dc_1892_21

Sequences in Diophantine Number Theory

Szabolcs Tengely

A doctoral dissertation submitted to the Hungarian Academy of Sciences

2021

dc_1892_21

Contents

Part I

Introduction

dc_1892_21

Chapter 1 Short overview of the subject

In the thesis we shall solve Diophantine problems effectively by various methods. To put our results in the proper context we summarize some of the relevant history.

A Diophantine equation is an equation of the form $f(x_1, x_2, \ldots, x_n) = 0$, where f is a given function and the unknowns $x_1, x_2, \ldots, x_n$ are required to be rational numbers or to be integers. As a generalization of the concept one may consider rational or integral solutions over a number field. In the study of Diophantine equations there are some natural questions:

- Is the equation solvable?
- Is the number of solutions finite or infinite?
- Is it possible to determine all solutions?

In Diophantine number theory one general goal is to provide a kind of framework that can be applied to a large family of equations, problems. Such collections of arguments exist for example in case of Pellian equations, Runge type equations, Thue equations, elliptic-, hyperelliptic- and superelliptic equations. In what follows we consider problems related to sequences, either to arithmetic sequences/progressions or recurrence sequences. In the literature there are many nice motivating examples, let us mention a few of them. In 1997 Darmon and Merel [47] proved (following Wiles' approach) that there are no 3-term (non-trivial) arithmetic progressions of equal powers greater than two, that is they studied the equation

$$x^n + y^n = 2z^n.$$

Bugeaud, Mignotte and Siksek [35] applied a combination of Baker's method, modular approach and some classical techniques to show that the perfect powers in the Fibonacci sequence are 0,1,8 and 144, and the perfect powers in the Lucas sequence are 1 and 4, that is they considered the Diophantine equations

$$F_{m_1} = x^{n_1} \quad \text{and} \quad L_{m_2} = y^{n_2}.$$

There are two classes of problems we investigate in this thesis. In the first class we have a general family of Diophantine equations and we are interested in solutions coming from a given sequence. In the second class we deal with problems in which the corresponding Diophantine equations contains certain type of sequences. Now we provide detailed descriptions of results related to problems in these ballparks.

An arithmetic progression on a curve $F(x, y) = 0$, is an arithmetic progression in either the x or y coordinates. One can pose the following natural question. What is the longest arithmetic progression in the x coordinates? In case of linear polynomials, Fermat claimed and Euler proved that four distinct squares cannot form an arithmetic progression. Allison [3] found an infinite family of quadratics containing an integral arithmetic progression of length eight and González-Jiménez and Xarles [63] proved that this family has not examples of length

longer than eight. Arithmetic progressions on Pellian equations $x^2 - dy^2 = m$ have been considered by many mathematicians. Dujella, Pethő and Tadić [50] proved that for any four-term arithmetic progression, except $\{0, 1, 2, 3\}$ and $\{-3, -2, -1, 0\}$, there exist infinitely many pairs (d, m) such that the terms of the given progression are y-components of solutions. Pethő and Ziegler [101] dealt with 5-term progressions on Pellian equations. Aguirre, Dujella and Peral [1] constructed 6-term arithmetic progression on Pellian equations parametrized by points on elliptic curve having positive rank. Pethő and Ziegler posed several open problems. One of them is as follows: "Can one prove or disprove that there are d and m with $d > 0$ and not a perfect square such that $y = 1, 3, 5, 7, 9$ are in arithmetic progression on the curve $x^2 - dy^2 = m$?" Recently, González-Jiménez [60] answered the question: there is not m and d not a perfect square such that $y = 1, 3, 5, 7, 9$ are in arithmetic progression on the curve $x^2 - dy^2 = m$. He constructed the related diagonal genus 5 curve and he applied covering techniques and the so-called elliptic Chabauty's method. Bremner [25] provided an infinite family of elliptic curve of Weierstrass form with 8 points in arithmetic progression. González-Jiménez [60] showed that these arithmetic progressions cannot be extended to 9 points arithmetic progressions. Bremner, Silverman and Tzanakis [27] dealt with the congruent number curve $y^2 = x^3 - n^2x$, they considered integral arithmetic progressions. If F is a cubic polynomial, then the problem is to determine arithmetic progressions on elliptic curves. Bremner and Campbell [37] found distinct infinite families of elliptic curves, with arithmetic progression of length eight. Campbell [37] produced infinite families of quartic curves containing an arithmetic progression of length 9. Ulas [140] constructed an infinite family of quartics containing a progression of length 12. Restricting to quartics possessing central symmetry MacLeod [88] discovered four examples of length 14 progressions. Alvarado [4] extended MacLeod's list by determining 11 more examples of length 14 progressions. Moody [92] proved that there are infinitely many Edwards curves with 9 points in arithmetic progression. Bremner [26] and independently González-Jiménez [60, 61] proved using elliptic Chabauty's method that Moody's examples cannot be extended to longer arithmetic progressions. Moody [93] produced six infinite families of Huff curves having the property that each has rational points with x-coordinate $x = -4, -3, \ldots, 3, 4$. That is he obtained arithmetic progressions of length 9. Choudhry [40] improved the result of Moody, he found infinitely many parametrized families of Huff curves on which there are arithmetic progressions of length 9, as well as several Huff curves on which there are arithmetic progressions of length 11. Buchmann and Pethő [32] found an interesting unit in the number field $K = \mathbb{Q}(\alpha)$ with $\alpha^7 - 3 = 0$. The unit is given by

$$10 + 9\alpha + 8\alpha^2 + 7\alpha^3 + 6\alpha^4 + 5\alpha^5 + 4\alpha^6.$$

That is the coordinates $(x_0, \ldots, x_6) \in \mathbb{Z}^7$ of a solution of the norm form equation $N_{K/\mathbb{Q}}(x_0 + x_1\alpha + \ldots + x_6\alpha^6) = 1$ form an arithmetic progression. In [17] Bérczes and Pethő considered

norm form equations

$$N_{K/\mathbb{Q}}(x_0 + x_1\alpha + \ldots + x_{n-1}\alpha^{n-1}) = m \quad \text{in } x_0, x_1, \ldots, x_{n-1} \in \mathbb{Z}, \tag{1.1}$$

where $K = \mathbb{Q}(\alpha)$ is an algebraic number field of degree n, and m is a given integer such that $x_0, x_1, \ldots, x_{n-1}$ are consecutive terms in an arithmetic progression. They proved that (1.1) has only finitely many solutions if neither of the following two cases hold:

- α has minimal polynomial of the form

$$x^n - bx^{n-1} - \ldots - bx + (bn + b - 1)$$

  with $b \in \mathbb{Z}$,
- $\frac{n\alpha^n}{\alpha^n - 1} - \frac{\alpha}{\alpha - 1}$ is a real quadratic number.

In 2006 Bérczes, Pethő and Ziegler [19] studied norm form equations related to Thomas polynomials such that the solutions are coprime integers in arithmetic progression. Bérczes and Pethő [18] considered (1.1) in cases where the defining polynomials of the number fields are given by $x^n - T, (n \geq 3, 4 \leq T \leq 100)$ and $m = 1$. They proved that the norm form equation has no solution in integers which are consecutive elements in an arithmetic progression.

Let us define

$$f(x, k, d) = x(x + d) \cdots (x + (k - 1)d).$$

Erdős [52] and independently Rigge [105] proved that $f(x, k, 1)$ is never a perfect square. A celebrated result of Erdős and Selfridge [53] states that $f(x, k, 1)$ is never a perfect power of an integer, provided $x \geq 1$ and $k \geq 2$. That is, they completely solved the Diophantine equation

$$f(x, k, d) = y^l \tag{1.2}$$

with $d = 1$. The literature of this type of Diophantine equations is very rich. First consider some results related to $l = 2$. Euler proved (see [48] pp. 440 and 635) that a product of four terms in arithmetic progression is never a square solving (1.2) with $k = 4, l = 2$. Obláth [95] obtained a similar statement for $k = 5$. Saradha and Shorey [110] proved that (1.2) has no solutions with $k \geq 4$, provided that d is a power of a prime number. Laishram and Shorey [78] extended this result to the case where either $d \leq 10^{10}$, or d has at most six prime divisors. Bennett, Bruin, Győry and Hajdu [14] solved (1.2) with $6 \leq k \leq 11$ and $l = 2$. Hirata-Kohno, Laishram, Shorey and Tijdeman [73] completely solved (1.2) with $3 \leq k < 110$.

Now assume for this paragraph that $l \geq 3$. Many authors have considered the more general equation

$$f(x, k, d) = by^l, \tag{1.3}$$

where $b > 0$ and the greatest prime factor of b does not exceed k. Saradha [109] proved that (1.3) has no solution with $k \geq 4$. Győry [66] studied the cases $k = 2, 3$, he determined all solutions. Győry, Hajdu and Saradha [68] proved that the product of four or five consecutive terms of an arithmetical progression of integers cannot be a perfect power, provided that the initial term is coprime to the difference. Hajdu, Tengely and Tijdeman [71] proved that the product of k

coprime integers in arithmetic progression cannot be a cube when $2 < k < 39$. Győry, Hajdu and Pintér proved that for any positive integers x, d and k with $\gcd(x, d) = 1$ and $3 < k < 35$, the product $x(x + d) \cdots (x + (k - 1)d)$ cannot be a perfect power.

Erdős and Graham [51] asked if the Diophantine equation

$$\prod_{i=1}^{r} f(x_i, k_i, 1) = y^2$$

has, for fixed $r \geq 1$ and $\{k_1, k_2, \ldots, k_r\}$ with $k_i \geq 4$ for $i = 1, 2, \ldots, r$, at most finitely many solutions in positive integers $(x_1, x_2, \ldots, x_r, y)$ with $x_i + k_i \leq x_{i+1}$ for $1 \leq i \leq r - 1$. Skałba [119] provided a bound for the smallest solution and estimated the number of solutions below a given bound. Ulas [141] answered the above question of Erdős and Graham in the negative when either $r = k_i = 4$, or $r \geq 6$ and $k_i = 4$. Bauer and Bennett [11] extended this result to the cases $r = 3$ and $r = 5$, they also mention the case considered in the present work, it is written that an argument of P. G. Walsh based on the ABC conjecture makes it very likely that in case of $r = 2, k_1 = k_2 = 4$ there are only finitely many solutions. They also pointed out the solution with $x = 33$. Bennett and Van Luijk [16] constructed an infinite family of $r \geq 5$ non-overlapping blocks of five consecutive integers such that their product is always a perfect square. Luca and Walsh [85] studied the case $(r, k_i) = (2, 4)$. They used the identity $(x-1)x(x+1)(x+2) = (x^2+x-1)^2-1$ to reduce the original problem to a Pellian equation

$$(x^2 + x - 1)^2 - dy^2 = 1,$$

where $d > 1$ is a squarefree integer. If (T, U) denotes the minimal solution of the equation $X^2 - dY^2 = 1$, then one obtains that

$$T_i = x^2 + x - 1$$

for some i, where $T_i + U_i\sqrt{d} = (T + U\sqrt{d})^i$. Luca and Walsh conjectures that the equation $T_i = x^2 + x - 1$ implies that $i \in \{1, 2\}$ and $d = 39270$. We note that it corresponds to the solution

$$33 \times 34 \times 35 \times 36 \times 1680 \times 1681 \times 1682 \times 1683 = 3361826160^2,$$

the one appearing in [11].

There are many articles concerning the Diophantine equation

$$R_n = P(x),$$

where R_n is a linear recursive sequence and $P \in \mathbb{Z}[X]$ is a polynomial. Several papers have been published identifying perfect powers, products of consecutive integers, binomial coefficients, figurate numbers and power sums in the Fibonacci, Lucas, Pell and associated Pell sequences.

These binary recurrence sequences are defined by

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 2,$$
$$L_0 = 2, \quad L_1 = 1, \quad L_n = L_{n-1} + L_{n-2} \text{ for } n \geq 2,$$
$$P_0 = 0, \quad P_1 = 1, \quad P_n = 2P_{n-1} + P_{n-2} \text{ for } n \geq 2,$$
$$Q_0 = 1, \quad Q_1 = 1, \quad Q_n = 2Q_{n-1} + Q_{n-2} \text{ for } n \geq 2.$$

It follows from a result by Ljunggren [82] that the only squares in the Fibonacci sequence are $F_0 = 0, F_1 = F_2 = 1, F_{12} = 144$. Later it was rediscovered by Cohn [42, 43] and Wyler [147]. Alfred [2] and Cohn [44] determined the perfect squares in the Lucas sequence. In case of the Pell sequence Pethő [99] and independently Cohn [45] obtained the complete list of perfect squares. London and Finkelstein [83] and Pethő [97] proved that the only cubes in the Fibonacci sequence are $F_0 = 0, F_1 = F_2 = 1$ and $F_6 = 8$. London and Finkelstein [83] also showed the the only cube in the Lucas sequence is 1. Higher powers were determined by Pethő [98]. Bugeaud, Mignotte and Siksek [35] applied a combination of Baker's method, modular approach and some classical techniques to show that the perfect powers in the Fibonacci sequence are 0,1,8 and 144, and the perfect powers in the Lucas sequence are 1 and 4.

Another interesting problem is to determine triangular numbers, numbers of the form $T_x = \frac{x(x+1)}{2}$ in binary recurrence sequences. Ming [86] proved that the only triangular numbers in the Fibonacci sequence are $F_0 = 0, F_1 = F_2 = 1, F_4 = 3, F_8 = 21$ and $F_{10} = 55$. It was shown by Ming [87] that $L_1 = 1, L_2 = 3$ and $L_{18} = 5778$ are the triangular numbers in the Lucas sequence. In case of the Pell sequence McDaniel [91] proved that the only triangular number is 1. Since $T_x = \binom{x}{2}$, it was a natural question to ask for all solutions of the Diophantine equations

$$F_n = \binom{x}{k}, \quad L_n = \binom{x}{k},$$
$$P_n = \binom{x}{k}, \quad Q_n = \binom{x}{k}.$$

It was Szalay [130] who solved the equations $F_n, L_n, P_n = \binom{x}{3}$. Later Szalay [129] also treated the equations $F_n, L_n = \binom{x}{3}$ and $F_n, L_n, P_n = \sum_{i=1}^{x} i^3$. Kovács [77] solved completely some related combinatorial Diophantine equations, e.g.

$$P_n = \binom{x}{4}$$

and

$$F_n = \Pi_4(x) = x(x+1)(x+2)(x+3).$$

Tengely [133] determined the g-gonal numbers in the Fibonacci, Lucas, Pell and associated Pell sequences for $g \leq 20$, where the m-th g-gonal number is defined by

$$\frac{m\left((g-2)m - (g-4)\right)}{2}.$$

In case of genus 2 curves there are two methods to compute the complete set of integral solutions if the rank of the Mordell-Weil group of the curve is larger. One such method is due to Bugeaud,

Mignotte, Siksek, Stoll and Tengely [36], it combines Baker's method and the so-called Mordell-Weil sieve. A different approach is the hyperelliptic logarithm method developed by Gallegos-Ruiz [56]. These methods have been applied to combinatorial Diophantine equations that reduce to genus 2 curves having Mordell-Weil ranks at least 3, see e.g. [57, 134, 135]. As a concrete example consider binomial near collisions. Blokhuis, Brouwer and de Weger [22] provided the following identities

$$\binom{10}{5}+1=\binom{23}{2}, \quad \binom{22}{5}+1=\binom{230}{2}, \quad \binom{62}{5}+1=\binom{3598}{2}$$

in these cases the problem can be reduced to genus 2 curves. Motivated by the above examples Gallegos-Ruiz, Katsipis, Tengely and Ulas [57] determined the complete set of integral solutions of the equation

$$\binom{n}{2}=\binom{m}{5}+d, \text{ with } -3\leq d\leq 3.$$

If $d=3$, then the rank of the Mordell-Weil group is 6 and the non-trivial solutions with $n\geq 5$ are as follows

$$\begin{aligned}
\binom{11}{5}+3 &= \binom{31}{2},\\
\binom{16}{5}+3 &= \binom{94}{2},\\
\binom{375}{5}+3 &= \binom{346888}{2},\\
\binom{379}{5}+3 &= \binom{356263}{2}.
\end{aligned}$$

The rank of the Mordell-Weil group is also 6 if $d=1$. In this case the non-trivial solutions are as follows

$$\begin{aligned}
\binom{10}{5}+1 &= \binom{23}{2},\\
\binom{22}{5}+1 &= \binom{230}{2},\\
\binom{62}{5}+1 &= \binom{3598}{2},\\
\binom{135}{5}+1 &= \binom{26333}{2},\\
\binom{139}{5}+1 &= \binom{28358}{2}.
\end{aligned}$$

Part II

Sequences in solution sets

dc_1892_21

Chapter 2 Norm form equations and arithmetic progressions

2.1 A problem of Pethő

In 2010 Pethő [96] collected 15 problems in number theory, Problem 6 is based on the results given in [17].

Problem 2.1. (Problem 6 in [96]): Does there exist infinitely many quartic algebraic integers α such that

$$\frac{4\alpha^4}{\alpha^4-1}-\frac{\alpha}{\alpha-1}$$

is a quadratic algebraic number?

The only example mentioned is $x^4+2x^3+5x^2+4x+2$ such that the corresponding element is a real quadratic number (that is a root of x^2-4x+2). Moreover, Bérczes, Pethő in [17] remark that there are many solutions if we drop assumption of integrality of α. As we will see the problem in this case is equivalent to the study of existence of rational zeros of family of four polynomials in six variables. Using Gröbner bases techniques we reduce our problem to the study of rational zeros of only one (reducible) polynomial. A careful analysis of the corresponding variety allow us to get 2 infinite families of quartic polynomials defining quartic algebraic integers such that the algebraic number $\frac{4\alpha^4}{\alpha^4-1}-\frac{\alpha}{\alpha-1}$ is quadratic. Unfortunately, in this case we get real quadratic number only in finitely many cases. However, we are able to show that the set of quartic algebraic numbers such that the algebraic number $\frac{4\alpha^4}{\alpha^4-1}-\frac{\alpha}{\alpha-1}$ is quadratic, is contained in a certain set given by (explicit) system of algebraic inequalities.

In particular the following is true:

Theorem 2.1

There are infinitely many quartic algebraic integers defined by $\alpha^4+a\alpha^3+b\alpha^2+c\alpha+d=0$ *for which*

$$\beta=\frac{4\alpha^4}{\alpha^4-1}-\frac{\alpha}{\alpha-1}$$

is a quadratic algebraic number. Moreover, there are infinitely many quartic algebraic numbers α *such that* β *is real quadratic.*

2.2 Auxiliary results

We provide two families with infinitely many quadratic polynomials, and we prove that each of these families contains infinitely many irreducible polynomials.

Lemma 2.1

Let $t \in \mathbb{Z}$. The polynomials defined by

$$f_1(x) = x^4 + 2x^3 + (2t^2+2)x^2 + (4t^2 - 4t + 2)x + 6t^2 - 4t + 1$$

are irreducible over $\mathbb{Q}$ if and only if $t \notin \{0, 1\}$.

Proof. If there is a linear factor of f_1, then there is an integral root. Hence we have that

$$f_1(x) = (x + s_1)(x^3 + s_2x^2 + s_3x + s_4).$$

By comparing coefficients one gets that

$$\begin{aligned} -s_1 - s_2 + 2 &= 0 \\ -s_1s_2 + 2t^2 - s_3 + 2 &= 0 \\ -s_1s_3 + 4t^2 - s^4 - 4t + 2 &= 0 \\ -s_1s_4 + 6t^2 - 4t + 1 &= 0. \end{aligned}$$

Solving for s_2, and s_3 from the first two equations and substituting in the others, we get

$$\begin{aligned} -s_1s_4 + 6t^2 - 4t + 1 &= 0 \\ -s_1^3 - 2s_1t^2 + 2s_1^2 + 4t^2 - 2s_1 - s_4 - 4t + 2 &= 0. \end{aligned}$$

The resultant of the two polynomials with respect to s_4 is quadratic in t. The discriminant of this quadratic polynomial is

$$(-8)(s_1 - 1)^2(s_1^4 - 2s_1^3 + 4s_1^2 - 2s_1 + 1).$$

If $s_1 = 1$, then we obtain that $t = 0$. In this case $f_1(x) = (x+1)^2(x^2+1)$ is reducible. If $s_1 \neq 1$, then $-2(s_1^4 - 2s_1^3 + 4s_1^2 - 2s_1 + 1) = U^2$, since to get an integral t the discriminant has to be a square. This equations has no rational solution since $-2(s_1^4 - 2s_1^3 + 4s_1^2 - 2s_1 + 1) < 0$ for all $s_1 \in \mathbb{Q}$. If there are two quadratic factors, then

$$f_1(x) = (x^2 + s_1x + s_2)(x^2 + s_3x + s_4).$$

As in the previous case we compare coefficients to obtain a system of equations

$$\begin{aligned} -s_1^2s_2 - 2s_2t^2 + 2s_1s_2 + s_2^2 + 6t^2 - 2s_2 - 4t + 1 &= 0 \\ -s_1^3 - 2s_1t^2 + 2s_1^2 + 2s_1s_2 + 4t^2 - 2s_1 - 2s_2 - 4t + 2 &= 0. \end{aligned}$$

The resultant of the above equations with respect to s_2 is

$$(-1)(s_1^2 + 2t^2 - 2s_1 - 4t + 2)(s_1^4 + 2s_1^2t^2 - 4s_1^3 + 4s_1^2t - 4s_1t^2 + 6s_1^2 - 8s_1t - 4s_1 + 8t).$$

If $s_1^2 + 2t^2 - 2s_1 - 4t + 2 = 0$, then we have a quadratic polynomial in t with discriminant $-8s_1^2 + 16s_1$. It is non-negative if $s_1 \in \{0, 1, 2\}$. If $s_1 \in \{0, 1, 2\}$, then $t = 0$ or $t = 1$. Earlier we handled the case with $t = 0$, if $t = 1$, then we have $f_1(x) = (x^2+1)(x^2+2x+3)$.

If $s_1^4 + 2s_1^2t^2 - 4s_1^3 + 4s_1^2t - 4s_1t^2 + 6s_1^2 - 8s_1t - 4s_1 + 8t = 0$, then the discriminant with respect to t is

$$(-8)(s_1^2 - 2s_1 + 2)(s_1^4 - 4s_1^3 + 2s_1^2 + 4s_1 - 4).$$

It remains to determine the rational points on the genus 2 curve

$$C:\ (-8)(s_1^2-2s_1+2)(s_1^4-4s_1^3+2s_1^2+4s_1-4)=U^2.$$

If $s_1 \notin [-1,3]$ then the left hand side is negative, hence there are no rational points (s_1,U) on C with $s_1 \in \mathbb{Z}$. As s_1 is an integer, it can take only the values $-1,0,1,2,3$. The values $0,1,2$ were considered earlier. If $s_1=-1$ or 3, then the left hand side of C is 40, which is not a square.

Lemma 2.2

Let $t \in \mathbb{Z}$. The polynomials defined by

$$f_2(x)=x^4+2tx^3+(t^2+2t+2)x^2+(2t^2+2t)x+3t^2-2t+1$$

are irreducible over $\mathbb{Q}$ if and only if $t \notin \{0,2\}$.

Proof. The approach we apply here is similar to that used in the proof of the previous lemma, therefore here we only indicate the main steps. First we try to determine linear factors, that we write

$$f_2(x)=(x+s_1)(x^3+s_2x^2+s_3x+s_4).$$

By comparing coefficients one gets that

$$\begin{aligned}
-s_1-s_2+2t &= 0\\
-s_1s_2+t^2-s_3+2t+2 &= 0\\
-s_1s_3+2t^2-s_4+2t &= 0\\
-s_1s_4+3t^2-2t+1 &= 0.
\end{aligned}$$

Solving for s_2, and s_3 from the first two equations and substituting in the others, we get

$$\begin{aligned}
-s_1s_4+3t^2-2t+1 &= 0\\
-s_1^3+2s_1^2t-s_1t^2-2s_1t+2t^2-2s_1-s_4+2t &= 0.
\end{aligned}$$

The resultant of the two polynomials with respect to s_4 is quadratic in t. The discriminant of this quadratic polynomial is

$$(-8)(s_1^4-2s_1^3+4s_1^2-2s_1+1).$$

This expression is negative for all rational s_1, hence there exists no rational solution in t.

If there are two quadratic factors, then

$$f_2(x)=(x^2+s_1x+s_2)(x^2+s_3x+s_4).$$

As in the previous case we compare coefficients to obtain a system of equations

$$\begin{aligned}
-s_1^2s_2+2s_1s_2t-s_2t^2+s_2^2-2s_2t+3t^2-2s_2-2t+1 &= 0\\
-s_1^3+2s_1^2t-s_1t^2+2s_1s_2-2s_1t-2s_2t+2t^2-2s_1+2t &= 0.
\end{aligned}$$

The latter equation can be written as

$$(-1)(-s_1+t)(-s_1^2+s_1t+2s_2-2t-2)=0.$$

If $s_1 = t$, then $s_2^2 - 2s_2t + 3t^2 - 2s_2 - 2t + 1 = 0$. The discriminant of this equation with respect to s_2 is $(-8)t(t-2)$. Hence $t \in \{0, 2\}$. If $t = 0$, then $f_2(x) = (x^2+1)^2$. If $t = 2$, then $f_2(x) = (x^2+2x+3)^2$. Consider the case $-s_1^2 + s_1t + 2s_2 - 2t - 2 = 0$. We get that $s_2 = \frac{s_1^2 - s_1t + 2t + 2}{2}$. Thus we obtain a polynomial equation only in s_1 and t given by

$$(1/4)(-s_1^4 + 4s_1^3t - 5s_1^2t^2 + 2s_1t^3 - 4s_1^2t + 8s_1t^2 - 4t^3 - 4s_1^2 + 8s_1t + 4t^2 - 16t) = 0.$$

The discriminant with respect to s_1 factors as follows

$$(-1/32)t(t-2)(t^4 - 8t^3 + 40t^2 - 32t + 16)^2.$$

The latter expression is a square only if $t = 0$ or $t = 2$, so we do not get new reducible polynomials.

2.3 Proof of Theorem 2.1

Proof. Let $f(x) = x^4 + ax^3 + bx^2 + cx + d$ with $a, b, c, d \in \mathbb{Z}$ be an irreducible polynomial in $\mathbb{Z}[x]$ and $g(x) = x^2 + px + q$ with $p, q \in \mathbb{Q}$. Assume that α is a root of $f(x)$ and $\beta = \frac{4\alpha^4}{\alpha^4-1} - \frac{\alpha}{\alpha-1}$ is a root of $g(x)$. From $g(\beta) = 0$ we get a degree 6 polynomial for which α is a root. Therefore it is divisible by $f(x)$. Computing the reminder we obtain a cubic polynomial $e_1 + e_2x + e_3x^2 + e_4x^3$ which has to be zero. The coefficients $e_1, \ldots, e_4$ are as follows:

$$\begin{aligned}
e_1 :\quad & -3dpa^2 + 5dpa + 3dpb - 6dp - dqa^2 + 2dqa + dqb - 3dq - 9da^2 + 12da + 9db - 10d + q,\\
e_2 :\quad & 3dpa - 5dp + dqa - 2dq + 9da - 12d - 3pa^2c + 5pac + 3pbc - 6pc + p - qa^2c + 2qac +\\
& +qbc - 3qc + 2q - 9a^2c + 12ac + 9bc - 10c,\\
e_3 :\quad & -3dp - dq - 9d - 3pa^2b + 5pab + 3pac + 3pb^2 - 6pb - 5pc + 3p - qa^2b + 2qab + qac +\\
& +qb^2 - 3qb - 2qc + 3q - 9a^2b + 12ab + 9ac + 9b^2 - 10b - 12c + 1,\\
e_4 :\quad & -3pa^3 + 5pa^2 + 6pab - 6pa - 5pb - 3pc + 6p - qa^3 + 2qa^2 + 2qab - 3qa - 2qb - qc + 4q -\\
& -9a^3 + 12a^2 + 18ab - 10a - 12b - 9c + 4.
\end{aligned}$$

The Gröbner basis (with respect to the lex ordering $d > p > q > a > b > c$, the ordering used throughout the section) for $< e_1, e_2, e_3, e_4 >$ contains 19 polynomials. An element of this basis factors as follows

$$\begin{aligned}
&\left(\frac{1}{233}\right) \cdot (a - 2b + c) \cdot\\
&\cdot(233a^4 - 352a^3b + 108a^3c + 168a^3 + 368a^2b^2 - 264a^2bc -\\
&-624a^2b + 46a^2c^2 - 184a^2c - 544a^2 - 160ab^3 + 128ab^2c +\\
&352ab^2 - 16abc^2 + 64abc + 128ab - 4ac^3 - 8ac^2 + 768ac +\\
&+640a + 48b^4 - 64b^3c - 256b^3 + 32b^2c^2 + 288b^2c + 384b^2 -\\
&-8bc^3 - 144bc^2 - 512bc + c^4 + 24c^3 + 96c^2 - 640c - 256).
\end{aligned}$$

Let us consider the case $c = 2b - a$. Denote by $e_{1,c}, e_{2,c}, e_{3,c}, e_{4,c}$ the polynomials obtained by substituting $c = 2b - a$ into e_1, e_2, e_3 and e_4. Let us denote by G_c the Gröbner basis for

$< e_{1,c}, e_{2,c}, e_{3,c}, e_{4,c} >$ and compute the ideal $I_{c,p,q} =< G_c > \cap \mathbb{Q}[a,b,d]$, i.e., we eliminate the variables p, q. We get that

$$I_{c,p,q} =< (9b - 12a - 3d + 5)^2 - 4(3a-2)^2 + 48d > .$$

The equation $(9b - 12a - 3d + 5)^2 - 4(3a-2)^2 + 48d = 0$ defines a curve, say C, defined over $\mathbb{Q}(a)$ of genus 0 (in the plane (b,d), the conic is irreducible, the determinant of the matrix of the conic is -46656). The standard method allows us to find the parametrization of C in the following form

$$b = \frac{1}{36}(9a^2 + 36a - 16 - 8u - u^2), \quad d = \frac{1}{36}(9a^2 + 36a - 16 + 8u - u^2).$$

However, with b, d given above and the corresponding $c = 2b - a$ we get

$$f(x) = \frac{1}{36}(6x + u + 3a - 2)\left(6x^3 + (3a - u + 2)x^2 + 2(3a - u - 1)x + 3(3a - u - 2)\right),$$

a reducible polynomial.

Let us consider the second factor that is

$$\begin{aligned} F(a,b,c) \;=\; & 233a^4 - 352a^3b + 108a^3c + 168a^3 + 368a^2b^2 - 264a^2bc - \\ & -624a^2b + 46a^2c^2 - 184a^2c - 544a^2 - 160ab^3 + 128ab^2c + \\ & 352ab^2 - 16abc^2 + 64abc + 128ab - 4ac^3 - 8ac^2 + 768ac + \\ & +640a + 48b^4 - 64b^3c - 256b^3 + 32b^2c^2 + 288b^2c + 384b^2 - \\ & -8bc^3 - 144bc^2 - 512bc + c^4 + 24c^3 + 96c^2 - 640c - 256. \end{aligned} \tag{2.1}$$

First we compute the polynomial for some small fixed values of a. It turns out that $F(2,b,c)$ is a reducible polynomial given by

$$(12b^2 - 4bc - 96b + c^2 + 12c + 196)(4b^2 - 4bc - 16b + c^2 + 4c + 20).$$

Let us study this special case when $a = 2$. Consider the equation $12b^2 - 4bc - 96b + c^2 + 12c + 196 = 0$. It follows that $(c - 2b + 6)^2 + 2(2b - 9)^2 = 2$. The only integral solutions correspond with $b = 4$ or $b = 5$. If $b = 4$, then $c = 2$ and $d = 3$. We obtain the reducible polynomial $x^4 + 2x^2 + 4x^2 + 2x + 3 = (x^2 + 1)(x^2 + 2x + 3)$. If $b = 5$, then it follows that $c = 4$ and $d = 2$, so we get the polynomial $x^4 + 2x^3 + 5x^2 + 4x + 2$. It is the polynomial that also appears in Pethő's paper. The set of rational solutions of $(c - 2b + 6)^2 + 2(2b - 9)^2 = 2$ can be easily parametrized with

$$b = \frac{8t^2 + 5}{2t^2 + 1}, \quad c = \frac{4(t^2 - t + 1)}{2t^2 + 1}.$$

With $a = 2$ and b, c given above we easily compute the values

$$\begin{aligned} d &= \frac{2\left(3t^2 - 2t + 1\right)}{2t^2 + 1}, \\ p &= \frac{4\left(2t^3 - 5t^2 + t - 1\right)}{4t^2 + 1}, \\ q &= -\frac{2(4t - 1)\left(3t^2 - 2t + 1\right)}{4t^2 + 1}. \end{aligned}$$

With p, q given above one can easily check that the discriminant of $x^2 + px + q$ is positive for

all $t \in \mathbb{R}$ (and thus for all $t \in \mathbb{Q}$).

