Fibonacci like sequences as polynomial values and almost universal Hilbert sets

Danny Neftin and Adi Ostrov

Technion Israel Institute of Technology and Bar Ilan University

Online Number Theory Seminar
University of Debrecen, Hungary

Motivation - Unlikely Intersections

General principle: If a curve X: $P(t,x)=0$ contains infinitely many special points, then the curve is special.

Motivation - Unlikely Intersections

General principle: If a curve X: $P(t,x) = 0$ contains infinitely many special points, then the curve is special.
Let X be the (smooth projective) curve defined by $P(t,x) = 0$ and $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ the projection to the t-coordinate.

Example

Let $f \in \mathbb{Q}(x)$ of $\deg f \geq 2$. Suppose $P(t,x) \in \mathbb{Q}(t)[x]$ is irreducible and $P(\beta, x) \in \mathbb{Q}[x]$ has a root for infinitely many $\beta \in f(\mathbb{Q})$. Then $\pi \circ u = f \circ v$ for some $u : Y \to X$, $v : Y \to \mathbb{P}^1_{\mathbb{Q}}$ where $g_Y \leq 1$ (by Faltings).

Motivation - Unlikely Intersections

General principle: If a curve X: $P(t,x)=0$ contains infinitely many special points, then the curve is special.
Let X be the (smooth projective) curve defined by $P(t,x)=0$ and $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ the projection to the t-coordinate.

Example

Let $f \in \mathbb{Q}(x)$ of $\deg f \geq 2$. Suppose $P(t,x) \in \mathbb{Q}(t)[x]$ is irreducible and $P(\beta,x) \in \mathbb{Q}[x]$ has a root for infinitely many $\beta \in f(\mathbb{Q})$. Then $\pi \circ u = f \circ v$ for some $u : Y \to X$, $v : Y \to \mathbb{P}^1_{\mathbb{Q}}$ where $g_Y \leq 1$ (by Faltings).

Theorem (Dèbes 1992)

Let $\alpha \in \mathbb{Q} \setminus \{\pm 1\}$. Suppose $P(t,x) \in \mathbb{Q}(t)[x]$ is geometrically irreducible but $P(\alpha^n, x)$ has a rational root for infinitely many n's. Then $P(t,x) \,|\, A(t,x)^e - \alpha^{-u} t$ for some $e, u \in \mathbb{Z}$ with $e > 1$.

The divisibility condition is equivalent to $\pi = (\alpha^u x^e) \circ \pi'$ for some π'.

Fibonacci sequences as values

$F_0^{a,b} = a, F_1^{a,b} = b$, and $F_{n+1}^{a,b} = F_n^{a,b} + F_{n-1}^{a,b}$, $n \in \mathbb{N}$. $F_n := F_n^{0,1}$.

Theorem (Cohn 1964)

The only perfect squares in the Fibonacci sequence F_n are $0, 1$ and 144.

Theorem (Bugeaud-Mignotte-Siksek 2006)

The only perfect powers in the Fibonacci sequence F_n are $0, 1, 8$ and 144.

Fibonacci sequences as values

$F_0^{a,b} = a, F_1^{a,b} = b$, and $F_{n+1}^{a,b} = F_n^{a,b} + F_{n-1}^{a,b}$, $n \in \mathbb{N}$. $F_n := F_n^{0,1}$.

Theorem (Cohn 1964)

The only perfect squares in the Fibonacci sequence F_n are $0, 1$ and 144.

Theorem (Bugeaud-Mignotte-Siksek 2006)

The only perfect powers in the Fibonacci sequence F_n are $0, 1, 8$ and 144.

Question

For which rational maps f does $f(\mathbb{Q})$ contain infinitely many $F_n^{a,b}$, $n \in \mathbb{N}$?

E.g. $F_{3n} = 5F_n^3 + 3(-1)^n F_n$, so $\# f(\mathbb{Q}) \cap (F_n)_{n\in\mathbb{N}} = \infty$, $f(x) = 5x^3 \pm 3x$.

Fibonacci sequences as values

$F_0^{a,b} = a, F_1^{a,b} = b$, and $F_{n+1}^{a,b} = F_n^{a,b} + F_{n-1}^{a,b}$, $n \in \mathbb{N}$. $F_n := F_n^{0,1}$.

Theorem (Cohn 1964)

The only perfect squares in the Fibonacci sequence F_n are $0, 1$ and 144.

Theorem (Bugeaud-Mignotte-Siksek 2006)

The only perfect powers in the Fibonacci sequence F_n are $0, 1, 8$ and 144.

Question

For which rational maps f does $f(\mathbb{Q})$ contain infinitely many $F_n^{a,b}$, $n \in \mathbb{N}$?

