DIOPHANTINE EQUATIONS OF THE PILLAI TYPE: EXTENSIONS & APPLICATIONS

Catalan problem: $a^x - b^y = 1$

$3^2 - 2^3 = 1$ is the only solution with $a, b, x, y \in \mathbb{N}\setminus\{1\}$

[Mihailescu 2004]

Pillai problem: (P) $a^x - b^y = c$ $(c \in \mathbb{N})$

[widely open in general]

Partial results:

(i) abc-conjecture $\Rightarrow$ (P) has only finitely many solutions

(ii) $3^x - 2^y = c$ has at most 1 solution

[Stroeker - Tijdeman]

(iii) $a^x - b^y = c$ $(a, b, c$ fixed$)$ has at most 2 solutions

[Bennett 2001]

(iv) Extensions to diophantine equations in finitely generated domains

[Evertse, Győry, Koymans]

DIOPHANTINE EQUATIONS INVOLVING LINEAR RECURRENCES

$a^x \rightsquigarrow U_n \qquad b^y \rightsquigarrow V_m$

U_n, V_m l.r.s. of order k

$$G_n = a_1 G_{n-1} + \dots + a_k G_{n-k}$$

$x^k - a_1 x^{k-1} - \quad - a_k$ char. Pol. with integer coeff.

dominating characteristic root α :

$$\underset{\alpha_1}{\overset{\|}{|\alpha|}} > |\alpha_2| \geq \dots \geq |\alpha_k|$$

Problem PR $\quad U_n - V_m = c$

There exists a finite (and effectively computable) set $\mathcal{C}$ such that PR has at least 2 solutions (n, m) if and only if $c \in \mathcal{C}$.

[Chim - Pink - Ziegler]

Survey Lecture summer 2022 :

discussion of many special cases

e.g. $U_n =$ Fibonacci numbers, Tribonacci

$V_m = 2^m, 3^m$

RECURRENCES AND POWER SEQUENCES

U_n ... binary linear r. s.

$U_n - p_1^{x_1} \cdots p_s^{x_s} = c$ (p_i ... prime numbers)

has at most s solutions for $c > C^+$
(effect. comp.)

has at most $s+1$ solutions for $c < C^-$

[Ziegler, Debrecen 2022]

$U_n = a\alpha^n + a_2\alpha_2^n + \ldots a_k\alpha_k^n$ ($\alpha > 1$ irrational dominant root)

$a > 0$; a, α mult. independent

and <u>techn. cond:</u> $\alpha^z - 1 = a^x \alpha^y$ has no solutions
$z \in \mathbb{N}$; $x, y \in \mathbb{Q}$; $-1 < x < 0$

Then $U_n - b^m = c$ has at most 2
solutions (n, m) for $b > B$, $n > N_0$
(effect. computable)

[Heintze, Ti, Vukusic, Ziegler]

<u>Remarks</u>
- techn. cond. can be algorithm. checked for any given recurrence (U_n)
- without techn. cond. at most 3 solutions

Several Examples and Problems

- U_n Fibonacci sequence

  U_n Tribonacci sequence $U_{n+3} = U_{n+2} + U_{n+1} + U_n$

  $U_{n+2} = U_{n+1} + 3U_n \qquad (U_0 = 0,\ U_1 = 1)$

- In the Tribonacci case we found the following pairs (b,c) with 2 solutions:

  $(2,-8), (2,-3), (2,-1), (2,0), (2,5)$
  $(3,-2), (3,4), (5,-121), (5,-1), (5,19)$
  $(7,-5), (17,-15), (54,220), (641,-137)$

  Are there further pairs (b,c) such that there are at least 2 solutions? Are there cases with at least 3 solutions?

Tools for the proofs

- Linear forms in logarithms [Mateer, Laurent]
- Algebraic computations
- LLL - reduction

PILLAI'S DENSITY PROBLEM

PILLAI'S CONJECTURE: For given $c \in \mathbb{N}$, the equation (P) $a^n - b^m = c$ has at most 1 solution (a, b, n, m) in integers ≥ 2.

PILLAI'S THEOREM: For fixed a, b there is $c_0 = c_0(a,b)$ such that $\forall c > c_0$ the equation (P) has at most 1 solution and furthermore

$$\#\{c \in [1, x] : c = a^n - b^m \text{ for some } n, m \in \mathbb{N}\} \sim$$

$$\sim \frac{(\log x)^2}{2 \log a \cdot \log b} \qquad (x \to \infty)$$

LINEAR RECURRENCES U_n, V_m with dominating roots α, β (resp.) replacing powers a^n, b^m.