Consider the other possibility, that is the equation $4b^2 - 4bc - 16b + c^2 + 4c + 20 = 0$. We have

$$(2b - c)^2 + 20 = 4(4b - c).$$

Let $u = 2b - c$ and $v = 4b - c$. We get that $v = \frac{u^2+20}{4}$ and $b = \frac{u^2-4u+20}{8}, c = \frac{u^2-8u+20}{4}$. Thus

$$\begin{aligned} b &= 2t^2 + 2, \\ c &= 4t^2 - 4t + 2, \end{aligned}$$

where $u = 4t + 2$. Let us denote by e'_1, e'_2, e'_3 and e'_4 the corresponding polynomials e_1, e_2, e_3 and e_4 after the substitution $a = 2, b = 2t^2 + 2, c = 4t^2 - 4t + 2$. Let G' be the Gröbner basis of the ideal $< e'_1, e'_2, e'_3, e'_4 >$ with respect to the variables d, p, q over polynomial ring $\mathbb{Q}[t]$. We get that

$$< G' > \cap\ \mathbb{Q}[t][d] = \\ < t(d - 1 + 4t - 6t^2)(t^3 + t^2 - t - 2), (d - 1 + 4t - 6t^2)(7 + d + 12t - 6t^2 - 8t^3) >$$

and thus $d = 6t^2 - 4t + 1$ or $t = 0$.

If $t = 0$, then $d = -7$ and $f(x)$ is reducible $x^4 + 2x^3 + 2x^2 + 2x - 7 = (x - 1)(x^3 + 3x^2 + 5x + 7)$, a contradiction. If $d = 6t^2 - 4t + 1$, then we have an infinite family of solutions of Pethő's question given by

$$\begin{aligned} a &= 2, \\ b &= 2t^2 + 2, \\ c &= 4t^2 - 4t + 2, \\ d &= 6t^2 - 4t + 1, \\ p &= -\frac{6\,t^2 - 6\,t + 1}{t^2 - t}, \\ q &= \frac{18\,t^3 - 18\,t^2 + 7\,t - 1}{2\,(t^3 - t^2)}. \end{aligned}$$

It follows from Lemma 2.1 that there are infinitely many irreducible polynomials in this family. By computing the discriminant of the polynomial $x^2 + px + q$ we observe that it has two real roots for $t \in \mathbb{Q}$ satisfying $t \in (1 - \sqrt{2}/2, 1 + \sqrt{2}/2) \setminus \{1\}$.

We computed all integral solutions of the equation $F(a, b, c)$ with $-200 \leq a, b \leq 200$. If $a = 2$, then we have all solutions provided by the above formulas and we also obtain $a = b = c = 2$ and $d = -7$. The corresponding polynomial is reducible, it is $(x - 1)(x^3 + 3x^2 + 5x + 7)$.

The remaining solutions are contained in the following table.

$(-30, 197, 420, 706)$	$(-12, 26, 60, 121)$	$(6, 17, 24, 22)$
$(-28, 170, 364, 617)$	$(-10, 17, 40, 86)$	$(8, 26, 40, 41)$
$(-26, 145, 312, 534)$	$(-8, 10, 24, 57)$	$(10, 37, 60, 66)$
$(-24, 122, 264, 457)$	$(-6, 5, 12, 34)$	$(12, 50, 84, 97)$
$(-22, 101, 220, 386)$	$(-4, 2, 4, 17)$	$(14, 65, 112, 134)$
$(-20, 82, 180, 321)$	$(-2, 1, 0, 6)$	$(16, 82, 144, 177)$
$(-18, 65, 144, 262)$	$(0, 2, 0, 1)$	$(18, 101, 180, 226)$
$(-16, 50, 112, 209)$	$(2, 5, 4, 2)$	
$(-14, 37, 84, 162)$	$(4, 10, 12, 9)$	

Integral solutions of the equation $F(a, b, c)$ with $-200 \le a, b \le 200$.

All these solutions can be described by the formulas

$$\begin{aligned} a &= 2t, \\ b &= t^2 + 2t + 2, \\ c &= 2t^2 + 2t, \\ d &= 3t^2 - 2t + 1, \\ p &= -\frac{2\left(3\,t^2 - 5\,t + 4\right)}{t^2 - 2\,t + 2}, \\ q &= \frac{9\,t^3 - 12\,t^2 + 7\,t - 2}{t^3 - 2\,t^2 + 2\,t}. \end{aligned} \tag{2.2}$$

It follows from Lemma 2.2 that there are infinitely many irreducible polynomials in this family. By computing the discriminant of the polynomial $x^2 + px + q$ we observe that it has two real roots for $t \in \mathbb{Q}$ satisfying $t \in (0, 2)$.

Remark. We extended the search of the solutions of $F(a, b, c) = 0$ up to $-10^4 \le a, b \le 10^4$ and found no additional solutions.

Remark. One can prove that the polynomial $f(x) = x^4 + ax^3 + bx^2 + cx + d$ with

$$a = 2, \quad b = \frac{8t^2 + 5}{2t^2 + 1}, \quad c = \frac{4(t^2 - t + 1)}{2t^2 + 1}, \quad d = \frac{2\left(3t^2 - 2t + 1\right)}{2t^2 + 1}.$$

has no rational roots for all $t \in \mathbb{Q}$. However, if $t = (2 - s^2)/(4s)$, where $s \in \mathbb{Q} \setminus \{0\}$, then

$$f(x) = \left(x^2 + \frac{4}{s^2 + 2}x + \frac{s^2 + 4s + 6}{s^2 + 2}\right)\left(x^2 + \frac{2s^2}{s^2 + 2}x + \frac{3s^2 - 4s + 2}{s^2 + 2}\right).$$

Let $\mathbb{P}$ be the set of prime numbers, $S \subset \mathbb{P} \cup \{\infty\}$, and recall that a rational number $r = r_1/r_2 \in \mathbb{Q}, \gcd(r_1, r_2) = 1$, is called S-integral if the set of prime factors of r_2 is a subset of S. For given S, the set of S-integers is denoted by $\mathbb{Z}_S$.

Although we were unable to prove that there are infinitely many quartic algebraic integers α such that the number $\beta = 4\alpha^4/(1 - \alpha^4) - \alpha/(\alpha - 1)$ is real quadratic, from our result we can deduce the following:

Corollary 2.1

Let $S \subset \mathbb{P}$. Then there are infinitely many $a, b, c, d \in \mathbb{Z}_S$ such that for one of the roots of $x^4 + ax^3 + bx^2 + cx + d = 0$, say α, the number β is real quadratic.

Proof. In order to get the result it is enough to use the parametrization (2.2) by taking $t \in \mathbb{Z}_S$ satisfying the condition $t \in (0, 2)$. Because there are infinitely many such t's we get the result.

Remark. As an immediate implication of the above result we get that if $t = \frac{2m+1}{2^n}$ for some $m, n \in \mathbb{N}$ satisfying $0 < m \leq 2^n - 1$, then there is a root α of the corresponding quartic $x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}_S[x]$, with a, b, c, d given by (2.2) and such that $\beta = 4\alpha^4/(\alpha^4 - 1) - \alpha/(\alpha - 1)$ is real quadratic. It is quite interesting that in this case (and in fact for any non-empty set $S \subset \mathbb{P}$) we get positive solution of Pethő's problem, where the phrase *quartic algebraic integer* α is replaced by *quartic algebraic S-integer* α (in the sense that α is a zero of a monic polynomial with coefficient in $\mathbb{Z}_S$).

Remark. Let us note that the equation $F(a, b, c) = 0$, where F is given by (2.1), defines (an affine) quartic surface, say V. The existence of the parametric solution presented above leads to the generic point (by taking $t = a/2$):

$$(a, b, c) = \left(a, \frac{a^2}{4} + a + 2, \frac{a^2}{2} + a\right)$$

lying on V. This suggest to consider V as a *quartic curve* defined over the rational function field $\mathbb{Q}(a)$. We call this curve $\mathcal{C}$. A quick computation in MAGMA [23] reveals that the genus of $\mathcal{C}$ is 0. This implies that $\mathcal{C}$ is $\overline{\mathbb{Q}(a)}$-rational curve. Moreover, the existence of a $\mathbb{Q}(a)$-rational point on $\mathcal{C}$ given by $P = \left(\frac{a^2}{4} + a + 2, \frac{a^2}{2} + a\right)$ allows us to compute rational parametrization which is defined over $\mathbb{Q}(a)$ as follows

$$\begin{aligned} b(t) &= \frac{\sum_{i=0}^{6} bn_i(t)a^i}{\sum_{i=0}^{4} bd_i(t)a^i}, \\ c(t) &= \frac{\sum_{i=0}^{6} cn_i(t)a^i}{\sum_{i=0}^{4} cd_i(t)a^i}, \\ d(t) &= \frac{\sum_{i=0}^{6} dn_i(t)a^i}{\sum_{i=0}^{4} dd_i(t)a^i}. \end{aligned}$$

where $t \in \mathbb{Q}$ and $bn_i(t), bd_i(t)$ are given by

i	$bn_i(t)$	$bd_i(t)$
0	$663552\,t^4 - 2211840\,t^3 + 2764800\,t^2 - 1536000\,t + 320000$	$331776\,t^4 - 1105920\,t^3 + 1382400\,t^2 - 768000\,t + 160000$
1	$-331776\,t^4 + 1050624\,t^3 - 1244160\,t^2 + 652800\,t - 128000$	$-331776\,t^4 + 1050624\,t^3 - 1244160\,t^2 + 652800\,t - 128000$
2	$-41472\,t^3 + 105984\,t^2 - 90240\,t + 25600$	$124416\,t^4 - 373248\,t^3 + 419328\,t^2 - 209280\,t + 39200$
3	$38016\,t^3 - 89280\,t^2 + 69696\,t - 18080$	$-20736\,t^4 + 58752\,t^3 - 62784\,t^2 + 30048\,t - 5440$
4	$12960\,t^4 - 47520\,t^3 + 62928\,t^2 - 36240\,t + 7748$	$1296\,t^4 - 3456\,t^3 + 3528\,t^2 - 1632\,t + 288$
5	$-3888\,t^4 + 11664\,t^3 - 13248\,t^2 + 6792\,t - 1332$	0
6	$324\,t^4 - 864\,t^3 + 900\,t^2 - 432\,t + 81$	0

$cn_i(t)$ and $cd_i(t)$ are as follows

i	$cn_i(t)$	$cd_i(t)$
0	0	$165888\,t^4 - 552960\,t^3 + 691200\,t^2 - 384000\,t + 80000$
1	$165888\,t^4 - 552960\,t^3 + 691200\,t^2 - 384000\,t + 80000$	$-165888\,t^4 + 525312\,t^3 - 622080\,t^2 + 326400\,t - 64000$
2	$-82944\,t^4 + 235008\,t^3 - 241920\,t^2 + 105600\,t - 16000$	$62208\,t^4 - 186624\,t^3 + 209664\,t^2 - 104640\,t + 19600$
3	$-20736\,t^4 + 86400\,t^3 - 126720\,t^2 + 79296\,t - 18080$	$-10368\,t^4 + 29376\,t^3 - 31392\,t^2 + 15024\,t - 2720$
4	$20736\,t^4 - 66528\,t^3 + 79920\,t^2 - 42744\,t + 8620$	$648\,t^4 - 1728\,t^3 + 1764\,t^2 - 816\,t + 144$
5	$-4536\,t^4 + 13176\,t^3 - 14580\,t^2 + 7308\,t - 1404$	0
6	$324\,t^4 - 864\,t^3 + 900\,t^2 - 432\,t + 81$	0

$dn_i(t)$ and $dd_i(t)$ are given by

i	$cn_i(t)$	$cd_i(t)$
0	$331776\,t^4 - 1105920\,t^3 + 1382400\,t^2 - 768000\,t + 160000$	$331776\,t^4 - 1105920\,t^3 + 1382400\,t^2 - 768000\,t + 160000$
1	$-663552\,t^4 + 2211840\,t^3 - 2764800\,t^2 + 1536000\,t - 320000$	$-331776\,t^4 + 1050624\,t^3 - 1244160\,t^2 + 652800\,t - 128000$
2	$705024\,t^4 - 2350080\,t^3 + 2939904\,t^2 - 1635840\,t + 341600$	$124416\,t^4 - 373248\,t^3 + 419328\,t^2 - 209280\,t + 39200$
3	$-393984\,t^4 + 1271808\,t^3 - 1540224\,t^2 + 829536\,t - 167680$	$-20736\,t^4 + 58752\,t^3 - 62784\,t^2 + 30048\,t - 5440$
4	$115344\,t^4 - 353376\,t^3 + 407880\,t^2 - 210624\,t + 41148$	$1296\,t^4 - 3456\,t^3 + 3528\,t^2 - 1632\,t + 288$
5	$-16848\,t^4 + 48384\,t^3 - 52992\,t^2 + 26304\,t - 5004$	0
6	$972\,t^4 - 2592\,t^3 + 2700\,t^2 - 1296\,t + 243$	0

The above parametrizations yield formulas for p and q as well, we have

$$p(t) = \frac{\sum_{i=0}^{8} pn_i(t)a^i}{\sum_{i=0}^{8} pd_i(t)a^i},$$

$$q(t) = \frac{\sum_{i=0}^{8} qn_i(t)a^i}{\sum_{i=0}^{8} qd_i(t)a^i},$$

where $pn_i(t)$ and $pd_i(t)$ are as follows

i	$pn_i(t)$
0	$-764411904\,t^6 + 3853910016\,t^5 - 8095334400\,t^4 + 9068544000\,t^3 - 5713920000\,t^2 + 1920000000\,t - 268800000$
1	$1624375296\,t^6 - 8066138112\,t^5 + 16689659904\,t^4 - 18417991680\,t^3 + 11433369600\,t^2 - 3785472000\,t + 522240000$
2	$-1576599552\,t^6 + 7711801344\,t^5 - 15724855296\,t^4 + 17109688320\,t^3 - 10477670400\,t^2 + 3424128000\,t - 466560000$
3	$901767168\,t^6 - 4328681472\,t^5 + 8665989120\,t^4 - 9262688256\,t^3 + 5575491072\,t^2 - 1792177920\,t + 240364800$
4	$-328458240\,t^6 + 1538403840\,t^5 - 3007901952\,t^4 + 3143418624\,t^3 - 1852477056\,t^2 + 583908864\,t - 76936320$
5	$77262336\,t^6 - 350884224\,t^5 + 666600192\,t^4 - 678507840\,t^3 + 390510720\,t^2 - 120573504\,t + 15612432$
6	$-11384064\,t^6 + 49828608\,t^5 - 91598688\,t^4 + 90593856\,t^3 - 50882400\,t^2 + 15399264\,t - 1963512$
7	$956448\,t^6 - 4012416\,t^5 + 7116336\,t^4 - 6832512\,t^3 + 3747096\,t^2 - 1113696\,t + 140292$
8	$-34992\,t^6 + 139968\,t^5 - 239112\,t^4 + 222912\,t^3 - 119556\,t^2 + 34992\,t - 4374$

i	$pd_i(t)$
0	$191102976\,t^6 - 955514880\,t^5 + 1990656000\,t^4 - 2211840000\,t^3 + 1382400000\,t^2 - 460800000\,t + 64000000$
1	$-382205952\,t^6 + 1879179264\,t^5 - 3849928704\,t^4 + 4206919680\,t^3 - 2586009600\,t^2 + 847872000\,t - 115840000$
2	$346374144\,t^6 - 1676132352\,t^5 + 3381460992\,t^4 - 3640578048\,t^3 + 2206264320\,t^2 - 713625600\,t + 96256000$
3	$-185131008\,t^6 + 879869952\,t^5 - 1744478208\,t^4 + 1847079936\,t^3 - 1101689856\,t^2 + 351010560\,t - 46678400$
4	$63452160\,t^6 - 294865920\,t^5 + 572209920\,t^4 - 593720064\,t^3 + 347511168\,t^2 - 108828288\,t + 14251040$
5	$-14183424\,t^6 + 64074240\,t^5 - 121124160\,t^4 + 122713920\,t^3 - 70316928\,t^2 + 21620544\,t - 2788424$
6	$2006208\,t^6 - 8755776\,t^5 + 16052256\,t^4 - 15836256\,t^3 + 8873352\,t^2 - 2679360\,t + 340884$
7	$-163296\,t^6 + 684288\,t^5 - 1212408\,t^4 + 1162944\,t^3 - 637200\,t^2 + 189216\,t - 23814$
8	$5832\,t^6 - 23328\,t^5 + 39852\,t^4 - 37152\,t^3 + 19926\,t^2 - 5832\,t + 729$

finally, the formulas for $qn_i(t)$ and $qd_i(t)$

i	$qn_i(t)$
0	$-382205952\,t^6 + 1911029760\,t^5 - 3981312000\,t^4 + 4423680000\,t^3 - 2764800000\,t^2 + 921600000\,t - 128000000$
1	$1242169344\,t^6 - 6210846720\,t^5 + 12939264000\,t^4 - 14376960000\,t^3 + 8985600000\,t^2 - 2995200000\,t + 416000000$
2	$-1934917632\,t^6 + 9650700288\,t^5 - 20059840512\,t^4 + 22242263040\,t^3 - 13875148800\,t^2 + 4617216000\,t - 640320000$
3	$1821450240\,t^6 - 9005727744\,t^5 + 18560544768\,t^4 - 20410417152\,t^3 + 12630919680\,t^2 - 4170854400\,t + 574144000$
4	$-1091377152\,t^6 + 5298628608\,t^5 - 10725198336\,t^4 + 11586309120\,t^3 - 7046019072\,t^2 + 2287269120\,t - 309668800$
5	$422143488\,t^6 - 1995010560\,t^5 + 3934065024\,t^4 - 4144690944\,t^3 + 2461317120\,t^2 - 781454784\,t + 103672320$
6	$-104789376\,t^6 + 478690560\,t^5 - 914397984\,t^4 + 935521920\,t^3 - 541037520\,t^2 + 167812512\,t - 21823272$
7	$16119648\,t^6 - 70777152\,t^5 + 130483872\,t^4 - 129400416\,t^3 + 72863136\,t^2 - 22105152\,t + 2825172$
8	$-1399680\,t^6 + 5878656\,t^5 - 10437336\,t^4 + 10031040\,t^3 - 5506488\,t^2 + 1638144\,t - 206550$

i	$qd_i(t)$
0	0
1	$191102976\,t^6 - 955514880\,t^5 + 1990656000\,t^4 - 2211840000\,t^3 + 1382400000\,t^2 - 460800000\,t + 64000000$
2	$-382205952\,t^6 + 1879179264\,t^5 - 3849928704\,t^4 + 4206919680\,t^3 - 2586009600\,t^2 + 847872000\,t - 115840000$
3	$346374144\,t^6 - 1676132352\,t^5 + 3381460992\,t^4 - 3640578048\,t^3 + 2206264320\,t^2 - 713625600\,t + 96256000$
4	$-185131008\,t^6 + 879869952\,t^5 - 1744478208\,t^4 + 1847079936\,t^3 - 1101689856\,t^2 + 351010560\,t - 46678400$
5	$63452160\,t^6 - 294865920\,t^5 + 572209920\,t^4 - 593720064\,t^3 + 347511168\,t^2 - 108828288\,t + 14251040$
6	$-14183424\,t^6 + 64074240\,t^5 - 121124160\,t^4 + 122713920\,t^3 - 70316928\,t^2 + 21620544\,t - 2788424$
7	$2006208\,t^6 - 8755776\,t^5 + 16052256\,t^4 - 15836256\,t^3 + 8873352\,t^2 - 2679360\,t + 340884$
8	$-163296\,t^6 + 684288\,t^5 - 1212408\,t^4 + 1162944\,t^3 - 637200\,t^2 + 189216\,t - 23814$

The reader interested in the details of mathematics behind the computation of parametrizations of rational curves can consult the excellent book of Rafael Sendra, Winkler and Pérez-Díaz [115]. Let us also note that for p, q given above the discriminant of $P(x) = x^2 + px + q$ takes the form

$$\mathrm{Disc}(P) = -2aP_1(a,t) \cdot P_2(a,t)Q(a,t)^2,$$

where Q is a rational function, P_2 is the polynomial of degree 2 (with respect to the variable t) with negative discriminant for $a \in \mathbb{R} \setminus \{4\}$ and

$$P_1(a,t) = (9a^3 - 116a^2 + 524a - 800)t^2 - 24(a-5)(a-4)^2t + 18(a-4)^3.$$

We thus see that the polynomial $P(x)$ will have two real roots iff $-aP_1(a,t) > 0$ and $Q(a,t) \neq 0$. We observe that if $a < 0$ then $-aP(a,t)$ is always negative and we get no solutions. Indeed, if $a < 0$ then $P(a,t)$ need to be positive. However, $9a^3 - 116a^2 + 524a - 800 < 0$ and $\mathrm{Disc}_t(P_1) = -72(a-4)^3(a-2)^2a < 0$ and thus $P_1(a,t) < 0$ for all $a, t \in \mathbb{R}$. If $a > 0$ and $a \neq 4$ there are solutions but the analytic expressions are quite complicated. Instead, in **Figure** 2.1, we present a plot of the solutions of the system $-aP(a,t) > 0 \wedge Q(a,t) \neq 0$ satisfying $(a,t) \in [0,10] \times [-10,10]$. In particular, if $a \in (0,2)$ and $t \in \mathbb{Q}$ we get solutions we are interested in. Unfortunately, we were not able to characterize all pairs (a,t) such that the corresponding polynomial $f(x) = x^4 + ax^3 + b(t)x^2 + c(t)x + d(t)$ is irreducible. It seems to be a rather difficult question.

Finally, if $a = 4$ then we get $(b,c,d,p,q) = (46/3, 20, 25, 165/26, 525/52)$ and the polynomial $x^2 + px + q$ has complex roots.

We were trying to use the obtained parametrization to find other integer points on the surface V but without success. If α is not an algebraic integer, then using the above parametrizations we may obtain real quadratic algebraic numbers. Indeed, if α is a root of the polynomial $x^4 + ax^3 + bx^2 + cx + d$ then write $\beta = \frac{4\alpha^4}{\alpha^4 - 1} - \frac{\alpha}{\alpha - 1}$. As an example let us consider the case $a = 1, t = 1$. The above formulas provide that α is a root of the polynomial

$$x^4 + x^3 + 97/24x^2 + 3/4x + 17/8$$

then β is a root of the following polynomial having two real roots

$$x^2 - 6/13x - 51/5.$$

We can also notice "near misses" solutions of Pethő's problem, where among the numbers a, b, c, d only one is genuine rational. All these solutions correspond to $a = 2$. More precisely, if α is solution of

$$x^4 + 2x^3 + \frac{14}{3}x^2 + 2x + 1$$

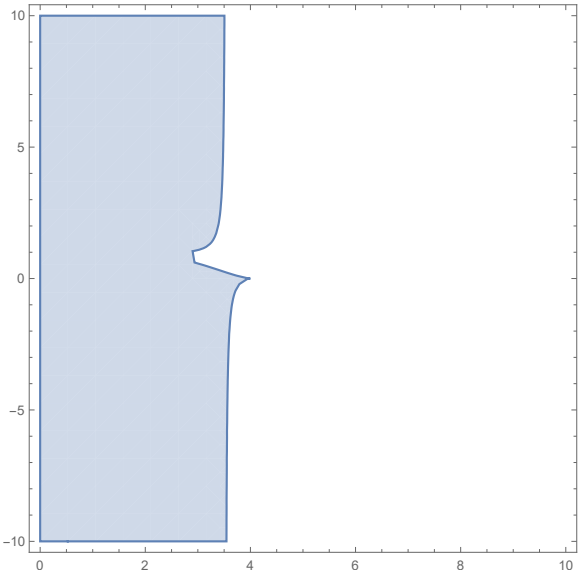


Figure 2.1: Real solutions of the inequality $-aP_1(a,t) > 0, (a,t) \in [0,10] \times [-10,10]$, are in shaded region

then β is a root of the polynomial

$$x^2 + 3x - \frac{3}{4}.$$

Similarly, if α is a root of

$$x^4 + 2x^3 + \frac{13}{3}x^2 + 4x + 4$$

then β is a root of

$$x^2 + \frac{36}{5}x + 12.$$

dc_1892_21

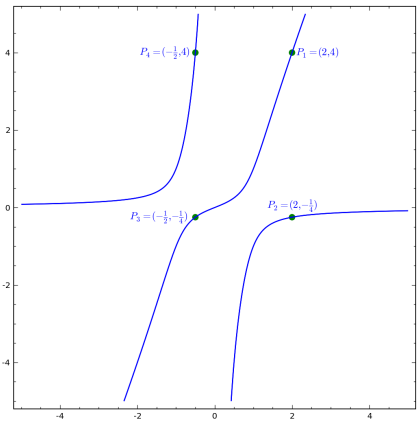
Chapter 3 Algebraic curves and arithmetic progressions

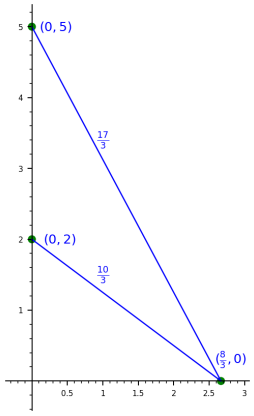
3.1 Generalized Huff models of elliptic curves

In 1948 Huff [75] studied a geometric problem and related to it a family of curves now called Huff curves. He considered rational distance sets. Given $a, b \in \mathbb{Q}^*$ such that $a^2 \neq b^2$. Determine the set of points $(x, 0) \in \mathbb{Q}^2$ satisfying that $d((0, \pm a), (x, 0))$ and $d((0, \pm b), (x, 0))$ are rational numbers, where d denotes the usual Euclidean distance. Consider the Huff curve $ax(y^2 - 1) = by(x^2 - 1)$. If there is a rational point (x, y) on the curve, then the point $P = \left(\frac{2by}{y^2-1}, 0\right)$ is in the distance set. For example, with $(a, b) = (2, 5)$, then the curve $2x(y^2 - 1) = 5y(x^2 - 1)$ contains the point $(2, 4)$, and so

$$\left(\frac{2 \cdot 5 \cdot 4}{4^2 - 1}, 0\right) = \left(\frac{8}{3}, 0\right)$$

lies in the distance set.





Elliptic curves can be represented in different forms having different arithmetic properties. Many models have been studied recently: Edwards curves, Huff curves, Montgomery curves, Weierstrass curves, Hessian curves, Jacobi quartic curves and generalizations. In this section we deal with arithmetic properties of two generalized Huff models introduced by Wu and Feng [146] and by Ciss and Sow [41]. These models are as follows

$$H_{a,b}: \quad x(ay^2 - 1) = y(bx^2 - 1)$$

with $a, b \in \mathbb{Z}$ and

$$H_{a,b}^{c,d}: \quad ax(y^2 - c) = by(x^2 - d)$$

with $a, b, c, d \in \mathbb{Z}$. We provide bounds for the size of integral solutions using Runge's method [107] combined with reduction method from [131]. In case of the family $H_{a,b}$ all integral solutions are classified and in case of $H_{a,b}^{c,d}$ the obtained bound is polynomial in a, b, c, d and in case of many concrete equations the largest integral point is very close to this bound.

Siegel [116] in 1926 proved that the equation

$$y^2 = a_0x^n + a_1x^{n-1} + \ldots + a_n =: f(x)$$

has only a finite number of integer solutions if f has at least three simple roots. In 1929 Siegel [117] classified all irreducible algebraic curves over $\mathbb{Q}$ on which there are infinitely many integral points. These curves must be of genus 0 and have at most 2 infinite valuations. These results are ineffective, that is, their proofs do not provide any algorithm for finding the solutions. In the 1960's Baker [6, 8] gave explicit lower bounds for linear forms in logarithms of the form

$$\Lambda = \sum_{i=1}^{n} b_i \log \alpha_i \neq 0$$

where $b_i \in \mathbb{Z}$ for $i = 1, \ldots, n$ and $\alpha_1, \ldots, \alpha_n$ are algebraic numbers $(\neq 0, 1)$, and

$$\log \alpha_i, \ldots, \log \alpha_n$$

denote fixed determinations of the logarithms. Baker [7] used his fundamental inequalities concerning linear forms in logarithms to derive bounds for the solutions of the elliptic equation

$$y^2 = ax^3 + bx^2 + cx + d.$$

This bound were improved by several authors see e.g. [24, 69]. Baker and Coates [10] extended this result to general genus 1 curves. Lang [80] proposed a different method to prove the finiteness of integral points on genus 1 curves. This method makes use of the group structure of the genus 1 curve. Stroeker and Tzanakis [126] and independently Gebel, Pethő and Zimmer [58] worked out an efficient algorithm based on this idea to determine all integral points on elliptic curves. The elliptic logarithm method for determining all integer points on an elliptic curve has been applied to a variety of elliptic equations (see e.g. [127, 128, 137–139]). The disadvantage of this approach is that there is no known algorithm to determine the rank of the so-called Mordell-Weil group of an elliptic curve, which is necessary to determine all integral points on the curve. There are other methods that can be used in certain cases to determine all integral solutions of genus 1 curves. Poulakis [104] provided an elementary algorithm to determine all integral solutions of equations of the form $y^2 = f(x)$, where $f(x)$ is quartic monic polynomial with integer coefficients. Using the theory of Pellian equations, Kedlaya [76] described a method to solve the system of equations

$$\begin{cases} x^2 - a_1y^2 = b_1, \\ P(x, y) = z^2, \end{cases}$$

where P is a given integer polynomial.

In this section we characterize the arithmetic progressions in case of the curve $H_{a,b}$ and we provide infinite families of curves $H_{a,b}^{c,d}$ containing arithmetic progressions of length 9. It is important to note that we only consider arithmetic progressions related to integral points.

3.2 Integral points on generalized Huff curves

In the following theorem we characterize the integral points on the curve $H_{a,b}$.

Theorem 3.1

The Diophantine equation $H_{a,b}: \quad x(ay^2-1) = y(bx^2-1)$ *with* $a,b,x,y \in \mathbb{Z}$ *has precisely the following solutions*

$$\begin{aligned}
(a,b,x,y) &= (a,b,0,0) \text{ with } a,b \in \mathbb{Z},\\
(a,b,x,y) &= (a,a,x,x) \text{ with } a,x \in \mathbb{Z},\\
(a,b,x,y) &= (1,1,-1,1),\\
(a,b,x,y) &= (1,1,1,-1),\\
(a,b,x,y) &= (-1,-1,-1,1),\\
(a,b,x,y) &= (-1,-1,1,-1),\\
(a,b,x,y) &= (a,2-a,-1,1) \text{ with } a \in \mathbb{Z},\\
(a,b,x,y) &= (a,2-a,1,-1) \text{ with } a \in \mathbb{Z}.
\end{aligned}$$

A direct consequence of the above theorem is as follows.

Corollary 3.1

Let $(x_1,y_1),(x_2,y_2),(x_3,y_3)$ *be solutions of the equation* $H_{a,b}$ *for some* $a,b \in \mathbb{Z}$ *such that* (x_1,x_2,x_3) *forms an arithmetic progression and at most one solution* (x_i,y_i) *satisfies the condition* $x_i = y_i$. *Then* $(x_1,x_2,x_3) = (-3,-1,1),(-1,0,1),(1,0,-1)$ *or* $(1,-1,-3)$.

