Diophantine Equations and Linear Recurrences

Mahadi Ddamulira

Institute of Analysis and Number Theory

Graz University of Technology

Ph.D. Thesis Defense

Supervisors: Robert TICHY and Florian LUCA (Johannesburg)

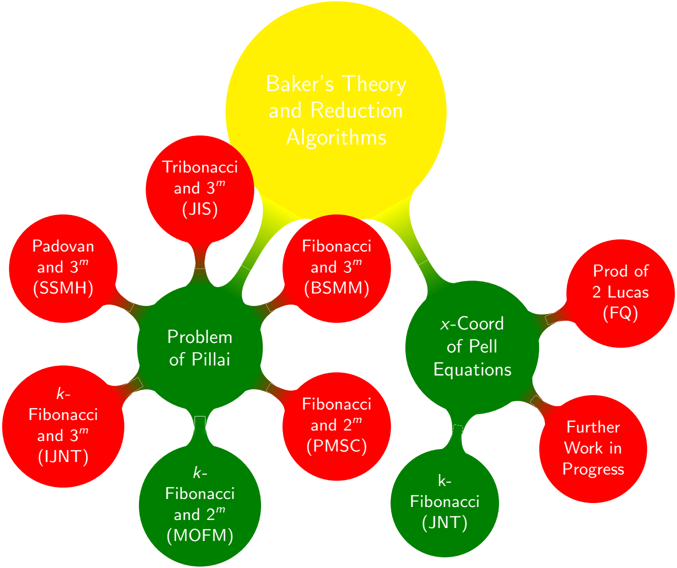
DOCTORAL PROGRAM
DISCRETE MATHEMATICS

TU & KFU GRAZ • MU LEOBEN
AUSTRIA

Der Wissenschaftsfonds.

Graz, 5 June 2020

Overview of Our Work



Outline

Problem of Pillai

Pillai's problem

- Pillai's problem asks to prove that, for any positive integer c, there exist finitely many positive integers $a,\ b,\ x,\ y$ with $\min\{x,y\} \geq 2$ such that

$$a^x - b^y = c. \tag{1}$$

- It was conjectured by Pillai in 1936, and proved by Stroecker and Tijdeman in 1982, that the only integers c admitting at least two representations of the form $2^x - 3^y$ are

$$\begin{aligned} &2^3 - 3^2 = 2^1 - 3^1 = -1; \quad 2^5 - 3^3 = 2^3 - 3^1 = 5; \\ &2^8 - 3^5 = 2^4 - 3^1 = 13. \end{aligned} \tag{2}$$

- While many other cases have been studied – including the famous case $c = 1$ (Catalan's problem), resolved by Mihăilescu in 2006 – Pillai's problem remains open in general.

k–generalized Fibonacci numbers

- For an integer $k \geq 2$, the k–generalized Fibonacci sequence is defined by the recurrence relation

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

with the initial conditions

$$F_{-(k-2)}^{(k)} = F_{-(k-3)}^{(k)} = \cdots = F_0^{(k)} = 0, \quad F_1^{(k)} = 1.$$

- The case $k = 2$ recovers the classical Fibonacci sequence, the case $k = 3$ recovers the Tribonacci sequence, etc.
- The generalized Fibonacci analogue of Pillai's problem is concerned with the study, for any fixed positive integers k, ℓ, c, of the solutions in positive integers n, m, to the equation

$$F_n^{(k)} - F_m^{(\ell)} = c. \tag{3}$$

Recent results I

Particular cases have been studied: $(n, m) \neq (n_1, m_1)$.

