Common values of a class of linear recurrences

Attila Pethő

Department of Computer Science
University of Debrecen, Debrecen, Hungary

Online Number Theory Seminar, November 11, 2022.

Talk is based on my paper: *Common values of a class of linear recurrences, Indagationes Math.(N.S.) 33 (2022), 1172 – 1188.*

1. Notations and history

Let $(a_n), (b_n)$ be linear recursive sequences of integers (lrs) with characteristic polynomials $A(X), B(X) \in \mathbb{Z}[X]$ of degree d_A, d_B respectively. Let $\alpha_1, \ldots, \alpha_k$ and $\beta_1, \ldots, \beta_l$ be the distinct roots of $A(X)$ as well as of $B(X)$ with multiplicities $m_1, \ldots, m_k$ and $n_1, \ldots, n_l$ respectively.
There exist $A_1(X), \ldots, A_k(X) \in \mathbb{Q}(\alpha_1, \ldots, \alpha_k)[X]$, $\deg A_i < m_i$ and $B_1(X), \ldots, B_l(X) \in \mathbb{Q}(\beta_1, \ldots, \beta_l)[X]$, $\deg B_i < n_i$ such that

$$a_n = \sum_{i=1}^{k} A_i(n)\alpha_i^n, \quad b_n = \sum_{i=1}^{l} B_i(n)\beta_i^n$$

for all $n \in \mathbb{Z}$.

We study the diophantine equation

$$|a_n| = |b_m|$$

in $n, m \in \mathbb{N}$ or more generally for lower bound for

$$||a_n| - |b_m||,$$

in terms of $max\{n, m\}$ provided n, m are large enough.

The first results are numerical. *THE four numbers* $1, 3, 8, 120$ *have the property that the product of any two, increased by* 1*, is a perfect square.* Baker and Davenport, 1969 (inspired by a talk of van Lint) proved that 120 cannot be replaced by an other positive integer.

They proved actually:

Let $a_0 = 1, a_1 = 2,\ a_{n+1} = 6a_n - a_{n-1}$ and $b_0 = 1, b_1 = 3,\ b_{n+1} = 4b_n - b_{n-1}$. Then $a_n = b_m$ has only the solutions
$n = m = 0, 2,\ a_2 = b_2 = 11$.

To prove this they used the Baker-Davenport reduction.

Intermezzo. Warning

A. Dujella and A. Pethő, *Generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford (2), 49 (1998), 291–30.

Lemma 5 *Suppose that M is a positive integer. Let p/q be the convergent of the continued fraction expansion of κ such that $q > 6M$ and let $\varepsilon := \| \mu q \| - M \| \kappa q \|$, where $\| . \|$ denotes the distance from the nearest integer.*

a) *If $\varepsilon > 0$, then there is no solution of the inequality*

$$0 < m\kappa - n + \mu < AB^{-m}$$

in integers m and n with $\log(Aq/\varepsilon)/\log B \leq m \leq M$.

b)

It is cited very often in the form:

Lemma 3. *Let M be a positive integer, let p/q be a convergent of the continued fraction of the irrational τ such that $q > 6M$, and let A, B, μ be some real numbers with $A > 0$ and $B > 1$. Let further $\varepsilon := \| \mu q \| - M \| \tau q \|$. If $\varepsilon > 0$, then there is no solution to the inequality*

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

in positive integers u, v and s with $u \leq M$ and $s \geq \log(Aq/\varepsilon)/\log B$.

The authors do not take care of the irrationality of the actual τ!

1. Notations and history, continuation

Mignotte, 1979: Assume $|\alpha_1| > |\alpha_2| \geq \ldots \geq |\alpha_k|$ and $|\beta_1| > |\beta_2| \geq \ldots \geq |\beta_l|$. There exists an effectively computable constant N_0 such that if $a_n = b_m$ holds for $n + m > N_0$ then $A_1(n)\alpha_1^n = B_1(m)\beta_1^m$.

The linear recursive sequence (a_n) is non-degenerate if the ratios of the distinct roots of its characteristic polynomial are not roots of unity.

Evertse (1984) and Laurent (1985): If (a_n) and (b_n) are non-degenerate then $a_n = b_m$ *can have infinitely many solutions* m, n *only in the "obvious" cases.* This is not effective!