In case of the second family $H_{a,b}^{c,d}$ we have the following result. Define $\varphi(a,b,c,d) = (a^2c-81)(a^2c-81-b^2d)$.

Theorem 3.2

Let $a,b,c,d \in \mathbb{Z}$ *such that* $abcd(a^2c-b^2d) \neq 0$. *Define* L_1, L_2, U_1, U_2 *as follows*

$$L_1 = -\tfrac{1}{9}\sqrt{\varphi(a,b,c,d)}, \qquad U_1 = \tfrac{1}{9}\sqrt{\varphi(a,b,c,d)},$$

$$L_2 = -\tfrac{1}{9}\sqrt{-\varphi(a,b,-c,-d)}, \qquad U_2 = \tfrac{1}{9}\sqrt{\varphi(a,b,-c,-d)}.$$

Let $m_0 = \min(\{0\} \cup \{L_i : i = 1,2, L_i \in \mathbb{R}\})$ *and* $M_0 = \max(\{0\} \cup \{U_i : i = 1,2, U_i \in \mathbb{R}\})$. *If* (x,y) *is an integral point on* $H_{a,b}^{c,d}$, *then we have that either*

$$x = \pm\frac{\sqrt{(2a^2c-t)(2a^2c-t-2b^2d)}}{b\sqrt{2t}} \quad t \in \{-161,\ldots,161\}$$

or

$$\frac{m_0}{b} \leq x \leq \frac{M_0}{b} \text{ if } b > 0,$$
$$\frac{M_0}{b} \leq x \leq \frac{m_0}{b} \text{ if } b < 0.$$

Remark. In case of the curve $H_{5,2}^{-17,-6}$ there is no solution coming from the formula for x, the

bound is $-29 \leq x \leq 29$. The integral solutions are given by $(x, y) \in \{(-27, -9), (0, 0), (27, 9)\}$, that is the largest solution is just 2 away from the bound.

On the curves $H_{a,b}^{c,d}$ we consider the question of long arithmetic progressions, we have the following statement.

Theorem 3.3

There exist infinitely many tuples $(a, b, c, d) \in \mathbb{Z}^4$ such that there is a length 9 arithmetic progression formed by x-coordinates of integral points on the curve $H_{a,b}^{c,d}$.

3.3 Proof of the results

In the proofs of the results the we use several time that the discriminant of a degree 2 polynomial (in some variable) must be a rational square. This is a necessary condition to obtain integer solutions.

Proof. [Proof of Theorem 3.1] Consider the case $a = b$. We obtain that

$$axy(y - x) = x - y.$$

Therefore $x = y$ is a solution for all $x \in \mathbb{Z}$. Assume that $x \neq y$. We get that $axy = -1$. Hence $(a, b, x, y) \in \{(-1, -1, \mp 1, \pm 1), (1, 1, \mp 1, \pm 1)\}$ are the possible solutions of the equation, and one can check that these are in fact solutions.

We may assume that $|a| > |b|$. We rewrite the equation in the form

$$byx^2 + (1 - ay^2)x - y = 0.$$

A necessary condition to obtain integer solution is that the discriminant of the above quadratic polynomial in x must be a rational square. Thus there exists an integer t such that

$$F(y) := a^2y^4 + (4b - 2a)y^2 + 1 = t^2. \tag{3.1}$$

We apply Runge's method [107] to determine all the integral solutions. Define $P(y) = ay^2 + \frac{2b-a}{a}$. We have that

$$\begin{aligned} F(y) - \left(P(y) - \frac{1}{a}\right)^2 &= 2y^2 + \frac{4b}{a} - \frac{2}{a} - \frac{4b^2}{a^2} + \frac{4b}{a^2} - \frac{1}{a^2}, \\ F(y) - \left(P(y) + \frac{1}{a}\right)^2 &= -2y^2 + \frac{4b}{a} + \frac{2}{a} - \frac{4b^2}{a^2} - \frac{4b}{a^2} - \frac{1}{a^2}. \end{aligned}$$

These two quadratic polynomials have opposite signs if $|y| \geq 3$, since $|a| > |b|$. Therefore one has that

$$\left(P(y) - \frac{1}{a}\right)^2 < F(y) = t^2 < \left(P(y) + \frac{1}{a}\right)^2$$

if $|y| \geq 3$. It yields that $t = \pm(ay^2 + \frac{2b-a}{a})$. Equation (3.1) implies that $b = 0$. In this case

$$y \in \left\{ \frac{-1}{2ax} \pm \sqrt{\frac{1}{4a^2x^2} + \frac{1}{a}} \right\}$$

and we obtain that $|y| \leq 1$. Therefore we have that $|y| < 3$. It remains to check the cases $y \in \{0, \pm 1, \pm 2\}$. If $y = 0$, then it follows that $x = 0$. If $y = \pm 1$, then

$$\pm bx^2 - (a-1)x \mp 1 = 0.$$

Hence $x = \pm 1$ and $b = a$ or $b = 2 - a$. If $y = \pm 2$, then we get that

$$\pm 2bx^2 - (4a-1)x \mp 2 = 0.$$

Therefore $x \in \{\pm 1, \pm 2\}$. If $x = \pm 2$, then we get that $a = b$, a case that has been considered. If $x = \pm 1$, then no solution exists.

Proof. [Proof of Theorem 3.2] Rewrite the equation of $H_{a,b}^{c,d}$ as follows

$$axy^2 - b(x^2 - d)y - acx = 0.$$

A necessary condition to obtain integer solution is that the discriminant of the above quadratic polynomial in y must be a rational square. Hence there exists an integer u for which

$$G(X) := X^4 + (4a^2c - 2b^2d)X^2 + b^4d^2 = u^2,$$

where $X = bx$. Let $R(X) = X^2 + 2a^2c - b^2d$, that is the polynomial part of the Puiseux expansion of $\sqrt{G(X)}$. We obtain that

$$\begin{aligned} G(X) - (R(X) - 162)^2 &= 324\,X^2 - 4\,a^4c^2 + 4\,a^2b^2cd + \\ &\quad 648\,a^2c - 324\,b^2d - 26244, \\ G(X) - (R(X) + 162)^2 &= -324\,X^2 - 4\,a^4c^2 + 4\,a^2b^2cd - \\ &\quad 648\,a^2c + 324\,b^2d - 26244. \end{aligned}$$

The roots of the above polynomials are defined in Theorem 3.2 as L_1, U_1 and L_2, U_2 respectively. If X is not an element of the interval

$$[\min(L_1, L_2), \max(U_1, U_2)],$$

then

$$G(X) > (R(X) - 162)^2 \quad \text{and } G(X) < (R(X) + 162)^2.$$

Since $G(X) = u^2$ we get that $u = \pm(R(X) - t)$ for some integer $|t| < 162$. It follows that

$$x = \frac{X}{b} = \pm \frac{\sqrt{(2a^2c - t)(2a^2c - t - 2b^2d)}}{b\sqrt{2t}} \quad t \in \{-161, \ldots, 161\}.$$

It remains to bound the "small" solutions, that is to compute $\min(L_1, L_2)$ and $\max(U_1, U_2)$, these are roots of the above defined polynomials. We note that we fixed the number 162 appearing in the above computation based on numerical experiences. It can be replaced by an other constant, say T. If a and b are large, then a baby step - giant step type algorithm can be used to find a near optimal value for T, for which the number of integers in the intervals $[\min(L_1, L_2), \max(U_1, U_2)]$ and $[-T + 1, T - 1]$ is almost as small as possible.

Proof. [Proof of Theorem 3.3] First notice that if $(x, y) \in H_{a,b}^{c,d}$ then $(-x, -y) \in H_{a,b}^{c,d}$. Based on numerical experience we fix $b = ma$ and $d = a + 1$ for some integer m. The integral point $(0, 0)$ is on the curve $H_{a,b}^{c,d}$ for any integral tuple (a, b, c, d). If we have an integral solution with

$x = 1$, then $y^2 + amy - c = 0$ and a necessary condition to obtain integer solution is that the discriminant of the above quadratic polynomial in y must be a rational square. Hence

$$c = \frac{n^2 - m^2a^2}{4}$$

for some integer n. In a similar way $x = 2$ corresponds to an integral solution if $2y^2 - m(3 - a)y - \frac{n^2-m^2a^2}{2} = 0$. Hence $4n^2 - 3m^2(a^2 + 2a - 3)$ is a square. We look for solutions of the form $n = ua + v$ for some $u, v \in \mathbb{Z}$. We get that

$$(v - u)^2 - 4u^2 + 3m^2 = 0.$$

Parametric solution of the above equation is given by

$$(v - u, u, m) = (\frac{-2p^2 + 6q^2}{G_{p,q}}, \frac{p^2 + 3q^2}{G_{p,q}}, \frac{4pq}{G_{p,q}}),$$

for some integers p, q, where $G_{p,q} = \gcd(-2p^2 + 6q^2, p^2 + 3q^2, 4pq)$. To obtain an integral solution with $x = 3$, with a similar argument as the case $x = 1$ give us that the polynomial

$$9(a^2 - 2a + 1)p^4 - 2(37a^2 + 74a - 431)p^2q^2 + 81(a^2 + 6a + 9)q^4$$

has to be a square. The quartic is singular when its discriminant is 0, so for $a = -7, -4, 2$ or 5. Using the above formulas we obtain for $x = 3$ and each values of a the corresponding y-coordinate of the point in $H^{c,d}_{a,b}$ where a, b, c, d are as above:

a	y
-7	$2(2p - q)(p + 3q)$
-4	$\frac{1}{2}(5p + q)(p + 3q)$
2	$\frac{1}{2}(p + 5q)(p + 3q)$
5	$2(p - 2q)(p + 3q)$

.

We handle the case with $a = 2$, the other three can be treated in a similar way. When $a = 2$, then a point on the curve with $x = 4$ demands

$$p^4 - 34p^2q^2 + 225q^4 + 52pqy - 4y^2 = 0,$$

so that necessarily its discriminant, $p^4 + 135p^2q^2 + 225q^4$, is square. Hence we have a genus 1 curve which has an affine model of the form

$$C : v^2 = u^4 + 135u^2 + 225\,, \qquad \text{where } u = p/q.$$

The quartic curve C has the rational point $[0 : 1 : 0]$, then it is an elliptic curve defined over $\mathbb{Q}$. A Weierstrass model for C is

$$E_2 : Y^2 = X^3 + 45X^2 - 6300X,$$

and the isomorphism given in affine coordinates by:

$$\varphi : C \longrightarrow E_2\,, \qquad \varphi(u, v) = (30 + 2u^2 + 2v, 270u + 4u^3 + 4uv).$$

We use the computer algebra software Magma [8] to compute the generator of the Mordell-Weil group of E_2. The points $(60, 0)$, $(0, 0)$ generate the torsion subgroup and the free part is generated

by

$$(-30, 450), (-90, 450).$$

The point $(x, y) = (3, \frac{1}{2}(p+5q)(p+3q)) \in H_{a,b}^{c,d}$ is supposed to be an integral point, therefore we need to scale p and q such that they have the same parity. To avoid cases with $abcd(a^2c-b^2d) = 0$ we need points in C with u-coordinate different from $\pm 1, \pm 3, \pm 5, \pm 15$. That is the points that are not coming from the following points on E_2:

$$(70, \pm 350), (-6, \pm 198), (126, \pm 1386), (-30, \pm 450), (210, \pm 3150),$$
$$(-50, \pm 550), (1050, \pm 34650), (-90, \pm 450), (6, 0), (0, 0), (-105, 0).$$

As examples we compute the cases corresponding to the points $3(-90, 450)$ and $2(-30, 450)$. From $3(-90, 450)$ we get that $p/q = 182745/68681$, so we do not need to scale. From $2(-30, 450)$ we obtain that $p/q = 8/13$, so we fix $(p, q) = (16, 26)$ to make the y-coordinate corresponding with the point with x-coordinate equal to 3 an integer.

(p, q)	$(182745, 68681)$	$(16, 26)$
points on $H_{2,b}^{c,3}$	$(0, 0)$	$(0, 0)$
	$(\pm 1, \pm 1871528340)$	$(\pm 1, \pm 3534)$
	$(\pm 2, \pm 31231340040)$	$(\pm 2, \pm 5358)$
	$(\pm 3, \pm 102280403100)$	$(\pm 3, \pm 6862)$
	$(\pm 4, \pm 164329281885)$	$(\pm 4, \pm 8322)$
b	100408874760	3328
c	191420673028273854000	24250308

We note that for $a = -7, -4, 5$ the corresponding elliptic curve E_a have positive ranks as well (1, 2 and 1 respectively). More over E_2 and E_{-4} (and E_5 and E_{-7}) are isomorphic over $\mathbb{Q}$.

dc_1892_21

Chapter 4 Markoff-Rosenberger triples with Fibonacci components

4.1 Markoff and Markoff-Rosenberger equations

Markoff [89] obtained many nice results related to the equation

$$x^2 + y^2 + z^2 = 3xyz.$$

He showed that there exist infinitely many integral solutions. The so-called Markoff equation defined above has been generalized in many directions by several authors. We focus on the generalization considered by Rosenberger [106]

$$ax^2 + by^2 + cz^2 = dxyz. \tag{4.1}$$

Rosenberger proved that if $a, b, c, d \in \mathbb{N}$ are integers such that $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$ and $a, b, c|d$, then non-trivial solutions exist only if

$$(a, b, c, d) \in \{(1, 1, 1, 1), (1, 1, 1, 3), (1, 1, 2, 2), (1, 1, 2, 4), (1, 1, 5, 5), (1, 2, 3, 6)\}.$$

Silverman [118] studied equation (4.1) with $a = b = c = 1$ over imaginary quadratic number fields. Baer and Rosenberger [5] considered solutions of equation (4.1) over imaginary quadratic number fields. González-Jiménez and Tornero [62] looked for solutions of equation (4.1) in arithmetic progression that lie in the ring of integers of a number field. González-Jiménez [59] studied solutions of (4.1) whose coordinates belong to the ring of integers of a number field and form a geometric progression. A well-known identity related to the Fibonacci numbers

$$1 + F_{2n-1}^2 + F_{2n+1}^2 = 3F_{2n-1}F_{2n+1}$$

shows that $(x, y, z) = (1, F_{2n-1}, F_{2n+1})$ is a solution of the Markoff equation for any $n \in \mathbb{N}$. Luca and Srinivasan [84] proved that there are infinitely many solutions (F_i, F_j, F_k) to the classical Markoff equations (given by the above identity). In this section we extend the result of Luca and Srinivasan, we determine the solutions $(x, y, z) = (F_i, F_j, F_k)$ of equation (4.1) for

$$(a, b, c, d) \in \{(1, 1, 1, 1), (1, 1, 2, 2), (1, 1, 2, 4), (1, 1, 5, 5), (1, 2, 3, 6)\}.$$

In the proofs, we simplify the strategy described by Luca and Srinivasan, by providing a direct way to get a bound for $k - j$ from above.

4.2 Fibonacci components

Theorem 4.1

If $(x,y,z) = (F_i,F_j,F_k)$ *is a solution of equation* (4.1) *and* $(a,b,c,d) \in \{(1,1,1,1),(1,1,2,2),(1,1,2,4),(1,1,5,5),(1,2,3,6)\}$, *then the complete list of solutions are given by*

(a,b,c,d)	*solutions*
$(1,1,1,1)$	$\{(3,3,3)\}$
$(1,1,2,2)$	$\{(2,2,2)\}$
$(1,1,2,4)$	$\{(1,1,1),(1,3,1),(1,3,5),(3,1,1),(3,1,5)\}$
$(1,1,5,5)$	$\{(1,2,1),(1,3,1),(1,3,2),(2,1,1),(3,1,1),(3,1,2)\}$
$(1,2,3,6)$	$\{(1,1,1),(1,2,1),(1,2,3),(5,1,1)\}$

Proof. A well-known fact is that the n-th Fibonacci number can be written as follows

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \text{ where } \alpha = \frac{1+\sqrt{5}}{2} \text{ and } \beta = \frac{1-\sqrt{5}}{2}.$$

We also have that for all $n \geq 1$

$$\alpha^{n-2} \leq F_n \leq \alpha^{n-1}.$$

We note that in the Markoff case, $a = b = c$ and the equation is fully symmetric in (x,y,z). This symmetry is no longer present in the case of the Rosenberg equation. In the proof we assume that $x \leq y \leq z$ hence we need to consider not only the equation $ax^2 + by^2 + cz^2 = dxyz$ but also all the permutations of (a,b,c). We provide a bound for i for general (a,b,c,d) and we use it to get an upper bound for $k-j$. Based on inequalities from [84] we have

$$\frac{aF_i^2 + bF_j^2}{F_k} \leq (a+b)\alpha^j\,, \quad \left|\frac{\beta^k}{\sqrt{5}}\right| \leq \frac{\alpha^j}{5}\,, \quad \left|\alpha^i\beta^j + \alpha^j\beta^i - \beta^{i+j})\right| \leq 3\alpha^j. \tag{4.2}$$

Suppose $(x,y,z) = (F_i,F_j,F_k)$ for $i \leq j \leq k$ is a solution of

$$aF_i^2 + bF_j^2 + cF_k^2 = dF_iF_jF_k.$$

We obtain that

$$c\frac{\alpha^k}{\sqrt{5}} - d\frac{\alpha^{i+j}}{5} = -\frac{aF_i^2 + bF_j^2}{F_k} + c\frac{\beta^k}{\sqrt{5}} - \frac{d}{5}(\alpha^i\beta^j + \alpha^j\beta^i - \beta^{i+j}).$$

Taking absolute values and using the inequalities at (4.2) we obtain:

$$\left|c\frac{\alpha^k}{\sqrt{5}} - d\frac{\alpha^{i+j}}{5}\right| \leq \frac{\alpha^j}{5}(5a+5b+c+3d),$$

and dividing by $\frac{\alpha^{i+j}}{\sqrt{5}}$:

$$\left|c\,\alpha^{k-i-j} - \frac{d}{\sqrt{5}}\right| \leq \frac{5a+5b+c+3d}{\sqrt{5}\alpha^i}. \tag{4.3}$$

Now define $f(n) = \left|c\,\alpha^n - \frac{d}{\sqrt{5}}\right|$ and let $t_0 \in \mathbb{Z}$ such that $f(t_0) \leq f(n)$ for any $n \in \mathbb{Z}$. Then

$$\alpha^i \leq \frac{5a+5b+c+3d}{\sqrt{5}f(t_0)}. \tag{4.4}$$

For a given tuple (a,b,c,d) equation (4.4) provides an upper bound for i, denote it by $\mathfrak{ub}(a,b,c,d)$. For a given i equation (4.3) yields an upper bound for $k-j$. For the concrete equations we consider these bounds are as follows:

$$\begin{aligned}
&\mathfrak{ub}(1,1,1,1) = 9,\\
&\mathfrak{ub}(1,1,2,2) = 8, \mathfrak{ub}(1,2,1,2) = \mathfrak{ub}(2,1,1,2) = 9,\\
&\mathfrak{ub}(1,1,2,4) = \mathfrak{ub}(1,2,1,4) = \mathfrak{ub}(2,1,1,4) = 8,\\
&\mathfrak{ub}(1,2,3,6) = \mathfrak{ub}(2,1,3,6) = 8, \mathfrak{ub}(1,3,2,6) = \mathfrak{ub}(3,1,2,6) = 7,\\
&\mathfrak{ub}(2,3,1,6) = \mathfrak{ub}(3,2,1,6) = 11,\\
&\mathfrak{ub}(1,1,5,5) = 7, \mathfrak{ub}(1,5,1,5) = \mathfrak{ub}(5,1,1,5) = 8.
\end{aligned}$$

For each (a,b,c,d) and any $i \le \mathfrak{ub}(a,b,c,d)$ one needs to compute the (finitely many) possibilities for $m = k-j$. That is, fixing (a,b,c,d), i and m we study the equation

$$aF_i^2 + bF_j^2 + cF_{j+m}^2 - dF_iF_jF_{j+m} = 0.$$

We note that the equation above only depends on j. To deal with the concrete cases we use the following arguments.

(I) We eliminate as many values of i as possible by checking solvability of quadratic equations

$$aF_i^2 + by^2 + cz^2 - F_iyz = 0.$$

(II) For fixed m we eliminate equations $aF_i^2 + bF_j^2 + cF_{j+m}^2 - dF_iF_jF_{j+m} = 0$ modulo p, where p is a prime.

(III) We consider the equation $aF_i^2 + bF_j^2 + cF_{j+m}^2 = dF_iF_jF_{j+m}$ as a quadratic in F_j. Then its discriminant $d^2F_i^2F_{j+m}^2 - 4b(aF_i^2 + cF_{j+m}^2)$ must be a square. A fundamental identity for the Fibonacci and Lucas numbers (denoted by L_n, defined by $L_0 = 2, L_1 = 1$ and $L_n = L_{n-1} + L_{n-2}$ for $n \ge 2$) says that

$$L_n^2 = 5F_n^2 \pm 4.$$

That is we have the system of equations

$$\begin{aligned}
Y_1^2 &= 5X^2 \pm 4,\\
Y_2^2 &= d^2F_i^2X^2 - 4b(aF_i^2 + cX^2),
\end{aligned}$$

where $X = F_{j+m}$. Multiplying these equations together yields

$$Y^2 = (5X^2 \pm 4)(d^2F_i^2X^2 - 4b(aF_i^2 + cX^2)).$$

Therefore we reduce our problem to obtain integral points on the above quartic genus 1 curves. This will be realized using the Magma [23] function `SIntegralLjunggrenPoints`.

We implemented the above procedure in SageMath [122] and the code can be downloaded from the URL address `http://shrek.unideb.hu/~tengely/MarkoffSolver.sage`. Detailed computations can be found at

`http://shrek.unideb.hu/~tengely/Markoff-Rosenberger-Fibonacci.pdf`.

4.2.1 The case with $d = 1$

We have that $2 \leq i \leq 9$. In this range the Diophantine equation $F_i^2 + y^2 + z^2 = F_i yz$ is solvable only for $i = 4$. If $i = 4$, then we have that $0 \leq k - j \leq 4$. The equation $9 + F_j^2 + F_{j+m}^2 - 3F_jF_{j+m} = 0$ has no solution modulo 3 for $m = 1, 2, 3$, and it is not solvable modulo 11 for $m = 4$. It remains to consider the case $m = 0$. We have that $k = j$, therefore the equation is simply $9 = F_j^2$. Hence, we get the solution $(x, y, z) = (3, 3, 3)$.

4.2.2 Cases with $d = 2$

Consider the tuple $(a, b, c, d) = (1, 1, 2, 2)$. The bound for i is 8, however only the quadratic equation related to $i = 3$ is solvable in integers. If $i = 3$, then $0 \leq k - j \leq 3$. We eliminate the cases $m = 1, 2$ modulo 7 and the case $m = 3$ modulo 23. If $k = j$, then we get that $4 = F_j^2$. Hence, we obtain the solution $(x, y, z) = (2, 2, 2)$. There are 2 other subcases here, $(a, b, c, d) = (1, 2, 1, 2)$ and $(2, 1, 1, 2)$ having the same upper bound for i, namely 9. In case of $(a, b, c, d) = (1, 2, 1, 2)$ we can eliminate all values of i except $i = 3$ and 9. If $i = 3$ we have

$$4 + 2F_j^2 + F_{j+m}^2 - 4F_jF_{j+m} = 0,$$

where $0 \leq m \leq 5$. Congruence arguments eliminate the cases with $m \in \{1, 2, 3, 4, 5\}$ as follows:

m	1	2	3	4	5
mod	17	7	19	3	13

The remaining value of m is 0, that yields the equation $4 = F_j^2$, so we obtain the solution $(x, y, z) = (2, 2, 2)$. If $i = 9$, then the corresponding equation is

$$1156 + 2F_j^2 + F_{j+m}^2 - 68F_jF_{j+m} = 0,$$

where $0 \leq m \leq 9$. The following table contains the primes used to get a contradiction

m	0	1	2	3	4	5	6	7	8	9
mod	3	7	11	19	11	5	11	7	3	29

In case of $(a, b, c, d) = (2, 1, 1, 2)$ we only need to handle $i = 3$ for which we get that $0 \leq m \leq 5$. The equation is given by

$$8 + F_j^2 + F_{j+m}^2 - 4F_jF_{j+m} = 0,$$

and we can eliminate all these (except $m = 0$) as the table below shows

m	1	2	3	4	5
mod	11	7	11	3	13

If $m = 0$, then we have $8 = 2F_j^2$ and the only solution is $(x, y, z) = (2, 2, 2)$.

4.2.3 Cases with $d = 4$

If $(a, b, c, d) = (1, 1, 2, 4)$, then if follows that $i = 2$ or 4. If $(a, b, c, d) = (1, 2, 1, 4)$, then we obtain that $i = 2$ or 4. The last tuple to consider here is $(a, b, c, d) = (2, 1, 1, 4)$ and we get that $i = 2$ or 5. We need to handle the equations

$$\begin{aligned} 1 + F_j^2 + 2F_{j+m}^2 - 4F_jF_{j+m} &= 0, \\ 9 + F_j^2 + 2F_{j+m}^2 - 12F_jF_{j+m} &= 0, \\ 1 + 2F_j^2 + F_{j+m}^2 - 4F_jF_{j+m} &= 0, \\ 9 + 2F_j^2 + F_{j+m}^2 - 12F_jF_{j+m} &= 0, \\ 2 + F_j^2 + F_{j+m}^2 - 4F_jF_{j+m} &= 0, \\ 50 + F_j^2 + F_{j+m}^2 - 20F_jF_{j+m} &= 0. \end{aligned}$$

We provide details in the case of the first equation, the other 5 can be solved in a similar way. We consider the equation as a quadratic in F_j and follow the argument described in (III). It remains to solve the quartic Diophantine equations

$$y^2 = 10x^4 - 13x^2 + 4, \qquad y^2 = 10x^4 + 3x^2 - 4.$$

The integral solutions of these equations can be completely determined using the Magma [23] procedure `SIntegralLjunggrenPoints`. In the former case we get that $x \in \{0, \pm 1, \pm 5\}$. In case of the latter equation we have that $x \in \{\pm 1\}$. It follows that $F_{j+m} = 1$ or 5 and we get the solutions $(x, y, z) = (1, 1, 1)$ and $(x, y, z) = (1, 3, 5)$.

4.2.4 Cases with $d = 5$

Here, we get the following possibilities for i for the 3 tuples

(a, b, c, d)	i
$(1, 1, 5, 5)$	$\{2, 3, 4\}$
$(1, 5, 1, 5)$	$\{2, 3, 4\}$
$(5, 1, 1, 5)$	$\{2, 3, 5, 7\}$

.

Consider the tuple $(5, 1, 1, 5)$. If $i = 5$, then $0 \le m \le 7$ and if $i = 7$, then $0 \le m \le 9$. All these cases can be eliminated using congruence arguments: if $i = 5$, then we have

m	0	1	2	3	4	5	6	7
mod	7	11	11	11	3	11	17	11

and if $i = 7$, then we obtain

m	0	1	2	3	4	5	6	7	8	9
mod	3	11	13	29	11	19	11	29	3	11

It remains to check the solutions for $i = 2$ and 3. The equations can be written as follows

$$\begin{aligned} 5 + F_j^2 + F_{j+m}^2 - 5F_jF_{j+m} &= 0, \\ 20 + F_j^2 + F_{j+m}^2 - 10F_jF_{j+m} &= 0. \end{aligned}$$

As before we reduce the problem to genus 1 curves, we obtain the following 4 equations

$$\begin{aligned} y^2 &= 105x^4 - 184x^2 + 80, \\ y^2 &= 105x^4 - 16x^2 - 80, \\ y^2 &= 30x^4 - 49x^2 + 20, \\ y^2 &= 30x^4 - x^2 - 20. \end{aligned}$$

The complete set of possible values for F_j is given by $\{1, 2, 3, 987\}$. We also know that $F_i \in \{1, 2\}$, hence one can easily determine F_k. The solutions of the equation $x^2 + y^2 + 5z^2 = 5xyz$ from these cases are given by $(x, y, z) = (1, 2, 1), (2, 1, 1), (1, 3, 1), (3, 1, 1), (1, 3, 2)$ and $(3, 1, 2)$.

4.2.5 Cases with $d = 6$

Let us consider the equation $x^2+2y^2+3z^2 = 6xyz$. Here we can eliminate many quadratic equations. In the table below we collect the remaining cases.

(a, b, c, d)	i
$(1, 2, 3, 6)$	$\{2, 5\}$
$(2, 1, 3, 6)$	$\{2, 3\}$
$(1, 3, 2, 6)$	$\{2, 5\}$
$(3, 1, 2, 6)$	$\{2, 4\}$
$(2, 3, 1, 6)$	$\{2, 3\}$
$(3, 2, 1, 6)$	$\{2, 4, 11\}$

.

We provide details in case of the tuple $(3, 2, 1, 6)$ only, the remaining ones can be treated in a similar way. We have three values for i, these correspond to the equations

$$\begin{aligned} 3 + 2F_j^2 + F_{j+m}^2 - 6F_jF_{j+m} &= 0, \\ 27 + 2F_j^2 + F_{j+m}^2 - 18F_jF_{j+m} &= 0, \\ 23763 + 2F_j^2 + F_{j+m}^2 - 534F_jF_{j+m} &= 0. \end{aligned}$$

The last equation corresponds to $i = 11$. Here, we do not expect any solution so we compute the possible values of m and try to get a contradiction modulo some prime. It turns out that $0 \leq m \leq 13$ and all these cases can be handled using congruence arguments. We summarize the computation in the following table

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13
mod	5	17	19	7	13	5	17	13	7	17	13	13	17	29

Solving the remaining two equations as described in (III) we get that we need to find the

integral solutions of the Diophantine equations

$$\begin{aligned} y^2 &= 35x^4 - 43x^2 + 12, \\ y^2 &= 35x^4 + 13x^2 - 12, \\ y^2 &= 395x^4 - 451x^2 + 108, \\ y^2 &= 395x^4 + 181x^2 - 108. \end{aligned}$$

We use the Magma function `SIntegralLjunggrenPoints` to determine the integral solutions and we get that $F_j \in \{1, 2\}$. The tuple we consider is given by $(3, 2, 1)$ and the corresponding equation is $3F_i^2 + 2F_j^2 + F_k^2 = 6F_iF_jF_k$. Since $i = 2$ or 4 we have $F_i \in \{1, 3\}$. These possibilities yield the solutions $(x, y, z) = (1, 1, 1), (1, 1, 5), (1, 2, 1)$ and $(3, 2, 1)$.

dc_1892_21

Part III

Sequences in Diophantine problems

dc_1892_21

Chapter 5 Erdős-Graham type Diophantine problems

5.1 Product of two blocks of length 4

In this section we consider the Diophantine equation

$$x(x+1)(x+2)(x+3)(x+m)(x+m+1)(x+m+2)(x+m+3) = y^2, \tag{5.1}$$

where $4 \leq m \in \mathbb{N}$ is a parameter. We provide bounds for the size of solutions and an algorithm to determine all solutions $(x, y) \in \mathbb{N}^2$. The method of proof is based on Runge's method [64, 72, 107, 108, 112, 131, 145].

Theorem 5.1

If $(x, y) \in \mathbb{N}^2$ is a solution of (5.1) then

$$1 \leq x \leq 1.08m.$$

We apply the above theorem to determine all positive integral solutions of (5.1) with $4 \leq m \leq 10^6$.

Theorem 5.2

The only solution $(x, y) \in \mathbb{N}^2$ of (5.1) with $4 \leq m \leq 10^6$ is

$$(x, y) = (33, 3361826160)$$

with $m = 1647$.

