Some Diophantine problems connected to binary recurrences

A. Bérczes

Dubrovnik, 2025

1. Introduction
   - Binary recurrent sequences
2. Diophantine results for recurrences
   - Products of consecutive terms
   - Additive Diophantine equations containing recurrences
   - The restricted sumset of Lucas sequences
3. Diophantine problems connected to recurrences
   - Geometric progressions in binary linear recurrences
   - Quadratic factors of trinomials

Binary recurrent sequences

Binary recurrences

The sequence $\{u_n\}_{n\geq 1}$ is called a non-degenerate binary recurrent sequence of integers if

- $u_{n+2} = ru_{n+1} + su_n$, for all $n \geq 1$, where r and s are fixed nonzero integers
- u_0 and u_1 are given integers
- the characteristic equation $x^2 - rx - s = 0$ has two roots $\alpha \neq \beta$ (so $\Delta = r^2 + 4s \neq 0$)
- α/β is not a root of 1.

Lucas sequences

A non-degenerate binary recurrence is called a Lucas sequence if

$$u_0 = 0 \qquad \text{and} \qquad u_1 = 1$$

Binet's formula

For the terms of a non-degenerate binary recurrence we have

$$u_n = c\alpha^n + d\beta^n \qquad \text{for all} \qquad n \geq 1, \tag{1}$$

where c and d can be computed in terms of $u_1,\ u_2$. In fact,

$$(c, d) = \left(\frac{u_2 - \beta u_1}{\alpha^2 - \alpha\beta}, \frac{u_2 - \alpha u_1}{\beta^2 - \alpha\beta} \right). \tag{2}$$

Binet's formula for Lucas sequences

For Lucas sequences we have

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Diophantine properties of binary recurrence

Many Diophantine properties of binary linear recurrence sequences have been investigated either in general, or for special sequences

- divisibility properties of members of recurrence sequences
- prime values in recurrence sequences
- integral S-units in recurrence sequences
- perfect powers in recurrence sequences
- linear combinations of prime powers in recurrence sequences
- combinatorial numbers in recurrence sequences
- sums of factorial and integral S-units in recurrence sequences
- Diophantine triples and quadruples in recurrence sequences
- perfect powers in the sum-set of recurrence sequences

Primitive prime divisors of binary recurrences

Definition

A prime p is a primitive prime divisor of a linear binary recurrence u_n by definition if $p \mid u_n$ but $p \nmid (\alpha - \beta)^2 \cdot u_1 \dots u_{n-1}$.

Results for Lucas sequences:

- Zsigmondy (1892): existence of p.p.d. for $n > 6$, if $\alpha, \beta \in \mathbb{Z}$
- Carmichael (1913): existence of p.p.d for $n > 12$, if $\alpha, \beta \in \mathbb{R}$
- Schinzel (1974): existence of p.p.d for $n > n_0$ (absolute, effective), if $\alpha, \beta \in \mathbb{C}$
- Stewart (1977): existence of p.p.d for $n > e^{452}4^{67}$, if $\alpha, \beta \in \mathbb{C}$
- Voutier (1996): existence of p.p.d for $n > 2 \cdot 10^{10}$, if $\alpha, \beta \in \mathbb{C}$
- Voutier (1998): existence of p.p.d for $n > 30030$, if $\alpha, \beta \in \mathbb{C}$
- Bilu, Hanrot, Voutier (2001): complete solution for Lucas sequences

Proposition (Bilu, Hanrot, Voutier (2001))

If u_n is a Lucas sequence then

- *For $n > 30$ u_n always has a primitive prime divisor.*
- *For $n = 5$ and $7 \leq n \leq 30$ u_n always has a primitive prime divisor, except when (up to equivalence given by $\alpha_1/\alpha_2 = \beta_1/\beta_2 = \pm 1$):*

n	(r, s)
5	$(1,5), (1,-7), (2,-40), (1,-11), (1,-15), (12,-76), (12,-1364)$
7	$(1,-7), (1,-19)$
8	$(2,-24), (1,-7)$
10	$(2,-8), (5,-3), (5,-47)$
12	$(1,5), (1,-7), (1,-11), (2,-56), (1,-15), (1,-19)$
13	$(1,-7)$
18	$(1,-7)$
30	$(1,-7)$