Cerliengo, Mignotte and Piras (1984). There exists $k > 0$ such that if $(a_n^{(1)}), \dots, (a_n^{(k)})$ denote linear recursive sequences of integers then the property: there exist $(n_1, \dots, n_k) \in \mathbb{N}^k$ such that

$$a_{n_1}^{(1)} + \dots + a_{n_k}^{(k)} = 0$$

is algorithmically undecidable.

In the 21th century many equations $a_n = b_m$ were solved completely for given sequences.

This talk is inspired by the work of Bravo, Gómez, Luca, Togbé and Kafle (2020).

Let (T_n) denotes the tribonacci sequence, which is defined by the initial terms $T_{-1} = T_0 = 0, T_1 = 1$ and by the recursion $T_{n+3} = T_{n+2} + T_{n+1} + T_n, n \geq -1$. They determined all solutions $n, m \in \mathbb{Z}$ of the diophantine equation $T_n = T_m$ in $n, m \in \mathbb{Z}$.

Three cases:

$$(sg(n), sg(m)) = \begin{cases} (+,+), & \text{easy} \\ (-,-), & \text{easy} \\ (+,-), & \text{new idea} \end{cases}$$

Set $T'_n = T_{-n}$ for the negative branch of the tribonacci numbers. Then $T'_{n+3} = -T'_{n+2} - T'_{n+1} + T'_n$. The characteristic polynomial of (T_n) has a dominating real root, while it of T'_n a dominating conjugate complex pair of roots. **Mignotte's result is not applicable.** The good news is that "Bakery" still works.

2. Main results

• $H(P)$, $\overline{|P|}$: the maximum of absolute values of the coefficients as well as of the roots of $P \in \mathbb{Z}[X]$,
• $(a_n), (b_n)$ be lrs of integers with characteristic polynomials $A(X), B(X) \in \mathbb{Z}[X]$,
• $d_A = \deg A, d_B = \deg B$,
• $\alpha_1, \ldots, \alpha_k$ and $\beta_1, \ldots, \beta_l$ be the distinct roots of $A(X)$ as well as of $B(X)$ with multiplicities $m_1, \ldots, m_k$ and $n_1, \ldots, n_l$ respectively.

$$a_n = \sum_{i=1}^{k} A_i(n)\alpha_i^n, \quad b_n = \sum_{i=1}^{l} B_i(n)\beta_i^n$$

for all $n \in \mathbb{Z}$,
• $H_A = H(A)$ and $H_B = H(B)$,
• $\Gamma_A = \max\{|a_0|, \ldots, |a_{d_A-1}|, 2\}$ and $\Gamma_B = \max\{|b_0|, \ldots, |b_{d_B-1}|, 2\}$.

Theorem 1. *Assume that*

$|\alpha_1| > |\alpha_2| \geq |\alpha_3| \geq \ldots \geq |\alpha_k|$, $m_1 = 1$,
$\beta_2 = \bar{\beta}_1$, $|\beta_1| = |\beta_2| > |\beta_3| \geq \ldots \geq |\beta_l|$, $n_1 = n_2 = 1$,
α_1/β_1 *and* β_2/β_1 *are not roots of unity,*
$\delta = \log|\beta_1|/\log|\alpha_1| \in \mathbb{Q}$, *i.e.* $|\alpha_1|, |\beta_1|$ *are multiplicatively dependent.*
Put

$$c_0 = \frac{1.02 \cdot 10^{30} \cdot (d_A! d_B!)^4 d_A^7 d_B^{10} \log^2(H_A+1)\log^2(H_B+1)(\log \Gamma_A)(\log \Gamma_B)}{\min\{1, \log|\alpha_1|\}^2}.$$

Then there is an effectively computable positive number c_1 *depending on* $d_A, d_B, H_A, H_B, \Gamma_A, \Gamma_B$ *such that the diophantine inequality*

$$||a_n| - |b_m|| > |a_n|^{1-(c_0 \log^2 n)/n} \qquad (1)$$

holds for all non-negative integers n, m *with* $\max\{n, m\} > c_1$.