5.2 Proof of the results

Proof. [Proof of Theorem 5.1] We apply Runge's method and we prove that large solutions do not exists and we provide bound for size of the possible small solutions. A solution to the equation (5.1) gives rise a solution to the equation

$$F(X) := X(X+m+2)(X+2m+2)(X+3m) = Y^2, \tag{5.2}$$

where $X = x^2 + (m+3)x$. The polynomial part of the Puiseux expansion of $F(X)^{(1/2)}$ is

$$P(X) = X^2 + (3m+2)X + m^2 + 3m.$$

We obtain that

$$\begin{aligned} F(X) - (P(X)-1)^2 &= 2X^2 - (4m^2 - 6m + 4)X - m^4 - 6m^3 - 7m^2 + 6m - 1, \\ F(X) - (P(X)+1)^2 &= -2X^2 - (4m^2 + 6m + 4)X - m^4 - 6m^3 - 11m^2 - 6m - 1. \end{aligned}$$

Let α_1, α_2 be the roots of the quadratic polynomial $F(X) - (P(X) - 1)^2$ and α_3, α_4 be the roots of $F(X) - (P(X) + 1)^2$. We define $\beta_i, i = 1, 2, 3, 4$ as follows

$$\beta_i = \begin{cases} \alpha_i & \text{if } \alpha_i \in \mathbb{R}, \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$F(X) - (P(X) - 1)^2 > 0, \quad \text{if } X \notin [\min_i\{\beta_i\}, \max_i\{\beta_i\}]$$

and

$$F(X) - (P(X) + 1)^2 < 0, \quad \text{if } X \notin [\min_i\{\beta_i\}, \max_i\{\beta_i\}].$$

Hence we get that

$$(P(X) - 1)^2 < F(X) < (P(X) + 1)^2, \quad \text{if } X \notin [\min_i\{\beta_i\}, \max_i\{\beta_i\}].$$

If (X, Y) is a solution of (5.2) with $X \notin [\min_i\{\beta_i\}, \max_i\{\beta_i\}]$, then

$$Y = P(X).$$

It implies that

$$0 = F(X) - P(X)^2 = -4m^2X - m^4 - 6m^3 - 9m^2.$$

That is

$$X = -\left(\frac{m+3}{2}\right)^2.$$

Since $X = x^2 + (m + 3)x$ we get that

$$x = \frac{-m-3}{2}.$$

It means that if there exists a large solution, then m has to be odd, $x = \frac{-m-3}{2}$ and $y = \frac{(m-3)(m-1)(m+1)(m+3)}{16}$. It is a contradiction since $m \geq 4$ and therefore $0 > \frac{-m-3}{2} = x$.

It remains to deal with the small solutions that is those with

$$X \in [\min_i\{\beta_i\}, \max_i\{\beta_i\}].$$

Hence we need to compute the roots of the polynomials $F(X) - (P(X) - 1)^2$ and $F(X) - (P(X) + 1)^2$. These are as follows

$$\begin{aligned} \alpha_1 &= m^2 - \frac{3}{2}m - 1 - \frac{1}{2}\sqrt{6\,m^4 + 15\,m^2 + 6}, \\ \alpha_2 &= m^2 - \frac{3}{2}m - 1 + \frac{1}{2}\sqrt{6\,m^4 + 15\,m^2 + 6}, \\ \alpha_3 &= -m^2 - \frac{3}{2}m - 1 - \frac{1}{2}\sqrt{2\,m^4 - 5\,m^2 + 2}, \\ \alpha_4 &= -m^2 - \frac{3}{2}m - 1 + \frac{1}{2}\sqrt{2\,m^4 - 5\,m^2 + 2}. \end{aligned}$$

Since $m \geq 4$, we obtain that $6\,m^4 + 15\,m^2 + 6 \geq 0$ and $2\,m^4 - 5\,m^2 + 2 \geq 0$. Therefore $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{R}$ and we have

$$\alpha_3 < \alpha_4 < \alpha_1 < \alpha_2.$$

We need to solve the system of inequalities

$$\begin{aligned} 0 &\leq x^2+(m+3)x-\alpha_3, \\ 0 &\geq x^2+(m+3)x-\alpha_2. \end{aligned}$$

The first inequality is true for all $x \geq 1$. The second inequality implies that

$$-\frac{1}{2}\,m-\frac{1}{2}\,\sqrt{5\,m^2+2\,\sqrt{6\,m^4+15\,m^2+6}+5}-\frac{3}{2} \leq x$$

and

$$x \leq -\frac{1}{2}\,m+\frac{1}{2}\,\sqrt{5\,m^2+2\,\sqrt{6\,m^4+15\,m^2+6}+5}-\frac{3}{2}.$$

The lower bound is negative if $m > 0$, hence we have that $x > 0$, in case of the upper bound we obtain that $x \leq 1.08m$ if $m \geq 4$.

5.3 Algorithm to solve (5.1) for fixed m

Theorem 5.1 says that if there is a solution $(x, y) \in \mathbb{N}^2$ of the Diophantine equation (5.1), then $1 \leq x \leq 1.08m$. If m is small, then one can easily enumerate all solutions since the bound is linear in m. For larger values of m one can apply a sieve method similar to the Sieve of Eratosthenes, which eliminates composite numbers using small primes. There are many generalizations of the Sieve of Eratosthenes to solve different problems in number theory, cryptography (see e.g. [120] III.4.). We followed the steps described below to solve completely (5.1) in case of $4 \leq m \leq 10^6$.

(i) Define

$f(x) = x(x+1)(x+2)(x+3)(x+m)(x+m+1)(x+m+2)(x+m+3)$,

$F(p) = \{a : a \in [0 \ldots p-1]$ and $f(a) \bmod p$ is a square in $\mathbb{F}_p\}$ and for a given interval I

$S_I = \{a : a \in I \cap \mathbb{N}$ such that $f(a)$ is a square$\}$.

(ii) If $4 \leq m \leq 1000$ one computes $S_{[1,1.08m]}$ by direct enumeration.

(iii) If $m > 1000$. Let $N = \log_{30} 1.08m$ and $M = \sqrt[N]{1.08m}$.

(iv) Let $p_1, p_2, \ldots, p_{2N}$ be primes such that

$p_1 < p_2 < \ldots < p_N \leq M < p_{N+1} < \ldots < p_{2N}$.

(v) Compute $F(p_i)$ for all $i = 1, 2, \ldots, 2N$.

(vi) Sort the sets $F(p_i)$ such that

$$\frac{|F(p_{i_j})|}{p_{i_j}} < \frac{|F(p_{i_{j+1}})|}{p_{i_{j+1}}}.$$

(vii) Using the Chinese remainder theorem determine $I = \{a : a \in [1, 1.08m] \cap \mathbb{N}, a \bmod p_{i_1} \in F(p_{i_1}), a \bmod p_{i_2} \in F(p_{i_2}), \ldots, a \bmod p_{i_N} \in F(p_{i_N})\}$.

(viii) Compute S_I.

Note that here we used small primes around 30 having product about $1.08m$. For very small primes $|F(p)|/p$ is close to one since in this case for a given $a \in [0, \ldots, p-1]$ we have that a

is a root of $f(x)$. As an example consider the case $m = 1647$. Here we have $p_{i_1} = 47, p_{i_2} = 37$ and

$$\frac{|F(p_{i_1})|}{p_{i_1}} \approx 0.4468, \quad \frac{|F(p_{i_2})|}{p_{i_2}} \approx 0.5676.$$

Using the Chinese remainder theorem we obtain a set I having cardinality 441. So the cardinality of the search space is reduced by a factor about 4. We implemented the above algorithm in Sage [122].

5.4 On products of disjoint blocks of arithmetic progressions

In this section we present some related Diophantine equations involving products of consecutive integers. Let us recall that Bauer and Bennett [11] proved that for each positive integer j and a j tuple $(k_1, \ldots, k_j)$ the Diophantine equation

$$y^2 = x(x+1)\prod_{i=1}^{j}\prod_{l=0}^{k_i-1}(x_i + l) \tag{5.3}$$

has infinitely many solutions in positive integers $x, x_1, \ldots, x_j$. However, the proof they presented produces solutions which grow exponentially. In the light of this result one can ask whether in some cases we can find solutions in polynomials with integer coefficients. In this direction we offer the following:

Theorem 5.3

The Diophantine equations

$$x(x+1)y(y+1)(y+2) = z^2, \tag{5.4}$$

$$x(x+1)y(y+1)(y+2)(y+3) = z^2 \tag{5.5}$$

have infinitely many solutions in the ring $\mathbb{Z}[t]$. Moreover, the Diophantine equation

$$x(x+1)y(y+1)(y+2)(y+3)(y+4) = z^2 \tag{5.6}$$

has at least two solutions in the ring $\mathbb{Z}[t]$.

Let us introduce the notation

$$f(x,k,d) = x(x+d)\cdots(x+(k-1)d).$$

The next results deal with the question of whether the product of disjoint blocks of consecutive integers can be a product of two consecutive integers. We thus consider the Diophantine equation

$$\prod_{i=1}^{r} f(x_i, k_i, 1) = y(y+1). \tag{5.7}$$

This question concerning the solvability in integers of the equation (5.7) can be seen as a variation on Erdős and Graham question. We have the following:

Theorem 5.4

The Diophantine equations

$$x(x+1)y(y+1)(y+2) = z(z+1), \tag{5.8}$$

$$x(x+1)y(y+1)(y+2)(y+3) = z(z+1) \tag{5.9}$$

have infinitely many solutions in the ring $\mathbb{Z}[t]$*. Moreover, for* $k_1 = 3$*,* $r \geq 2$ *and each* $r-1$*-tuple* $k_2, \ldots, k_r$ *of positive integers the Diophantine equation (5.7) has at least six solutions in the ring* $\mathbb{Z}[x_2, \ldots, x_r]$*.*

Theorem 5.5

The Diophantine equation

$$x(x+1)y(y+1) = z(z+1)(z+2)(z+3) \tag{5.10}$$

has infinitely many solutions in positive integers satisfying the condition $(z-x)(z-x+2) \neq 0$*.*

In [142] the second author proved that the system of Diophantine equations

$$\begin{cases} x(x+1)+y(y+1) = p(p+1) \\ y(y+1)+z(z+1) = q(q+1) \\ z(z+1)+x(x+1) = r(r+1) \end{cases}$$

has infinitely many solutions in integers satisfying the condition $0 < x < y < z$. One can ask whether similar phenomenon holds for the multiplicative version of the above system. More precisely: does the system of Diophantine equations

$$\begin{cases} x(x+1)y(y+1) = p(p+1) \\ y(y+1)z(z+1) = q(q+1) \\ z(z+1)x(x+1) = r(r+1) \end{cases} \tag{5.11}$$

have infinitely many solutions in integers satisfying the condition $1 < x < y < z$? Motivated by this question we prove the following:

Theorem 5.6

The system (5.11) has infinitely many solutions in the ring of polynomials $\mathbb{Z}[t]$*.*

Consider the Diophantine equations

$$(x-b)x(x+b)(y-b)y(y+b) = z^2 \tag{5.12}$$

and

$$(x-b)x(x+b)(y-b)y(y+b) = (z-b)z(z+b) \tag{5.13}$$

where $b \in \mathbb{N}$ is a parameter. If a solution (x, y, z) satisfies $b \mid x$ and $b \mid y$, we call it trivial. If $b = 1$, then Sastry [65] noted that (5.12) has infinitely many positive integer solutions (x, y, z), where $y = 2x - 1$ and $(x+1)(2x-1)$ is a square. Zhang and Cai [148] proved that there exist

infinitely many nontrivial positive integer solutions of the Diophantine equation (5.12) if $b \geq 2$ is an even integer. They note that it is likely that for odd $b \geq 3$ integers there are also infinitely many solutions. They showed that (5.13) has infinitely many nontrivial positive integer solutions for $b = 1$, and the set of rational solutions of it is dense in the set of real solutions for $b \geq 1$. They posed the following question. Are all the nontrivial positive integer solutions of (5.13) for $b = 1$ with $x \leq y$ given by $(F_{2n-1}, F_{2n+1}, F_{2n}^2)$, $n \geq 1$? We prove that all "large" solutions have this shape while "small" solutions belong to certain intervals. We have the following statements.

Theorem 5.7

Let (x, y, z) be a nontrivial positive integer solution of equation (5.12) and $k = y - x$. Either

$$x = -\frac{48\,b^2k - 3\,k^3 \pm 2\left(4\,b^2 - k^2\right)\sqrt{-48\,b^2 + 3\,k^2}}{6\left(16\,b^2 - k^2\right)}$$

or

$$1 \leq x \leq \max_{1 \leq i \leq 3} B_i,$$

where

$$\begin{aligned} B_1 &= 2\max\left|-6\,b^2k^2 + \frac{3}{8}\,k^4 \pm \frac{3}{2}\,k\right|, \\ B_2 &= 2\max\left|-6\,b^2k^3 + \frac{3}{8}\,k^5 \mp b^2 \pm \frac{3}{8}\,k^2\right|^{1/2}, \\ B_3 &= 2\max\left|-b^4k^2 - \frac{1}{4}\,b^2k^4 - \frac{1}{64}\,k^6 \pm \frac{1}{4}\,b^2k \pm \frac{1}{32}\,k^3 - \frac{1}{64}\right|^{1/3}. \end{aligned}$$

Corollary 5.1

If $3 \leq b \leq 13$, b is odd and $2b < k \leq 300$, then all nontrivial positive integer solutions of equation (5.12) are as follows

b	(x, y, z)	b	(x, y, z)	b	(x, y, z)
3	(5, 12, 360)	5	(145, 343, 11083800)	7	(250, 507, 45103500)
3	(7, 18, 1260)	5	(33, 280, 877800)	9	(15, 36, 9720)
3	(4, 21, 504)	5	(16, 275, 277200)	9	(21, 54, 34020)
3	(8, 33, 3960) , (35, 60, 95760)	7	(10, 27, 3060)	9	(12, 63, 13608)
3	(10, 42, 8190)	7	(105, 128, 1552320)	9	(24, 99, 106920) , (105, 180, 2585520)
3	(7, 45, 5040)	7	(8, 42, 2940) , (41, 75, 167280)	9	(11, 90, 17820)
3	(32, 87, 146160)	7	(34, 75, 125460)	9	(30, 126, 221130)
3	(93, 245, 3437280)	7	(9, 56, 7056)	9	(21, 135, 136080)
3	(125, 363, 9662400)	7	(32, 91, 152880)	9	(25, 153, 220320)
3	(77, 333, 4102560)	7	(13, 98, 38220)	9	(10, 171, 30780)
5	(7, 30, 2100)	7	(42, 128, 388080)	9	(96, 261, 3946320)
5	(11, 49, 11088)	7	(8, 105, 11760)	11	(91, 119, 1113840)
5	(6, 49, 2772)	7	(8, 128, 15840)	11	(13, 132, 37752)
5	(11, 55, 13200)	7	(12, 140, 55860)	11	(12, 253, 66792)
5	(6, 55, 3300) , (21, 70, 54600)	7	(18, 169, 154440)	13	(22, 77, 55440)
5	(7, 75, 8400)	7	(32, 189, 458640)	13	(14, 169, 42588)
5	(19, 100, 79800)	7	(11, 169, 61776)	13	(15, 182, 70980)
5	(3605, 3703, 48773919600)	7	(185, 363, 17387040)	13	(99, 288, 4767840)

Table 1

Remark. We computed all nontrivial solutions with $3 \leq b \leq 25$, b is odd and $2b < k \leq 300$. There are 144 such solutions, the list can be downloaded from http://math.unideb.hu/

media/tengely-szabolcs/XblockYblockZ2.txt. We note that the total running time of our calculations was 11.6 hours on an Intel Core i5 2.6GHz PC.

Theorem 5.8

Let (x, y, z) be a nontrivial positive integer solution of equation (5.13) with $b = 1$. Either

$$(x, y, z) = (F_{2n-1}, F_{2n+1}, F_{2n}^2) \quad \text{for some } n \geq 1$$

or

$$1 \leq x \leq -\frac{1}{2}\,k + \frac{1}{2}\,\sqrt{3\,k^2 + 2\,k\sqrt{k^2+4} + 4},$$

where $k = y - x$.

Based on the previous theorem we have the following numerical result.

Corollary 5.2

If $4 \leq k \leq 5000$, then all nontrivial positive integer solutions of equation (5.13) with $b = 1$ have the form $(x, y, z) = (F_{2n-1}, F_{2n+1}, F_{2n}^2)$ for some $n \geq 1$.

5.5 Proofs of the results

Before we present the proofs let us note that if (Z', X') is a solution of the Diophantine equation $Z^2 - AX^2 = B$ and (Z, X) is s solution of $Z^2 - AX^2 = 1$ with $X \neq 0$, then for each n the pair (Z_n, X_n), where

$$Z_0 = Z' \quad X_0 = X', \quad Z_n = Z \cdot Z_{n-1} + AX \cdot X_{n-1}, \quad X_n = X \cdot Z_{n-1} + Z \cdot X_{n-1}$$

is solution of $Z^2 - AX^2 = B$.

In order to shorten the notation we write

$$f_k(x) := f(x, k, 1) = x(x+1) \cdot \ldots \cdot (x+k-1).$$

Proof. [Proof of Theorem 5.3] We observe that the equation (5.4) can be rewritten in the following form

$$Z^2 - f_3(y)X^2 = -f_3(y). \tag{5.14}$$

with $Z = 2z$ and $2x + 1 = X$. In order to solve this equation we take $y = t^2 + 1$ and we observe that the equation (5.14) has the solution

$$Z' = tf_3(t^2+1), \quad X' = t^4 + 3t^2 + 1.$$

Moreover, we note that the Diophantine equation $Z^2 - f_3(t^2+1)X^2 = 1$ has the nontrivial solution

$$Z = t^4 + 3t^2 + 1, \quad X = t.$$

According to remark given at the beginning of the section we see that for each n the pair of

polynomials (Z_n, X_n) defined by the recurrence relations

$$\begin{cases} Z_0 &= tf_3(t^2+1), \\ X_0 &= t^4+3t^2+1, \\ Z_n &= (t^4+3t^2+1)Z_{n-1}+tf_3(t^2+1)X_{n-1}, \\ X_n &= tZ_{n-1}+(t^4+3t^2+1)X_{n-1}, \end{cases}$$

is a solution of the equation (5.14). It is clear from the definition that $Z_n, X_n \in \mathbb{Z}[t]$ for each $n \in \mathbb{N}$. Moreover, by simple induction on n we check that $X_n(2t) \equiv 1 \pmod 2$ and $Z_n(2t) \equiv 0 \pmod 2$ in the ring of polynomials $\mathbb{Z}[t]$. As a consequence we get that for each n the pair of polynomials

$$x_n(t) = \frac{1}{2}(X_n(2t)-1), \quad z_n(t) = \frac{1}{2}Z_n(2t)$$

is the solution of equation (5.4) in the ring $\mathbb{Z}[t]$.

In order to get the polynomial solutions of the equation (5.5) we use the same method as above. We take $y = t$, where t is a variable and we rewrite our equation in the form

$$Z^2 - f_4(t)X^2 = -f_4(t) \tag{5.15}$$

with $Z = 2z$ and $X = 2x+1$. We found that

$$Z' = f_4(t), \quad X' = t^2+3t+1$$

is a solution of the equation (5.15) and the pair

$$Z = t^2+3t+1, \quad X = 1$$

solves the equation $Z^2 - f_4(t)X^2 = 1$. We thus see that for each $n \in \mathbb{N}$ the pair of polynomials (Z_n, X_n) defined by the recurrence relations

$$\begin{cases} Z_0 &= f_4(t), \\ X_0 &= t^2+3t+1, \\ Z_n &= (t^2+3t+1)Z_{n-1}+f_4(t)X_{n-1}, \\ X_n &= Z_{n-1}+(t^2+3t+1)X_{n-1}, \end{cases}$$

is a solution of the equation (5.15) in the ring $\mathbb{Z}[t]$. Similarly as in the previous case one can easily check that $X_n(2t) \equiv 1 \pmod 2$ and $Z_n(2t) \equiv 0 \pmod 2$ in $\mathbb{Z}[t]$ and in consequence, for each n the pair of polynomials with integer coefficients

$$x_n(t) = \frac{1}{2}(X_n(2t)-1), \quad z_n(t) = \frac{1}{2}Z_n(2t)$$

is the solution of the equation (5.5).

Finally, in order to show that the equation (5.6) has polynomial solutions we performed numerical search and found that triplets of polynomials

$$x = 2t(t+1)(2t-1)(2t+3), \quad y = 4t^2+4t-3, \quad z = 2x(y+2)(2t+1)(2t^2+2t-1),$$
$$x = (2t^2+2t+1)(4t^2+4t+5), \quad y = (2t+1)^2, \quad z = 4x(y+2)(2t+1)(t^2+t+1)$$

satisfy the equation (5.6).

Proof. [Proof of Theorem 5.4] We proceed in the same way as in the proof of Theorem 5.3. This time we take $y = 4t^2 + 1$, where t is a variable. In this situation our equation (5.8) is equivalent with the following one:

$$Z^2 - f_3(4t^2 + 1)X^2 = 1 - f_3(4t^2 + 1), \tag{5.16}$$

where $Z = 2z + 1$ and $X = 2x + 1$. We found that the pair of polynomials

$$Z' = 128t^7 + 192t^5 - 16t^4 + 88t^3 - 12t^2 + 12t - 1, \quad X' = 16t^4 + 12t^2 - 2t + 1$$

satisfies the equation (5.16). Moreover, the pair

$$Z = 16t^4 + 12t^2 + 1, \quad X = 2t$$

satisfies the corresponding equation $Z^2 - f_3(4t^2 + 1)X^2 = 1$. As a consequence we see that for each $n \in \mathbb{N}$ the pair of polynomials (Z_n, X_n) defined by the recurrence relations

$$\begin{cases} Z_0 &= 128t^7 + 192t^5 - 16t^4 + 88t^3 - 12t^2 + 12t - 1, \\ X_0 &= 16t^4 + 12t^2 - 2t + 1, \\ Z_n &= (16t^4 + 12t^2 + 1)Z_{n-1} + 2tf_3(4t^2 + 1)X_{n-1}, \\ X_n &= 2tZ_{n-1} + (16t^4 + 12t^2 + 1)X_{n-1}, \end{cases}$$

is a solution of the equation (5.15) in the ring $\mathbb{Z}[t]$. A simple induction shows that for each $n \in \mathbb{N}$ we have $X_n Z_n \equiv 1 \pmod 2$ in the ring $\mathbb{Z}[t]$ and thus the pair

$$x_n = \frac{1}{2}(X_n - 1), \quad z_n = \frac{1}{2}(Z_n - 1)$$

is the solution of the equation (5.8) with $y = 4t^2 + 1$.

We consider now the equation (5.9) with $y = t$. It is equivalent with the following one:

$$Z^2 - f_4(t)X^2 = 1 - f_4(t), \tag{5.17}$$

where $Z = 2z + 1$ and $X = 2x + 1$. We found that the pair of polynomials

$$Z' = 2t^6 + 18t^5 + 58t^4 + 78t^3 + 36t^2 - 1, \quad X' = 2t^4 + 12t^3 + 20t^2 + 6t - 1$$

satisfies the equation (5.17). Moreover, the pair

$$Z = t^2 + 3t + 1, \quad X = 1$$

satisfies the corresponding equation $Z^2 - f_4(t)X^2 = 1$. As a consequence we see that for each $n \in \mathbb{N}$ the pair of polynomials (Z_n, X_n) defined by the recurrence relations

$$\begin{cases} Z_0 &= 2t^6 + 18t^5 + 58t^4 + 78t^3 + 36t^2 - 1, \\ X_0 &= 2t^4 + 12t^3 + 20t^2 + 6t - 1, \\ Z_n &= (t^2 + 3t + 1)Z_{n-1} + f_4(t)X_{n-1}, \\ X_n &= Z_{n-1} + (t^2 + 3t + 1)X_{n-1}, \end{cases}$$

is a solution of the equation (5.17) in the ring $\mathbb{Z}[t]$. A simple induction shows that for each $n \in \mathbb{N}$ we have $X_{2n}(2t + 1)Z_{2n}(2t + 1) \equiv 1 \pmod 2$ in the ring $\mathbb{Z}[t]$ and thus the pair

$$x_n = \frac{1}{2}(X_{2n}(2t + 1) - 1), \quad z_n = \frac{1}{2}(Z_{2n}(2t + 1) - 1)$$

is the solution of the equation (5.9) with $y = t$.

Finally, in order to prove the last statement of our theorem let us put

$$A = \prod_{i=2}^{r} f(x_i, k_i, d)$$

and consider the curve

$$C: \ Ax(x+d)(x+2d) = y(y+d).$$

From geometric point of view C can be seen as a genus one curve defined over rational function field $\mathbb{Q}(A, d)$. The Weierstrass equation for C is given by

$$C': \ Y^2 = X^3 + 12AdX^2 + 32A^2d^2X + 16A^2d^2,$$

where the corresponding maps are the following:

$$\begin{aligned} \varphi: \ C \ni (x,y) &\mapsto (X,Y) = (4Ax, 4A(2y+d)) \in C', \\ \varphi^{-1}: \ C' \ni (X,Y) &\mapsto (x,y) = \left(\tfrac{X}{4A}, \tfrac{Y-4Ad}{8A}\right) \in C. \end{aligned}$$

Now using the trivial points with $y = 0$ lying on C we can define the points

$$\begin{aligned} P_1 &= \varphi((0,0)) = (0, 4Ad), \\ P_2 &= \varphi((-d,0)) = (-4Ad, 4Ad), \\ P_3 &= \varphi((-2d,0)) = (-8Ad, 4Ad). \end{aligned}$$

One can easily check that for each $i, j \in \{1,2,3\}$, $i \neq j$ the points $2P_i$ and $2P_i + 2P_j$ have polynomials with integer coefficients as coordinates and the same is true for the points $\varphi^{-1}(2P_i)$ and $\varphi^{-1}(2P_i + 2P_j)$. This leads us to the solutions of the equation defining C:

$$\begin{aligned} x &= Ad^2 - d, & y &= -A^2d^3 \\ x &= Ad^2 - d, & y &= A^2d^3 - d, \\ x &= 4Ad^2 + d, & y &= 8A^2d^3 + 6Ad^2 \\ x &= 4Ad^2 + d, & y &= -8A^2d^3 - 6Ad^2 - d \\ x &= 4Ad^2 - 3d, & y &= 8A^2d^3 - 6Ad^2 \\ x &= 4Ad^2 - 3d, & y &= -8A^2d^3 + 6Ad^2 - d. \end{aligned}$$

From the definition of A we know that it is essentially a polynomial in $\mathbb{Z}[x_2, \ldots, x_r]$ and hence we get the statement of our theorem.

Proof. [Proof of Theorem 5.5] In order to get the statement of our theorem we consider the intersection of the surface, say S, defined by the equation (5.10) and the plane L defined by the equation

$$L: \ x + y = 4z + 5.$$

We then observe that $S \cap L = C_1 \cup C_2$, where

$$\begin{aligned} C_1: &\quad (2z - 4x + 1)^2 - 3(2x+1)^2 = -2, \\ C_2: &\quad (2z + 4x + 5)^2 - 5(2x+1)^2 = -4. \end{aligned}$$

Using standard methods we find that all solutions in positive integers of corresponding Pell type

equations $U^2 - 3V^2 = -2$ and $U'^2 - 5V'^2 = -4$ are

$$U_0 = 1, V_0 = 1, \quad U_{n+1} = 2U_n + 3V_n, \quad V_{n+1} = U_n + 2V_n,$$
$$U'_0 = 1, V'_0 = 1, \quad U'_{n+1} = 9U'_n + 20V'_n, \quad V'_{n+1} = 4U'_n + 9V'_n$$

respectively. One can easily check, by induction on n, that $V_nV'_n \equiv 1 \pmod 2$ and $U_nU'_n \equiv 1 \pmod 2$ and in consequence, for each $n \in \mathbb{N}$ the triplets

$$x_n = \tfrac{1}{2}(V_n - 1), \quad y_n = \tfrac{1}{2}(4U_n + 7V_n - 1), \quad z_n = \tfrac{1}{2}(U_n + 2V_n - 3),$$
$$x_n = \tfrac{1}{2}(V'_n - 1), \quad y_n = \tfrac{1}{2}(9V'_n - 4U_n - 1), \quad z_n = \tfrac{1}{2}(U'_n - 2V'_n - 3)$$

are non-trivial solutions in non-negative integers of the equation (5.10).

Remark. Without much of work one can find that the related Diophantine equation

$$x(x+1)y(y+1) = z(z+1)(z+2)$$

has infinitely many solutions in positive integers satisfying the condition $x + 1 < y, (y - z)(y - z - 1) \neq 0$. In fact, the above equation has polynomial solutions of the following form:

$$\begin{aligned}
&x = t, && y = t^2 + t - 2, && z = (t-1)(t+2),\\
&x = t, && y = t^2 + t + 1, && z = t(t+1),\\
&x = 8t + 3, && y = 8t^2 + 7t + 1, && z = 2(8t^2 + 7t + 1),\\
&x = 8t + 4, && y = 8t^2 + 9t + 2, && z = 2(8t^2 + 9t + 2).
\end{aligned}$$

Proof. [Proof of Theorem 5.6] In fact we prove a slightly stronger result, i.e. that the system (5.11) has infinitely many polynomial solutions with $x = t$. In order to do that let us observe that the first equation from the system (5.11) is equivalent with the following one:

$$P^2 - t(t+1)Y^2 = 1 - t(t+1), \tag{5.18}$$

with $P = 2p + 1$ and $Y = 2y + 1$. This equation has infinitely many solutions in polynomials $P, Y \in \mathbb{Z}[t]$. Indeed, the equation (5.18) is satisfied by $P = 1$, $Y = 1$ and the related equation $P^2 - t(t+1)Y^2 = 1$ has the solution

$$P' = 2t + 1, \quad Y' = 2.$$

As a consequence we see that for each $n \in \mathbb{N}$ the pair (P_n, Y_n) of polynomials defined by the recurrence relations

$$\begin{cases}
P_0 &= 1\\
Y_0 &= 1\\
P_n &= (2t+1)P_{n-1} + 2t(t+1)Y_{n-1}\\
Y_n &= 2P_{n-1} + (2t+1)Y_{n-1}
\end{cases}$$

is a solution of the equation (5.18). We thus see that the polynomials

$$y = y_n = \tfrac{1}{2}(Y_n - 1) \quad p = p_n = \tfrac{1}{2}(P_n - 1)$$
$$z = z_n = y_{n+1} \qquad r = r_n = p_{n+1}$$

satisfy the first and third equation in the system (5.11). In order to get the result it is enough to prove that with our choice of x, y, z the second equation in the system (5.11) is satisfied too, i.e.

$y(y+1)z(z+1) = y_n(y_n+1)y_{n+1}(y_{n+1}+1) = q(q+1)$ for some $q \in \mathbb{Z}[t]$. This is easy due to the identity

$$f\left(\frac{u-1}{2}\right) \qquad f\left(\frac{2v+(2t+1)u-1}{2}\right) - f\left(\frac{(v-u)((2t^2+4t+1)u+(2t+3)v)}{4(t^2+t-1)}\right)$$
$$= (v^2 - t(t+1)u^2 - 1 + t(t+1))H(u,v),$$

where $4(t^2+t-1)H$ is a polynomial in $\mathbb{Z}[u,v,t]$ and $f(x) = x(x+1)$. If we put now $u = Y_n$, $v = P_n$ then we have the equalities

$$y_n = \frac{1}{2}(u-1), \quad y_{n+1} = \frac{2v+(2t+1)u-1}{2},$$

and simple induction reveals that

$$v - u = P_n - Y_n \equiv 0 \pmod{2(t^2+t-1)} \quad \text{and} \quad uv = Y_nP_n \equiv 1 \pmod 2$$

in the ring $\mathbb{Z}[t]$. As a consequence of our reasoning we see that for each $n \in \mathbb{N}$ the function

$$q_n = \frac{(P_n - Y_n)((2t^2+4t+1)Y_n + (2t+3)P_n)}{4(t^2+t-1)}$$

is a polynomial in $\mathbb{Z}[t]$ and thus we get the result.

Proof. [Proof of Theorem 5.7] In the proof we will use the following result of Fujiwara [55].