Diophantine equations containing the product of consecutive terms of recurrences

- **Marques (2011)**
  - $F_1 \cdot F_2 \cdots F_n + 1 = F_m^t$ has only finitely many positive integer solutions (n, m)
  - computed all solutions when $t \in [1, 10]$
- **Bravo, Komatsu, Luca (2013):** the largest integer solution (k, ℓ, m, n) of

$$|F_n F_{n+1} \cdots F_{n+k-1} - F_m^\ell| \leq 100$$

with $k \geq 1,\ \ell \geq 1,\ m \geq 3,\ n \geq 3$ (and $m \neq n$ when $k = \ell = 1$) is

$$|F_9 \cdots F_{13} - F_{11}^5| = 89.$$

Diophantine equations containing the product of consecutive terms of recurrences

- **Szalay (2012)**: solved completely the Diophantine equation

$$G_{n_1} G_{n_2} \cdots G_{n_k} + 1 = G_m^2$$

in positive integer unknowns k, m and $n_1 < n_2 < \cdots < n_k$ where $\{G_n\}_{n \geq 1}$ is the Fibonacci sequence, the sequence of Lucas numbers, and the balancing sequence.

- **Pink and Szikszai (2017):** completely solved the equation

$$u_{n_1} u_{n_2} \cdots u_{n_k} + 1 = u_m^2$$

for a wide class of Lucas sequences.

Main tool

The proofs of the above results all have in common that **they use the existence of primitive divisors** for terms of Lucas sequences.

Diophantine equations containing the product of consecutive terms of recurrences

Theorem (B., Bilu, Luca (2018))

Assume that $u_n = ru_{n-1} \pm u_{n-2} = c\alpha^n + d\beta^n$ $(n \geq 0)$ *is a nondegenerate binary recurrent sequence of integers. Assume that in the* c/d *and* α/β *are multiplicatively independent. Then the Diophantine equation*

$$u_n u_{n+1} \cdots u_{n+k-1} \pm 1 = \pm u_m^2 \tag{3}$$

has at most finitely many positive integer solutions (k, m, n)*. Moreover, the solutions are effectively computable and satisfy*

$$m < 10^{53}(Y+2)^{64}, \tag{4}$$

where $Y := \max\{|u_0|, |u_1|, |r|\}$.

Diophantine equations containing the product of consecutive terms of recurrences

Theorem (B., Bilu, Luca (2018))

For the sequence $\{u_n\}_{n\geq 0}$ *given by* $u_1 = -9,\ u_2 = 7$ *and* $u_{n+2} = u_{n+1} + u_n$ *for all* $n \geq 1$, *the only solutions of equation (3) are*

$$\begin{aligned} u_3 - 1 &= u_2^2, \\ u_4 + 1 &= u_2^2, \\ u_5 + 1 &= u_4^2, \\ u_0 u_1 - 1 &= -u_5^2, \\ u_2 u_3 + 1 &= -u_4^2, \\ u_4 u_5 + 1 &= u_3^2, \\ u_3 u_4 u_5 + 1 &= u_6^2. \end{aligned}$$

On the equation $u_n = a_1 m_1! + \ldots + a_k m_k! + bs$

Consider the Diophantine equation

$$u_n = a_1 m_1! + \ldots + a_k m_k! + bs, \qquad \max\{|a_1|, |a_2|, \ldots, |a_k|, |b|\} \leq A \tag{5}$$

in integer unknowns $m_1 > m_2 > \ldots > m_k \geq 1$ and $s \in \mathscr{S}$.

- $b = 0$ Grossman and Luca (2002)
- $k = 1$ Gúzman Sanchez and Luca (2014)

B., Hajdu, Luca, Pink (2023)

- Equation (5) has finitely many solutions (effective)
- For $u_n = F_n$, $k = 2$ and $S = \{2, 3, 5, 7\}$ complete solution of (5)

On the equation $F_n^x + F_k^y = F_m^z$

Consider the Diophantine equation

$$F_n^x + F_k^y = F_m^z, \tag{6}$$

in positive integer unknowns $x, y, z, k, m, n,\ k \leq n$.