An immediate consequence of our theorem is

Corollary 1. *Under the assumptions of Theorem 1 the equation*

$$|a_n| = |b_m| \tag{2}$$

has only finitely many solutions in $n, m \in \mathbb{Z}^2_{\geq 0}$*, and these can be computed effectively.*

• The assumptions that α_1/β_1 and β_2/β_1 are not roots of unity are natural because, otherwise, $|a_n| = |b_m|$ may have infinitely many solutions.

• The assumption that α_1 and $|\beta_1|$ are multiplicatively dependent is not at al natural, moreover it is quite restrictive, but without it we can prove only finiteness.

Theorem 2. *With $a, b, p, q \in \mathbb{Z}, p, q > 0$ and q even if b is not a square define $Q_1(X) = X^2 + aX + b^p$ and $Q_2(X) = X^3 + aX^2 + bX + 1$ such that $Q_2(X)$ has one real root outside the unit circle and a pair of conjugate complex roots. Assume that $P_1(X), P_2(X) \in \mathbb{Z}[X]$ and*
either

- $|b| > 1, a^2 - 4b^p < 0, b^p \nmid a^2$ *and either* $b^{q/2-p}a \in \mathbb{Z}$ *and* $|b^{q/2-p}a| \geq 3$, *or* $b^{q/2-p}a \notin \mathbb{Z}$,
- $\overline{|P_1|} < |b^{q/2}|, \ \overline{|P_2|} < \overline{|Q_1|}$,
- $A(X) = (X \pm b^{q/2})P_1(X), \ B(X) = Q_1(X)P_2(X)$,

or

- $\overline{|P_1|} < \overline{|Q_2|}, \ \overline{|P_2|} < \overline{|X^3 Q_2(1/X)|}$,
- $A(X) = Q_2(X)P_1(X), \ B(X) = X^3 Q_2(1/X)P_2(X)$.

Then $A(X)$ has a dominating real root α, $B(X)$ has a pair of dominating conjugate complex roots $\beta, \bar{\beta}$, moreover $\alpha, \beta, \alpha/\beta$ and $\beta/\bar{\beta}$ are not roots of unity, finally α and β are multiplicatively dependent.

Question: *Are that the only polynomials* $A, B \in \mathbb{Z}[X]$, *such that* $A(X)$ *has a dominating real root* α, $B(X)$ *has a pair of dominating conjugate complex roots* $\beta, \bar{\beta}$, *moreover* $\alpha, \beta, \alpha/\beta$ *and* $\beta/\bar{\beta}$ *are not roots of unity, finally* α *and* β *are multiplicatively dependent?*

Corollary 2. *Let* $a, b \in \mathbb{Z}$ *such that* $X^3 - aX^2 - bX \pm 1 \notin \{(X \pm 1)^3, (X \pm 1)^2(X \mp 1), (X^2 + 1)(X \pm 1), (X^2 \pm X + 1)(X \pm 1)\}$*. Let* $f_0, f_1, f_2 \in \mathbb{Z}$ *not all zero and*

$$f_{n+3} = af_{n+2} + bf_{n+1} \pm f_n, \; n \in \mathbb{Z}.$$

Then there are only finitely many effectively computable $n, m \in \mathbb{Z}, n \neq m$ *with* $|f_n| = |f_m|$*.*

Conjecture 1. *Let* $b \in \mathbb{Z}$ *be fixed and the lrs* (g_n) *be defined by the initial terms* $g_0 = g_1 = 0, g_2 = 1$ *and by the recursion* $g_{n+3} = ag_{n+2} + bg_{n+1} \pm g_n$*. Then there is an effectively computable constant* $C = C(b)$ *such that* $|g_n| \neq |g_m|$ *for any* $a \in \mathbb{Z}, |a| > 3$ *and for all* $n, m \in \mathbb{Z}, n \neq m, |n|, |m| > C$*.*