Lemma 5.1

Put $p(z) = \sum_{i=0}^{n} a_i z^i$, $a_n \neq 0$, where $a_i \in \mathbb{R}$ for all $i = 0, 1, \ldots, n$. Then

$$\max\{|\zeta| : p(\zeta) = 0\} \leq 2\max\left\{\left|\frac{a_{n-1}}{a_n}\right|, \left|\frac{a_{n-2}}{a_n}\right|^{1/2}, \ldots, \left|\frac{a_0}{2a_n}\right|^{1/n}\right\}.$$

Without loss of generality we may assume $k > 0$. We apply Runge's method to determine a bound for the size of integral solutions. Let $F(x) = (x-b)x(x+b)(x+k-b)(x+k)(x+k+b)$.The polynomial part of the Puiseux expansion of

$$((x-b)x(x+b)(x+k-b)(x+k)(x+k+b))^{1/2}$$

is

$$P(x) = x^3 + \frac{3}{2}kx^2 + \left(-b^2 + \frac{3}{8}k^2\right)x - \frac{1}{2}b^2k - \frac{1}{16}k^3.$$

We have that

$$256F(x) - (16P(x)-1)^2 = 32x^3 + \left(-192\,b^2k^2 + 12\,k^4 + 48\,k\right)x^2 +$$
$$+ \left(-192\,b^2k^3 + 12\,k^5 - 32\,b^2 + 12\,k^2\right)x - 64\,b^4k^2 - 16\,b^2k^4 - k^6 - 16\,b^2k - 2\,k^3 - 1,$$
$$256F(x) - (16P(x)+1)^2 = -32x^3 + \left(-192\,b^2k^2 + 12\,k^4 - 48\,k\right)x^2 +$$
$$+ \left(-192\,b^2k^3 + 12\,k^5 + 32\,b^2 - 12\,k^2\right)x - 64\,b^4k^2 - 16\,b^2k^4 - k^6 + 16\,b^2k + 2\,k^3 - 1.$$

Fujiwara's result implies that all roots of these cubic polynomials satisfy $|x| \leq \max_{1\leq i\leq 3} B_i$,

where

$$\begin{aligned} B_1 &= 2\max\left|-6\,b^2k^2+\frac{3}{8}\,k^4\pm\frac{3}{2}\,k\right|,\\ B_2 &= 2\max\left|-6\,b^2k^3+\frac{3}{8}\,k^5\mp b^2\pm\frac{3}{8}\,k^2\right|^{1/2},\\ B_3 &= 2\max\left|-b^4k^2-\frac{1}{4}\,b^2k^4-\frac{1}{64}\,k^6\pm\frac{1}{4}\,b^2k\pm\frac{1}{32}\,k^3-\frac{1}{64}\right|^{1/3}. \end{aligned}$$

Therefore if $|x|>\max_{1\le i\le 3}B_i$, then either

$$(16P(x)+1)^2<256F(x)=(16y)^2<(16P(x)-1)^2$$

or

$$(16P(x)-1)^2<256F(x)=(16y)^2<(16P(x)+1)^2.$$

Hence $y=\pm P(x)$. It remains to solve the equation $F(x)=P(x)^2$. It follows that

$$x=-\frac{48\,b^2k-3\,k^3\pm2\left(4\,b^2-k^2\right)\sqrt{-48\,b^2+3\,k^2}}{6\left(16\,b^2-k^2\right)}.$$

Proof. [Proof of Theorem 5.8] We apply Runge's method to determine an upper bound for the size of possible positive integer solutions of the equation

$$F(x):=(x-1)x(x+1)(x+k-1)(x+k)(x+k+1)=(z-1)z(z+1),$$

where $y=x+k$ for some positive integer k. We have that

$$(x^2+kx-1)^3<F(x)<(x^2+kx)^3$$

if x is large. In fact, the second inequality is true if $k>1$. The roots of the polynomial $F(x)-(x^2+kx-1)^3$ are as follows

$$\begin{aligned} -\frac{1}{2}\,k-\frac{1}{2}\,\sqrt{3\,k^2+2\,k\sqrt{k^2+4}+4} &\approx -\frac{1}{2}\,k\Big(\sqrt{5}+1\Big),\\ -\frac{1}{2}\,k-\frac{1}{2}\,\sqrt{3\,k^2-2\,k\sqrt{k^2+4}+4} &\approx -k,\\ -\frac{1}{2}\,k+\frac{1}{2}\,\sqrt{3\,k^2-2\,k\sqrt{k^2+4}+4} &\approx \frac{1}{k^3},\\ -\frac{1}{2}\,k+\frac{1}{2}\,\sqrt{3\,k^2+2\,k\sqrt{k^2+4}+4} &\approx \frac{1}{2}\,k\Big(\sqrt{5}-1\Big). \end{aligned}$$

Therefore if

$$x>-\frac{1}{2}\,k+\frac{1}{2}\,\sqrt{3\,k^2+2\,k\sqrt{k^2+4}+4},$$

then the first inequality is valid. Similarly we obtain that

$$(z-1)^3<(z-1)z(z+1)<(z+1)^3$$

if $z\notin\{-1,1\}$. Assume that $x>-\frac{1}{2}\,k+\frac{1}{2}\,\sqrt{3\,k^2+2\,k\sqrt{k^2+4}+4}$ and $z\notin\{-1,1\}$. We obtain that

$$(x^2+kx-1)^3-(z+1)^3<0<(x^2+kx)^3-(z-1)^3.$$

It follows that $z=x^2+kx-1$ or $z=x^2+kx$. If $z=x^2+kx$, then $(k^2+2kx+2x^2-2)(k+x)x=0$ and we get that either $x=0, x=-k$ or $|k|\le 2$. In the latter case $k=1$ or 2 and we obtain

overlapping blocks, a contradiction.

If $z = x^2 + kx - 1$, then $(k^2 - kx - x^2 + 1)(k + x)x = 0$ and we have that $x = 0, x = -k$ or

$$x = -\frac{1}{2}k \pm \frac{1}{2}\sqrt{5k^2 + 4}.$$

Since x is a positive integer it follows that $k = F_{2n}$. It yields that either $x = F_{2n-1}$ or $x = -F_{2n+1}$. The latter is negative so the only possible positive solution is $x = F_{2n-1}$. Since $y = x + k$, we obtain that $y = F_{2n+1}$. Thus $(x, y, z) = (F_{2n-1}, F_{2n+1}, F_n^2)$ provides solutions.

Proof. [Proof of Corollary 5.2] We wrote a Sage [122] code to determine all integral solution of equation (5.13) with $b = 1$ in the interval provided by Theorem 5.8.

5.6 An additive Erdős-Graham type problem

For $k = 0, 1, 2, \ldots$ put

$$f_k(x) = \sum_{i=0}^{k} \prod_{j=0}^{i} (x + j).$$

For the first few values of k we have

$$f_0(x) = x, \quad f_1(x) = x + x(x + 1) = x(x + 2),$$
$$f_2(x) = x + x(x + 1) + x(x + 1)(x + 2) = x(x + 2)^2.$$

In general, $f_k(x)$ is a monic polynomial of degree $k + 1$. Further, the coefficients of the $f_k(x)$ are positive integers, which could easily be expressed as sums of consecutive Stirling numbers of the first kind.

In this section we are interested in the equation

$$f_k(x) = y^n \tag{5.19}$$

in integers x, y, k, n with $k \geq 0$ and $n \geq 2$. Without loss of generality, throughout the section we shall assume that n is a prime. Our first theorem gives a general effective finiteness result for equation (5.19).

Theorem 5.9

For the solutions of equation (5.19) we have the following:

i) if $k \geq 1$ and $y \neq 0, -1$ then $n < c_1(k)$,

ii) if $k \geq 1$ and $n \geq 3$ then $\max(n, |x|, |y|) < c_2(k)$,

iii) if $k \geq 1$, $k \neq 2$, and $n = 2$ then $\max(|x|, |y|) < c_3(k)$.

Here $c_1(k), c_2(k), c_3(k)$ are effectively computable constants depending only on k.

The following theorem describes all solutions of equation (5.19) for $k \leq 10$.

Theorem 5.10

Let $1 \le k \le 10$ such that $k \ne 2$ if $n = 2$. Then equation (5.19) has the only solutions $(x, y) = (-2, 0), (0, 0)$, k, n arbitrary; $(x, y) = (-1, -1)$, k, n arbitrary with $n \ge 3$; $(x, y, k, n) = (-4, 2, 1, 3), (2, 2, 1, 3), (2, 2, 2, 5)$.

Remark. Note that the assumptions in Theorems 5.9 and 5.10 are necessary: equation (5.19) has infinitely many solutions (x, y, k, n) with $k = 0$, with $y = 0$ or -1, and with $k = 2$, $n = 2$. These solutions can be described easily.

5.7 Proof of Theorem 5.9

To prove Theorem 5.9 we need three lemmas. To formulate them, we have to introduce some notation. Let $g(x)$ be a non-zero polynomial with integer coefficients, of degree d and height H. Consider the Diophantine equation

$$g(x) = y^n \tag{5.20}$$

in integers x, y, n with n being a prime.

The next lemma is a special case of a result of Tijdeman [132]. For a more general version, see [113].

Lemma 5.2

If $g(x)$ has at least two distinct roots and $|y| > 1$, then in equation (5.20) we have $n < c_4(d, H)$, where $c_4(d, H)$ is an effectively computable constant depending only on d, H.

The next lemma is a special case of a theorem of Brindza [28].

Lemma 5.3

Suppose that one of the following conditions holds:

i) $n \ge 3$ and $g(x)$ has at least two roots with multiplicities coprime to n,

ii) $n = 2$ and $g(x)$ has at least three roots with odd multiplicities.

Then in equation (5.20) we have $\max(|x|, |y|) < c_5(d, H)$, where $c_5(d, H)$ is an effectively computable constant depending only on d, H.

The last assertion needed to prove Theorem 5.9 describes the root structure of the polynomial family $f_k(x)$.

Lemma 5.4

We have

$$f_0(x) = x, \quad f_1(x) = x(x + 2), \quad f_2(x) = x(x + 2)^2.$$

Beside this, for $k \ge 3$ all the roots of the polynomial $f_k(x)$ are simple. In particular, 0 is

a root of $f_k(x)$ for all $k \geq 0$, and -2 is a root of $f_k(x)$ for all $k \geq 1$.

Proof. For $k = 0, 1, 2$ the statement is obvious. In the rest of the proof we assume that $k \geq 3$.

It follows from the definition that x is a factor of $f_k(x)$ (or, 0 is a root of $f_k(x)$) for all $k \geq 0$. Further, since

$$x + x(x+1) = x(x+2),$$

the definition clearly implies that $x+2$ is a factor (or, -2 is a root) of $f_k(x)$ for $k \geq 1$. So it remains to prove that all the roots of $f_k(x)$ $(k \geq 3)$ are simple.

For this observe that by the definition we have

$$f_k(1) > 0, \quad f_k(-1) = -1 < 0, \quad f_k(-1.5) > 0.$$

The last inequality follows from the fact that writing

$$P_i(x) = x(x+1)\dots(x+i)$$

for $i = 0, 1, 2, \dots$, we have that $P_i(-1.5) > 0$ for $i \geq 1$. Hence $f_k(-1.5) \geq -1.5 + 0.75 + 0.375 + 0.5625 > 0$ for $k \geq 3$. Further, as one can easily check, for $i = -3, \dots, -k-1$ we have

$$(-1)^i f_k(i) > 0.$$

These assertions (by continuity) imply that $f_k(x)$ has roots in the intervals

$$(-1, 1),\ (-1.5, -1),\ (-3, -1.5),\ (-4, -3),\ (-5, -4),\ \dots,\ (-k-1, -k).$$

(Note that in the first and third intervals the roots are 0 and -2, respectively.) Hence $f_k(x)$ has $\deg(f_k(x)) = k+1$ distinct real roots, and the lemma follows.

Now we are ready to give the proof of Theorem 5.9.

Proof. [Proof of Theorem 5.9] i) Let $k \geq 1$. By Lemma 5.4 we have that $f_k(x)$ is divisible by $x(x+2)$ in $\mathbb{Z}[x]$. In particular, the polynomial $f_k(x)$ has two distinct roots, namely 0 and -2. Further, observe that $f_k(x)$ does not take the value 1 for $x \in \mathbb{Z}$. Indeed, since $x(x+2)$ divides $f_k(x)$, it would be possible only for $x = -1$. However, for that choice by definition we clearly have $f_k(-1) = -1$ for any $k \geq 0$. Hence equation (5.19) has no solution with $y = 1$, and our claim follows by Lemma 5.2.

ii) Let $k \geq 1$ and $n \geq 3$. Recall that n is assumed to be a prime. By the explicit form of $f_1(x)$ and $f_2(x)$ we see that 0 and -2 are roots of these polynomials of degrees coprime to n. Hence the statement follows from part i) of Lemma 5.3 in these cases. Let $k \geq 3$. Then by Lemma 5.4, all the roots of $f_k(x)$ are simple. Since now the degree $k+1$ of $f_k(x)$ is greater than two, our claim follows from part i) of Lemma 5.3.

iii) Let $k \geq 1$, $k \neq 2$ and $n = 2$. In case of $k = 1$, equation (5.19) now reads as

$$x(x+2) = y^2.$$

Since $x(x+2) = (x+1)^2 - 1$, our claim obviously follows in this case. Let now $k \geq 3$. Then

by Lemma 5.4, all the roots of $f_k(x)$ are simple. As now the degree $k+1$ of $f_k(x)$ is greater than two, by part ii) of Lemma 5.3 the assertion follows also in this case.

5.8 Linear forms in logarithms

In this section, we use linear forms in logarithms to give a bound for n for the solution (u, v, n) of equations of the form

$$au^n - bv^n = c$$

under certain conditions. These bounds will be used in the proof of Theorem 5.10 for $n \geq 3$. Such equations have been studied by many authors. Note that bounds for such equations were obtained in [12, 67]. We refer to [12] for earlier results. However, in these papers the restrictions put on the coefficients a, b, c are not valid in the cases we need later on.

We begin with some preliminaries for linear forms in logarithms. For an algebraic number α of degree d over $\mathbb{Q}$, the *absolute logarithmic height* $h(\alpha)$ of α is given by

$$h(\alpha) = \frac{1}{d}\left(\log|a| + \sum_{i=1}^{d} \log\max(1, |\alpha^{(i)}|)\right)$$

where a is the leading coefficient of the minimal polynomial of α over $\mathbb{Z}$ and the $\alpha^{(i)}$'s are the conjugates of α. When $\alpha = \frac{p}{q} \in \mathbb{Q}$ with $(p, q) = 1$, we have $h(\alpha) = \max(\log|p|, \log|q|)$.

The following result is due to Laurent [81, Theorem 2].

Theorem 5.11

Let a_1, a_2, h, ϱ and μ be real numbers with $\varrho > 1$ and $1/3 \leq \mu \leq 1$. Set

$$\sigma = \frac{1 + 2\mu - \mu^2}{2}, \quad \lambda = \sigma\log\varrho, \quad H = \frac{h}{\lambda} + \frac{1}{\sigma},$$
$$\omega = 2\left(1 + \sqrt{1 + \frac{1}{4H^2}}\right), \quad \theta = \sqrt{1 + \frac{1}{4H^2}} + \frac{1}{2H}.$$

Let α_1, α_2 be non-zero algebraic numbers and let $\log\alpha_1$ and $\log\alpha_2$ be any determinations of their logarithms. Without loss of generality we may assume that $|\alpha_1| \geq 1, |\alpha_2| \geq 1$. Let

$$\Lambda = |b_2\log\alpha_1 - b_2\log\alpha_2| \quad b_1, b_2 \in \mathbb{Z}, b_1 > 0, b_2 > 0,$$

where b_1, b_2 are positive integers. Suppose that α_1 and α_2 are multiplicatively independent. Put $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]/[\mathbb{R}(\alpha_1, \alpha_2) : \mathbb{R}]$ and assume that

$$\begin{aligned} &h \geq \max\left\{D\left(\log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log\lambda + 1.75\right) + 0.06, \lambda, \frac{D\log 2}{2}\right\}, \\ &a_i \geq \max\left\{1, \varrho\log|\alpha_i| - \log|\alpha_i| + 2Dh(\alpha_i)\right\}, \ (i = 1, 2), \\ &a_1 a_2 \geq \lambda^2. \end{aligned} \tag{5.21}$$

Then

$$\log \Lambda \geq -C\left(h+\frac{\lambda}{\sigma}\right)^2 a_1a_2 - \sqrt{\omega\theta}\left(h+\frac{\lambda}{\sigma}\right) - \log\left(C'\left(h+\frac{\lambda}{\sigma}\right)^2 a_1a_2\right)$$

with

$$C = \frac{\mu}{\lambda^3\sigma}\left(\frac{\omega}{6}+\frac{1}{2}\sqrt{\frac{\omega^2}{9}+\frac{8\lambda\omega^{5/4}\theta^{1/4}}{3\sqrt{a_1a_2H^{1/2}}}}+\frac{4}{3}\left(\frac{1}{a_1}+\frac{1}{a_2}\right)\frac{\lambda\omega}{H}\right)^2,$$

$$C' = \sqrt{\frac{C\sigma\omega\theta}{\lambda^3\mu}}.$$

We use Theorem 5.11 to give a bound for n for the equation $au^n - bv^n = c$. For this, we need the following lemma.

Lemma 5.5

Let a, b, c be positive integers with $b > a > 0$ and $abc \leq 4 \cdot 2018957 \cdot 99 \cdot 467$. Then the equation $au^n - bv^n = \pm c$ with $u > v > 1$ implies

$$\frac{u}{v} \leq \begin{cases} 1.00462 & \text{if } b \leq 100 \text{ and } n \geq 1000 \\ 1.00462 & \text{if } b \leq 10000 \text{ and } n \geq 2000 \\ 1.00267 & \text{if } n \geq 10000 \end{cases} \tag{5.22}$$

and

$$u > v \geq \begin{cases} 217 & \text{if } b \leq 100 \text{ and } n \geq 1000 \\ 217 & \text{if } b \leq 10000 \text{ and } n \geq 2000 \\ 375 & \text{if } n \geq 10000. \end{cases} \tag{5.23}$$

Proof. From $au^n - bv^n = \pm c$, we get $(\frac{u}{v})^n = \frac{b}{a} \pm \frac{c}{av^n} \leq b + 1/4$ since $n \geq 1000$ and $c \leq 2^{100}a$. Therefore

$$\frac{u}{v} \leq \begin{cases} \sqrt[1000]{100+1/4} & \text{if } b \leq 100 \text{ and } n \geq 1000 \\ \sqrt[2000]{10000+1/4} & \text{if } b \leq 10000 \text{ and } n \geq 2000 \\ \sqrt[10000]{4 \cdot 2018957 \cdot 99 \cdot 467 + 1/4} & \text{if } n \geq 10000 \end{cases}$$

implying (5.22). The assertion (5.23) follows easily from (5.22) by observing that $1 \leq u - v \leq 0.00462v, 0.00462v, 0.00267v$ according as $b \leq 100, n \geq 1000$ or $b \leq 10000, n \geq 2000$, or $n \geq 10000$, respectively.

Proposition 5.1

Let a, b, c be positive integers with $c \leq 2ab$. Then the equation

$$au^n - bv^n = \pm c \tag{5.24}$$

in integer variables $u > v > 1, n > 3$ *implies*

$$n \leq \begin{cases} \max\{1000, 824.338 \log b + 0.258\} & \text{if } b \leq 100 \\ \max\{2000, 769.218 \log b + 0.258\} & \text{if } 100 < b \leq 10000 \\ \max\{10000, 740.683 \log b + 0.234\} & \text{if } b > 10000. \end{cases} \tag{5.25}$$

In particular, $n \leq 3796, 7084, 19736$ *when* $b \leq 100, 10000, 4 \cdot 9 \cdot 11 \cdot 467 \cdot 2018957$*, respectively.*

Remark. We note here that when $c \leq 3$, we can get a much better bound, see [15]. However, we will follow a more general approach.

Proof. We can rewrite (5.24) as

$$\left| \frac{b}{a} \left(\frac{u}{v} \right)^n - 1 \right| = \frac{c}{au^n}.$$

Let

$$\Lambda = \left| n \log \frac{u}{v} - \log \frac{b}{a} \right|.$$

Then $\Lambda \leq \frac{2c}{au^n}$ implying

$$\log \Lambda \leq -n \log u + \log \left(\frac{2c}{a} \right) \leq -n \log u + \log(4b) \tag{5.26}$$

since $c \leq 2ab$. We now apply Theorem 5.11 to get a lower bound for Λ. We follow the proof of [81, Corollary 1, 2]. Let

$$\alpha_1 = \frac{u}{v}, \ \alpha_2 = \frac{b}{a}, \ b_1 = n, \ b_2 = 1$$

so that $h(\alpha_1) = \log u, h(\alpha_2) = \log b$ and $D = 1$. Let $m = 8$ and we choose $\varrho, \mu, q_0, u_0, b_0$ as follows:

b	ϱ	μ	q_0	u_0	b_0
$b \leq 100$	5.7	0.54	$\log 1.00462$	218	$\log 4$
$b \leq 10000$	5.6	0.57	$\log 1.00462$	218	$\log 5$
$b > 10000$	5.6	0.59	$\log 1.00267$	$\log 376$	$\log 10000$

By Lemma 5.5, we have $u \geq u_0, \log(u/v) \leq q_0$ and $b \geq b_0$. We take

$$a_1 = (\varrho - 1)q_0 + 2 \log u, \ a_2 = (\varrho + 1) \log b,$$

and

$$h = \max \left\{ m, \log \left(\frac{n}{a_2} + \frac{1}{a_1} \right) + 1.81 + \log \lambda \right\}.$$

Then (5.21) is satisfied. In fact, we have

$$h \geq m, \ a_1 \geq (\varrho - 1)q_0 + 2 \log u_0, \ a_2 \geq (\varrho + 1) \log b_0.$$

As in the proof of [81, Corollary 1, 2], we get

$$\log \Lambda \geq -C''_m(\varrho + 1)(\log b)((\varrho - 1)q_0 + 2 \log u), h^2$$

where C''_m is the constant C'' obtained in [81, Section 4, (28)] by putting $h = m, a_1 =$

$(\varrho-1)q_0+2\log u_0$ and $a_2 \geq (\varrho+1)\log b_0$. Putting $C_m = C_m''(\varrho+1)$, we get

$$\log\Lambda \geq -C_m(\log b)((\varrho-1)q_0+2\log u)(\max(m,h_n))^2,$$

where

$$h_n = \log\left(\frac{n}{(\varrho+1)\log b}+\frac{1}{2\log u+(\varrho-1)q_0}\right)+\varepsilon_m,$$

and

$$(C_m,\varepsilon_m) = \begin{cases} (5.8821, 2.2524) & \text{if } b \leq 100, \\ (5.4890, 2.2570) & \text{if } b \leq 10000, \\ (5.3315, 2.2662) & \text{if } b > 10000. \end{cases}$$

Comparing this lower bound of $\log\Lambda$ with the upper bound (5.26), we obtain

$$\begin{aligned} n &\leq C_m(\max(m,h_n))^2(\log b)\left(2+\frac{(\varrho-1)q_0}{\log u}\right)+\frac{\log 4b}{\log u} \\ &\leq C_m(\max(m,h_n))^2(\log b)\left(2+\frac{(\varrho-1)q_0}{\log u_0}+\frac{1}{\log u_0}\right)+\frac{\log 4}{\log u_0} \end{aligned} \tag{5.27}$$

since $u \geq u_0$. Recall that $m = 8$. We now consider two cases.

Assume $h_n \geq 8$. Then

$$n \geq n_0 := \left\{\exp(m-\varepsilon_m)-\frac{1}{2\log u+(\varrho-1)q_0}\right\}(\varrho+1)\log b$$

and $h_{n_0} = 8$. Since the last expression of (5.27) is a decreasing function of n, we have for $n \geq n_0$ that

$$\begin{aligned} 0 \leq & \frac{C_m h_n^2(\log b)\left(2+\frac{(\varrho-1)q_0}{\log u_0}+\frac{1}{\log u_0}\right)+\frac{\log 4}{\log u_0}-n}{\log b} \\ \leq & \frac{C_m h_{n_0}^2(\log b)\left(2+\frac{(\varrho-1)q_0}{\log u_0}+\frac{1}{\log u_0}\right)+\frac{\log 4}{\log u_0}-n_0}{\log b} \\ \leq & C_m m^2\left(2+\frac{(\varrho-1)q_0}{\log u_0}+\frac{1}{\log u_0}\right)+\frac{\log 4}{(\log u_0)(\log b)} \\ & -(\varrho+1)\exp(m-\varepsilon_m)+\frac{\varrho+1}{2\log u+(\varrho-1)q_0} \\ \leq & C_m m^2\left(2+\frac{(\varrho-1)q_0}{\log x_0}+\frac{1}{\log u_0}\right)+\frac{\log 4}{(\log u_0)(\log b_0)} \\ & -(\varrho+1)\exp(m-\varepsilon_m)+\frac{\varrho+1}{2\log u_0+(\varrho-1)q_0} < 0 \end{aligned}$$

since $u \geq u_0$ and $b \geq b_0$. This is a contradiction.

Therefore $h_n < 8$. Then from (5.27), we get

$$n \leq C_m m^2(\log b)\left(2+\frac{(\varrho-1)q_0}{\log u_0}+\frac{1}{\log u_0}\right)+\frac{\log 4}{\log u_0},$$

where $m = 8$. Hence we get the assertion (5.25) by putting explicit values of $m = 8, C_m, \varrho, \mu, q_0, u_0, b_0$ in the above inequality. The statement following (5.25) is clear.

5.9 Proof of Theorem 5.10 for $n \geq 3$

Throughout this section we assume that $n \geq 3$ is a prime.

Suppose first that $k = 1$ or 2. Then equation (5.19) can be rewritten as

$$x(x+2)^k = y^n.$$

We see that for every n odd, $(x, n) = (-1, n)$ is a solution. Hence we may suppose that $x \notin \{-2, -1, 0\}$. Hence $\gcd(x, x+2) \leq 2$ gives

$$x = 2^\alpha u^n, \quad x+2 = 2^\beta v^n$$

with non-negative integers α, β and coprime integers u, v. This implies

$$2^\beta v^n - 2^\alpha u^n = 2(1)^n.$$

Using now results of Darmon and Merel [47] and Ribet [105], our statement easily follows in this case.

Let $k \geq 3$. Then equation (5.19) can be rewritten as

$$y^n = f_k(x) = x(x+2)g_k(x)$$

where $g_k(x)$ is a polynomial of degree $k-1$. We see that for every k, $(x, n) = (-1, n)$ is a solution. Hence we may suppose that $x \notin \{-2, -1, 0\}$. Then we have either $x > 0$ or $x < x+2 < 0$.

We see that $(x, x+2) = 1, 2$ with 2 only if x is even, $(x, g_k(x))|g_k(0)$ and $(x+2, g_k(x))|g_k(-2)$. Also $g_k(x)$ is odd for every x. The values of $g_k(0)$ and $-g_k(-2)$ are given in **Table** 5.1.

k	3	4	5	6	7	8	9	10
$g_k(0)$	5	17	$7 \cdot 11$	$19 \cdot 23$	2957	23117	204557	2018957
$-g_k(-2)$	1	3	3^2	$3 \cdot 11$	$3^2 \cdot 17$	$3^2 \cdot 97$	$3^4 \cdot 73$	$3^2 \cdot 11 \cdot 467$

Table 5.1: Values of $g_k(0)$ and $-g_k(-2)$ for $3 \leq k \leq 10$

If $x = v^n$, $x+2 = u^n$ are both n-th powers, then we have $u^n - v^n = 2$ giving the trivial solution $x+2 = 1$, $x = -1$ which is already excluded. Hence we can suppose that either x or $x+2$ is not n-th power. Thus we can write

$$x = 2^{\delta_1} s_1 t_1^{n-1} u_1^n, \; x+2 = 2^{\delta_2} 3^{\nu_2} s_2 t_2^{n-1} u_2^n, \; g_k(x) = 3^{\nu_3} (s_1 s_2)^{n-1} t_1 t_2 u_3^n,$$

where

$$s_1 t_1 | g_k(0), \; s_2 t_2 | g_k(-2) \text{ with } (s_1, t_1) = (s_2, t_2) = 1, 3 \nmid s_1 s_2 t_1 t_2,$$

and

$$\delta_1, \delta_2 \in \{(0,0), (1, n-1), (n-1, 1)\},$$

and $(\nu_2, \nu_3) = (0, 0)$ or

$$\nu_2 \in \{1, \cdots, \mathrm{ord}_3(g_k(-2))\}, \; \nu_3 = n - \nu_2 \text{ or vice versa.}$$

Further, each of s_i, t_i is positive and u_1, u_2 are of the same sign. From $x+2-x=2$, we get

$$3^{\nu_2}s_2t_1(t_2u_2)^n - s_1t_2(t_1u_1)^n = 2t_1t_2 \text{ if } \delta_1=\delta_2=0, \nu_2 \le \mathrm{ord}_3(g_k(-2));$$
$$s_2t_1(3t_2u_2)^n - 3^{\nu_3}s_1t_2(t_1u_1)^n = 2\cdot 3^{\nu_3}t_1t_2 \text{ if } \delta_1=\delta_2=0, \nu_2 > \mathrm{ord}_3(g_k(-2));$$
$$3^{\nu_2}s_2t_1(2t_2u_2)^n - 4s_1t_2(t_1u_1)^n = 4t_1t_2 \text{ if } \delta_1=1, \nu_2 \le \mathrm{ord}_3(g_k(-2));$$
$$4\cdot 3^{\nu_2}s_2t_1(t_2u_2)^n - s_1t_2(2t_1u_1)^n = 4t_1t_2 \text{ if } \delta_2=1, \nu_2 \le \mathrm{ord}_3(g_k(-2));$$
$$s_2t_1(6t_2u_2)^n - 4\cdot 3^{\nu_3}s_1t_2(t_1u_1)^n = 4\cdot 3^{\nu_3}t_1t_2 \text{ if } \delta_1=1, \nu_2 > \mathrm{ord}_3(g_k(-2));$$
$$4s_2t_1(3t_2u_2)^n - 3^{\nu_3}s_1t_2(2t_1u_1)^n = 4\cdot 3^{\nu_2}t_1t_2 \text{ if } \delta_2=1, \nu_2 > \mathrm{ord}_3(g_k(-2)).$$

These equations are of the form $au^n - bv^n = c$ with u, v of the same sign. Note that from the equation $au^n - bv^n = c$, we can get back $x, x+2$ by

$$x = \frac{2bv^n}{c}, \quad x+2 = \frac{2au^n}{c}.$$

We see from Table 1 that the largest value of $\max(a,b)$ is given by $k=10$ and equation

$$(6\cdot 11\cdot 467u_2)^n - 4\cdot 3^2\cdot 11\cdot 467\cdot 2018957u_1^n = 4\cdot 3^2\cdot 11\cdot 467.$$

We observe that $|c| \le \frac{2ab}{s_1s_2} \le 2ab$. Further, from $(g_k(0), g_k(-2)) = 1$, we get $(s_2t_1, s_1t_2) = 1$ giving $(a,b)=1$. We first exclude the trivial cases.

1. Let $a=b$. Then $a=b=1$ since $\gcd(a,b)=1$. Further $s_1t_2 = s_2t_1 = 1$ and $3^{\nu_2}=1$ or $3^{\nu_3}=1$ implying $c=2$ and we have $u^n - v^n = 2$ for which we have the trivial solution $u=1, v=-1$. Then $x=-1, x+2=1$ which gives $f_k(x) = (-1)^n$ for all odd n which is a trivial solution. Thus we now assume $a \neq b$ and further $x \neq -1$.