- $x = y,\ z = 1,\ k = n - 1$ - partial result:
- $x = y,\ z = 1,\ k = n - 1$ - complete solution: Luca and Oyono, (2011)
- $x = y,\ k = n - 1$ - complete solution: Luca and Hirata-Kohno, (2015)

B., Hajdu, Luca, Pink (202?)

- Complete solution of (6) with $x = y$ in positive integesr (n, k, m, x, z).

The restricted sumset of Lucas sequences

Definition (Sumset of two sets)

For a subset $\mathcal{A}$ of $\mathbb{Z}$ we define the restricted sumset of $\mathcal{A}$ by

$$\mathcal{A}\hat{+}\mathcal{A} := \{a + b : a \in \mathcal{A}, b \in \mathcal{A}, a \neq b\}.$$

Theorem (B., Pethő (2014))

Let u_n be a non-degenerate Lucas sequence with $\Delta = r^2 + 4s < 0$, and put $\mathcal{A} := \{u_n | n \in \mathbb{Z}, 0 \leq n \leq N\}$, with $N \geq 3$. Then we have

$$|\mathcal{A}\hat{+}\mathcal{A}| = \frac{N(N+1)}{2} - O(1).$$

The restricted sumset of Lucas sequences

Theorem (B., Pethő (2014))

Let R_n be a non-degenerate Lucas sequence with $A^2+4B>0$, and put $\mathcal{A}:=\{R_n|n\in\mathbb{Z},0\leq n\leq N\}$, with $N\geq 3$. Then we have the following statements:

- *If $(A,B)\notin\{(1,1),(-1,1)\}$*

$$|\mathcal{A}\widehat{+}\mathcal{A}|=\frac{N(N+1)}{2}.$$

- *If $(A,B)\in\{(1,1),(-1,1)\}$*

$$|\mathcal{A}\widehat{+}\mathcal{A}|=\frac{N(N+1)}{2}-(N-2).$$

The restricted sumset of Lucas sequences - On the proofs

Ingredients of the proofs

- To prove the above results we had to estimate the number of solutions of the equation

$$u_a + u_d = u_b + u_c$$

in the 4-tuples $(a, b, c, d) \in \mathbb{Z}^4_{\geq 0}$ with distinct entries.

- Properties and estimates for the polynomial

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) := x^a - x^b - x^c + x^d$$

- Unit equations in several unknowns
- The Evertse-Schlickewei-Schmidt Theorem
- Handling the case of vanishing subsums

Balancing numbers

Definition (Behera and Panda (1999))

A positive integer n is called a *balancing number* if for some $k \in \mathbb{N}$

$$1 + 2 + \cdots + (n-1) = (n+1) + (n+2) + \cdots + (n+k)$$

- **Behera and Panda (1999)**: Balancing numbers fulfill the following recurrence relation

$$B_{n+1} = 6B_n - B_{n-1} \quad (n > 1),$$

where $B_0 = 1$ and $B_1 = 6$.

- **Various generalizations and diophantine equations involving balancing numbers:** Alvarado, Behera, Chern, Dujella, Gözeri, Irmak, Komatsu, Kovács, Karaath, Keskin, Kumar, Liptai, Luca, Panda, Pintér, Rakaczki, Oljos, Ray, Rout, Szakács, Tekcan, Tengely, etc.

Definition

A binary recurrence u_n is called a *balancing sequence* if

$$u_1 + u_2 + \ldots + u_{n-1} = u_{n+1} + u_{n+2} + \ldots + u_{n+k} \tag{7}$$

holds for some $k \geq 1$ and $n \geq 2$.

Theorem (B., Liptai, Pink (2010))

There is no balancing sequence $u_n = r \cdot u_{n-1} + s \cdot u_{n-2}$ with $u_0 = 0$, $\Delta = r^2 + 4s > 0$, except for $(r, s) = (0, 1)$ in which case (7) has infinitely many solutions $(n, k) = (n, n-1)$ and $(n, k) = (n, n)$ for $n \geq 2$.

