacci numbers

For an integer $k \geq 2$ consider the following generalization of the Fibonacci sequence $\mathcal{F}^{(k)} = \{F_n^{(k)}\}_{n \geq -(k-2)}$ given by

$$F_n^{(k)} = F_{n-1}^{(k)} + \cdots + F_{n-k}^{(k)} \qquad n \geq 2,$$

where $F_{2-k}^{(k)} = F_{3-k}^{(k)} = \cdots = F_0^{(k)} = 0,\ F_1^{(k)} = 1$. When $k = 2,\ 3$ one obtains the Fibonacci and Tribonacci sequences, respectively.

Theorem

*(Ddamulira, L., **2018**). Let $k \geq 4$ be a fixed integer. Let $d \geq 2$ be a square-free integer. Assume that*

$$X_{n_1} = F_{m_1}^{(k)}, \qquad \text{and} \quad X_{n_2} = F_{m_2}^{(k)} \tag{8}$$

for positive integers $m_2 > m_1 \geq 2$ and $n_2 > n_1 \geq 1$, where X_n is the x–coordinate of the nth solution of the Pell equation

$$X^2 - dY^2 = \pm 1.$$

Put $\epsilon = X_1^2 - dY_1^2$. Then, either:

(i) $n_1 = 1,\ n_2 = 2,\ m_1 = (k+3)/2,\ m_2 = k+2$ *and* $\epsilon = 1$*; or*

(ii) $n_1 = 1,\ n_2 = 3,\ k = 3 \times 2^{a+1} + 3a - 5,\ m_1 = 3 \times 2^a + a - 1,\ m_2 = 9 \times 2^a + 3a - 5$ *for some positive integer a and* $\epsilon = 1$.

Explanations for the exceptions

For $k \geq 2$ one has

$$
\begin{array}{rclll}
F_n^{(k)} & = & 2^{n-2} & \text{for} & n \in [2, k+1]; \\
F_n^{(k)} & = & 2^{n-2} - (n-k)2^{n-k-3} & \text{for} & n \in [k+2, 2k+1].
\end{array}
$$

For suitable n and k it might happen that

$$F_n^{(k)} = 2^{n-2} - (n-k)2^{n-k-3} = 2x^2 - 1,\ 4x^3 - 3x$$

for some positive integer x which is necessarily a power of 2.

Mahadi Ddamulira

With factorials

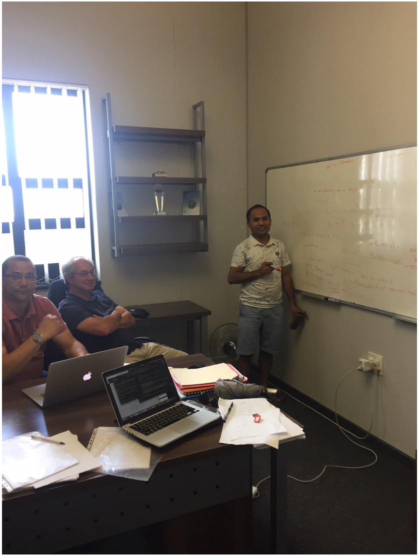
Let $\mathcal{F}act = \{m! : m \geq 1\}$.

Theorem

*(Laishram, L., Sias, **2020**). Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = \pm 1. \quad (9)$$

The equation $X_n \in \mathcal{F}act$ implies $n = 1$.



Shanta Laishram, Marc Sias

What about Y-coordinates?

What can we say about Y-coordinates of Pell equations in a sequence $\mathcal{U}$? Here the answer is different. Say $\mathcal{U}$ contains 1 and infinitely many even integers. Let $d = u^2 - 1$, where u will be determined later. Then $(X_1, Y_1) = (u, 1)$ since

$$u^2 - d \cdot 1^2 = 1.$$

Next

$$(X_2, Y_2) = (2X_1^2 - 1, 2X_1 Y_1) = (2u^2 - 1, 2u).$$

Thus, if $2u \in \mathcal{U}$ then $Y_2 \in \mathcal{U}$ and also $1 = Y_1 \in \mathcal{U}$. Hence, there are parametric families of d's such that $Y_n \in \mathcal{U}$ has two solutions n.

The Bennett–Pintér phenomenon still occurs but not always. To see why, this time

$$Y_n = \frac{\alpha_1^n - \alpha_2^n}{2\sqrt{d}}.$$

Thus, $P_1 = 1/(2\sqrt{d}),\ P_2 = -1/(2\sqrt{d})$. This gives $M \asymp \log d$. Thus, the condition

$$\log|\alpha_1| > CM^2 \log^3 M$$

becomes

$$\alpha_1 > e^{C'(\log d)^2(\log\log d)^3}$$

with some constant C'. Thus, their theorem still works for Pell equations which have a large fundamental unit (in terms of d), but it turns out the exceptions (cases when two solutions exist) correspond to d's for which the fundamental unit is not large.

The following theorems appeared in print in **2020** in joint work with B. Faye.

Theorem

*(Faye, L., **2020**). Let $\mathcal{U} = \{U_n\}_{n\geq 0}$ be any binary recurrent sequence of integers. Then the equation $Y_m \in \mathcal{U}$ has at most two positive integers solutions m provided $d > d(\mathcal{U})$, a computable constant depending on $\mathcal{U}$.*

Theorem

The equation $Y_m = 2^n - 1$ has at most two positive integer solutions (m, n).