Assuming α, β multiplicatively independent:

$$\#\{c \in [-x, x] : c = U_n - V_m \text{ for some } n, m \in \mathbb{N}\} \sim$$

$$\sim \#\{(n,m) \in \mathbb{N}^2 : |U_n - V_m| \leq x\} \sim$$

$$\sim \frac{(\log x)^2}{\log |\alpha| \log |\beta|} \qquad (\text{as } x \to \infty)$$

[Ti - Vukusic - Yang - Ziegler]

EQUIVALENT RESULT for multiplicatively independent algebraic numbers, $|\alpha|, |\beta| > 1$

$$T_{\alpha,\beta}(x) = \# \{ (n,m) \in \mathbb{N}^2 : \ |\alpha^n - \beta^m| \leq x \} \sim \frac{(\log x)^2}{\log|\alpha| \cdot \log|\beta|}$$

QUESTION: α, β transcendental ?

COUNTEREXAMPLE : $c = \sum_{i=0}^{\infty} 10^{-a(i)}$ with $a(0) = 1$, $a(i+1) = 10^{a(i)}$

extremely well approximable Liouville number

$$\beta = 2, \ \alpha = 2^c \implies \frac{\log \alpha}{\log \beta} = c \notin \overline{\mathbb{Q}}$$

and $|\alpha^n - \beta^m| \leq 1$ has infinitely many solutions $(n,m) \in \mathbb{N}^2$.

METRIC RESULT for Lebesgue almost all (α, β) in $\mathbb{C}^2$ with $|\alpha|, |\beta| > 1$:

$$T_{\alpha,\beta}(x) \sim \frac{(\log x)^2}{\log|\alpha| \cdot |\log \beta|} \qquad (x \to \infty)$$

with remainder terms

$$\mathcal{O}\left(\log x \, (\log \log x)^2 \right) \quad \text{(above)}$$

$$\mathcal{O}\left(\log x \, (\log \log x) \right) \quad \text{(below)}$$

SPECIAL CASES:

(1) $\alpha, \gamma \in \overline{\mathbb{Q}}$, $|\alpha| > 1$, $\gamma > 0$ real, $\beta = e^{\gamma}$

Then
$$T_{\alpha,\beta}(x) \sim \frac{(\log x)^2}{\gamma \log|\alpha|} \qquad (x \to \infty)$$

(2) $\gamma_1, \gamma_2 > 0$ real algebraic and $\mathbb{Q}$-lin. indep.
$\alpha = e^{\gamma_1}$, $\beta = e^{\gamma_2}$.

Then
$$T_{\alpha,\beta}(x) \sim \frac{(\log x)^2}{\gamma_1 \cdot \gamma_2} \qquad (x \to \infty)$$

with remainder terms as above, O-constants are effective.

TOOL FOR PROOF: Waldschmidt's inhomogeneous linear form theorem

WALDSCHMIDT'S THEOREM

Let $\gamma_1, \dots, \gamma_t \in \bar{\mathbb{Q}} \setminus \{0\}$ and let $\log \gamma_1, \dots, \log \gamma_t$ be $\mathbb{Q}$-lin. indep and let $\beta_0, \beta_1, \dots, \beta_t \in \bar{\mathbb{Q}}$, not all $= 0$. Then

$$\log |\beta_0 + \beta_1 \log \gamma_1 + \dots + \beta_t \log \gamma_t| \geq$$

$$\geq -2^{t+25}\, t^{3t+9} (1 + \log k) \log B \, k^{t+2} \log A_1 \cdot \ldots \cdot \log A_t ,$$

where k is degree of $\mathbb{Q}(\gamma_1, \dots, \gamma_t, \beta_0, \dots, \beta_t)$ over $\mathbb{Q}$

and
$$\log A_i \geq \max \left\{ h(\gamma_i), \frac{e}{k} |\log \gamma_i|, \frac{1}{k} \right\}$$

$$B \geq \max \left\{ k+1, \max_i k \log A_i, \max_i e^{h(\beta_i)} \right\}$$

logarithmic height
$$h(\eta) = \frac{1}{k} \left(\log |a_0| + \sum_{i=1}^{k} \log \left(\max \{ |\eta^{(i)}|, 1 \} \right) \right)$$