Corollary (B., Liptai, Pink (2010))

A Lucas-sequence u_n with $r^2 + 4s > 0$ is not a balancing sequence.

Generalized Ramanujan-Nagell equations

The Ramanujan-Nagell equation

$$x^2 + 7 = 2^n \qquad \text{in } x \in \mathbb{Z} \text{ and } n \in \mathbb{N}_{\geq 3}$$

The generalized Ramanujan-Nagell equation

$$D_1 x^2 + D_2 = a \cdot b^n \qquad \text{in } x \in \mathbb{Z} \text{ and } n \in \mathbb{N}_{\geq 3}$$

The generalized Lebesgue-Nagell equation

$$x^2 + D = y^n \qquad \text{in } x, y \in \mathbb{Z} \text{ and } n \in \mathbb{N}_{\geq 3}$$

The equation $x^2 + 11^a 17^b = y^n$

Theorem (B., Pink (2014))

All solutions of the equation

$$x^2 + 11^a 17^b = y^n \tag{8}$$

in nonnegative integer unknowns (x, y, a, b, n) *with*

$$x \geq 1, y \geq 2, a \geq 0, b \geq 0, n \geq 3 \text{ and } \gcd(x, y) = 1 \tag{9}$$

are

$$(x, y, a, b, n) \in \{(4, 3, 1, 0, 3), (58, 15, 1, 0, 3), (2, 5, 2, 0, 3), (9324, 443, 3, 0, 3), (14, 15, 1, 2, 3), (7670, 389, 2, 2, 3), (670, 111, 1, 4, 3), (8, 3, 0, 1, 4)\}$$

On the proof

- Write $x^2 + 11^a 17^b = y^n$ in the form

$$x^2 + dc^2 = y^n,$$

where $dc^2 = 11^a 17^b$ and $d > 0$ is the square-free part of $11^a 17^b$, that is $d \in \{1, 11, 17, 187\}$.

- By factorizing in the field $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ we get

$$(x + c\sqrt{-d})(x - c\sqrt{-d}) = y^n. \tag{10}$$

- By simple considerations on class number and unit group we get

$$x + c\sqrt{-d} = \gamma^n, \tag{11}$$

for some algebraic integer γ.

- By conjugating relation (11) we get

$$\gamma^n - \overline{\gamma}^n = 2c\sqrt{-d}. \tag{12}$$

On the proof

- Since $\{1, \sqrt{-d}\}$ is an integral basis for $O_{\mathbb{K}}$ if $d \in \{1, 17\}$, while if $d \in \{11, 187\}$ then $\{1, \frac{1+\sqrt{-d}}{2}\}$ is an integral basis for $O_{\mathbb{K}}$. Hence we may write γ occurring in (11) in the form

$$\gamma = u + v\sqrt{-d}, \tag{13}$$

where either both u and v are integers, or both $2u$ and $2v$ are odd integers, the last case occurring when $d = 11$ or $d = 187$.

- By (12) and (13) we get

$$L_n = \frac{\gamma^n - \overline{\gamma}^n}{\gamma - \overline{\gamma}} = \frac{(u + v\sqrt{-d})^n - (u - v\sqrt{-d})^n}{2v\sqrt{-d}} = \frac{c}{v}. \tag{14}$$

On the proof

- We easily see that the sequence L_n above is a Lucas sequence.
- Further, obviously $v \mid c$ holds and the prime factors of c belong to $\{11, 17\}$.
- By the primitive prime divisor theorem we conclude that for $n \geq 5$ prime the Lucas sequence L_n always has a primitive prime divisor except for finitely many exceptions, which are explicitly given.
- Now a finite computation and solving some diophantine equations with given n concludes the proof.