E.g. $F_{3n} = 5F_n^3 + 3(-1)^n F_n$, so $\# f(\mathbb{Q}) \cap (F_n)_{n\in\mathbb{N}} = \infty$, $f(x) = 5x^3 \pm 3x$.

Theorem (Corvaja–Zannier 02)

Supopse $F_n = \sum_{i=1}^r c_i\alpha_i^n$, $c_i \in \mathbb{Q}$ and $\alpha_i \in \mathbb{Q}$ admit a dominant root. If $F_n \in f(\mathbb{Q})$ for infinitely many n, then $F_{mn+k} = f(G_{mn+k})$ for some G, m, k.

Reducible Fibonacci values

Definition

A sequence $a_n, n \in \mathbb{N}$ is a *universal Hilbert set* if for every irreducible polynomial $P(t,x) \in \mathbb{Q}(t)[x]$, the specialization $P(a_n, x) \in \mathbb{Q}[x]$ is irreducible for all but finitely many n.

Ex: $2^n + 5^n$ (Dèbes–Zannier 98), density 1 (Zannier 96, Bilu 96,...), $\sum_{i=1}^r c_i a_i^n$ for mult. independent $a_i \in \mathbb{Z}$ and $c_i \in \mathbb{Q}$ (Corvaja–Zannier 98).

Reducible Fibonacci values

Definition

A sequence $a_n, n \in \mathbb{N}$ is a *universal Hilbert set* if for every irreducible polynomial $P(t,x) \in \mathbb{Q}(t)[x]$, the specialization $P(a_n, x) \in \mathbb{Q}[x]$ is irreducible for all but finitely many n.

Ex: $2^n + 5^n$ (Dèbes–Zannier 98), density 1 (Zannier 96, Bilu 96,...), $\sum_{i=1}^r c_i a_i^n$ for mult. independent $a_i \in \mathbb{Z}$ and $c_i \in \mathbb{Q}$ (Corvaja–Zannier 98).

Theorem (Dèbes 92)

Let $P(t,x) \in \mathbb{Q}(t)[x]$ be irreducible and $\alpha \in \mathbb{Q} \setminus \{\pm 1\}$. Suppose that $P(\alpha^n, x) \in \mathbb{Q}[x]$ is reducible for infinitely many n's. Then $P(t,x)$ divides $A(t,x)^p - \alpha^{-u} t$ or $4A(t,x)^4 + \alpha^{-u} t$, for some prime p and $u \in \mathbb{Z}$.

Remark: Equivalently, $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ factors as $\pi = (\alpha^u x^p) \circ \pi'$, p prime, or $\pi = (-4\alpha^u x^4) \circ \pi'$ for some map $\pi' : X \to \mathbb{P}^1_{\mathbb{Q}}$.

Reducible Fibonacci values

Definition

A sequence $a_n, n \in \mathbb{N}$ is a *universal Hilbert set* if for every irreducible polynomial $P(t,x) \in \mathbb{Q}(t)[x]$, the specialization $P(a_n, x) \in \mathbb{Q}[x]$ is irreducible for all but finitely many n.

Ex: $2^n + 5^n$ (Dèbes–Zannier 98), density 1 (Zannier 96, Bilu 96,...), $\sum_{i=1}^r c_i a_i^n$ for mult. independent $a_i \in \mathbb{Z}$ and $c_i \in \mathbb{Q}$ (Corvaja–Zannier 98).

Theorem (Dèbes 92)

Let $P(t,x) \in \mathbb{Q}(t)[x]$ be irreducible and $\alpha \in \mathbb{Q} \setminus \{\pm 1\}$. Suppose that $P(\alpha^n, x) \in \mathbb{Q}[x]$ is reducible for infinitely many n's. Then $P(t,x)$ divides $A(t,x)^p - \alpha^{-u} t$ or $4A(t,x)^4 + \alpha^{-u} t$, for some prime p and $u \in \mathbb{Z}$.

Remark: Equivalently, $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ factors as $\pi = (\alpha^u x^p) \circ \pi'$, p prime, or $\pi = (-4\alpha^u x^4) \circ \pi'$ for some map $\pi' : X \to \mathbb{P}^1_{\mathbb{Q}}$.

Question

For which irreducible P is $P(F_n, x) \in \mathbb{Q}[x]$ reducible for infinitely many n?

Fibonacci Numbers as Polynomial Values

Let $F_n = F_n^{0,1}$ stand for the Fibonacci sequence. The Dickson polynomial $D_{\alpha,d}$ is the unique polynomial satisfying $D_{\alpha,d}(x + \alpha/x) = x^d + \alpha^d/x^d$.