Example

For $d = 2^{2\ell} - 1$, we have

$$(X_1, Y_1) = (2^\ell, 1) \quad \text{and} \quad (X_3, Y_3) = (2^{3\ell+2} - 3 \cdot 2^\ell, 2^{2\ell+2} - 1).$$

Some concrete examples

The case of $Y_m = 2^n - 1$ was a bit particular as we could use the properties of the 2-adic valuation of $\{Y_n\}_{n\geq 1}$. So, we decided to attack a more random example like

$$Y_n = F_m \quad \text{or} \quad Y_n = L_m,$$

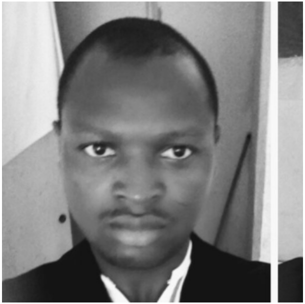
where $\{L_n\}_{n\geq 0}$ is the companion sequence of the Fibonacci numbers given by $L_0 = 2,\ L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$.

Theorem

(Edjeou, Faye, Gómez, L. **2022***). The only $d > 1$ which are not squares such that the equation $Y_n = L_m$ has at least three solutions is $d = 2$ for which $Y_1 = L_1,\ Y_2 = L_0$ and $Y_5 = L_7$.*

Theorem

(L., Zottor **2022***). The only $d > 1$ which are not squares such that the equation $Y_n = Y_m$ has at least three solutions is $d = 2$ for which $Y_1 = F_1 = F_2,\ Y_2 = F_3$ and $Y_3 = F_5$.*



Bilizimbéyé Edjeou

Main steps

The **NYJM** paper is very general. Given any binary recurrent sequence $\mathbf{v} = (v_n)_{n\geq 0}$ it outlines a program to decide whether $Y_n = v_m$ has three solutions.

Let us look at $Y_n = L_m$ having 3 solutions. Assume they are

$$(m_1, n_1), \qquad (m_2, n_2), \qquad (m_3, n_3)$$

with $m_1 < m_2 < m_3$. Then

$$\frac{\alpha_1^m - \alpha_2^m}{2\sqrt{d}} = \beta_1^n + \beta_2^n \qquad (m, n) = (m_i, n_i), \quad i = 1, 2, 3.$$

This implies

$$m \log \alpha_1 - n \log \beta_1 - \log(2\sqrt{d}) = O\left(\max\left\{\frac{\sqrt{d}}{\alpha_1^m}, \frac{1}{\beta_1^n}\right\}\right).$$

We want to apply Matveev but what if the left–hand side is zero?

In this case we get

$$\alpha_1^{2m}/\beta_1^{2n} = 4d^2 \in \mathbb{Q}(\beta),$$

which shows that α_1 is a unit in $\mathbb{Q}(\beta_1) = \mathbb{Q}(\sqrt{5})$. This shows that $d = 5u^2$, and letting

$$\alpha_1 = X_1 + \sqrt{5u^2}\,Y_1$$

be such that $U_1^2 - d_1 V_1^2 = \pm 1$, we get that $Y_1 = F_k/(2u)$, where k is minimal such that $2u \mid F_k$. Thus, $Y_m = F_{km}/(2u)$. Asking of this to be a Lucas number for three m's amounts to representing $2u$ as a ratio between a Fibonacci and Lucas number in three different ways and we get an easy contradiction for large u by the Primitive Divisor Theorem for Fibonacci and Lucas numbers.

From now on the linear form is not zero so using Matveev, we get

$$\max\{m, n\} < 8 \cdot 10^{15} (\log \alpha_1)^3.$$

Unfortunately we don't know either $\log \alpha_1$ or $(2\sqrt{d})$. This is similar to the small linear form for the problem $X_m = F_n$, except that we have the additional $\log(2\sqrt{d})$ which we don't know. But we have three such solutions instead of just two.

So, we write

$$m \log \alpha_1 - n \log \beta_1 - \log(2\sqrt{d}) = O\left(\max\left\{\frac{\sqrt{d}}{\alpha_1^m}, \frac{1}{\beta_1^n}\right\}\right)$$

for $(m, n) = (m_i, n_i),\ i = 1, 2, 3$ and distinguishing whether the rank of the matrix

$$\begin{pmatrix} m_1 & n_1 & 1 \\ m_2 & n_2 & 1 \\ m_3 & n_3 & 1 \end{pmatrix}$$

is $1,\ 2,\ 3$, we get in all cases that

$$n_1 < 42.25 + 2.08 \log \log \alpha_1.$$

When $m_1 \geq 2$, we get immediately that $\log \alpha_1 \ll \log \log \alpha_1$, which gives $\alpha_1 < 10^{11}$ and we find the solutions. So, it remains to deal with $m_1 = 1$.

To get a general bound on α_1 we may play with the above inequalities getting

$$|(m_3-1)n_2-(m_2-1)n_3)\log\beta_1+(m_3-m_2)\log L_{n_1}|=O\left(\frac{m_3}{\alpha_1^2}\right).$$

In the above,

$$\begin{aligned} n_1 &= O(h(L_{n_1}))=O(\log\log\alpha_1); \\ m_3 &= O(\log\alpha_1). \end{aligned}$$

A linear form in 2-logs in the left gives

$$\log\alpha_1=O((\log\log\alpha_1)^2),$$

which bounds α_1. A lot of work is needed to lower it. Some ingredients are computations with continued fractions (Legendre and Worley's theorem), and a sharpening of Matveev's bounds due to Mignotte.

THANK YOU!