The equation $x^2 + p^{2k} = y^n$

Theorem (B., Pink (2008))

Let $2 \leq p < 100$ be a rational prime. Then all solutions of the equation

$$x^2 + p^{2k} = y^n \tag{15}$$

in integer unknowns x, y, n, k satisfying

$$x \geq 1, y > 1, n \geq 3 \ prime, \ k \geq 0 \text{ and } gcd(x, y) = 1.$$

are

$$(x, y, p, n, k) \in \{(11, 5, 2, 3, 1), (46, 13, 3, 3, 2), (524, 65, 7, 3, 1),$$
$$(2, 5, 11, 3, 1), (278, 5, 29, 7, 1)(38, 5, 41, 5, 1),$$
$$(52, 17, 47, 3, 1), (1405096, 12545, 97, 3, 1)\}.$$

The equation $x^2 + d^{2l+1} = y^n$

Theorem. (B., Pink (2012))
Let $d > 0$ be a squarefree integer and denote by $h = h(-d)$ the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. Consider the following equation

$$x^2 + d^{2l+1} = y^n \text{ with } h(-d) \in \{2, 3\} \tag{16}$$

in integer unknowns x, y, l, n satisfying

$$x \geq 1, y > 1, n \geq 3, \ l \geq 0 \text{ and } \gcd(x, y) = 1.$$

Further, if $d \equiv 7 \pmod 8$ also suppose that y is odd. Then all solutions of equation (16) are

$$(x, y, n, d, l) \in \{(2, 3, 3, 23, 0), (588, 71, 3, 23, 1), (6, 7, 3, 307, 0), (32, 11, 3, 307, 0), (598, 71, 3, 307, 0), (911054064, 939787, 3, 307, 0), (28, 11, 3, 547, 0), (70, 17, 3, 13, 0), (36, 11, 3, 35, 0), (702, 79, 3, 235, 0), (322, 47, 3, 139, 0), (2158, 167, 3, 499, 0)\}$$

On the proof

Ingredients of the proof

- tools from algebraic number theory
- the Primitive Prime Divisor Theorem of f Bilu, Hanrot and Voutier
- local methods
- the modular method of Bennett and Skinner for solving ternary diophantine equations of signature $(n, n, 2)$.
- determining S-integral points on elliptic curves
- the method of Chabauty concerning the determination of all rational points of a hyperelliptic curve of genus 2
- reduction of the problem to the resolution of several Thue-Mahler equations of degree 3

Geometric progressions in Lucas sequences

Theorem (B., Ziegler (2013))

Let $(u_n)_{n\geq 1}$ be a Lucas sequence and assume that there are three distinct indices n, k, l such that $u_k u_l = u_n^2$. Except the trivial case where $u_k, u_l, u_n \in \{\pm 1\}$ the only solutions are $(u_1, u_2, u_4) = (u_3, u_2, u_4) = (1, -2, 4)$ with $a = -2$ and $b = -8$.

Main tools of the proof

- use of the Primitive Prime Divisor Theorem
- elementary methods to treat the remaining cases

Geometric progressions in the solution set of Pellian equations

Consider the Pellian equation

$$X^2 - dY^2 = m, \quad \text{in} X, Y \in \mathbb{Z}, \tag{17}$$

for some $d, m \in \mathbb{Z}$ such that $d > 0$ is not a square.

Known facts

- a Pellian equation may have infinitely many solutions
- the set of solutions is the union of several binary recurrence sequences

Theorem

Let $X_1 < X_2 < X_3$ be the X-components of three positive distinct solutions to equation (17) for some $d, m \in \mathbb{Z}$ such that they form a geometric progression, i.e. fulfill $X_1 X_3 = X_2^2$. Then we have

$$X_3 < 1645683|m|^{20}.$$

Similarly assume that $Y_1 < Y_2 < Y_3$ are the Y-components of three positive distinct solutions to (17) which form a geometric progression. Then we have

$$Y_3 < \frac{1645683|m|^{20}}{d}.$$

Corollary

Let $m \in \mathbb{Z}$, $m \neq 0$ be fixed and assume (17) provides a non-trivial geometric progression in its solution set. Then we have

$$d \leq \frac{m^2(13+\sqrt{7})}{2}.$$

In particular this yields an effective algorithm to find all geometric progressions in the solution set of Pell equations (17) with $|m| \leq C$, with C a given constant.