- D.–Luca–Rakotomalala (2017)

$$F_n - 2^m = F_{n_1} - 2^{m_1} = c; \quad c \in \{-30, -11, -3, 0, 1, 5, 85\}.$$

- Bravo–Luca–Yazán (2017)

$$T_n - 2^m = T_{n_1} - 2^{m_1} = c; \quad c \in \{-8, -3, -1, 0, 5\}.$$

- Chim–Pink–Ziegler (2017)

$$F_n - T_m = F_{n_1} - T_{m_1} = c; \quad c \in$$

$$\{-271, -60, -41, -23, -22, -11, -10, -5, -3, -2, -1, 0, 1, 4, 6, 8, 11\}.$$

Recent results II

- D. (2019)

$$F_n - 3^m = F_{n_1} - 3^{m_1} = c; \quad c \in \{-26, -6, -1, 0, 2, 4, 7, 12\}.$$

- D. (2019)

$$T_n - 3^m = T_{n_1} - 3^{m_1} = c; \quad c \in \{-2, 0, 1, 4\}.$$

- D. (2019)

$$P_n - 3^m = P_{n_1} - 3^{m_1} = c; \quad c \in \{-6, 0, 1, 22, 87\}.$$

  $\{P_n\}_{n\geq 0}$ – Padovan sequence given by $P_0 = 0$, $P_1 = 1 = P_2$, and $P_{n+3} = P_{n+1} + P_n$ for all $n \geq 0$.

- Similar problems have been solved by several other authors ...

Main results I

- D.–Gómez–Luca (2018)

Assume that $k \geq 4$. Then, the Diophantine equation $F_n^{(k)} - 2^m = F_{n_1}^{(k)} - 2^{m_1} = c$ with $n > n_1 \geq 2$, $m > m_1 \geq 0$ has the following families of solutions (c, n, m, n_1, m_1).

(i) In the range $2 \leq n_1 < n \leq k+1$, we have the following solution:

$$(0, s, s-2, t, t-2) \qquad \text{for} \qquad 2 \leq t < s \leq k+1.$$

(ii) In the ranges $2 \leq n_1 \leq k+1$ and $k+2 \leq n \leq 2k+2$, we have the following solutions:

(*a*) when $n_1 = n-1$:

$$\left(2^{k-1} - 1, k+2, k-1, k+1, 0\right)$$

Main results II

(b) when $n_1 < n - 1$:

$$\left(2^\gamma - 2^\rho, k + 2^a - 2^b, k + 2^a - 2^b - 2, \gamma + 2, \rho\right),$$

with $\gamma = b - 3 + 2^a - 2^b$ and $\rho = a - 3 + 2^a - 2^b$, where $a > b \geq 0$, $(a, b) \neq (1, 0)$ and $\gamma + 3 \leq k + 2$.

(iii) In the range $k + 2 \leq n_1 < n \leq 2k + 2$, we have the following solutions: if the integer a is maximal such that $2^a \leq k + 2$ satisfies $a + 2^a = k + 1 + 2^b$ for some positive integer b, then

$$(-2^{a+2^a-3}, k + 2^a, k + 2^a - 2, k + 2^b, b + 2^b - 3).$$

(iv) If $n = 2k + 3$, and additionally $k = 2^t - 3$ for some integer $t \geq 3$, then:

$$(1 - 2^{t+2^t-3}, 2^{t+1} - 3, 2^{t+1} - 5, 2, t + 2^t - 3).$$

The equation has no solutions with $n > 2k + 3$.

Main results III

Theorem (D.–Luca, 2020)

Let $k \geq 4$ be fixed. Then, $F_n^{(k)} - 3^m = F_{n_1}^{(k)} - 3^{m_1} = c$, with $n > n_1 \geq 2$ and $m > m_1 \geq 1$ has solutions with

(i) $c \in \{-1, 5, 13\}$ *and* $2 \leq n \leq k+1$ *as follows: (cf. Pillai 1936)*

$$\begin{aligned} F_5^{(k)} - 3^2 = F_3^{(k)} - 3^1 &= -1, \quad k \geq 4, \\ F_7^{(k)} - 3^3 = F_5^{(k)} - 3^1 &= 5, \quad k \geq 6, \\ F_{10}^{(k)} - 3^5 = F_6^{(k)} - 3^1 &= 13, \quad k \geq 9; \end{aligned}$$