$\eta^{(i)}$ conjugates of algebraic number η

PILLAI - TIJDEMAN EQUATION

$$A x^m + B y^m = C x^n + D y^n$$ with $A \cdot B \neq 0$, $|x| \neq |y|$, $0 \leq n < m$, $Ax^m \neq Cx^n$

$\Longrightarrow$ $m \leq E$ (effectively computable)

[Shorey - Tijdeman]

LUCAS SEQUENCES $(U_n)_{n \geq 0}$, $U_0 = 0$, $U_1 = 1$

$$U_{n+2} = r U_{n+1} + U_n \qquad (r \in \mathbb{N})$$

special case $r = 1$ Fibonacci sequence

$$A U_n + B U_m = C U_{n_1} + D U_{m_1}$$ with $A B \neq 0$, $n > m \geq 0$, $n_1 > m_1 \geq 0$, $AU_n \neq C U_{n_1}$

Then $r < 14 \max\{|A|, |B|, |C|, |D|\}$

[Ddamulira - Luca - Ti]

Proof based on elementary algebraic computations and the following properties of Lucas numbers:

- $\gcd(U_n, U_m) = U_{\gcd(n,m)}$
- $\alpha^{n-2} \leq U_n \leq \alpha^{n-1}$
- $\alpha \geq \phi = \frac{\sqrt{5}+1}{2}$

complete solution possible for small values of r

BINOMIAL POLYNOMIALS

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!} \in \mathbb{Q}[x] \qquad (n \geq 1)$$

are integer-valued, i.e elements of

$$\operatorname{Int} \mathbb{Z} = \{ f \in \mathbb{Q}[x] : f(\mathbb{Z}) \subseteq \mathbb{Z} \}.$$

$\binom{x}{n}$ is irreducible in the commutative ring $\operatorname{Int}\mathbb{Z}$, i.e. $a = bc$ implies that b or c is a unit. An element a in a domain D is called <u>absolutely</u> <u>irreducible</u> if a^m factors uniquely into irreducible elements ($\forall m \in \mathbb{N}$).

(•) $\binom{x}{p}$ is absolutely irreducible (abs-irr) $\forall p$ prime number

[Frisch – Nakato via a graph-theoretic criterion]

(•) $\binom{x}{n}$ is abs-irr $\forall n \in \mathbb{N}$

[Rissner – Windisch via diophantine number theory
J. Algebra 2021]

(•) Assume that for $n > 10$ the k consecutive numbers $n, (n-1), \ldots, n-k+1$ are composite, then one of these numbers has a prime factor $p > 2k$.

BASIC FACTS

(i) $\binom{x}{1} = x$ is abs-irr

(ii) The property

$$\binom{x}{n}^m = f\cdot g \Rightarrow f = \pm \binom{x}{n}^k, \; g = \pm \binom{x}{n}^l$$

implies that $\binom{x}{n}$ is abs-irr.

(iii) Let $n, m \geq 2$; $f, g \in \mathrm{Int}\,\mathbb{Z}$ with $\binom{x}{n}^m = f\cdot g$.

Then for $0 \leq i \leq n-1$ there exist k_i, l_i with $k_i + l_i = m$ and

$$f = \pm \prod_{i=0}^{n-1} \left(\frac{x-i}{n-i}\right)^{k_i} ; \; g = \pm \prod_{i=0}^{n-1} \left(\frac{x-i}{n-i}\right)^{l_i}$$

holds.

[Newton interpolation polynomials]

(iv)

$$\nu_p(f(s)) = \sum_{j=0}^{n-1} (\nu_p(s-j) - \nu_p(n-j))\, k_j \geq 0$$

$$\nu_p(g(s)) = \sum_{j=0}^{n-1} (\nu_p(s-j) - \nu_p(n-j))\, l_j \geq 0$$

for all $s \in \mathbb{Z}$ and p prime, where $\nu_p(w)$ denotes the p-adic valuation of $w \in \mathbb{Q}$.