Theorem

- *Let* $0 < Y_1 < Y_2 < Y_3 < Y_4 < Y_5$ *be a given geometric progression. Then there are at most finitely many* $d, m \in \mathbb{Z}$ *such that* d *is not a square,* $m \neq 0$ *and* $\gcd(d, m)$ *is square-free such that* Y_1, Y_2, Y_3, Y_4, Y_5 *are the* Y*-components of solutions to* $X^2 - dY^2 = m$.
- *Further, Let* $0 < Y_1 < Y_2 < Y_3 < Y_4$ *be a given geometric progression. Then there exist infinitely many* $d, m \in \mathbb{Z}$ *such that* d *is not a square,* $m \neq 0$ *and* $\gcd(d, m)$ *is square-free such that* Y_1, Y_2, Y_3, Y_4 *are the* Y*-components of solutions to* $X^2 - dY^2 = m$.
- *On the other hand for a given geometric progression* $0 < X_1 < X_2 < X_3$ *there exist at most finitely many* $d, m \in \mathbb{Z}$ *such that* d *is not a square,* $m \neq 0$ *and* $\gcd(d, m)$ *is square-free such that* X_1, X_2, X_3 *are the* X*-components of solutions to* $X^2 - dY^2 = m$.

Quadratic factors of $f(x) = X^n - BX + A \in \mathbb{Z}[X]$

- 1968 Rabinowitz: if $n = 5$, $B = \pm 1$ and $f(X)$ has an irreducible quadratic factor then we have $A \in \{\pm 1, \pm 6, \pm 15, \pm 22440, \pm 2759640\}$.
- 1991 Ribenboim: bounded $|A|$ by a constant depending on n and $|B|$, and $|B|$ by a constant depending on n and $|A|$
- 1994 Herendi and Pethő: the same for general trinomials
- 2014 Yang and Fu for $n > 40000$ bounded $|A|$ by a constant depending on $|B|$, and $|B|$ by a constant depending on $|A|$
- determination of all trinomials $f(X)$ having an irreducible quadratic factor
  - 2002 Chen: for $B = 1$ and $n > 512880$
  - 2004 Le: for $B = 1$ and $n > 5$
  - 2006 Lin: for $B = -1$ and $n > 5$
  - 2004 Yang: $n > \max\{512900, \frac{8}{7}B\}$
  - 2007 Liu: for $n > \max\{30, \frac{1}{2}|B| + 1\}$

Quadratic factors of $f(x) = X^n - BX + A \in \mathscr{S}[X]$

Notations

- Let S be a finite set of positive primes
- Denote by $\mathscr{S}$ the set of all integers having no prime factors outside of S.
- Denote by s the cardinality of S and by P the largest prime in S.
- Although $\mathscr{S}$ is not a ring, we will denote by $\mathscr{S}[X]$ the set of all polynomials with coefficients in $\mathscr{S}$.
- If we speak of the factorization of $f(X) \in \mathscr{S}[X]$ we always mean its factorization as a polynomial in $\mathbb{Z}[X]$.
- We will consider polynomials $f(x) = X^n - BX + A \in \mathscr{S}[X]$ which have a quadratic factor.

Quadratic factors of $f(x) = X^n - BX + A \in \mathscr{S}[X]$

Theorem (B., Luca, Pink, Ziegler)

Assume that the polynomial $f(X) = X^n - BX + A \in \mathscr{S}[X]$ *with* $\gcd(A, B) = 1$ *has a quadratic factor* $g(X) = X^2 - bX + a$. *Then we have one of the following cases:*