(ii) $c \in \{-25, -7, 5\}$ *and* $n \geq k+2$ *and* $k \in \{4, 5, 6\}$ *as follows:*

$$\begin{aligned} F_8^{(4)} - 3^4 &= F_3^{(4)} - 3^3 = -25, \\ F_{10}^{(5)} - 3^5 &= F_3^{(5)} - 3^2 = -7, \\ F_{10}^{(6)} - 3^5 &= F_6^{(6)} - 3^1 = 5. \end{aligned}$$

x-Coordinates of Pell Equations

Pell Equations

- Let $d \geq 2$ be a positive integer which is not a perfect square. It is well known that the Pell equation

$$x^2 - dy^2 = \pm 1 \tag{4}$$

has infinitely many positive integer solutions (x, y).

- By putting (x_1, y_1) for the smallest such solution, all solutions are of the form (x_n, y_n) for some positive integer n, where

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \qquad \text{for all} \quad n \geq 1. \tag{5}$$

- Furthermore, the sequence $\{x_n\}_{n\geq 1}$ is binary recurrent. The following formula

$$x_n = \frac{(x_1 + y_1\sqrt{d})^n + (x_1 - y_1\sqrt{d})^n}{2}, \tag{6}$$

holds for all positive integers n.

Some recent results

- Luca–Togbé (2018)

$$x_n = F_m \tag{7}$$

  Eq. (7) has at most one solution in positive integers except for $d = 2$ with $(n, m) = (1, 1), (1, 2), (2, 4)$.

- Luca–Montejano–Szalay–Togbé (2017)

$$x_n = T_m \tag{8}$$

  Eq. (8) has at most one solution in positive integers except for:
  $d = 2$ with $(n, m) = (1, 1), (1, 2), (3, 5)$, and
  $d = 3$ with $(n, m) = (1, 3), (2, 5)$.

Main results I

Put $\epsilon := x_1^2 - dy_1^2$. Note that $dy_1^2 = x_1^2 - \epsilon$, so the pair (x_1, ϵ) determines d and y_1.

Theorem (D.–Luca, 2020)

Let $k \geq 4$ be a fixed integer. Let $d \geq 2$ be a square-free integer. Assume that

$$x_{n_1} = F_{m_1}^{(k)}, \qquad \text{and} \quad x_{n_2} = F_{m_2}^{(k)} \tag{9}$$

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 (4). 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* $\epsilon = 1$.

Main results II

$\{L_n\}_{n\geq 0}$ – sequence of Lucas numbers given by $L_0 = 2,\ L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$.
Consider the Diophantine equation

$$x_k = L_n L_m, \tag{10}$$

in nonnegative integers (k, n, m) with $k \geq 1$ and $0 \leq m \leq n$.

Theorem (D., 2020)

For each square-free integer $d \geq 2$, there is at most one integer k such that the equation (10) holds, except for $d \in \{2, 3, 5, 15, 17, 35\}$ for which $x_1 = 1,\ x_2 = 3, x_3 = 7, x_9 = 1393$ (for $d = 2$), $x_1 = 2,\ x_2 = 7$ (for $d = 3$), $x_1 = 2,\ x_2 = 9$ (for $d = 5$), $x_1 = 4,\ x_5 = 15124$ (for $d = 15$), $x_1 = 4,\ x_2 = 33$ (for $d = 17$), and $x_1 = 6,\ x_3 = 846$ (for $d = 35$).

Baker's Methods

Effective bounds I

Let η be an algebraic number of degree d with minimal primitive polynomial over the integers

$$a_0x^d + a_1x^{d-1} + \cdots + a_d = a_0 \prod_{i=1}^{d}(x - \eta^{(i)}),$$

where the leading coefficient a_0 is positive and the $\eta^{(i)}$'s are the conjugates of η. Then the *logarithmic height* of η is given by

$$h(\eta) := \frac{1}{d}\left(\log a_0 + \sum_{i=1}^{d} \log\left(\max\{|\eta^{(i)}|, 1\}\right)\right).$$