Question: *Is the same true interchanging the roles of* a *and* b*?*

3. Bound for parameters of lrs'

Lemma 1. *Let* (g_n) *be a lrs with initial values* $g_0, \ldots, g_{M-1} \in \mathbb{Z}$ *and with characteristic polynomial* $G(X) = X^M - p_{M-1}X^{M-1} - \cdots - p_0 \in \mathbb{Z}[X]$*. Assume that* $G(X) = G_1^{u_1}(X) \cdots G_s^{u_s}(X)$ *with irreducible polynomials* $G_1(X), \ldots, G_s(X) \in \mathbb{Z}[X]$ *and positive integers* $u_1, \ldots, u_s$*. Denote by* v_i *the degree of* $G_i(X)$*, and* $\gamma_{ij},\ j = 1, \ldots, u_i$ *the distinct zeros of it,* $i = 1, \ldots, s$*. Set* $\mathbb{K} = \mathbb{Q}(\gamma_{11}, \ldots, \gamma_{su_s})$ *and* $G_{ij}(X) \in \mathbb{K}[X]$ *of degree at most* $u_i - 1, i = 1, \ldots, s,\ j = 1, \ldots, v_i$ *such that*

$$g_n = \sum_{i=1}^{s} \sum_{j=1}^{v_i} G_{ij}(n)\gamma_{ij}^n \qquad (3)$$

holds for all $n \geq 0$*. Let* $J = H(G)$ *and* $\Gamma = \max\{|g_0|, \ldots, |g_{M-1}|\}$*.*

Then

$$H(G_{ij}) \leq J_1 = \Gamma \cdot (J+1)^{M(M-1)/2}(M!)^M. \tag{4}$$

If γ_{11} *is real, simple and dominating among the roots of* $G(X)$ *then* $G_{11}(X)$ *is a constant and*

$$|G_{11}| \geq J_1^{1-2M}. \tag{5}$$

If the pair $(\gamma_{11}, \gamma_{12})$ *with* $\gamma_{12} = \bar{\gamma}_{11}$ *is simple and dominating among the roots of* $G(X)$ *then* $G_{12}(X)$ *and* $G_{11}(X)$ *are complex conjugate constants and*

$$|G_{11}| = |G_{12}| \geq J_1^{1-M} \tag{6}$$

and

$$h(G_{11}/G_{12}) \leq 2\log(J_1). \tag{7}$$

In the very technical proof I used a theorem of Flowe and Harris (1993), which we found in C. Krattenthaler, Advanced determinant calculus, Séminaire Lotharingien Combin. 42 ("The Andrews Festschrift") (1999), Article B42q, 67 pp.

Reach source on the computation of determinants.

4. Tools from the transcendental number theory

For an algebraic number η with minimal polynomial

$$f(X) = a_0(X - \eta^{(1)}) \cdots (X - \eta^{(N)}) \in \mathbb{Z}[X]$$

with positive a_0 and with coefficients having greatest common divisor 1 define the *absolut logarithmic height* of η as

$$h(\eta) = \frac{1}{N} \left(\log a_0 + \sum_{j=1}^{N} \max\{0, \log |\eta^{(j)}|\} \right).$$

Important properties of the function h are:

Lemma 2. *Let γ, η be algebraic numbers of degree at most d and $u \in \mathbb{Q}$. Then we have*

- $h(\gamma \pm \eta) \leq h(\gamma) + h(\eta) + \log 2$,
- $h(\gamma\eta^{\pm 1}) \leq h(\gamma) + h(\eta)$,
- $h(\gamma^u) = |u| h(\gamma)$.

Let $\mathbb{K}$ be an algebraic number field of degree $d_{\mathbb{K}}$,
let $\eta_1, \eta_2, \ldots, \eta_t \in \mathbb{K}$ not 0 or 1,
$e_1, \ldots, e_t$ be nonzero integers. Put

$$E = \max\{|e_1|, \ldots, |e_t|, 3\} \qquad \text{and} \qquad \Gamma = \prod_{i=1}^{t} \eta_i^{e_i} - 1.$$

Let $F_1, \ldots, F_t$ be such that

$$F_j \geq \max\{d_{\mathbb{K}} h(\eta_j), |\log \eta_j|, 1\}, \quad \text{for} \quad j = 1, \ldots t.$$

Matveev (2000) proved

Lemma 3. *If* $\Gamma \neq 0$, *then*

$$\log |\Gamma| > -3 \cdot 30^{t+4} (t+1)^{5.5} d_{\mathbb{K}}^2 (1 + \log d_{\mathbb{K}})(1 + \log tE) F_1 F_2 \cdots F_t.$$