2. Suppose $uv=1$. Then $c|2a$ and $c|2b$ giving $c=2$ since $(a,b)=1$ and hence we have $a-b=\pm 2$. This implies $3^{\nu_2}s_2(\pm 1) - s_1(\pm 1) = 2$ as in other cases, $c>2$. We find that the only such possibilities are $3(1)-1(1)=2, 9(-1)-11(-1)=2, 9(1)-7(1)=2$. Hence $x \in \{1, -11, 7\}$. This with $x = 2^{\delta_1}s_1t_1^{n-1}u_1^n = s_1(\pm 1)$ gives $x=1, k \le 10$ or $(x,k) \in \{(-11,5),(7,5)\}$ and we check that $x=1, k=2$ is the only solution. Thus we now suppose that $uv>1$.

3. Suppose $u=v$. Then $(a-b)v^n = c$ implying $\frac{c}{a-b} \in \mathbb{Z}$. Further $\frac{c}{a-b} = v^n$ is an n-th power. We can easily find such triples (a,b,c) and exponents n. For such triples, we have $x = \frac{bc}{a-b}$ and we check for $f_k(x)$ being an n-th power. There are no solutions. Thus we can now suppose $u \neq v$.

4. Suppose $u=\pm 1$. Then $c|2a$, $v \neq \pm 1$ and $v^n = \frac{\pm a - c}{b} \in \mathbb{Z}$. We find all such triplets (a,b,c) and the exponents n. Then $x+2 = \pm\frac{2a}{c}$ or $x = \pm\frac{2a}{c} - 2$. We check for $f_k(x)$ being an n-th power. We find that there are no solutions. Hence we now assume $u \neq \pm 1$.

5. Suppose $v=\pm 1$. Then $c|2b$ and $u^n = \frac{c \mp b}{a} \in \mathbb{Z}$ is a power. We find such triples (a,b,c) and the exponent n. Then $x = \pm\frac{2b}{c}$ and we check for $f_k(x)$ being an n-th power. There are no solutions.

Hence from now on, we consider the equation $au^n - bv^n = c$ with

$$a \geq 1, b \geq 1, c > 1, |u| > 1, |v| > 1 \text{ and } a \neq b, u \neq v.$$

If u, v is a solution of $au^n - bv^n = c$ with u, v negative, then we have $a(-u)^n - b(-v)^n = -c$ with $-u, -v$ positive. Therefore it is sufficient to consider the equation $au^n - bv^n = \pm c$ with $u > 1$, $v > 1$. Recall that $abc \leq 4 \cdot 9 \cdot 11 \cdot 467 \cdot 2018957$. Hence we have for $n \geq 40$ that

$$\left(\frac{u}{v}\right)^n = \frac{b}{a} \pm \frac{c}{v^n} \geq \frac{b}{a} - \frac{c}{2^n} \geq 1 + \frac{1}{a} - \frac{c}{2^{40}} > 1 \text{ if } a < b;$$
$$\left(\frac{v}{u}\right)^n = \frac{a}{b} \pm \frac{c}{u^n} \geq \frac{a}{b} - \frac{c}{2^n} \geq 1 + \frac{1}{b} - \frac{c}{2^{40}} > 1 \text{ if } a > b.$$

Thus for $n > 37$, we have $u > v$ if $a < b$ and $v > u$ if $a > b$. By Proposition 5.1, we get

$$n \leq \begin{cases} \max\{1000, 824.338 \log b + 0.258\} & \text{if } b \leq 100 \\ \max\{2000, 769.218 \log b + 0.258\} & \text{if } 100 < b \leq 10000 \\ \max\{10000, 740.683 \log b + 0.234\} & \text{if } b > 10000. \end{cases} \tag{5.28}$$

when $a < b$. We now exclude these values of n.

For every prime n, let r be the least positive integer such that $nr + 1 = p$ is a prime. Then both u^n and v^n are r-th roots of unity modulo p. Since $f_k(x) = y^n$, $f_k(x)$ is also an r-th root of unity modulo p. Let $U(p, r)$ be the set of r-th roots of unity modulo p. Recall that $x = \frac{2bv^n}{c}$.

For every $3 \leq k \leq 10$, we first list all possible triples (a, b, c). Given a triple (a, b, c), we have a bound $n \leq n_0 := n_0(a, b, c)$ given by (5.28). For every prime $n \leq n_0$, we check for solutions $a\alpha - b\beta \equiv \pm c$ modulo p for $\alpha, \beta \in U(p, r)$. We now restrict to such pairs (α, β). For any such pair (α, β), we check if $f_k(\frac{2\beta}{c})$ modulo p is in $U(p, r)$. We find that there are no such pairs (α, β). The case $a > b$ can be handled similarly, and now new solutions arise.

Therefore, we have no further solutions (k, x, y) of the equation $f_k(x, y)$. Hence the proof of Theorem 5.10 is complete for $n \geq 3$.

5.10 Proof of Theorem 5.10 for $n = 2$

For $k = 1$ equation (5.19) reads as

$$f_1(x) = (x + 1)^2 - 1 = y^2.$$

Hence the statement trivially follows in this case.

Let $k = 3$. Equation (5.19) has the form

$$x^4 + 7x^3 + 15x^2 + 10x = x(x + 2)(x^2 + 5x + 5) = y^2.$$

Here we use the MAGMA [23] procedure

```
IntegralQuarticPoints([1,7,15,10,0])
```

to determine all integral points. We only obtain the solutions with $x = 0, -2$ and $y = 0$.

Consider the case $k = 4$. The hyperelliptic curve is as follows

$$x(x + 2)(x^3 + 9x^2 + 24x + 17) = y^2.$$

We obtain that

$$\begin{aligned} x &= d_1 u_1^2, \\ x+2 &= d_2 u_2^2, \\ x^3+9x^2+24x+17 &= d_3 u_3^2, \end{aligned}$$

where $d_3 \in \{\pm 1, \pm 3, \pm 17, \pm 3 \cdot 17\}$. It remains to determine all integral points on certain elliptic curves defined by the third equation, that is we use the MAGMA procedure

$$\texttt{IntegralPoints(EllipticCurve([}0, 9d_3, 0, 24d_3^2, 17d_3^3\texttt{]))}.$$

We note that these procedures are based on methods developed by Gebel, Pethő and Zimmer [58] and independently by Stroeker and Tzanakis [126]. Once again, we obtain the solutions with $x = 0, -2$ and $y = 0$.

We apply Runge's method [64, 107, 145] in the cases $k = 5, 7, 9$. We follow the algorithm described in [131]. First we determine the polynomial part of the Puiseux expansions of $\sqrt{f_k(x)}$. These expansions yield polynomials $P_1(x), P_2(x)$ such that either

$$\begin{aligned} d^2 f_k(x) - P_1(x)^2 &> 0, \\ d^2 f_k(x) - P_2(x)^2 &< 0 \end{aligned}$$

or

$$\begin{aligned} d^2 f_k(x) - P_1(x)^2 &< 0, \\ d^2 f_k(x) - P_2(x)^2 &> 0 \end{aligned}$$

for some $d \in \mathbb{Z}$ and $x \notin I_k$, where I_k is a finite interval. We summarize some data in **Table** 5.2.

k	d	$P_1(x), P_2(x)$	I_k
5	1	$P_1(x) = x^3 + 8x^2 + 16x + 5$ $P_2(x) = x^3 + 8x^2 + 16x + 6$	$[-10, 3]$
7	16	$P_1(x) = 16x^4 + 232x^3 + 1070x^2 + 1693x + 473$ $P_2(x) = 16x^4 + 232x^3 + 1070x^2 + 1693x + 474$	$[-282, 148]$
9	2	$P_1(x) = 2x^5 + 46x^4 + 378x^3 + 1331x^2 + 1819x + 528$ $P_2(x) = 2x^5 + 46x^4 + 378x^3 + 1331x^2 + 1819x + 530$	$[-291, 278]$

Table 5.2: Data corresponding to the values $k = 5, 7, 9$

We only provide details of the method in case of $k = 9$, the other two cases can be solved in a similar way. We obtain that

$$\begin{aligned} 4f_9(x) - P_1(x)^2 &= 4x^5 - 1045x^4 - 17958x^3 - 108973x^2 - 284408x - 278784, \\ 4f_9(x) - P_2(x)^2 &= -4x^5 - 1229x^4 - 19470x^3 - 114297x^2 - 291684x - 280900. \end{aligned}$$

If $x > 278$, then

$$(P_1(x) - 2y)(P_1(x) + 2y) < 0 < (P_2(x) - 2y)(P_2(x) + 2y).$$

If $P_2(x) - 2y < 0$ and $P_2(x) + 2y < 0$, then $P_1(x) - 2y < -2$ and $P_1(x) + 2y < -2$, which implies that $(P_1(x) - 2y)(P_1(x) + 2y) > 0$, a contradiction. If $P_2(x) - 2y > 0$ and

$P_2(x) + 2y > 0$, then $P_1(x) - 2y > -2$ and $P_1(x) + 2y > -2$. It follows that

$$P_1(x) - 2y = -1 \text{ or } P_1(x) + 2y = -1.$$

Consider the case $x < -291$. Here we get that

$$(P_2(x) - 2y)(P_2(x) + 2y) < 0 < (P_1(x) - 2y)(P_1(x) + 2y).$$

If $P_1(x) - 2y > 0$ and $P_1(x) + 2y > 0$, then we have a contradiction. If $P_1(x) - 2y < 0$ and $P_1(x) + 2y < 0$, then $P_2(x) - 2y < 2$ and $P_2(x) + 2y < 2$, therefore

$$P_2(x) - 2y = 1 \text{ or } P_2(x) + 2y = 1.$$

Thus if we have a solution $(x, y) \in \mathbb{Z}^2$, then either $x \in I_9$ (provided in Table 2.) or $y = \pm(x^5 + 23x^4 + 189x^3 + 1331/2x^2 + 1819/2x + 529/2)$. We obtain only the trivial integral solutions $(x, y) = (-2, 0), (0, 0)$.

It remains to handle the cases $k = 6, 8, 10$. Observe that since in this case the degree of $f_k(x)$ is odd, the solutions to (5.19) with $x \leq 0$ can be easily found. In fact, we get that all such solutions have $x = 0, -2$. So in what follows, without loss of generality we may assume that $x > 0$.

Consider the equation related to $k = 6$. We have

$$\begin{aligned} x &= d_1 u_1^2, \\ x + 2 &= d_2 u_2^2, \\ x^5 + 20x^4 + 151x^3 + 529x^2 + 833x + 437 &= d_3 u_3^2, \end{aligned}$$

with some positive integers d_1, d_2, d_3. Checking the possible values of d_1, d_2, d_3, we get that

$$\begin{aligned} x &= 2^{\alpha_1} 19^{\alpha_4} 23^{\alpha_5} u_1^2, \\ x + 2 &= 2^{\alpha_1} 3^{\alpha_2} 11^{\alpha_3} u_2^2, \\ x^5 + 20x^4 + 151x^3 + 529x^2 + 833x + 437 &= 3^{\alpha_2} 11^{\alpha_3} 19^{\alpha_4} 23^{\alpha_5} u_3^2, \end{aligned}$$

where $\alpha_i \in \{0, 1\}$ and $u_i \in \mathbb{Z}$. Working modulo 720 it follows that the above system of equations has solutions only if $(\alpha_2, \alpha_3, \alpha_4, \alpha_5) \in$

$$\begin{aligned} &\{(0, 0, 0, 1), (0, 0, 1, 0), (0, 0, 1, 1), (0, 1, 0, 0), \\ &(0, 1, 0, 1), (0, 1, 1, 1), (1, 0, 0, 0), (1, 0, 0, 1), \\ &(1, 0, 1, 1), (1, 1, 0, 1), (1, 1, 1, 0), (1, 1, 1, 1)\}. \end{aligned}$$

We describe an argument which works for all cases except the one with $(\alpha_2, \alpha_3, \alpha_4, \alpha_5) = (0, 0, 0, 1)$. Combining the first two equations yields

$$(x + 1)^2 - 3^{\alpha_2} 11^{\alpha_3} 19^{\alpha_4} 23^{\alpha_5} (2^{\alpha_1} u_1 u_2)^2 = 1,$$

a Pell equation. Computing the fundamental solution of the Pell equation provides a formula for x. Substituting it into the equation

$$x^5 + 20x^4 + 151x^3 + 529x^2 + 833x + 437 = 3^{\alpha_2} 11^{\alpha_3} 19^{\alpha_4} 23^{\alpha_5} u_3^2$$

we get a contradiction modulo some positive integer m. The following table contains the possible

tuples and the corresponding integer m.

$(\alpha_2,\alpha_3,\alpha_4,\alpha_5)$	m	$(\alpha_2,\alpha_3,\alpha_4,\alpha_5)$	m
$(0,0,1,0)$	11	$(0,0,1,1)$	13
$(0,1,0,0)$	13	$(0,1,0,1)$	29
$(0,1,1,1)$	37	$(1,0,0,0)$	5
$(1,0,0,1)$	11	$(1,0,1,1)$	29
$(1,1,0,1)$	13	$(1,1,1,0)$	29
$(1,1,1,1)$	43		

As an example we deal with $(\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(0,1,1,1)$. The fundamental solution of the Pell equation is

$$208-3\sqrt{11\cdot 19\cdot 23}.$$

If there exists a solution, then

$$x=\frac{(208-3\sqrt{11\cdot 19\cdot 23})^k+(208+3\sqrt{11\cdot 19\cdot 23})^k}{2}-1$$

for some $k\in\mathbb{N}$. If x satisfies the above equation, then

$$x^5+20x^4+151x^3+529x^2+833x+437 \pmod{37}\in\{17,20,22,29\}$$

and $11\cdot 19\cdot 23u_3^2 \pmod{37}\in$

$$\{0,1,3,4,7,9,10,11,12,16,21,25,26,27,28,30,33,34,36\},$$

a contradiction. It remains to resolve the equation corresponding to the tuple $(\alpha_2,\alpha_3,\alpha_4,\alpha_5)=(0,0,0,1)$. Here we have that

$$F(x)=x(x^5+20x^4+151x^3+529x^2+833x+437)=(23u_1u_3)^2$$

a Diophantine equation satisfying Runge's condition. Define

$$\begin{aligned}P_1(x) &= 2x^3+20x^2+51x+18,\\ P_2(x) &= 2x^3+20x^2+51x+20.\end{aligned}$$

The two cubic polynomials

$$4F(x)-P_1(x)^2=4x^3+11x^2-88x-324$$

and

$$4F(x)-P_2(x)^2=-4x^3-69x^2-292x-400$$

have opposite signs if $x\notin[-12,5]$. The inequalities

$$\begin{aligned}P_1(x)^2-4y^2 &< 0 < P_2(x)^2-4y^2,\\ P_2(x)^2-4y^2 &< 0 < P_1(x)^2-4y^2\end{aligned}$$

imply that if there exists a solution, then $y=x^3+10x^2+\frac{51}{2}x+\frac{19}{2}$. The polynomial

$$(x+2)F(x)-\left(x^3+10x^2+\frac{51}{2}x+\frac{19}{2}\right)^2$$

has no integral root. Thus it remains to check the cases $x \in [-12, 5]$. We obtain only the trivial solutions.

The above procedure also works in the cases $k = 8$ and 10. For $k = 8$ we get that

$$\begin{aligned} x &= 2^{\alpha_1} 23117^{\alpha_4} u_1^2, \\ x+2 &= 2^{\alpha_1} 3^{\alpha_2} 97^{\alpha_3} u_2^2, \\ \frac{f_8(x)}{x(x+2)} &= 3^{\alpha_2} 97^{\alpha_3} 23117^{\alpha_4} u_3^2 \end{aligned}$$

for some $\alpha_i \in \{0, 1\}$ and $u_i \in \mathbb{Z}$, and in case of $k = 10$ we can write

$$\begin{aligned} x &= 2^{\alpha_1} 2018957^{\alpha_5} u_1^2, \\ x+2 &= 2^{\alpha_1} 3^{\alpha_2} 11^{\alpha_3} 467^{\alpha_4} u_2^2, \\ \frac{f_{10}(x)}{x(x+2)} &= 3^{\alpha_2} 11^{\alpha_3} 467^{\alpha_4} 2018957^{\alpha_5} u_3^2 \end{aligned}$$

for some $\alpha_i \in \{0, 1\}$ and $u_i \in \mathbb{Z}$. After that, we exclude as many putative exponent tuples working modulo 720 as we can. The remaining exponent tuples are treated via Pell equations and congruence arguments. Everything worked in a similar way as previously. The largest modulus used to eliminate tuples is 37.

Remark. We note that the total running time of our calculations was only half an our on a normal PC. The most time consuming part was the application of the Runge's method, it took approximately twenty minutes.

5.11 The equation $y^m = g_T(x)$ for $T \in A_n$, with $n \geq 3$

Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{N}_0$ the set of non-negative integers and $\mathbb{N}_{\geq k}$ will denote the set of non-negative integers $\geq k$. For $n \in \mathbb{N}_0$ we write

$$p_a(x) = \prod_{i=0}^{a} (x + j).$$

Moreover, we define the set

$$A_n = \{(a_1, \ldots, a_k) \in \mathbb{N}_0^k : \ a_i < a_{i+1} \text{ for } i = 1, 2, \ldots k-1, \ a_k < n \text{ and } k \in \{1, \ldots, n-1\}\}.$$

For given $m \in \mathbb{N}_{\geq 2}$ and $T = (a_1, \ldots, a_k) \in A_n$ we consider the Diophantine equation

$$y^m = g_T(x), \quad \text{where} \quad g_T(x) := p_n(x) + \sum_{i=1}^{k} p_{a_i}(x). \tag{5.29}$$

The cardinality of A_n is $2^n - 1$, hence for a given m we deal with $2^n - 1$ Diophantine equations.

We note that equation (5.29), in case of $T = (0, 1, \ldots, n-1) \in A_n$, was studied in a paper by Hajdu, Laishram and Tengely [70] see also Section 5.6. They proved that for $n \geq 1$ and $m \geq 2$ (with $n \neq 2$ in case of $m = 2$) equation (5.29) has only finitely many integer solutions. Moreover, they were also able to solve the equation explicitly for $n \leq 10$.

In this section we consider equation (5.29) for $T \in A_n, n \geq 3$ with some additional constraints on the shape of the sequence T. However, before we state our findings we will recall

some general results concerning the solvability in integers x, y, m of Diophantine equations of the form

$$y^m = g(x), \tag{5.30}$$

where $g \in \mathbb{Z}[x]$ is fixed of degree d and height H, where by height of the polynomial g we understand the maximum of the modulus of the coefficients.

The following lemma, due to Tijdeman [136], will be one of our main tools.

Lemma 5.6

If $g(x)$ has at least two distinct roots and $|y| > 1$, then in the Diophantine equation (5.30) we have $m < c_1(d, H)$, where $c_1(d, H)$ is an effectively computable constant depending only on d and H.

The next result is a special case of a theorem of Brindza [28].

Lemma 5.7

Suppose that one of the following conditions holds:

1. *$m \geq 3$ and $g(x)$ has at least two roots with multiplicities co-prime to m,*
2. *$m = 2$ and $g(x)$ has at least three roots with odd multiplicities.*

Then all integer solutions of equation (5.30) satisfies $\max\{|x|, |y|\} \leq c_2(d, H)$, where $c_2(d, H)$ is an effectively computable constant depending only on d and H.

In order to apply the above results to our Diophantine equation (5.29) we collect basic properties of the sequence of polynomials $(g_T)_{T \in A_n}$ in the following. We note that in [13] the authors provided effective finiteness result for the equation $g_T(x) = ay^m + b$ in case of $T = (0, 1, \ldots, n-1)$.

Lemma 5.8

Let $n \in \mathbb{N}_{\geq 2}, T = (a_1, \ldots, a_k) \in A_n$ and $a_1 \geq 1$.

1. *We have $g_T(x) = p_{a_1}(x)h_T(x)$, where $h_T \in \mathbb{Z}[x]$ and $\deg h_T = n - (a_1 + 1)$.*
2. *The roots $x = -i, i = 0, \ldots, a_1$ of the polynomial g_T are simple. In particular, the polynomial $g_T(x)$ has at least two roots with odd multiplicity.*
3. *If $n \geq 5$ and $a_1 = 1, a_2 = 3, a_3 \geq 5$, then the polynomial $h_T(x)$ is not a square of a polynomial with integer coefficients. In particular, the polynomial $g_T(x)$ has at least three roots with odd multiplicity.*
4. *The equation $g_T(x) = \pm 1$ has no solutions in integers.*

Proof. We have

$$g_T(x) = p_n(x) + \sum_{i=1}^{k} p_{a_i}(x),$$

where $1 \leq a_1 < a_2 < \ldots < a_k < n$. In particular, $p_{a_1}(x) | p_{a_i}(x)$ for $i = 1, \ldots, k$ and obviously

$p_{a_1}(x)|p_n(x)$. We also have the general identity

$$p_{a+b}(x) = p_b(x)p_{a-1}(x+b+1).$$

Consequently, we obtain the following relation

$$g_T(x) = p_{a_1}(x)(1 + g_{T'}(x + a_1 + 1)),$$

where $T' = (a_2 - a_1 - 1, a_3 - a_1 - 1, \ldots, a_k - a_1 - 1, n - a_1 - 1)$. We thus have $h_T(x) = 1 + g_{T'}(x + a_1 + 1)$. Now, let us observe that for $x_0 = 0, \ldots, -a_1$ and any $a > a_1$ we have $p_a(x_0 + a_1 + 1) > 0$. This implies that $h_T(x_0) = 1 + g_{T'}(x_0 + a_1 + 1) > 0$ and thus the roots $0, -1, \ldots, -a_1$, of the polynomial $g_T(x)$ are all simple. Consequently, under our assumptions on n and T, the polynomial $g_T(x)$ has at least two roots with multiplicity equal to one.

If $a_1 = 1, a_2 = 3$ and $a_3 \geq 5$ then we get that

$$h_T(0) = \lim_{x\to 0} \frac{g_T(x)}{x(x+1)} = 1 + g_{T'}(2) \equiv 1 + 2 \cdot 3 \equiv 3 \pmod 4,$$

$$h_T(-1) = \lim_{x\to -1} \frac{g_T(x)}{x(x+1)} = 1 + g_{T'}(1) \equiv 1 + 1 \cdot 2 \equiv 3 \pmod 4.$$

In particular, the polynomial $h_T(x)$ cannot be a square of a polynomial with integer coefficients and thus has at least one root of odd multiplicity. Consequently, the polynomial $g_T(x)$ has at least three roots of odd multiplicity.

Let us observe that if $g_T(x) = \pm 1$ for some $x \in \mathbb{Z}$, then necessarily $x \cdot \ldots \cdot (x + a_1) = \pm 1$, which is clearly impossible for $a_1 \geq 1$.

Remark. We note that in general we cannot have similar result in the case $a_1 = 0$. Indeed, if $n = 3$ and $T = (0, 1)$ then

$$g_T(x) = x(x + 2)^3.$$

Consequently, the equation $g_T(x) = y^3$ has infinitely many integer solutions of the form $(x, y) = (t^3, t(t^3 + 2))$, where $t \in \mathbb{Z}$. Moreover, let us note that in this case the equation $g_T(x) = y^4$ has infinitely many rational solutions. Indeed, let us take $y = t(x + 2)$. We get the equation $t^4(x + 2)^4 = x(x + 2)^3$. Consequently, by solving for x we see that for each $t \in \mathbb{Q} \setminus \{-1, 1\}$ the pair

$$(x, y) = \left(\frac{2t^4}{1 - t^4}, \frac{2t}{1 - t^4}\right)$$

is a solution of our equation.

Remark. Let us observe that the above lemma can be further generalized. Indeed, instead of working with the polynomial $p_n(x)$ one can consider a more general form. Let us consider the polynomial

$$P_{p,q,n}(x) = \prod_{i=0}^{n} (px + q),$$

where $p \in \mathbb{N}, q \in \mathbb{Z}$ and $|q| < p$. Then, for $T = (a_1, \ldots, a_k) \in A_n, n \in \mathbb{N}$, a similar lemma can

be proved for the polynomial

$$G_{p,q,T}(x) = P_{p,q,n}(x) + \sum_{i=1}^{k} P_{p,q,a_i}(x).$$

As an immediate consequence of the above lemmas we get the following result.

Theorem 5.12

Let $n \in \mathbb{N}_{\geq 2}, T = (a_1, \ldots, a_k) \in A_n$. If $a_1 \geq 2$ or $a_1 = 1, a_2 = 3, a_3 \geq 5$ then for the integer solutions of the Diophantine equation $y^m = g_T(x)$ we have:

1. *if $y \neq 0$, then $m < c_1(n)$,*
2. *if $m \geq 3$, then $\max\{m, |x|, |y|\} < c_2(n)$,*
3. *if $m = 2$, then $\max\{|x|, |y|\} < c_3(n)$.*

Here $c_1(n), c_2(n), c_3(n)$ are effectively computable constants depending only on n.

Proof. The first part is an immediate consequence of Lemma 5.8 and Lemma 5.6.

In order to get the second part we note that the roots $x = 0, -1$ of the polynomial $g_T(x)$ are simple. Moreover, the degree $\deg g_T(x) = n + 1$ is grater then two, and our claims follows from the second part of Lemma 5.7.

Finally, in order to get the last part from the statement we note that the roots $x = 0, -1, -2$ of the polynomial $g_T(x)$ are simple (in case of $a_1 \geq 2$) or that the roots $x = 0, -1$ are simple and we have one more root with odd multiplicity of the polynomial $h_T(x)$ (which is a consequence of the third part of Lemma 5.8). Moreover, the degree $\deg g_T(x) = n + 1$ is grater then two, and our claims follows from the second part of Lemma 5.7.

Remark. The crucial property which guarantees the finiteness of the set of integer solutions of equation (5.29) is the number of multiple roots of the polynomial g_T, with $T \in A_n$.

5.12 Rational solutions of the equation $y^2 = g_T(x)$ with $T \in A_n, n \leq 5$.

Let $n \in \mathbb{N}$ and for given $T \in A_n$ let us consider the algebraic curve $C_T : \ y^2 = g_T(x)$. Let us write $gen(T) := \text{genus}(C_T)$ - the genus of the curve C_T and $J_T := \text{Jac}(C_T)$ - the Jacobian variety associated with C_T. Moreover, we define $r(T) := \text{rank}(J_T)$ - the rank of the Jacobian variety J_T. As usual, by $C_T(\mathbb{Q})$ we will denote the set of all rational points on the curve C_T and by $C_T(\mathbb{Z})$ - the set of integral points on C_T.

If $T \in A_2, A_3$ or A_4, then using standard method of parametrization of curves we get the description of the set of rational points in cases such that $gen(T) = 0$, e.g. for $T = (0)$ we have $g_T(x) = x(x^2+5x+5)^2$ and the description of the set $C_T(\mathbb{Q})$ is $\{(t^2, t(t^4+5t^2+5)) : \ t \in \mathbb{Q}\}$. If $T \in A_2, A_3$ or A_4 and $gen(T) = 1$, then we get the list of integral points (rational points in case of rank 0 curves) by MAGMA [23]. If $T \in A_4$, then we also obtain genus 2 curves,

dc_1892_21

fortunately, in each case, the rank of the Jacobian variety J_T associated with C_T is bounded by 1. Thus in each case we can apply Chabauty's method [39] in order to find complete set of rational points on the curve C_T. The procedures in case of genus 2 curves were implemented in MAGMA based on papers by Stoll [123–125]. For example, if $n = 5$ and $T = (4)$, then $gen(T) = 2, r_T = 1$ and the set of finite rational points on the curve C_T is as follows

$$C_T(\mathbb{Q}) = \{(-6,0),(-4,0),(-3,0),(-2,0),(-1,0),(0,0),(-12/7,\pm 720/7)\}.$$

Similarly, if $T = (2,3,4)$ then $gen(T) = 2, r_T = 1$ and

$$C_T(\mathbb{Q}) = \{(-38/11,\pm 1368/11),(-4,0),(-2,0),(0,0)\}.$$

5.13 Application of Runge method for several equations $y^m = g_T(x)$.

Consider the Diophantine equations $y^2 = g_T(x)$ for $T \in A_5, A_7, A_9, A_{11}$ and A_{13}. In all cases $g_T(x)$ is a monic polynomial of degree 6, hence Runge's condition is satisfied. An algorithm to solve such Diophantine equations is given in [131], we followed it to determine the integral solutions. We note that in case of $T \in A_{13}$ there are $2^{13} - 1$ equations to be solved and the bounds obtained by Runge's method are of size 10^6. Therefore we applied a modified version of the reduction argument used in [131]. We illustrate the idea through an example. If $T = (2,3,4,5,7,9,10,12)$, then the equation is given by

$$\begin{aligned} y^2 &= (x^{10} + 85x^9 + 3200x^8 + 70211x^7 + 993342x^6 + 9458533x^5 + 61303921x^4 + 266606990x^3 + \\ &\quad 742982499x^2 + 1194792102x + 838752409)(x+4)(x+2)(x+1)x \end{aligned}$$

The polynomial part of the Puiseux expansion of $g_T(x)^{1/2}$ is given by

$$P_T(x) = x^7 + 46\,x^6 + \frac{1693}{2}\,x^5 + \frac{15931}{2}\,x^4 + \frac{323643}{8}\,x^3 + \frac{212995}{2}\,x^2 + \frac{1953743}{16}\,x + \frac{574129}{16}.$$

We obtain that

$$\begin{aligned} &256g_T(x) - (16P_T(x) - 1)^2 && \text{has roots in the interval } I_a := [-68, \ldots, 2.018 \times 10^6], \\ &256g_T(x) - (16P_T(x) + 1)^2 && \text{has roots in the interval } I_b := [-1.01 \times 10^6, \ldots, 0]. \end{aligned}$$

Hence it remains to solve the equations

$$\begin{aligned} y^2 &= g_T(x) \text{ with } x \in [-1.01 \times 10^6, \ldots, 2.018 \times 10^6], \\ P_T(x)^2 - g_T(x) &= 0. \end{aligned}$$

Therefore the total number of equations to handle is 3026952. We compute the appropriate intervals in case of two positive integers k_1, k_2 :

$$\begin{aligned} &256g_T(x) - (16P_T(x) - k_1)^2 && \text{has roots in the interval } I_1, \\ &256g_T(x) - (16P_T(x) + k_2)^2 && \text{has roots in the interval } I_2. \end{aligned}$$

For some fixed k_1, k_2 we determine the integral solutions of the equations

$$\begin{aligned} y^2 &= g_T(x) \text{ with } x \in I_1 \cup I_2, \\ (P_T(x) + k/16)^2 - g_T(x) &= 0 \text{ for some values of } k \text{ depending on } k_1, k_2. \end{aligned}$$

The goal is to reduce the number of these type of equations. Based on numerical experiences we start with $k_1 = |I_a|^{1/4}, k_2 = |I_b|^{1/4}$, where $|\cdot|$ denotes the number of integers in the given interval. We compute the intervals I_1, I_2 for these values of k_1, k_2. If the number of equations is smaller than in the previous step, then $k_1 = 2|I_a|^{1/4}$ and $k_2 = 2|I_b|^{1/4}$. Therefore at the end we will have $k_1 = i_1|I_a|^{1/4}$ and $k_1 = i_2|I_b|^{1/4}$ for some integers i_1, i_2. In the above example the interval I_a is reduced to $[-69, \dots, 2280]$ in 23 steps, so $k_1 = 851$, the interval I_b is reduced to $[-1674, \dots, 0]$ in 20 steps, thus $k_2 = 620$. The number of equations to handle before reduction was more than 3 million, after the above reduction it is less than 6000.