Theorem (Theorem A)

Let $\phi(z) \in \mathbb{Q}(z)$ be a rational function of degree $d \geq 2$, and suppose that $\phi(\mathbb{Q})$ contains infinitely many elements from the sequence F_n. Then either

- *d is odd and $\phi(z) = \frac{1}{(\pm 5)^{(d+1)/2}} D_{d,\pm 5}(\mu(z))$, where $\mu(z) \in \mathbb{Q}(z)$ is of degree 1, or*
- *d is even and $\phi(z) = q(w(z))$, for some quadratic $q \in \mathbb{Q}(w)$ with poles at $\pm\sqrt{5}$, and a cyclic $w \in \mathbb{Q}(z)$ fully ramified over $\pm\sqrt{5}$.*

Further, if the image contains infinitely many *even indexed* (*odd indexed*) elements, we may take $q(w) = \frac{4w}{5-w^2}$ ($q(w) = \frac{w^2+2w+5}{5-w^2}$).
Notice that $w(z)$ is of the form $\eta' \circ R_{5,d/2} \circ \eta$ for the Rédei function $R_{5,d/2}$ composed with two degree-1 rational functions $\eta, \eta' \in \mathbb{Q}(x)$.

Fibonacci Numbers as Polynomial Values

Theorem (O., N., Berman, Elrazik 2019)

Let $F_n = F_n^{a,b}$. Suppose that $g(x) \in \mathbb{Q}[x]$ is of degree $d = \deg g \geq 2$ and $g(\mathbb{Z})$ contains infinitely many elements from F_n. Then $g(x) = \pm\alpha_{a,b,d} D_{\pm 5,d}(\ell(x))$, where $\chi_{a,b} = a^2 + ab - b^2$, and $\alpha_{a,b,d} = \sqrt{\frac{\pm\chi_{a,b}}{5^{d+1}}}$ must be rational, and $\ell(x) \in \mathbb{Q}[x]$ is linear.

Example (Examples)

- Since $F_n = \frac{1}{\sqrt{5}}(\varphi^n + (-\varphi)^{-n})$, if n is even, for any odd $d \in \mathbb{N}$, $F_{nd} = \frac{1}{5^{(d+1)/2}} D_{5,d}(5F_n)$.
- Cassini's identity $5(F_n^{0,1})^2 + 4(-1)^n = (F_n^{2,1})^2$ shows that the curves $5t^2 \pm 4 = x^2$ have infinitely many Fibonacci values as the t-coordinate of a rational point. Indeed, since both the quadratic functions provide parameterizations of the curves, clearly their images contain all even/odd index Fibonacci numbers.

Fibonacci Numbers as Reducible Values of Polynomials

Conjecture B(N. O. Almost proved)

$F_n = F_n^{a,b}$. Let $P(t,x) \in \mathbb{Q}[t,x]$ be an irreducible polynomial, X the corresponding curve and $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ the projection to the t-coordinate. Suppose that $P(F_n, x) \in \mathbb{Q}[x]$ is reducible for infinitely many even n's. Then X is of genus zero, and either

1. $\pi = \mu \circ D_{\pm 5,d} \circ \pi'$, or
2. $\pi = \mu \circ \pi_c \circ \pi'$ where $\pi_c : \{5t^2 + 4\chi_{a,b} = x^2\} \to \mathbb{P}^1_{\mathbb{Q}}$ is the projection to the t-coordinate,

for some $\mu(x) \in \mathbb{Q}(x)$ of degree 1 and appropriate rational map π'.

Further, in the first case, when d is odd, there exists some $A(t,x) \in \mathbb{Q}[t,x]$, and a prime $p \mid n$ such that $P(t,x) \mid \frac{1}{(\pm 5)^{(p+1)/2}} D_{p,\pm 5}(A(t,x)) - t$. The second case is equivalent to saying that $P(t,x) \mid tA^2(t,x) - 4\chi_{a,b}A(t,x) - 5t$, for some $A(t,x) \in \mathbb{Q}[t,x]$.

Tools Used in the Proof

Theorem (Hilbert 1892)

For $P_t(x) = P(t,x) \in \mathbb{Q}(t)[x]$, the set of reducible values

$$\mathrm{Red}_P(\mathbb{Q}) = \{t_0 \in \mathbb{Q} : P(t_0, x) \text{ is undefined or reducible}\}$$

is a thin set, i.e. it is the union $\bigcup \phi_i(V_i(\mathbb{Q}))$ of finitely many value sets of rational maps $\phi_i : V_i \to \mathbb{P}^1_{\mathbb{Q}}$ ($\deg \phi_i \geq 2$), plus a finite set.

Theorem (Siegel 1929)

Suppose $\phi : V \to \mathbb{P}^1_{\mathbb{Q}}$ is a finite morphism such that $\#(\phi(V(\mathbb{Q})) \cap \mathbb{Z}) = \infty$. Then V is birationally equivalent to $\mathbb{P}^1_{\mathbb{Q}}$ (thus we can view $\phi \in \mathbb{Q}(x)$ as a rational function), and $\infty \in \mathbb{P}^1_{\mathbb{Q}}$ has at most two preimages, $\#\phi^{-1}(\infty) \leq 2$. Such ϕ are called Siegel functions.