5. Scatch of the proof of Theorem 1

5.1. Preparations

Set

$$\frac{\log|\alpha_i|}{\log|\alpha_1|} < \delta_a < 1,\ (2 \le i \le k), \qquad \frac{\log|\beta_j|}{\log|\beta_1|} < \delta_b < 1,\ (3 \le j \le l).$$

If n and m are large enough then

$$\begin{aligned}
|a_n - A_1\alpha_1^n| &< |\alpha_1|^{\delta_a n}, \\
\frac{|A_1|}{2}|\alpha_1|^n < |a_n| &< 2|A_1| \cdot |\alpha_1|^n && (8) \\
|b_m - (B_1\beta_1^m + B_2\beta_2^m)| &< |\beta_1|^{\delta_b m} && (9) \\
|\beta_1|^{m - c_2 \log m} < |B_1\beta_1^m + B_2\beta_2^m| &< 2|B_1| \cdot |\beta_1|^m && (10) \\
|\beta_1|^{m-(c_2+1)\log m} < |b_m| &< 3|B_1||\beta_1|^m, && (11)
\end{aligned}$$

where

$$c_2 = 3 \cdot 10^{13} d_B^6 (\log d_B)^2 (\log(H_B + 1)) \log \Gamma_B.$$

The proofs, except of the left hand side of (10), are simple. The exceptional case requires a Baker's type lower bound. An explicit lower bound for m was not computed.

Contrary to the statement of Theorem 1 we assume that there exist a $(n, m) \in \mathbb{Z}^2_{\geq 0}$ with $\max\{n, m\} > c_1$ for which (1) does not hold, i.e. for which

$$||a_n| - |b_m|| \leq |a_n|^{1-(c_0 \log^2 n)/n} \tag{12}$$

holds, where c_1 is effectively computable in terms of d_A, d_B, H_A, H_B, Γ_A, Γ_B and is sufficiently large to make all estimates in the proof work. We show that this leads to a contradiction.

First we have to exclude the solutions of (1) for which n or m is small. First we do this for m and then for n.

5.2. Simplifications

In the sequel we assume that $(n,m) \in \mathbb{Z}^2_{\geq 0}$ is a solution of (12) with $n \geq c_{A1}, m \geq f_2 \geq c_{B1}$ and $\max\{n,m\} > c_1$.

According the signs of a_n and b_m and the sizes of $|a_n|$ and $|b_m|$ one has to distinguish cases, but they can be handled similarly. We continue with the case $0 \leq b_m \leq a_n$, i.e. with the inequality

$$|a_n - b_m| \leq |a_n|^{1-(c_0 \log^2 n)/n}. \tag{13}$$

Instead of $a_n - b_m$, which may have many terms, we will study $A_{n,m} = A_1\alpha_1^n - (B_1\beta_1^m + B_2\beta_2^m)$, which has only three summands, and thus is much more easy to treat. We have

$$\begin{aligned}
|A_{n,m}| &\le |a_n - b_m| + |a_n - A_1\alpha_1^n| + |b_m - (B_1\beta_1^m + B_2\beta_2^m)| \\
&\le |a_n|^{1-c_0(\log^2 n)/n} + |\alpha_1|^{\delta_a n} + |\beta_1|^{\delta_b m} \qquad (14)\\
&\le 2|A_1|\cdot|\alpha_1|^{n-c_0\log^2 n} + 2\max\{|\beta_1|^{\delta_b m}, |\alpha_1|^{\delta_a n}\}.
\end{aligned}$$

Case I. $|\alpha_1|^{\delta_a n} \ge |\beta_1|^{\delta_b m}$. Then

$$\left|\frac{A_{n,m}}{\alpha_1^n}\right| < 2|\alpha_1|^{(\delta_a-1)n} + 2|A_1|\cdot|\alpha_1|^{-c_0\log^2 n} < 4|A_1|\cdot|\alpha_1|^{-c_0\log^2 n} < |A_1|/2,$$

whenever n is large enough.