We also note that equations for which $\gcd(m, n+1) \geq 2$ can be solved using Runge's method. For example if $n = 14$ and $T = (10, 11, 12, 13)$, then we have

$$y^m = \big(x^3 + 39\,x^2 + 504\,x + 2157\big)(x + 12)p_{10}(x),$$

an equation that can be solved using Runge's method for $m = 3, 5$ and 15. We note that in all cases only the trivial solutions with $y = 0$ exist. In this way we were able to determine all solutions of equation (5.29) with $(m, n) \in \{(5, 3), (8, 3), (11, 3), (4, 5), (9, 5), (6, 7)\}$. According to our computations we see that there are very few solutions of the equation $y^m = g_T(x)$ with $xy \neq 0$. This may suggest to treat the equation $y^m = g_T(x)$ as an equation in infinitely many variables and look for its solutions in $m \in \mathbb{N}_{\geq 2}, n \in \mathbb{N}, T = (a_1, \dots, a_k) \in A_n$ and $x, y \in \mathbb{Z}$ satisfying the condition $xy \neq 0$. However, stating the problem in this way one can easily get infinitely many solutions. We observed that the equation $y^3 = x(x+2)^3 = g_T(x)$, with $n = 3$ and $T = (0, 1)$ has infinitely many solutions of the form $(x, y) = (u^3, (u(u^3 + 2))$. Thus, by taking $u < 0$, we see that for each $n \in \mathbb{N}_{\geq 3}$ and $T' \in A_n$ of the form $T' = (0, 1, a_3, \dots, a_k)$, where $a_3 \geq |u|$ we have $g_{T'}(u) = (u(u^3 + 2))^3$. This is a consequence of the vanishing of $p_{a_i}(u)$ for $a_i \geq |u|$. Let us also note that essentially each negative value of x which is a solution of the equation $y^m = g_T(x)$ for some $m \in \mathbb{N}$ and $T \in A_n$ leads in the same way to infinitely many of T' such that $y^m = g_{T'}(x)$.

Let us introduce the set

$$\mathcal{N} := \{x \in \mathbb{N}_{\leq 0} : \text{ there is } (m, n, T) \in \mathbb{N}_{\geq 2} \times \mathbb{N}_{\geq 2} \times A_n : \ y^m = g_T(x) \text{ for some } y > 0\}.$$

We saw that $-u^3 \in \mathcal{N}$ for $u \in \mathbb{N}$. Let us also note that $-9, -5, -4 \in \mathcal{N}$. Indeed, the pair $(x, y) = (-9, 252)$ is a solution of the equation $y^2 = g_T(x)$ for $n = 5, T = (3)$ and $(x, y) = (-5, -5)$ is a solution of the equation $y^3 = g_T(x)$ for $n = 4, T = (0)$. Moreover, $(x, y) = (-4, 6)$ is a solution of the equation $y^2 = g_T(x)$ for $n = 3, T = (1)$. We do not know any other elements of $\mathcal{N}$. However, if we allow x to be *rational*, then we get some additional

interesting solutions. Indeed, one can easily prove the identities:

$$p_{4k+3}\left(-\frac{4k-1}{2}\right)+p_{4k-1}\left(-\frac{4k-1}{2}\right)=\left(\frac{16k^2+32k+11}{4^{k+1}}\prod_{i=0}^{2k-1}(2i+1)\right)^2,$$

$$p_{4k+1}\left(-\frac{4k-1}{2}\right)+p_{4k}\left(-\frac{4k-1}{2}\right)+p_{4k-1}\left(-\frac{4k-1}{2}\right)=\left(\frac{4k+3}{2^{2k+1}}\prod_{i=0}^{2k-1}(2i+1)\right)^2$$

In order to prove the first equality we note $p_{4k+3}(x)+p_{4k-1}(x)=p_{4k-1}(x)(x^2+(8k+3)x+16k^2+12k+1)^2$. Moreover,

$$\begin{aligned}p_{4k-1}\left(-\frac{4k-1}{2}\right)&=\prod_{i=0}^{2k-1}\left(-\frac{4k-1}{2}+i\right)\left(-\frac{4k-1}{2}+i+2k\right)\\&=\frac{1}{4^{2k}}\prod_{i=0}^{2k-1}(4k-2i-1)(2i+1)=\frac{1}{4^{2k}}\prod_{i=0}^{2k-1}(2i+1)^2,\end{aligned}$$

where last equality follows from the equality of sets $\{2i+1:\ i\in\{0,2k-1\}\}=\{4k-2i-1:\ i\in\{0,2k-1\}\}$.

In order to prove the second equality it is enough to note the identity $p_{4k+1}(x)+p_{4k}(x)+p_{4k-1}(x)=p_{4k-1}(x)(x+1)^2$.

We known only very few solutions of the equation from the question above. For the convenience of the reader we collect them in the table below:

x	$[m,\ n,\ T]$
1	$[2,4,(0)],[2,5,(0,4)],[2,5,(0,1,2)],[2,6,(0)],[2,6,(3,4)],[2,7,(0,3,4,5,6)],$
	$[2,8,(0,3,7)],[2,8,(0,1,2,5)],[2,9,(0,1,2,5,6,7],[2,14,(0,1,2,6,\ldots,13)]$
	$[3,5,(0,1,2)],[5,3,(1,2)],[7,4,(1,2)]$
2	$[2,3,(2)],[2,5,(2,3)],[7,3,(0,1)]$
4	$[2,6,(0,4)]$

Solutions of the equation $y^m=g_T(x)$ with positive values of x.

One can also ask about positive *rational* solutions but we were unable to prove anything similar like in the case of negative solutions.

Let us also observe that the problem concerning the existence of solutions with $x=1$ is equivalent with the problem of finding integer solutions of the Diophantine equation of polynomial-factorial type

$$y^m=\sum_{i=1}^{n}(a_i+1)!$$

in non-negative integers $a_1,a_2,\ldots$ and $y,m\in\mathbb{N}$. This is a consequence of the equality $p_a(1)=(a+1)!$.

5.14 Some results concerning an additive version of Erdős-Graham question

The problem of Erdős and Graham [51] asking for the integer solution of the equation given by

$$y^m = P_T(x_1, \ldots, x_n), \tag{5.31}$$

where $T \in B_n, P_T(x_1, \ldots, x_n) = p_{a_1}(x_1) \cdot \ldots \cdot p_{a_n}(x_n)$ and

$$B_n = \{(a_1, \ldots, a_n) \in \mathbb{N}^n : \ a_i \leq a_{i+1} \text{ for } i = 1, 2, \ldots n-1\}.$$

Here we impose the natural condition for solutions: $x_i + a_i < x_{i+1}$ for $i = 1, \ldots, k-1$. In the literature there are many nice results dealing with special cases of the problem of Erdős and Graham and its various generalizations. In order to get more information on this problem one can consult the papers [11, 16, 85, 119, 141].

Motivated by research devoted to the study of equation (5.31) it is quite natural to consider a multi-variable and additive version of the classical equation $y^m = p_n(x)$. as well. More precisely, we are interested in the problem of existence of integer solution of the Diophantine equation

$$z^m = G_T(x_1, \ldots, x_n), \tag{5.32}$$

where for a given $T = (a_1, \ldots, a_n) \in B_n$ we put

$$G_T(x_1, \ldots, x_n) = \sum_{i=1}^{n} p_{a_i}(x_i).$$

In this section we study the problem of existence of integer solutions of the Diophantine equation (5.32). We are mainly interested in the case when $m = 2, 3$ and consider the related Diophantine equations for certain sequences chosen from the set B_2.

From geometric point of view equation (5.32) defines an algebraic variety of dimension n and degree $\max\{m, a_n + n\}$. As usual, the general expectation (when dealing with Diophantine equations with small degree and many variables) is the following. If m is not too large and $\max\{a_1, \ldots, a_m\}$ is relatively small compared with m, then equation (5.32) should have infinitely many solutions in integers.

Remark. Let us recall that if $a_1 = 2$ or $a_1 = a_2 = 3$, then for each $n-2$ tuple $(a_3, \ldots, a_n) \in B_{n-2}$, the Diophantine equation

$$y^2 = p_{a_1}(x_1) p_{a_2}(x_2) \ldots p_{a_n}(x_n)$$

has infinitely many solutions in positive integers $(x_1, \ldots, x_n)$ satisfying the condition $x_i + a_i < x_{i+1}$ for $i = 1, \ldots, n-1$. This was proved by Bauer and Bennett in [11]. An (additive) analogue of the above result of Bauer and Bennett can be obtained via the identities

$$p_1(x-1) + x = x^2, \quad p_2(x-1) + x = x^3$$

with $x = \sum_{i=2}^{n} p_{a_i}(x_i)$.

By applying results from the theory of Pellian equations combining with certain polynomial identities we dealt with certain equations of the form $z^m = p_i(x) + p_i(y)$. We proved that there are infinitely many solutions (x, y, z) in integers (polynomials). For example, if $m \equiv 1 \pmod 2$ then the Diophantine equation

$$z^m = p_1(x) + p_1(y)$$

has a polynomial solution

$$x = 2^{\frac{n-1}{2}} t^m - 1, \quad y = 2^{\frac{n-1}{2}} t^m, \quad z = 2t^2.$$

Now we concentrate on the case $m = 3$ with $(n, a_1, a_2) = (2, 2, 2)$, i.e., we consider the Diophantine equation

$$z^3 = p_2(x) + p_2(y). \tag{5.33}$$

From the general observation given on the beginning of this section we have the solution $x = t, y = t(t+1)(t+2)-1$, where t is an integer parameter. We thus are interested in different solutions (x, y, z) of equation (5.33), i.e., do not satisfying the relation $y = x(x+1)(x+2)-1$. However, before we present our result we will need a well known property of Pell type equations. More precisely, if $(X, Z) = (X', Z')$ is a particular solution of the Diophantine equation $X^2 - AZ^2 = B$ and $(X, Z) = (X'', Z'')$ with $Z'' \neq 0$, is a solution of the equation $X^2 - AZ^2 = 1$, then for each $n \in \mathbb{N}$, the pair $(X, Z) = (X_n, Z_n)$, defined recursively by $X_0 = X', Z_0 = Z'$ and for $n \geq 1$ by

$$X_n = X'' \cdot X_{n-1} + AZ'' \cdot Z_{n-1}, \quad Z_n = Z'' \cdot X_{n-1} + X'' \cdot Z_{n-1}, \tag{5.34}$$

is the solution of the equation $X^2 - AZ^2 = B$.

Theorem 5.13

The Diophantine equation (5.33) has infinitely many solutions (x, y, z) in polynomials with integer coefficients and satisfying $\deg_t x = \deg_t y$.

Proof. The factorization $p_2(x) + p_2(y) = (x + y + 2)(x^2 - xy + y^2 + x + y)$ suggests a reasonable assumption that there are solutions of (5.33) satisfying the divisibility condition $(x+y+2)|z$. After some numerical experiments we observed that the quotient $z/(3(x+y+2))$ is square of an integer. We thus write $z = 3t^2(x + y + 2)$, where t is a variable taking integer values. We cancel the common factor $x + y + 2$ and left with the equation of Pell type

$$U^2 - 3(108t^6 - 1)V^2 = 12(2916t^6 - 135t^6 + 1), \tag{5.35}$$

where

$$U = 3(108t^6 - 1)(x + 1), \quad V = (54t^6 + 1)x + 2(27t^6 - 1)y + 108t^6 - 1$$

or equivalently

$$x = \frac{U}{3(108t^6 - 1)} - 1, \quad y = \frac{3(108t^6 - 1)V - (54t^6 + 1)U}{6(27t^6 - 1)(108t^6 - 1)} - 1.$$

In other words, in order to construct polynomial solutions of equation (5.33) it is enough to

prove that there are infinitely many polynomial solutions (U, V) of equation (5.35) satisfying the congruence relations

$$U \equiv 0 \pmod{3(108t^6-1)},$$
$$3(108t^6-1)V-(54t^6+1)U \equiv 0 \pmod{6(27t^6-1)(108t^6-1)}.$$

We observe that equation (5.35) has the solution

$$U' = 3(6t^3+1)(108t^6-1), \quad V' = 108t^6+18t^3-1.$$

Moreover, the equation

$$U^2-3(108t^6-1)V^2 = 1$$

has the solution

$$U'' = (6t^2-1)(36t^4+6t^2+1), \quad V'' = 12t^3.$$

Consequently, following the remark given before the statement of our theorem, we see that for each $n \in \mathbb{N}_0$ the pair (U_n, V_n) of polynomials, where $U_0 = U', V_0 = V'$ and

$$U_n = (6t^2-1)(36t^4+6t^2+1)U_{n-1}+36(108t^6-1)t^3V_{n-1},$$
$$V_n = 12t^3U_{n-1}+(6t^2-1)(36t^4+6t^2+1)V_{n-1},$$

for $n \geq 1$, is the solution of equation (5.35). First of all, we note that the leading coefficients of the polynomials U_n and V_n are positive. Consequently, by induction on n, we easily get the equalities:

$$\deg U_n(t) = 3(2n+3), \quad \deg V_n(t) = 6(n+1).$$

Moreover, having the values of degrees of our polynomials we can easily compute the leading coefficients:

$$\mathrm{LC}(U_n(t)) = \frac{9}{2}432^{n+1}, \quad \mathrm{LC}(V_n(t)) = \frac{1}{4}432^{n+1}.$$

Next, we observe that $U_0 = 3(6t^3+1)(108t^6-1) \equiv 0 \pmod{3(108t^6-1)}$ and from the recurrence relation for U_n we get that for $n \geq 1$ the following congruence holds

$$U_n \equiv U_{n-1} \pmod{3(108t^6-1)}.$$

Thus, by induction on n we immediately get that $U_n \equiv 0 \pmod{3(108t^6-1)}$ for each $n \in \mathbb{N}$.

The proof that for each $n \in \mathbb{N}_0$ we have $3(108t^6-1)V_n-(54t^6+1)U_n \equiv 0 \pmod{6(27t^6-1)(108t^6-1)}$ is more complicated. First of all we note that

$$3(108t^6-1)V_0-(54t^6+1)U_0 \equiv 6(1-6t^3)(27t^6-1)(108t^6-1)$$
$$\equiv 0 \pmod{6(27t^6-1)(108t^6-1)}.$$

and thus the congruence we are interested in is satisfied for $n = 0$. In order to prove that the

same is true for $n \in \mathbb{N}$, it is enough to prove the following congruences:

$$U_n \equiv (108t^6 - 1)\left(\frac{3}{4}(7A_n - A_{n-1})t^3 + A_n\right) \pmod{\lambda(t)},$$

$$V_n \equiv 9(63A_n - 9A_{n-1} - 72)t^9 + 108A_nt^6 - \frac{3}{4}(7A_n - A_{n-1} - 32)t^3 - A_n \pmod{\lambda(t)},$$

where $\lambda(t) = 6(27t^6 - 1)(108t^6 - 1)$, $A_0 = 1, A_1 = 15$ and for $n \geq 2$ we have $A_n = 14A_{n-1} - A_{n-2}$. We omit the tiresome proof of the above congruences and the fact that $7A_n - A_{n-1} \equiv 0 \pmod 4$ for $n \in \mathbb{N}$. It uses only induction and the recurrence relations satisfied by the sequences $(U_n)_{n\in\mathbb{N}_0}, (V_n)_{n\in\mathbb{N}_0}$ and $(A_n)_{n\in\mathbb{N}_0}$.

Consequently, we get that for each $n \in \mathbb{N}_0$ the polynomials x_n, y_n defined by

$$x_n(t) = \frac{U_n(t)}{3(108t^6 - 1)} - 1, \quad y_n(t) = \frac{3(108t^6 - 1)V_n(t) - (54t^6 + 1)U_n(t)}{6(27t^6 - 1)(108t^6 - 1)} - 1,$$

with $z_n(t) = 3t^2(x_n(t) + y_n(t) + 2)$ are the solutions of the Diophantine equation (5.33). Our theorem is proved.

For example, for $n = 1, 2$ we get the following polynomial solutions of equation (5.33):

$$x_1 = 2(1296t^9 + 216t^6 - 9t^3 - 1), \qquad x_2 = 6t^3(186624t^{12} + 31104t^9 - 2160t^6 - 216t^3 + 5),$$
$$y_1 = -2(1296t^9 - 216t^6 - 9t^3 + 1), \qquad y_2 = -6t^3(186624t^{12} - 31104t^9 - 2160t^6 + 216t^3 + 5),$$
$$z_1 = 6t^2(432t^6 - 1), \qquad z_2 = 6t^2(186624t^{12} - 1296t^6 + 1)$$

Remark. Tracing back our construction of the polynomials U_n, V_n from the proof of the above theorem one can easily prove that

$$\deg x_n(t) = \deg y_n(t) = 3(2n + 1)$$

for $n \in \mathbb{N}_0$ and the expressions for the leading coefficients are as follows

$$\mathrm{LC}(x_n(t)) = -\mathrm{LC}(y_n(t)) = 6 \cdot 432^n.$$

Moreover, one can prove (a rather unexpected) equality $y_n(t) = x_n(-t)$ for each $n \in \mathbb{N}$.

Remark. The family of polynomial solutions of equation (5.33) constructed in the proof of Theorem 5.13, has quite unexpected property: $x_n(t) = y_n(-t)$ for each $n \in \mathbb{N}_0$. Moreover, there are no $n \in \mathbb{Z}$ such that both $x_n(t)$ and $y_n(t)$ are positive. Consequently, an interesting question arises whether there are infinitely many solution of equation (5.33) satisfying $y > x > 0$ and $y \neq x(x + 1)(x + 2) - 1$. In order to find such solutions we performed numerical search and found that in the range $0 < x < y < 10^5$ we have only 10 solutions satisfying required conditions. The solutions are the following:

$$(x, y) = (97, 277), (176, 551), (263, 1104), (495, 503), (1244, 2472), (3986, 31706),$$
$$(4505, 12781), (24047, 30599), (26642, 40684), (94743, 96255).$$

Remark. In the range $1 \leq x \leq y \leq 10^5$, equation $z^2 = p_2(x) + p_2(y)$ has 619 integer solutions. This relatively large number suggests the existence of a polynomial solution. We were tried quite hard to construct parametric solutions but we failed.

Theorem 5.14

Let $i \in \{3,4\}$. The equation $z^2 = p_i(x) + p_i(y)$ has infinitely many solutions in positive integers.

Proof. In order to get the result we are looking for rational numbers a, b such that the polynomial $F_{a,b,i}(x) := p_i(x) + p_i(ax+b)$ has multiple roots. The necessary and sufficient condition for this property is the vanishing of the discriminant of the polynomial $F_{a,b,i}$. We define the curve in (a,b) plane in the following way:

$$C_i : \ \mathrm{Disc}(F_{a,b,i}(x)) = 0.$$

Let $i = 3$. The genus of the curve C_3 is equal to 3. As a consequence of Faltings theorem we get that there are only finitely many required pairs (a,b). Due to the identity $p_3(-x-3) = p_3(x)$ we can consider the points on C_3 with $a > 0$ only. Using MAGMA procedure `PointSearch` we found that there are only six pairs of required shape in the range $\max\{H(a), H(b)\} \leq 10^5$, where $H(r)$ is the height of the rational number r. There are in total 16 rational points on C_3 in this range. More precisely, we have $(a,b) \in \mathcal{A}_3$, where

$$\mathcal{A}_3 = \left\{(1,1), (1,-3), (3,-1), (3,7), \left(\frac{1}{3}, \frac{1}{3}\right), \left(\frac{1}{3}, -\frac{7}{3}\right)\right\}.$$

One can also observe that the pairs of points $(3,-1), (1/3, 1/3)$ and $(3,7), (1/3, -7/3)$ lead to the same quadratic equations. We thus left with the pairs $(1,1), (1,-3), (3,-1)$ and $(3,7)$.

If $(a,b) = (1,1)$, then $p_3(x) + p_3(x+1) = 2(x+1)(x+3)(x+2)^2$. The solutions of the quadratic equation $v^2 = 2(x+2)^2 - 2$ are given by

$$x = \frac{1}{2}((3+2\sqrt{2})^n + (3-2\sqrt{2})^n) - 2, \quad v = \sqrt{2}((3+2\sqrt{2})^n - (3-2\sqrt{2})^n),$$

and the corresponding value of z is then $z = (x+2)v$.

Using exactly the same methods we cover the cases $(a,b) = (3,-1), (3,7)$. In the former case we deal with the equation $v^2 = 2(41x^2 + 30x + 1)$, with non-trivial solution $(x,v) = (1,12)$ (the corresponding value of z is $z = xv$). In the letter case we deal with the equation $2(41x^2 + 216x + 280) = z^2$, with non-trivial solution $(x,v) = (4,60)$ (the corresponding value of $z = (x+3)v$. In both cases we get infinitely many positive solutions. We omit the standard details.

If $(a,b) = (1,-3)$ then $p_3(x) + p_3(x-3) = 2(x^2+11)x^2$. However, 2 is a quadratic non-residue of 11 and we get no solutions.

If $i = 4$ then

$$\mathrm{Disc}(F_{a,b,4}(x)) = G_1(a,b)G_2(a,b),$$

where

$G_1(a,b) = 24u^4 - 100u^3v + 105u^2v^2 - 40uv^3 + 5v^4$, where we put $\quad u = a+1, \quad v = b+4.$

The polynomial G_1 is irreducible and the unique solution of the equation $G_1(a,b) = 0$ is given by $(a,b) = (-1,-4)$. Then $p_4(x) + p_4(-x-4) = 0$ and we get infinitely many integer solutions

but with $z = 0$.

The second factor is a huge polynomial of degree 12 (with respect to each variable) which defines the curve in (a, b) plane in the following way:

$$C_4 : \ G_2(a, b) = 0.$$

The genus of the curve C_4 is 3 (relative small with comparison of the degree of the defining polynomial) and thus the set of rational points is finite. We used procedure `PointSearch` one more time and find that the curve C_4 contains relatively many rational points. Indeed, in the range $\max\{H(a), H(b)\} < 10^5$ we found 16 rational points. We have $(a, b) \in \mathcal{A}_4$, where

$$\mathcal{A}_4 = \{(-1,-8),(-1,-6),(-1,2),(-1,0),\left(\frac{1}{4},-\frac{15}{4}\right),\left(\frac{1}{4},-\frac{13}{4}\right),\left(\frac{1}{4},\frac{1}{4}\right),$$
$$\left(\frac{1}{4},\frac{3}{4}\right),\left(\frac{2}{3},-\frac{5}{3}\right),\left(\frac{2}{3},\frac{1}{3}\right),\left(\frac{3}{2},\frac{5}{2}\right),(4,-3),(4,-1),(4,13)\}.$$

If $(a, b) \in \mathcal{A}_4 \setminus \{(-1, 0), (-1, -2)\}$, then the equation $z^2 = p_4(x) + p_4(ax + b)$ defines a genus 1 curve (and thus there are only finitely many integer solutions in this case) or defines a genus 0 curve with only finitely many integral solutions.

In the first case we have $p_4(x) + p_4(-x) = 20x^2(x^2 + 5)$, i.e., $5(x^2 + 5)$ need to be square. Hence 5 divides x. Write $x = 5t$. That is we obtain an equation of the form

$$v^2 - 5t^2 = 4.$$

The solutions of the above equation are well-known: $(v, t) = (L_{2m}, F_{2m})$ for some $m \in \mathbb{N}$, where, as usual F_n denotes n-th Fibonacci number $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ and L_n denotes n-th Lucas number defined recursively by $L_0 = 2, L_1 = 1, L_n = L_{n-1} + L_{n-2}$. To obtain integral solution the number F_{2m} has to be even, therefore m is divisible by 3. It follows that if $t = 5F_{6n}, n \in \mathbb{N}$, then the pair

$$\left(\frac{-5F_{6n}}{2}, \frac{25F_{12n}}{2}\right)$$

is the solution of the equation $z^2 = p_4(x) + p_4(-x)$.

Using similar approach one can easily check that if $(a, b) = (-1, -2)$, then we get quadratic equation with infinitely many solutions. We omit the details.

Remark. Let us note the identities

$$p_4(x)+p_4(-x-6) = -10(x+2)(x+4)(x+3)^2,\ p_4(x)+p_4(-x-8) = -20(x^2+8x+21)(x+4)^2,$$

which can be used to prove that the equation $-z^2 = p_4(x) + p_4(y)$ has infinitely many solutions in integers.

Remark. It seems that the question concerning the existence of *positive* integer solutions of the equation $z^2 = p_4(x) + p_4(y)$ is more difficult. We performed numerical search for solutions in the range $0 < x \leq y \leq 10^5$ and found any.

dc_1892_21

Chapter 6 Polynomial values of recurrence sequences

6.1 A result by Nemes and Pethő

Let A, B, R_0, R_1 be integers. A binary linear recurrence sequence R_n is defined by two initial values (R_0, R_1) and by the relation

$$R_{n+1} = AR_n - BR_{n-1}, n \geq 1.$$

Such a sequence is called non-degenerate if $|R_0| + |R_1| > 0$ and the quotient of the roots, $\alpha_1, \alpha_2 \in \mathbb{C}$ of the characteristic polynomial of R_n (defined by $x^2 - Ax + B$) is not a root of unity. Let us introduce some additional notation. Let $D = A^2 - 4B$ and $C = R_1^2 - AR_1R_0 + BR_0^2$. Let $T_k(x)$ denote the Chebishev polynomial of degree k, defined by $T_0(x) = 2, T_1(x) = x$ and $T_{n+1}(x) = xT_n(x) - T_{n-1}(x)$ for $n \geq 1$. The following elegant characterization is due to Nemes and Pethő [94].

Theorem 6.1

Let R_n be a non-degenerated second order recurrence with $|B| = 1$, and $P = \sum_{k=0}^{d} A_k X^k$ be a polynomial with integer coefficients of degree $d \geq 2$. Let be $q = -B^m C/D$ and $E = 2(d-1)A_{d-1}^2 - 4dA_dA_{d-2}$. If the equation $R_n = P(x)$ has infinitely many integer solutions n, x, then

$$P(x) = \varepsilon\sqrt{q}T_d\left(\frac{2d|A_d|}{\eta\sqrt{E}} + \frac{2A_{d-1}}{\eta\sqrt{E}}\right),$$

where ε and η are either 1 or -1. Furthermore, either x is an integer root of $P'(x)$ or $d|A_d|x + A_{d-1}$ is contained in the union of finitely many second order recurrence sequences with discriminants D_i, where D/D_i are squares of integers.

Based on this result Nemes and Pethő noted that the equation $F_n = P(x)$ can have infinitely many solutions only when the degree of P is odd. They also remarked that the assumptions of the theorem are not sufficient, i.e., the equation $R_n = P(x)$ may have finitely many solutions even if the polynomial is of the expected form. In fact they noted that the equation $L_n = P(x) = 3x^2 - 2 = T_2(\sqrt{3}x)$ although of expected form, has no integer solutions. Thus, it is quite natural to ask whether we can construct an explicit form of polynomial P such that the equation $L_n = P(x)$ has infinitely many integer solutions. Similar question can be asked for the sequence of Fibonacci numbers $(F_n)_{n\in\mathbb{N}}$. As we will see such construction can be performed for quite general class of Lucas sequences, with particular examples being Fibonacci and Lucas sequences. Indeed, in Section 6.2 we consider the sequences $(P_n(a))_{n\in\mathbb{N}}, (Q_n(a))_{n\in\mathbb{N}}$, where $a \in \mathbb{C} \setminus \{-1, 0, 1\}$ and

$$P_n(a) = \frac{a^n - a^{-n}}{a - a^{-1}}, \quad Q_n(a) = a^n + a^{-n}.$$

We show that for each $k \in \mathbb{N}_+$ there is a square-free polynomial $F_k(a, t) \in \mathbb{Q}(a)[t]$ of degree

$2k-1$ such that the Diophantine equation $F_k(a,t) = P_m(a)$ has infinitely many solutions in positive integers t, m. Similarly, we prove that for each $k \in \mathbb{N}_+$ there is a polynomial $G_k \in \mathbb{Z}[t]$ of degree $k+1$ such that the Diophantine equation $G_k(t) = Q_m(a)$ has infinitely many solutions in positive integers t, m. By an appropriate specialization $a = a_0$ we get polynomials $F_k(a_0,t), G_k(t) \in \mathbb{Z}[t]$ such that the equations

$$F_k(a_0,t) = F_n, \quad G_k(t) = L_n$$

have infinitely many solutions in integers. Moreover, an additional advantage of our construction is the possibility to determine the explicit form of the discriminants of our polynomials. In Section 6.3 we present results of our numerical calculations concerning the existence of degree two polynomials f such that the Diophantine equation $f(x) = F_m$, where F_m is the mth Fibonacci number, has at least four solutions in integers x, m. Moreover, based on our computations we state several conjectures and certain general problems

Finally, in the last section we characterize integral solutions of several Diophantine equations related to representations of Fibonacci numbers by shifted triangular numbers, that is we resolve the equations

$$\binom{x}{2} + d = F_n \quad \text{for } -20 \le d \le 20.$$

Moreover, by investigating certain genus two curves we characterize all integral solutions of the Diophantine equation $\binom{x}{5} = F_n$. Our result complement earlier findings concerning integer solutions of the equation $\binom{x}{k} = F_n$, where $k \le 4$.

6.2 Polynomials representing infinitely many Fibonacci and related numbers

Which polynomials $P \in \mathbb{Z}[X]$ represent many different Fibonacci numbers? For a given polynomial we may expect only finitely many solutions of the equation $P(x) = F_n$. Indeed, we recall the identity $L_n^2 = 5F_n^2 \pm 4$ and thus, if we are interested in finding integer solutions of the equation $P(x) = F_n$, then it is enough to find all integer solutions of the Diophantine equation

$$y^2 = 5P(x)^2 \pm 4.$$

The above equation defines a hyperelliptic curve, say C. From Siegel theorem we know that if the polynomial $5P(x)^2 \pm 4$ can not be represented in the form $f_1(x)^2 f_2(x)$ for certain polynomials $f_1, f_2 \in \mathbb{Q}[x]$, where f_2 is a square-free polynomial of degree ≥ 3, then there are only finitely many integral points on the curve C. In consequence, we have only finitely many solutions of the related equation $P(x) = F_n$.

We would like to determine polynomials P_d of a given degree $d > 1$ such that the set $\{P_d(x) : x \in \mathbb{Z}\}$ contains many Fibonacci numbers.

In case of $d = 2$ the polynomials $P_{2,k}(x) = 3x^2 + (6k+2)x + k(3k+2)$ represent the

Fibonacci numbers $0, 1, 5, 8, 21, 4181$ since

$$P_{2,k}(-k) = 0, P_{2,k}(-k-1) = 1, P_{2,k}(-k+1) = 5,$$
$$P_{2,k}(-k-2) = 8, P_{2,k}(-k-3) = 21, P_{2,k}(-k+37) = 4181.$$

Here we remark that obviously the above family comes from a given polynomial, namely $3x^2+2x$ by applying the substitution $x := x+k$. Therefore, if we consider the question of representability of a given number by a polynomial $P_d(x) = A_d x^d + A_{d-1}x^{d-1} + \ldots$ of degree d with $A_d > 0$, then without loss of generality we can assume that $|A_{d-1}| \leq dA_d$. Indeed, we can always write $A_{d-1} = dA_d k + r$ for some $k \in \mathbb{Z}$ with $0 \leq r < dA_d$ and thus after the substitution $x := x + k$ we get a polynomial in the required form.

It is clear from Lagrange interpolation formula that for a given d we may construct a polynomial of degree d representing $d+1$ Fibonacci numbers. For example in case of $d = 3$ we use the points $(0,0), (1,1), (2,2), (3,F_n)$ to obtain the polynomial

$$\left(\frac{1}{6}F_n - \frac{1}{2}\right)x^3 + \left(-\frac{1}{2}F_n + \frac{3}{2}\right)x^2 + \frac{1}{3}F_n x.$$

The polynomial has integral coefficients if $n \equiv 0 \pmod 4$ and $n \not\equiv 0 \pmod 3$. Hence we may take $F_{16} = 987$ to get $164x^3 - 492x^2 + 329x$. The latter polynomial represents the Fibonacci numbers $0, 1, 2, 987$.

We prove that there exist odd degree polynomials representing infinitely many Fibonacci numbers and related sequences.

Theorem 6.2

For $a \in \mathbb{C} \setminus \{-1, 0, 1\}$ let us consider the sequence $(P_n(a))_{n\in\mathbb{N}}$, where

$$P_n = P_n(a) = \frac{a^n - a^{-n}}{a - a^{-1}}.$$

Then, for any given $k \in \mathbb{N}_+$ there is a square-free polynomial $F_k(a,t) \in \mathbb{Z}\left[\frac{1}{2}\right][t]$ of degree $2k-1$ such that the Diophantine equation $F_k(a,t) = P_n$ has infinitely many solutions in integers t, n.