Useful properties of the logarithmic height function $h(\cdot)$:

$$h(\eta_1 \pm \eta_2) \leq h(\eta_1) + h(\eta_2) + \log 2,$$
$$h(\eta_1\eta_2^{\pm 1}) \leq h(\eta_1) + h(\eta_2),$$
$$h(\eta^s) = |s|h(\eta) \qquad (s \in \mathbb{Z}).$$

Effective bounds II

Theorem (Matveev according to Bugeaud, Mignotte, Siksek)

Let $\eta_1, \ldots, \eta_t$ *be positive real numbers in a number field* $\mathbb{K}$ *of degree* D*, let* $b_1, \ldots, b_t$ *be nonzero integers, and assume that* $\Lambda := \eta_1^{b_1} \cdots \eta_t^{b_t} - 1$*, is nonzero. Then*

$$\log|\Lambda| > -1.4 \times 30^{t+3} \times t^{4.5} \times D^2(1 + \log D)(1 + \log B)A_1 \cdots A_t,$$

where

$$B \geq \max\{|b_1|, \ldots, |b_t|\},$$

and

$$A_i \geq \max\{Dh(\eta_i), |\log \eta_i|, 0.16\}, \qquad \text{for all} \qquad i = 1, \ldots, t.$$

Effective bounds III

For $t = 2$ and η_1, η_2 are positive and multiplicatively independent. Let in this case $B_1,\ B_2$ be real numbers larger than 1 such that

$$\log B_i \geq \max\left\{h(\eta_i), \frac{|\log \eta_i|}{D}, \frac{1}{D}\right\}, \qquad \text{for} \quad i = 1, 2.$$

Put $b' := \dfrac{|b_1|}{D \log B_2} + \dfrac{|b_2|}{D \log B_1}$ and $\Gamma := b_1 \log \eta_1 + b_2 \log \eta_2$.
$\Gamma \neq 0$ because η_1 and η_2 are multiplicatively independent.

Theorem (Laurent, Mignotte, Nesterenko)

With the above notations, assuming that η_1, η_2 are positive and multiplicatively independent, then

$$\log|\Gamma| > -24.34 D^4 \left(\max\left\{\log b' + 0.14, \frac{21}{D}, \frac{1}{2}\right\}\right)^2 \log B_1 \log B_2.$$

Reduction Procedure

Diophantine approximation

Homogeneous linear form in two $\mathbb{Z}$-variables: Classical result in the theory of Diophantine approximation.

Lemma (Legendre)

Let τ be an irrational number, $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$ be all the convergents of the continued fraction of τ, and M be a positive integer. Let N be a nonnegative integer such that $q_N > M$. Then, putting $a(M) := \max\{a_i : i = 0, 1, 2, \ldots, N\}$, the inequality

$$\left|\tau - \frac{r}{s}\right| > \frac{1}{(a(M)+2)s^2},$$

holds for all pairs (r, s) of positive integers with $0 < s < M$.

Baker-Davenport

Nonhomogeneous linear form in two $\mathbb{Z}$-variables: Baker-Davenport!

Lemma (Dujella, Pethő)

Let M be a positive integer, $\frac{p}{q}$ be a convergent of the continued fraction of the irrational number τ such that $q > 6M$, and A, B, μ be some real numbers with $A > 0$ and $B > 1$. Furthermore, let $\varepsilon = \|\mu q\| - M\|\tau q\|$. If $\varepsilon > 0$, then there is no solution to the inequality

$$0 < |u\tau - v + \mu| < AB^{-w},$$

in positive integers u, v, and w with

$$u \leq M \quad \text{and} \quad w \geq \frac{\log(Aq/\varepsilon)}{\log B}.$$

LLL algorithm

Lemma (LLL Algorithm)