VALUATION MATRIX

For $n \in \mathbb{N}$ some notation:

$\mathcal{P}_n = \{p : 0 < p \leq n, \ p \text{ prime}\}$

For $p \in \mathcal{P}_n$ let $0 \leq r_{n,p} < p$ be the uniquely determined integer such that $n \equiv r_{n,p} \mod p$.

$$\mathcal{R}_{n,p} = \begin{cases} \{1,2\} & \text{if } n = 2^s \text{ with } s > 1, \ p = 2 \\ \{1,2,3,4\} & \text{if } n = 9 \text{ and } p = 3 \\ \{r : 1 \leq r \leq p - r_{n,p} - 1\} & \text{else} \end{cases}$$

<u>Valuation</u> <u>Matrix</u>

$$A_n = \left(\nu_p(n+r-j) - \nu_p(n-j)\right)_{\substack{p \in \mathcal{P}_n, r \in \mathcal{R}_{n,p} \text{ rows} \\ 0 \leq j \leq n-1 \text{ columns}}}$$

(•) row sums $\displaystyle\sum_{j=0}^{n-1} \left(\nu_p(n+r-j) - \nu_p(n-j)\right) = 0$

$\Rightarrow$ rank $A_n < n$.

<u>Key</u> <u>Proposition</u>

$$\text{rank } A_n = n-1 \Rightarrow \binom{x}{n} \text{ is abs-irr.}$$

ANALYSIS OF THE BLOCK STRUCTURE

p-block $B_{n,p}$ is $|\mathcal{R}_{n,p}| \times n$ matrix

$$B_{n,p} = \left(\nu_p(n+r-j) - \nu_p(n-j) \right)_{\substack{r \in \mathcal{R}_{n,p} \\ 0 \le j \le n-1}}$$

investigation of leftmost p and rightmost $p-1$ columns

<u>Proposition 1.</u> Let $n \in \mathbb{N}$, $p \in \mathcal{P}_n$, $B_{n,p} = (b_{r,j})$. Then for $0 \le j \le p-1$, $1 \le r \le p - r_{n,p} - 1$:

$$b_{r,j} = \begin{cases} -\nu_p(n - r_{n,p}) & \text{if } j = r_{n,p} \\ \nu_p(n - r_{n,p}) & \text{if } j = r + r_{n,p} \\ 0 & \text{else} \end{cases}$$

for $n-(p-1) \le j \le n-1$, $1 \le r \le p - r_{n,p} - 1$:

$$b_{r,j} = \begin{cases} 1 & \text{if } j = n-p+r \\ 0 & \text{else} \end{cases}$$

<u>Proposition 2.</u> Let $P = \max \mathcal{P}_n$. Then

$$\operatorname{rank} A_n \ge 2P - n - 1 .$$

<u>Corollary 1</u> If $n = P$, $\operatorname{rank} A_n \ge P - 1$, thus $\operatorname{rank} A_n = n-1 \Rightarrow \binom{x}{n}$ is abs.-irr.

NUMBER-THEORETIC TOOLS FOR COMPOSITE n

<u>Theorem.</u> Let $n > 10$ and $2 \leq k < n - P$. Then there exists a prime $p > 2k$ which divides one of the numbers $n, n-1, \dots, n-k+1$.

<u>Proof by case study.</u>

(I) large $n \geqslant 4021520$.

<u>Fact 1</u> (Bertrand's postulate). For $n \geqslant 3$ there exists a prime p with $n/2 < p < n$.

<u>Fact 2</u> (Quantitative Cebyshev theorem). For $n \geqslant 2\,010\,760$ there exists a prime p with $n < p < (1 + \frac{1}{16597})n$.

<u>Fact 3</u> (Laishram–Shorey, 2005). Let $k \geqslant 2$ and $n > \max\{k+13, \frac{279}{262}k\}$. Then the product

$$n(n+1)\dots(n+k-1)$$

has a prime factor $p > 2k$.

(II) small $n < 4\,021\,520$ and $k \geqslant 5$.

<u>Fact 4</u> (Laishram–Shorey, 2006) Let $k < n < k + 1{,}9 \cdot 10^{10}$. Then there exist pairwise distinct primes $p_0, p_1, \dots, p_{k-1}$ with $p_i / n-i$ ($\forall\, i = 0, \dots, k-1$), provided that $n, n-1, \dots, n-k+1$ are composite numbers.

III Remaining cases $k = 2, 3, 4$ for small n.

Fact 5. By Mihailescu's result on the Catalan equation the only consecutive positive integers which are non-prime prime powers are 8 and 9.

Fact 6. The only non-prime prime powers p^x and q^y less than 10^{18} with $p^x - q^y = 2$ are 25 and 27.
[Numerical result for Pillai equation]

This yields a proof of the number-theoretic theorem $\Rightarrow$ $\binom{x}{n}$ is abs-irr.