1. $n < max\{30, P + 2\}$;
2. $f(X) = X^{6k} - 1$, $f(X) = X^{6k+1} - X$, $f(X) = X^{6k+2} - X + 1$, $f(X) = X^{6k+3} + 1$, $f(X) = X^{6k+4} + X$, $f(X) = X^{6k+5} + X - 1$ *for* $k \in \mathbb{Z}_{>0}$, *and these polynomials are all divisible by* $X^2 - X + 1$;
3. $f(X) = X^{3k} - 1$, $f(X) = X^{3k+1} - X$, $f(X) = X^{3k+2} + X + 1$ *for* $k \in \mathbb{Z}_{>0}$, *and these polynomials are all divisible by* $X^2 + X + 1$;
4. $f(X) = X^n + (-1)^n nX + (-1)^n(n-1)$ *for* $n \in \mathbb{Z}_{>1}$, *which polynomials are divisible by* $X^2 + 2X + 1$;
5. $f(X) = X^n - nX + (n-1)$ *for* $n \in \mathbb{Z}_{>1}$, *which polynomials are divisible by* $X^2 - 2X + 1$.

Quadratic factors of $f(x) = X^n - BX + A \in \mathscr{S}[X]$

The above Theorem shows that there are infinite families of polynomials $f(X) = X^n - BX + A \in \mathscr{S}[X]$ divisible by $X^2 \pm X + 1$. In the next theorem we exclude this case.

Theorem

Let $n \geq 3$, $A, B \in \mathscr{S}$ and $\gcd(A, B) = 1$. Then the tuples (n, A, B) for which $f(X) = X^n - BX + A$ has a quadratic factor $g(X) = X^2 - bX + a$ with $g(X) \neq X^2 \pm X + 1$ belong to a finite set which can be determined effectively.

The case $S := \{2, 3, 5, 7\}$

The set of those natural numbers, for which both $n \in \mathscr{S}$ and $n - 1 \in \mathscr{S}$ is $M := \{3, 4, 5, 6, 7, 8, 9, 10, 15, 16, 21, 25, 28, 36, 49, 50, 64, 81, 126, 225, 2401, 4375\}$.

The case $S := \{2, 3, 5, 7\}$

- Assume that the polynomial $f(X) = X^n - BX + A \in \mathscr{S}[X]$ with $\gcd(A, B) = 1$ has a quadratic factor different of $X^2 \pm X + 1$ and $X^2 \pm 2X + 1$. Then
  - if $n = 3$ there are 736 such polynomials $f(x)$
  - if $n = 4$ there are 64 such polynomials $f(x)$
  - if $n = 5$ there are 20 such polynomials $f(x)$
  - if $n = 6$ there are 16 such polynomials $f(x)$
  - if $n = 7$ there are 8 such polynomials $f(x)$
  - if $n = 8$ there are 8 such polynomials $f(x)$
  - if $n = 13$ there is 1 such polynomials $f(x)$
- If the polynomial $f(X) = X^n - BX + A \in \mathscr{S}[X]$ with $\gcd(A, B) = 1$ has the quadratic factor $X^2 + 2X + 1$, then we have $f(X) = X^n + (-1)^n nX + (-1)^n(n - 1)$ with $n \in M$.
- If the polynomial $f(X) = X^n - BX + A \in \mathscr{S}[X]$ with $\gcd(A, B) = 1$ has the quadratic factor $X^2 - 2X + 1$, then $f(X) = X^n - nX + (n - 1)$ with $n \in M$.

On the proofs

The main idea

- Let $f(X) = X^n - BX + A \in \mathbb{Z}[X]$ $(n \geq 3)$ and $g(X) = X^2 - bX + a \in \mathbb{Z}[X]$ be two polynomials with $a \neq 0$.
- Assume that $g(X) = (X - \alpha)(X - \beta)$ with $\alpha \neq \beta$
- Denote by u_n the Lucas sequence corresponding to the Lucas pair (α, β), i.e. $u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$.
- $g(X) \mid f(X) \iff \alpha$ and β are roots of $f(X) \iff$

$$\iff \begin{cases} \alpha^n - B\alpha + A = 0 \\ \beta^n - B\beta + A = 0 \end{cases} \iff \begin{cases} B = \frac{\alpha^n - \beta^n}{\alpha - \beta} \\ A = \alpha\beta \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} \end{cases}$$

- Thus we have $g(X) \mid f(X) \iff B = u_n$ and $A = a \cdot u_{n-1}$.
- Use the Primitive Prime Divisor Theorem for u_n

Happy Birthday!