Thus, when infinitely many of the reducible values are integral, at least one ϕ_i is a Siegel function.

Proof Outline: Theorem A

Let $\phi(z) \in \mathbb{Q}(z)$, $\deg \phi = d \geq 2$, such that $\phi(\mathbb{Q})$ contains infinitely Fibonacci numbers. Then either

- $\phi(z) = \frac{1}{(\pm 5)^{(d+1)/2}} D_{d,\pm 5}(\mu(z))$, for $\mu(z) \in \mathbb{Q}(z)$ of degree 1, or
- $\phi(z) = q(w(z))$, for some quadratic function $q \in \mathbb{Q}(w)$, and a cyclic function $w \in \mathbb{Q}(z)$.

Sketch of Proof.

1. ϕ is Siegel, $\#\phi^{-1}(\infty) \leq 2$.
2. One of the curves $5\phi(z)^2 \pm 4 = y^2$ has infinitely many rational points, and the projection on z is Siegel.
3. When $\#\phi^{-1}(\infty) = 1$, analysis of the monodromy group and ramification show that ϕ is Dihedral, hence $\psi = \mu' \circ D_{\alpha,n} \circ \mu$.
4. When $\#\phi^{-1}(\infty) = 2$, analysis of the monodromy group and ramification show that $\phi = q \circ w$, where w is fully ramified at $\pm\sqrt{5}$.

□

Proof Outline: Conjecture B

Suppose X is defined by $P(t,x) \in \mathbb{Q}[t,x]$ is irreducible, and has infinitely many even Fibonacci numbers as reducible values. Then the projection $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ to the t-coordinate factors through D_p or through $q \circ w$, for some quadratic $q \in \mathbb{Q}(x)$, and cyclic $w \in \mathbb{Q}(x)$.

Sketch of Proof.

1. By HIT and Siegel, there exists $\phi \in \mathbb{Q}(x)$ Siegel such that $P(\phi(z), x) \in \mathbb{Q}(z)[x]$ is reducible, and $\#\phi(\mathbb{Q}) \cap (F_{2n})_{n\in\mathbb{N}} = \infty$.
2. By Theorem A, $\phi = \nu \circ D_{5,n} \circ \mu$ or $\phi = q \circ w$.
3. If $\phi = \nu \circ D_{\pm 5,n} \circ \mu$, then π factors through $D_{\pm 5,p}$, for some prime p.
4. If $\phi = q \circ w$, and $P(q(z), x)$ is reducible: π factors through the t-coordinate projection $\pi_C : C \to \mathbb{P}^1_{\mathbb{Q}}$ from $C : 5t^2 + 4\chi_{a,b} = x^2$.
5. If $\phi = q(w(z))$ but $P(q(z), x)$ is irreducible, π factors through $D_{\pm 5,n}(x \pm 5/x)$ over $\mathbb{C}$ and hence through $\nu \circ D_{\pm 5,k} \circ \mu$ for some $k \in \mathbb{N}$ and linear η, μ.

□

Future Goals

Definition

A set U is called an *almost universal Hilbert set* if there exists a set of *exceptional polynomials* $E \subset \mathbb{Q}[A, t]$, which contains finitely many elements in each degree satisfying:
If $P(t,x) \in \mathbb{Q}[t,x]$ is irreducible but $P(u,x) \in \mathbb{Q}[x]$ is reducible for infinitely many $u \in U$, then $P(t,x) \mid e(A(t,x))$ for some $e \in E, A(t,x) \in \mathbb{Q}[t,x]$.

1. Finish the proof of the conjecture.
2. Show that each binary recurrence sequence is an almost universal Hilbert sets and effectively describe the exceptional polynomials.
3. Show that higher rank recurrence sequences give almost universal Hilbert sets.
4. Make Theorem A effective.

Future Goals

Definition

A set U is called an *almost universal Hilbert set* if there exists a set of *exceptional polynomials* $E \subset \mathbb{Q}[A, t]$, which contains finitely many elements in each degree satisfying:
If $P(t,x) \in \mathbb{Q}[t,x]$ is irreducible but $P(u,x) \in \mathbb{Q}[x]$ is reducible for infinitely many $u \in U$, then $P(t,x) \mid e(A(t,x))$ for some $e \in E, A(t,x) \in \mathbb{Q}[t,x]$.

1. Finish the proof of the conjecture.
2. Show that each binary recurrence sequence is an almost universal Hilbert sets and effectively describe the exceptional polynomials.
3. Show that higher rank recurrence sequences give almost universal Hilbert sets.
4. Make Theorem A effective.

Thank you for listening!

The slides are available upon request.