The last inequality implies

$$|A_1|\cdot|\alpha_1|^n/2 < |B_1\beta_1^m + B_2\beta_2^m| < 3|A_1|\cdot|\alpha_1|^n/2. \qquad (15)$$

A direct consequence of the left inequality of (15) and (10) is that

$$|A_1| \cdot |\alpha_1|^n/2 < 2|B_1| \cdot |\beta_1|^m,$$

thus

$$n - \delta m < c_3 \quad \text{with} \quad c_3 = \frac{\log(4 \cdot |B_1|/|A_1|)}{\log |\alpha_1|}.$$

On the other hand the right inequality of (15) and (9) imply,

$$3|A_1| \cdot |\alpha_1|^n/2 > |\beta_1|^{m - c_2 \log m},$$

thus

$$n - \delta m > -c_5 \log m \quad \text{with} \quad c_5 = \frac{c_2 \log(3|A_1|/2)}{\min\{1, \log |\alpha_1|\}}.$$

Case II. $|\alpha_1|^{\delta_a n} < |\beta_1|^{\delta_b m}$**.** We can prove the same inequalities.

5.3. The principal step

So far we proved that if $(n, m) \in \mathbb{N}^2$ is a solution of (13) such that n and m are large enough then

$$c_3 < |n - \delta m| < c_5 \log m, \tag{16}$$

and

$$|A_{n,m}| < 4|A_1| \cdot |\alpha_1|^{n - c_0 \log^2 n}. \tag{17}$$

Now we prove a lower bound for $|A_{n,m}|$. Here we use the innovation of Bravo et al (2020).

Write $\beta_1 = rz$ with $r \in \mathbb{R}_{>0}$ and $z \in \mathbb{C}, |z| = 1$, then we see that $\beta_2 = r/z$ and $B_1\beta_1^m + B_2\beta_2^m = r^m(B_1 z^m + B_2 z^{-m})$. Remember that $r = |\beta_1| = |\alpha_1|^\delta$. Substituting this into (14), dividing by $|B_1 r^m|$ and using (16) and (17) we get

$$\left| z^m - \frac{A_1\alpha_1^n}{B_1 r^m} + \frac{B_2}{B_1} z^{-m} \right| < c_7 |\alpha_1|^{-c_0 \log^2 n}, . \tag{18}$$

The zeroes of the quadratic polynomial $X^2 - \frac{A_1\alpha_1^n}{B_1 r^m} X + \frac{B_2}{B_1}$ are

$$\lambda_{1,2} = \frac{1}{2}\left(\frac{A_1\alpha_1^n}{B_1 r^m} \pm \sqrt{\left(\frac{A_1\alpha_1^n}{B_1 r^m}\right)^2 - 4\frac{B_2}{B_1}} \right),$$

thus

$$|z^m - \lambda_1| \cdot |z^m - \lambda_2| \leq c_7 |\alpha_1|^{-c_0 \log^2 n}.$$

We may assume without loss of generality $|z^m - \lambda_1| \le |z^m - \lambda_2|$, hence

$$|z^m - \lambda_1| \le \sqrt{c_7}|\alpha_1|^{-c_0(\log^2 n)/2},$$

which implies

$$|\lambda_1| \ge |z|^m - \sqrt{c_7}|\alpha_1|^{-c_0(\log^2 n)/2} \ge 1/2,$$

provided n is large enough. Thus

$$|z^m/\lambda_1 - 1| \le 2\sqrt{c_7}|\alpha_1|^{-c_0(\log^2 n)/2}. \tag{19}$$

5.4. Application of Bakery and conclusion

Set $\Gamma = z^m/\lambda_1 - 1$.
If $\Gamma = 0$ then $A_1\alpha^n = B_1\beta_1^m + B_2\beta_2^m$.
$P(\eta)$: the largest prime below the prime ideal divisors of (η).
Clearly $P(A_1\alpha^n)$ is uniformly bounded, but as β_1 and β_1/β_2 are not roots of unity $P(B_1\beta_1^m + B_2\beta_2^m)$ has an effective lower bound growing to infinity with m, see Pethő, 1990. Hence $\Gamma \neq 0$ provided that n, m are large enough. I do not know an explicit version of this theorem.