Let $X_1, X_2, \ldots, X_t$ be positive integers such that $X := \max\{X_i\}$ and $C > (tX)^t$ is a fixed sufficiently large constant. Let Ω be a lattice, we consider a reduced base $\{\mathbf{b}_i\}$ to Ω and its associated Gram-Schmidt orthogonalization base $\{\mathbf{b}_i^*\}$. We set

$$c_1 = \max_{1 \le i \le t} \frac{||\mathbf{b}_1||}{||\mathbf{b}_i^*||}, \ \theta = \frac{||\mathbf{b}_1||}{c_1}, \quad Q = \sum_{i=1}^{t-1} X_i^2, \ \& \ R = \frac{1}{2}\left(1 + \sum_{i=1}^{t} X_i\right).$$

If the integers x_i are such that $|x_i| \le X_i$, for $1 \le i \le t$ and $\theta^2 \ge Q + R^2$, then we have

$$\left|\sum_{i=1}^{t} x_i \tau_i\right| \ge \frac{\sqrt{\theta^2 - Q} - R}{C}.$$

Illustration of the proofs

Techniques for the proofs I [Theorem 1, D.–Luca(2020)]

$$F_n^{(k)} - 3^m = F_{n_1}^{(k)} - 3^{m_1} \ (= c). \tag{11}$$

- Assume $(n, m) \neq (n_1, m_1)$. If $m = m_1$, then $F_n^{(k)} = F_{n_1}^{(k)}$. Since $\min\{n, n_1\} \geq 2$, then $n = n_1$. So, $(n, m) = (n_1, m_1)$, a contradiction! Thus, assume $n > n_1 \geq 2$, then $m > m_1 \geq 1$.
- Assume $2 \leq n_1 < n \leq k+1$, then $F_{n_1}^{(k)} = 2^{n_1-2}$ and $F_n^{(k)} = 2^{n-2}$. $\Rightarrow \quad 2^{n-2} - 3^m = 2^{n_1-2} - 3^{m_1} = c$ (cf. Classical Pillai).
- Assume $n \geq k+2$. Claim: $F_n^{(k)} - 3^m = F_{n_1}^{(k)} - 3^{m_1}$ and $2^{n-2} - 3^m = 2^{n_1-2} - 3^{m_1}$ can not simultaneously hold. Idea: $2^{n-2} - F_n^{(k)} = 2^{n_1-2} - F_{n_1}^{(k)}$. Sequence $\{2^{n-2} - F_n^{(k)}\}_{n\geq 2}$ is 0 at $2 \leq n \leq k+1$, 1 at $n = k+2$, and increasing for $n > k+2$.
- Using $|F_n^{(k)} - \frac{\alpha-1}{2+(k+1)(\alpha-2)}\alpha^{n-1}| < 1/2$ and $\alpha^{n-2} \leq F_n^{(k)} \leq \alpha^{n-1}$, we successively apply Matveev's theorem on (11) to bound m, n polynomially in k. That is, $m \leq n < 4 \times 10^{42} k^{11} (\log k)^7$.

Techniques for the proofs II [Theorem 1, D.–Luca(2020)]

- The cutoff k. Asuume $n < 4 \times 10^{42} k^{11} (\log k)^7 < k^{k/2}$. Thus, $k > 600$. Two cases. The case of small k, $4 \leq k \leq 600$ and the case of large k, $k > 600$.
- For $4 \leq k \leq 600$. Very large bounds on n. We do Baker-Davenport! This reduces the bounds to $m \leq n \leq 500$.
  With the help of Mathematica, we intersect the sets

$$F_{n,k} := \left\{ F_n^{(k)} - F_{n_1}^{(k)} \pmod{10^{20}} : n \in [3, 600], n_1 \in [2, n-1] \right\},$$
$$D_{n,k} := \left\{ 3^m - 3^{m_1} \pmod{10^{20}} : m \in [2, 600], m_1 \in [1, m-1] \right\}.$$

  We get only the solutions listed in Theorem 1.
- For $k > 600$. Using $F_n^{(k)} = 2^{n-2}(1+\zeta)$, $|\zeta| < 5/2^{k/2}$, we again apply Matveev, Legendre criterion, and Baker-Davenport! The bounds obtained on k, n, m lead to the case of small k. □

End

Thank You!