We apply Matveev's theorem with the actual parameters:

$$\mathbb{K} = \mathbb{Q}(z, \lambda_1), t = 2, \eta_1 = z, \eta_2 = \lambda_1, e_1 = m, e_2 = 1.$$

$d_{\mathbb{K}} \leq 4k!l! \leq 4d_A!d_B!$, $E = m$.

$$h(\eta_1) = h(z) = h\left(\frac{\beta_1}{\beta_2}\right)^{1/2} = \frac{1}{2}h\left(\frac{\beta_1}{\beta_2}\right) = h(\beta_1) \leq \log(H_B + 1).$$

Estimation of $h(\eta_2)$ seems to be possible only if $\delta = \frac{\log|\beta_1|}{\log|\alpha_1|} \in \mathbb{Q}$.

In this case $u = n - m\delta \in \mathbb{Q}$ too, and as $\frac{\alpha_1^n}{r^m} = \pm|\alpha_1|^u$, we have

$$h\left(\frac{A_1}{B_1}\frac{\alpha_1^n}{r^m}\right) \leq |u|h(\alpha_1) + h\left(\frac{A_1}{B_1}\right) < |u|\log(H_A + 1) + h\left(\frac{A_1}{B_1}\right).$$

After some computation we obtain

$$h(\lambda_1) \leq 2|u|\log(H_A + 1) + c_8.$$

Finally, because $|n - m\delta| < c_5 \log m$, we get

$$h(\eta_2) = h(\lambda_1) \leq c_9 \log m + c_8.$$

Setting $F_1 = 8d_A!d_B! \log(H_B+1), F_2 = 4d_A!d_B!c_9 \log m + 4d_A!d_B!c_8$ the application of the theorem of Matveev yields

$$\log|\Gamma| > -c_{10} \log^2 m - c_{11}.$$

Comparing the lower and upper bounds for $\log|\Gamma|$ we obtain

$$c_0(\log|\alpha_1|)(\log^2 n)/2 - \log(2\sqrt{c_7}) < c_{10} \log^2 m + c_{11}.$$

After further manipulations we get

$$c_0 < \frac{1.018 \cdot 10^{30}(d_A!d_B!)^4 d_A^7 d_B^{10} \log^2(H_A+1) \log^2(H_B+1)(\log \Gamma_A)(\log \Gamma_B)}{\min\{1, \log|\alpha_1|\}^2},$$

which contradicts the choice of c_0.

6. Proof of Theorem 2

Theorem 2. *With $a, b, p, q \in \mathbb{Z}, p, q > 0$ and q even if b is not a square define $Q_1(X) = X^2 + aX + b^p$ and $Q_2(X) = X^3 + aX^2 + bX + 1$ such that $Q_2(X)$ has one real root outside the unit circle and a pair of conjugate complex roots. Assume that $P_1(X), P_2(X) \in \mathbb{Z}[X]$ and*

either

- $|b| > 1, a^2 - 4b^p < 0, b^p \nmid a^2$ *and either* $b^{q/2-p}a \in \mathbb{Z}$ *and* $|b^{q/2-p}a| \geq 3$, *or* $b^{q/2-p}a \notin \mathbb{Z}$,
- $\overline{|P_1|} < |b^{q/2}|,\ \overline{|P_2|} < \overline{|Q_1|}$,
- $A(X) = (X \pm b^{q/2})P_1(X),\ B(X) = Q_1(X)P_2(X)$,

or

- $\overline{|P_1|} < \overline{|Q_2|},\ \overline{|P_2|} < \overline{|X^3 Q_2(1/X)|}$,
- $A(X) = Q_2(X)P_1(X),\ B(X) = X^3 Q_2(1/X)P_2(X)$.

Then $A(X)$ has a dominating real root α, $B(X)$ has a pair of dominating conjugate complex roots $\beta, \bar{\beta}$, moreover $\alpha, \beta, \alpha/\beta$ and $\beta/\bar{\beta}$ are not roots of unity, finally α and β are multiplicatively dependent.

(i) $Q_1(X)$ has a pair of conjugate complex roots, while $X \pm b^{q/2}$ a real root, which satisfy the assertion.

(i) $Q_2(X)$ Denote α the real root, and $\beta_1, \bar{\beta_1}$ the complex roots of $Q_2(X)$. The relation $-1 = \alpha\beta_1\bar{\beta_1} = \alpha|\beta_1|^2$ proves that α and $|\beta_1|$ are multiplicatively dependent and as $|\alpha| > 1$ we have $|\beta_1| < 1$, hence they are not roots of unity. By $|\overline{P_1}| < |\overline{Q_2}| = |\alpha|$, the number α is the dominating real root of $A(X)$.

The roots of $X^3Q_2(1/X) \in \mathbb{Z}[X]$ are $\frac{1}{\alpha}, \beta = \frac{1}{\beta_1}, \bar{\beta} = \frac{1}{\bar{\beta}_1}$, hence $X^3Q_2(1/X)$ has a pair of dominating complex roots and a real root. The multiplicative dependence of α and $|\beta|$ and the dominance of β, $\bar{\beta}$ among the roots of $B(X)$ are clear.

We have

$$\frac{\alpha}{\beta} = \alpha\beta_1 = \frac{-1}{\bar{\beta}_1},$$

which together with $|\beta_1| < 1$ implies $|\alpha/\beta| > 1$, hence α/β cannot be a root of unity.

7. Proof of Corollary 2.

Corollary 2. *Let* $a, b \in \mathbb{Z}$ *such that* $X^3 - aX^2 - bX \pm 1 \notin \{(X \pm 1)^3, (X \pm 1)^2(X \mp 1), (X^2+1)(X \pm 1), (X^2 \pm X + 1)(X \pm 1)\}$. *Let* $f_0, f_1, f_2 \in \mathbb{Z}$ *not all zero and*

$$f_{n+3} = af_{n+2} + bf_{n+1} \pm f_n, \ n \in \mathbb{Z}.$$

Then there are only finitely many effectively computable $n, m \in \mathbb{Z}, n \neq m$ *with* $f_n = f_m$.

The characteristic polynomial $Q(X) = X^3 - aX^2 - bX \pm 1$ of (f_n) has a real root α. Denote α_2, α_3 its other roots. If $|\alpha| = 1$ then $\alpha = \pm 1$. The roots of the quadratic polynomial $Q(X)/(X - \alpha)$ are α_2, α_3. If $\alpha_3 = \bar{\alpha_2}$ then they are roots of unity, i.e. the roots of one of the polynomials $X^2 + 1, X^2 \pm X + 1$.

In the opposite case α_2, α_3 are real and either $|\alpha_2| = 1$, whence $\alpha_2 = \pm 1$ and $\alpha_3 = \pm 1$, delivering the excluded cases. Otherwise $|\alpha_2| > 1 = |\alpha| > |\alpha_3|$.

If $|\alpha| \neq 1$ and $Q(X)/(X - \alpha)$ has no real roots then, by Theorem 2, the pair of polynomials $Q(X), X^3 Q(1/X)$ satisfy the assumptions of Theorem 1. As the characteristic polynomial of $(f_n)_{n \geq 0}$ is $Q(X)$ and that of $(f_n)_{n \leq 0}$ is $X^3 Q(1/X)$ the equation $f_n = f_m$ has only finitely many effectively computable solutions.

If $Q(X)$ has three real roots then $|\alpha| = |\alpha_2|$ is only possible if $|\alpha| = 1$.

Hence if $Q(X)$ has three real roots, from which no is lying on the unit disc, then we can rearrange them such that $|\alpha| > |\alpha_2| > |\alpha_3|$.

The characteristic polynomial of $(f_n)_{n\geq 0}$ is $Q(X)$ and that of $(f_n)_{n\leq 0}$ is $X^3Q(1/X)$. $Q(X)$ has the dominant root α, while $X^3Q(1/X)$ the dominant root α_3. By MIgnotte's theorem there exists an effectively computable constant N_0 such that if $f_n = f_m, (n,m) \in \mathbb{Z}^2, n \neq m$ holds for $|n|+|m| > N_0$ then $A\alpha^n = A\alpha^m$ or $A\alpha^n = C\alpha_3^m$ is true with some real constants A, C. In the first case α is a root of unity, but it is impossible because $|\alpha| > 1$. In the second case n has to be positive, while m negative. The splitting field of Q has a Galois automorphism σ, which interchanges α and α_3. Applying σ to the last equation we obtain an absurdity.

Thank you for hearing my talk!