The most difficult part of the proof of the above theorem is square-freeness of polynomial $F_k(a,t)$. In order to do that we will compute discriminant of the polynomial $F_k(a,t)$. Thus, we recall below the notion of a resultant of two polynomials and a discriminant.

Let K be a field and consider the polynomials $F, G \in K[x]$ given by

$$\begin{aligned} F(x) &= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \\ G(x) &= b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0. \end{aligned} \tag{6.1}$$

The resultant of the polynomials F, G is defined as

$$\mathrm{Res}(F,G) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j),$$

where $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ are the roots of F and G respectively (viewed in an appropriate

field extension of K). We define the discriminant of the polynomial F in the following way:

$$\mathrm{Disc}(F) = \frac{(-1)^{\frac{n(n-1)}{2}}}{a_n}\,\mathrm{Res}(F, F').$$

We collect basic properties of the resultant of the polynomials F, G:

$$\mathrm{Res}(F, G) = a_n^m \prod_{i=1}^{n} G(\alpha_i) = b_m^n \prod_{i=1}^{m} F(\beta_i), \tag{6.2}$$

$$\mathrm{Res}(F, G) = (-1)^{nm}\,\mathrm{Res}(G, F), \tag{6.3}$$

$$\mathrm{Res}(F, G_1G_2) = \mathrm{Res}(F, G_1)\,\mathrm{Res}(F, G_2). \tag{6.4}$$

Moreover, if $F(x) = a_0$ is a constant polynomial then, unless $F = G = 0$, we have

$$\mathrm{Res}(F, G) = \mathrm{Res}(a_0, G) = \mathrm{Res}(G, a_0) = a_0^m. \tag{6.5}$$

Finally, we recall an important result concerning the formula for the resultant of the polynomial G and F, provided that $F(x) = q(x)G(x) + r(x)$. More precisely, we have the following.

Lemma 6.1

Let $F, G \in K[x]$ be given by (6.1) and suppose that $F(x) = q(x)G(x) + r(x)$ for some $q, r \in K[x]$. Then we have the formula

$$\mathrm{Res}(G, F) = b_m^{\deg F - \deg r}\,\mathrm{Res}(G, r).$$

The proof of the above lemma can be found in [102] (see also [49]).

Proof. [Proof of Theorem 6.2] We define the sequence $(F_k(a,t))_{n\in\mathbb{N}_+}$ of polynomials in a recursive way. More precisely, we put

$$F_1(a,t) = t,\ F_2(a,t) = \frac{1}{a^2}t((a^2-1)^2t^2 + 3a^2),$$
$$F_k(a,t) = \frac{(a^2-1)^2t^2 + 2a^2}{a^2}F_{k-1}(a,t) - F_{k-2}(a,t),\ k \geq 3,$$

and prove that for each $k, n \in \mathbb{N}_+$ the following identity holds

$$F_k(a, P_n) = P_{(2k-1)n}. \tag{6.6}$$

From the recursive definition it is clear that $\deg F_k(a,t) = 2k-1$ for $k \in \mathbb{N}_+$. The proof that the polynomial $F_k(a,t)$ has the property given by (6.6) can be easily performed by induction on k. Indeed, we note that $F_1(a, P_n) = P_n$ and the identity

$$P_n^3 = \frac{a^2}{(a^2-1)^2}(P_{3n} - P_n)$$

implies that $P_{3n} = \frac{1}{a^2}P_n((a^2-1)^2P_n^2 + 3a^2) = F_2(a, P_n)$. We thus proved that our statement is true for $k = 1, 2$. Assuming now that it is true for $k-1$ and $k-2$ and using the recurrence formula, it easy (but a bit tiresome) calculation to see that our statement holds also for k. Indeed, the only thing we need to check is that the following identity

$$P_{(2k-1)n}(a) = \frac{(a^2-1)^2t^2 + 2a^2}{a^2}P_{2(k-1)-1}(a) - P_{2(k-2)-1}(a)$$

holds. We omit the simple details.

In order to finish the proof we need to show that for any given k, the polynomial F_k is

square-free, i.e., it has not multiple roots (in a suitable field extension). To prove our result we compute the discriminant $\mathrm{Disc}(F_k(a,t))$. More precisely, we prove the formula

$$\mathrm{Disc}(F_k(a,t)) = (-1)^{k+1}2^{2(k-1)}(2k-1)^{2k-1}\left(\frac{a^2-1}{a}\right)^{2(k-1)(2k-3)}.$$

Here, and in the sequel, by a discriminant or a resultant we mean discriminant and resultant with respect to the variable t.

To compute the discriminant we are interested in, we will consider the polynomial $H_k(a,t)$ instead of $F_k(a,t)$, where $H_k(a,t) = F_k(a,t)/t$. Note that the sequence $(H_k(a,t))_{k\in\mathbb{N}_+}$ satisfies the same recurrence relation as the sequence $(F_k(a,t))_{k\in\mathbb{N}_+}$. The reason that we consider the polynomials $H_k(a,t)$ is the non-vanishing of the value of $H_k(a,0)$. In fact, by a simple induction we get that $H_k(a,0) = 2k-1$. It is clear that the computation of the discriminant of $F_k(a,t)$ is equivalent with the computation of the discriminant of $H_k(a,t)$. Indeed, from the identity $F_k(a,t) = tH_k(a,t)$ we get that $F_k'(a,t) = H_k(a,t) + tH_k'(a,t)$. This allow us to get the identity

$$\mathrm{Disc}(F_k(a,t)) = (2k-1)^2\,\mathrm{Disc}(H_k(a,t)).$$

In the sequel we will need the following formula connecting polynomials $H_{k-1}(a,t)$, $H_k(a,t), H_k'(a,t)$. More precisely, we have

$$f_1(a,t)H_k(a,t) = f_2(a,t)H_k'(a,t) + 2(2k-1)a^2H_{k-1}(a,t),$$

where

$$f_1(a,t) = 2((a^2-1)^2(k-1)t^2 + (2k-3)a^2), \quad f_2(a,t) = t((a^2-1)^2t^2 + 4a^2).$$

The above identity can be easily proved by induction on k. We are in position to compute the resultant of the polynomials $H_k(a,t), H_k'(a,t)$ and hence the discriminant of $H_k(a,t)$ via the formula

$$\mathrm{Disc}(H_k(a,t)) = (-1)^{(k-1)(2k-3)}\left(\frac{a}{a^2-1}\right)^{2(k-1)}\mathrm{Res}(H_k(a,t), H_k'(a,t)). \tag{6.7}$$

In order to simplify the notation we will write H_k instead of $H_k(a,t)$.

Instead of computing $\mathrm{Res}(H_k, H_k')$ we compute

$$\begin{aligned}
&\mathrm{Res}(H_k, f_2)\,\mathrm{Res}(H_k, H_k') = \mathrm{Res}(H_k, f_2H_k') \\
&\quad = \mathrm{Res}(H_k, f_1H_k - 2(2k-1)a^2H_{k-1}) && \text{by Lemma 6.1} \\
&\quad = \left(\tfrac{a^2-1}{a}\right)^{8(k-1)}\mathrm{Res}(H_k, -2(2k-1)a^2H_{k-1}) && \text{by (6.4)} \\
&\quad = \left(\tfrac{a^2-1}{a}\right)^{8(k-1)}\mathrm{Res}(H_k, -2(2k-1)a^2)\,\mathrm{Res}(H_k, H_{k-1}) && \text{by (6.5)} \\
&\quad = \left(\tfrac{a^2-1}{a}\right)^{8(k-1)}(2(2k-1)a^2)^{2(k-1)}\,\mathrm{Res}(H_k, H_{k-1}).
\end{aligned}$$

We show that if $V_k = \mathrm{Res}(H_k, H_{k-1})$, then the sequence $(V_k)_{k\in\mathbb{N}_+}$ satisfies a recurrence relation

$$V_k = \left(\frac{a^2-1}{a}\right)^{4(k-1)}V_{k-1}.$$

Indeed, we have the following chain of equalities

$$\begin{aligned} V_k &= \operatorname{Res}(H_k, H_{k-1}) = \operatorname{Res}(H_{k-1}, H_k) && \text{by (6.3)} \\ &= \operatorname{Res}\left(H_{k-1}, \tfrac{1}{a^2}((a^2-1)^2t^2+2a^2)H_{k-1} - H_{k-2}\right) \\ &= \left(\tfrac{a^2-1}{a}\right)^{8(k-2)} \operatorname{Res}(H_{k-1}, H_{k-2}) = \left(\tfrac{a^2-1}{a}\right)^{8(k-2)} V_{k-1} && \text{by Lemma 6.1.} \end{aligned}$$

Using the identity $V_2 = \operatorname{Res}(H_2, H_1) = 1$ we immediately get that for $k \geq 2$ we have the formula

$$V_k = \prod_{i=2}^{k} \left(\frac{a^2-1}{a}\right)^{8(i-2)} = \left(\frac{a^2-1}{a}\right)^{4(k-1)(k-2)}.$$

To finish the computation of $\operatorname{Res}(H_k, H_k')$ we need to compute the value of $\operatorname{Res}(H_k, f_2)$. The following formula can be deduced from the definition of the resultant:

$$\begin{aligned} \operatorname{Res}(H_k, f_2) &= \operatorname{Res}(H_k, t)\operatorname{Res}(H_k, (a^2-1)^2t^2+4a^2) \\ &= (2k-1)\operatorname{Res}(H_k, (a^2-1)^2t^2+4a^2) \\ &= (2k-1)(a^2-1)^{4(k-1)}. \end{aligned}$$

Finally, we obtain the formula for $\operatorname{Res}(H_k, H_k')$ in the following form

$$\operatorname{Res}(H_k, H_k') = \frac{\operatorname{Res}(H_k, f_2H_k')}{\operatorname{Res}(H_k, f_2)} = 2^{2(k-1)}(2k-1)^{2k-1}\left(\frac{a^2-1}{a}\right)^{4(k-1)^2}$$

and using the formula (6.7) we get the explicit value of $\operatorname{Disc}(H_k(a,t))$.

Remark. One can check by induction on k that each term of the sequence $(F_k(a,t))_{k\in\mathbb{N}_+}$ corresponds to a solution of a certain Pell type equation. More precisely, for each $k \in \mathbb{N}_+$ we have the identity

$$(2k-1)^2((a^2-1)^2F_k(a,t)^2+4a^2) = ((a^2-1)^2t^2+4a^2)F_k'(a,t)^2.$$

Our general result allow us to prove the following.

Corollary 6.1

If $a = i\frac{\sqrt{5}-1}{2}$, where $i^2 = -1$, then

$$P_{4n-3}(a) = F_{4n-3}, P_{1-4n}(a) = F_{4n-1}$$

and the polynomial $F_k(a,t)$ has integer coefficients, and for each $k \in \mathbb{N}_+$, the Diophantine equation

$$F_k\left(i\frac{\sqrt{5}-1}{2}, t\right) = F_n \tag{6.8}$$

has infinitely many solutions in integers t, n.

Proof. From the Binet formula for the nth Fibonacci number we easily get the expressions for $P_{4n-3}(a)$ and $P_{1-4n}(a)$. Moreover, we observe that for $a = i\frac{\sqrt{5}-1}{2}, i^2 = -1$, we have $(a^2-1)^2/a^2 = -5$ and thus from the definition of $F_k(a,t)$ we get that our polynomial has integer coefficients. The existence of infinitely many integer solutions of the equation (6.8) is

also clear. Indeed, from Theorem 6.2 for each $k, n \in \mathbb{N}_+$ we have the identity

$$F_k\left(i\frac{\sqrt{5}-1}{2}, (-1)^{k+1}F_{2n-1}\right) = F_{(2k-1)(2n-1)}.$$

Example 6.1. First few polynomials $F_k(a, (-1)^{k+1}t)$ for $a = i\frac{\sqrt{5}-1}{2}, i^2 = -1$, are given in the table below.

n	$F_k(a, (-1)^{k+1}t)$
2	$t\left(5t^2 - 3\right)$
3	$5t\left(5t^4 - 5t^2 + 1\right)$
4	$t\left(125t^6 - 175t^4 + 70t^2 - 7\right)$
5	$t\left(5t^2 - 3\right)\left(125t^6 - 150t^4 + 45t^2 - 3\right)$
6	$t\left(3125t^{10} - 6875t^8 + 5500t^6 - 1925t^4 + 275t^2 - 11\right)$
7	$t\left(15625t^{12} - 40625t^{10} + 40625t^8 - 19500t^6 + 4550t^4 - 455t^2 + 13\right)$

The polynomials $F_k(a, (-1)^{k+1}t)$ for $a = i\frac{\sqrt{5}-1}{2}, i^2 = -1$, and $k = 2, \ldots, 7$.

Remark. It is not difficult to observe that for the sequence $Q_n = Q_n(a) = a^n + a^{-n}$, where $a \in \mathbb{C} \setminus \{-1, 0, 1\}$, one can construct a polynomial $G_k \in \mathbb{Z}[t]$ of degree k such that the equation $G_k(x) = Q_m(a)$ has infinitely many solutions in $x, m \in \mathbb{N}_+$. Indeed, in order to do see that it is enough to observe that the following (easily to establish) identity holds:

$$Q_{kn}(a) = Q_n(a)Q_{(k-1)n}(a) - Q_{(k-2)n}(a).$$

Thus, if we define $G_1(t) = t, G_2(t) = t^2 - 2$ and $G_k(t) = tG_{k-1}(t) - G_{k-2}(t)$ for $k \geq 2$, then we have $G_k(Q_n) = Q_{kn}$ and hence the result. Moreover, it is not difficult to show that the polynomial G_k is square-free. Indeed, essentially the same type of reasoning as presented in the proof of second part of Theorem 6.2 can be used for the computation of $\mathrm{Disc}(G_k(t))$. Indeed, the only non-obvious fact we need to know is the existence of the formula connecting G_k, G_k', G_{k-1}. The mentioned formula takes the form

$$ktG_k(t) = (t^2 - 4)G_k'(t) + 2kG_{k-1}(t),$$

and the rest of the proof goes exactly in the same way as in the case of $F_k(a, t)$. As a final result we get the formula $\mathrm{Disc}(G_k(t)) = 2^{k-1}k^k$. Moreover, it is easy to prove (by induction on k) that the following identity holds:

$$(k+1)^2(G_k(t)^2 - 4) = (t^2 - 4)G_k'(t)^2.$$

We omit the details.

In particular, if $a = \frac{\sqrt{5}-1}{2}$, then one can easily check that $Q_{2n}(a) = L_{2n}$, where L_n is nth Lucas number. Thus, as consequence, we get that there is a polynomial $G_k \in \mathbb{Z}[t]$ of degree $k+1$ such that the Diophantine equation $G_k(t) = L_m$ has infinitely many solutions in integers k, m. Indeed, it is enough to note the identity

$$G_k(L_{2n}) = L_{2kn}.$$

6.3 Numerical and experimental results

In light of Theorem 6.2 it is natural to ask about construction of polynomials of even degree, say d, which represent "many" Fibonacci numbers. We are very modest here and asks about the existence of polynomials $f \in \mathbb{Q}[x]$ of degree d such that the Diophantine equation $f(x) = F_m$ has at least $d+2$ solutions. We are especially interested in the case $d = 2$.

To find interesting examples we performed the following search strategy. We first generated the set

$$A = \{(F_p, F_q, F_r, F_s) : \ p, q, r, s \in \{2, \ldots, 100\}\}$$

and then for each quadruple with pairwise distinct elements $v \in A$ (there are exactly 3764376 elements of this kind in A) we looked for the degree two polynomial f such that

$$f(1) = F_p, f(2) = F_q, f(3) = F_r, f(4) = F_s. \tag{6.9}$$

Note that a degree two polynomial is defined by three coefficients and thus our system of equation (6.9) is over-determined. Thus, we cannot expect too many solutions (if any). In fact, with this approach we found 93 polynomials with required properties. Browsing through the set of solutions we were able to find three infinite families $(f_{i,n})_{n\in\mathbb{N}_+}, i = 1, 2, 3$, of degree two polynomials satisfying required conditions. More precisely, we define

$$\begin{aligned}
f_{1,n}(x) &= (F_{2n+1}x - L_{2n})((3F_{2n+1} - F_{2n} - F_{2n-3})x - 2F_{2n} - 5F_{2n-1} + F_{2n-5}),\\
f_{2,n}(x) &= F_{2n+3}x^2 - (3F_{2n+3} - F_{2n})x + 2F_{2n+3} - F_{2n-2},\\
f_{3,n}(x) &= (F_{2n}x - F_{2n+1} + F_{2n-3})((F_{2n+2} - F_{2n-2})x - 5F_{2n-1}).
\end{aligned}$$

With $f_{i,n}$ defined above it is easy to check that the following equalities are true:

$$\begin{aligned}
&f_{1,n}(1) = F_{4n-2} \quad f_{1,n}(2) = F_{4n} \quad f_{1,n}(3) = F_{4n+4} \quad f_{1,n}(4) = F_{4n+6},\\
&f_{2,n}(1) = F_{2n-1} \quad f_{2,n}(2) = F_{2n+1} \quad f_{2,n}(3) = F_{2n+5} \quad f_{2,n}(4) = F_{2n+7},\\
&f_{3,n}(1) = F_{4n-4} \quad f_{3,n}(2) = F_{4n-2} \quad f_{3,n}(3) = F_{4n+2} \quad f_{3,n}(4) = F_{4n+4}.
\end{aligned}$$

Note that from the result of Nemes and Pethő we know that for each $n \in \mathbb{N}_+$ and $i \in \{1, 2, 3\}$ the Diophantine equation $f_{i,n}(x) = F_m$ has only finitely many solutions in integers.

It should be noted that among 93 polynomials found by the above described search, there is only one which do not belong to the sequences $(f_{i,n})_{n\in\mathbb{N}}, i \in \{1, 2, 3\}$. This sporadic polynomial is the following:

$$f(x) = \frac{1}{2}(x^2 - x + 4). \tag{6.10}$$

Unexpectedly, it represents five Fibonacci numbers. More precisely, all non-negative integer solutions (x, m) of the Diophantine equation $f(x) = F_m$ are

$$(x, m) = (0, 3), (1, 3), (2, 4), (3, 5), (4, 6), (22, 13).$$

For the proof of this result see Theorem 6.3 below. Let us also note that $f(x) = t_{x-1} + 2$,

where $t_x = x(x+1)/2$ is the xth triangular number. Thus the problem of finding non-negative solutions of Diophantine equation $f(x) = F_m$ is equivalent with the finding triangular numbers of the form $F_m - 2$.

We performed similar analysis in case of Lucas numbers and were able to spot one infinite family $(g_n)_{n\in\mathbb{N}_{\geq 4}}$, where

$$g_n(x) = L_n x^2 - (L_{n+2} + L_{n-4})x + 5L_{n-2}.$$

Then

$$g_n(1) = L_{n-4}, \quad g_n(2) = L_{n-2}, \quad g_n(3) = L_{n+2}, \quad g_n(4) = L_{n+4}.$$

Remarkably, if $g \in \mathbb{Z}[x]$ is of degree 2 and satisfies

$$g(1) = L_p, g(2) = L_q, g(3) = L_r, g(4) = L_s$$

for $p < q < r < s \leq 100$ then there is $n \leq 45$ satisfying $g(x) = g_n(x)$.

We performed similar search in the case of degree 4 polynomials. More precisely, we were interested in finding examples of polynomials $f \in \mathbb{Q}[x]$ of degree 4 such that f represents at least 6 Fibonacci numbers. We first generated the set

$$B = \{(F_p, F_q, F_r, F_s, F_u, F_v) : \ p, q, r, s, u, v \in \{2, \ldots, 60\}\}$$

and then for each sextuple with pairwise distinct elements $w \in B$ (there are exactly 45057474 elements of this kind in B) we looked for a polynomial f of degree ≤ 4 such that

$$f(1) = F_p, \quad f(2) = F_q, \quad f(3) = F_r, \quad f(4) = F_s, \quad f(5) = F_u, \quad f(6) = F_v. \tag{6.11}$$

In the considered range we found only four polynomials of degree ≤ 4 representing at least six Fibonacci polynomials. They are given in the table below together with the known integer solutions of the equation $f(x) = F_m, m \geq 0$.

$f(t)$	Known solutions of $f(x) = F_m$
$\left(t^3 - 6t^2 + 23t - 12\right)/6$	$(1,1), (1,2), (2,4), (3,5),$ $(4,6), (5,7), (6,8)$
$\left(101t^4 - 1064t^3 + 4369t^2 - 7162t + 3780\right)/12$	$(1,3), (2,4), (3,11),$ $(4,13), (5,15), (6,17)$
$\left(245t^4 - 3080t^3 + 13729t^2 - 23290t + 12420\right)/12$	$(1,3), (2,4), (3,13)$ $(4,14), (5,15), (6,17)$
$\left(t^4 - 6t^3 + 35t^2 - 6t + 96\right)/24$	$(-4,10), (-2,7), (1,5), (2,6),$ $(3,7), (4,8), (5,9), (6,10)$

The polynomials $f \in \mathbb{Q}[x]$ of degree $3 \leq d \leq 4$ such that $f(x)$ represents at least six Fibonacci numbers together with the set of known integral solutions of the corresponding Diophantine equation $f(x) = F_m$.

We note that in case of the polynomial $f(x) = (x^3 - 6x^2 + 23x - 12)/6$ the Diophantine equation $f(x) = F_m$ can be reduced to genus 2 curves by using the identity $L_n^2 = 5F_n^2 \pm 4$.

Therefore one may try to apply the method developed in [36] to determine a complete list of integral solutions. The hyperelliptic curves $y^2 = 5f(x)^2 \pm 4$ define genus 2 curves and their Jacobians have rank 4. It turns out to be difficult to provide generators of the Mordell-Weil groups that is required to apply the method based on Baker's linear forms in logarithms and the so-called Mordell-Weil sieve.

Remark. We note that for any given even $d \in \mathbb{N}_+$ it is possible to construct a polynomial $G_d \in \mathbb{Q}[x]$ of degree d such that the equation $G_d(x) = F_m$ has at least $d+2$ solutions in integers x, m. Indeed, we learned that if we define G_d as the unique polynomial of degree d with rational coefficients satisfying the system of equations

$$G_d(0) = F_{d+2},\ G_d(1) = F_{d+3},\ \ldots,\ G_d(d-1) = F_{2d},\ G_d(d) = F_{2d+2},$$

then additional the equality $G_d(-1) = F_{d+1}$ holds [74, Equation (3.1)].

6.4 Fibonacci numbers represented by shifted triangular numbers

Motivated by the example given by (6.10) we deal with the family of equations

$$t_{x-1} + d = \binom{x}{2} + d = F_n \quad \text{for } -20 \le d \le 20. \tag{6.12}$$

Theorem 6.3

All non-negative integral solutions n with $-20 \le d \le 20$ of equation (6.12) are as follows

$d = -20, n \in \{1, 2, 6, 13, 15\}, d = -19, n \in \{3\}, d = -18, n \in \{4\},$

$d = -16, n \in \{5, 11\}, d = -15, n \in \{0, 7, 8\}, d = -14, n \in \{1, 2\},$

$d = -13, n \in \{3, 6\}, d = -12, n \in \{4\}, d = -11, n \in \{9, 10\}, d = -10, n \in \{0, 5\},$

$d = -9, n \in \{1, 2, 12\}, d = -8, n \in \{3, 7\}, d = -7, n \in \{4, 6, 8\}, d = -6, n \in \{0\},$

$d = -5, n \in \{1, 2, 5, 19\}, d = -4, n \in \{3\}, d = -3, n \in \{0, 4, 16\},$

$d = -2, n \in \{1, 2, 6, 7, 9, 11\}, d = -1, n \in \{0, 3, 5, 14\}, d = 0, n \in \{0, 1, 2, 4, 8, 10\},$

$d = 1, n \in \{1, 2, 3, 17\}, d = 2, n \in \{3, 4, 5, 6, 13\}, d = 3, n \in \{4, 7\}, d = 4, n \in \{5\},$

$d = 5, n \in \{5, 6\}, d = 6, n \in \{8, 9\}, d = 7, n \in \{6, 7\}, d = 8, n \in \{6, 12, 24\},$

$d = 10, n \in \{7, 10\}, d = 11, n \in \{8, 11\}, d = 12, n \in \{7\} d = 13, n \in \{7, 9\},$

$d = 15, n \in \{8, 15\}, d = 18, n \in \{8\}, d = 19, n \in \{9, 10\}, d = 20, n \in \{8\}.$

Proof. We use the following well-known identity related to the sequences F_n and L_n

$$L_n^2 - 5F_n^2 = 4(-1)^n. \tag{6.13}$$

The above identity yields the hyperelliptic curves

$$C_{d,\pm}: \quad y^2 = 5x^4 - 10x^3 + (20d + 5)x^2 - 20dx + 20d^2 \pm 16.$$

We searched for small solutions on these curves. If no points were found, then we used the Magma procedure `TwoCoverDescent()` [30] to show that there exist no solutions. In case that

dc_1892_21

certain small solutions exist we used the Magma procedure `IntegralQuarticPoints()` based on results obtained by Tzanakis [137]. As an example consider the case $d = -5$. Since $(0, -22)$ is a point on the curve $C_{-5,-}$ we used `IntegralQuarticPoints([ 5, -10, -95, 100, 484 ],[0,-22])` to determine a complete list of integral solutions. It turns out that there are solutions only if

$$x \in \{-91, -4, -3, -2, 0, 1, 3, 4, 5, 92\}.$$

Similarly, $(-3, -6)$ is a point on $C_{-5,+}$. Therefore via `IntegralQuarticPoints([ 5, -10, -95, 100, 516 ],[-3,-6])` it follows that

$$x \in \{-3, 4\}.$$

Thus we have the solutions

$$\begin{aligned} \binom{4}{2} - 5 &= F_1 = F_2, \\ \binom{5}{2} - 5 &= F_5, \\ \binom{92}{2} - 5 &= F_{19}. \end{aligned}$$

6.5 The Diophantine equations $L_n = \binom{X}{5}$ and $F_n = \binom{X}{5}$

Let us consider the Diophantine equations

$$L_n = \binom{X}{5} \tag{6.14}$$

and

$$F_n = \binom{X}{5} \tag{6.15}$$

with $X \geq 5$. We have the following results.

Theorem 6.4

The only positive solution of equation (6.14) with $X \geq 5$ is $(n, X) = (1, 5)$.

Theorem 6.5

The integral solutions of equation (6.15) with $X \geq 5$ are given by $(n, X) \in \{(1, 5), (2, 5), (8, 7)\}$.

6.5.1 Integral points via Baker's method and the Mordell-Weil sieve

Consider the hyperelliptic curve

$$\mathcal{C}: \quad y^2 = F(x) := x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0, \tag{6.16}$$

where $b_i \in \mathbb{Z}$. Let α be a root of F and $J(\mathbb{Q})$ be the Jacobian of the curve $\mathcal{C}$. We have that

$$x - \alpha = \kappa\xi^2$$

where κ, $\xi \in K = \mathbb{Q}(\alpha)$ and κ comes from a finite set. By knowing the Mordell-Weil group of the curve $\mathcal{C}$ it is possible to provide a method to compute such a finite set. To each coset representative $\sum_{i=1}^{m}(P_i - \infty)$ of $J(\mathbb{Q})/2J(\mathbb{Q})$ we associate

$$\kappa = \prod_{i=1}^{m} \left(\gamma_i - \alpha d_i^2\right),$$

where the set $\{P_1, \ldots, P_m\}$ is stable under the action of Galois, all $y(P_i)$ are non-zero and $x(P_i) = \gamma_i/d_i^2$ where γ_i is an algebraic integer and $d_i \in \mathbb{Z}_{\geq 1}$. If P_i, P_j are conjugate then we may suppose that $d_i = d_j$ and so γ_i, γ_j are conjugate. We have the following lemma (Lemma 3.1 in [36]).

Lemma 6.2

Let $\mathcal{K}$ be a set of κ values associated as above to a complete set of coset representatives of $J(\mathbb{Q})/2J(\mathbb{Q})$. Then $\mathcal{K}$ is a finite subset of $\mathcal{O}_K$ and if (x, y) is an integral point on the curve (6.16) then $x - \alpha = \kappa\xi^2$ for some $\kappa \in \mathcal{K}$ and $\xi \in K$.

As an application of his theory of lower bounds for linear forms in logarithms, Baker [9] gave an explicit upper bound for the size of integral solutions of hyperelliptic curves. This result has been improved by many authors (see e.g. [20], [21], [28], [33], [103], [114], [121] and [144]).

In [36] an improved completely explicit upper bound were proved combining ideas from [33], [34], [35], [79], [90], [100], [144], [143]. Now we will state the theorem which gives the improved bound. We introduce some notation. Let K be a number field of degree d and let r be its unit rank and R its regulator. For $\alpha \in K$ we denote by $\mathrm{h}(\alpha)$ the logarithmic height of the element α. Let

$$\partial_K = \begin{cases} \frac{\log 2}{d} & \text{if } d = 1, 2, \\ \frac{1}{4}\left(\frac{\log\log d}{\log d}\right)^3 & \text{if } d \geq 3 \end{cases}$$

and

$$\partial_K' = \left(1 + \frac{\pi^2}{\partial_K^2}\right)^{1/2}.$$

Define the constants

$$c_1(K) = \frac{(r\,!)^2}{2^{r-1}d^r}, \qquad c_2(K) = c_1(K)\left(\frac{d}{\partial_K}\right)^{r-1},$$
$$c_3(K) = c_1(K)\frac{d^r}{\partial_K}, \qquad c_4(K) = rdc_3(K),$$
$$c_5(K) = \frac{r^{r+1}}{2\partial_K^{r-1}}.$$

Let

$$\partial_{L/K} = \max\left\{[L:\mathbb{Q}]\,,\ [K:\mathbb{Q}]\partial_K'\,,\ \frac{0.16[K:\mathbb{Q}]}{\partial_K}\right\},$$

where $K \subseteq L$ are number fields. Define

$$C(K, n) := 3 \cdot 30^{n+4} \cdot (n+1)^{5.5}\, d^2\, (1 + \log d).$$

The following theorem will be used to get an upper bound for the size of the integral solutions of our equation. It is Theorem 3 in [36].

Theorem 6.6

Let α be an algebraic integer of degree at least 3 and κ be an integer belonging to K. Denote by α_1, α_2, α_3 distinct conjugates of α and by κ_1, κ_2, κ_3 the corresponding conjugates of κ. Let

$$K_1 = \mathbb{Q}(\alpha_1, \alpha_2, \sqrt{\kappa_1\kappa_2}), \quad K_2 = \mathbb{Q}(\alpha_1, \alpha_3, \sqrt{\kappa_1\kappa_3}), \quad K_3 = \mathbb{Q}(\alpha_2, \alpha_3, \sqrt{\kappa_2\kappa_3}),$$

and

$$L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \sqrt{\kappa_1\kappa_2}, \sqrt{\kappa_1\kappa_3}).$$

In what follows R stands for an upper bound for the regulators of K_1, K_2 and K_3 and r denotes the maximum of the unit ranks of K_1, K_2, K_3. Let

$$c_j^* = \max_{1\le i\le 3} c_j(K_i)$$

and

$$N = \max_{1\le i,j\le 3} \left|\mathrm{Norm}_{\mathbb{Q}(\alpha_i,\alpha_j)/\mathbb{Q}}(\kappa_i(\alpha_i - \alpha_j))\right|^2$$

and

$$H^* = c_5^* R + \frac{\log N}{\min_{1\le i\le 3}[K_i : \mathbb{Q}]} + \mathrm{h}(\kappa).$$

Define

$$A_1^* = 2H^* \cdot C(L, 2r+1) \cdot (c_1^*)^2 \partial_{L/L} \cdot \left(\max_{1\le i\le 3} \partial_{L/K_i}\right)^{2r} \cdot R^2,$$

and

$$A_2^* = 2H^* + A_1^* + A_1^* \log\{(2r+1)\cdot \max\{c_4^*, 1\}\}.$$

If $x \in \mathbb{Z}\backslash\{0\}$ satisfies $x - \alpha = \kappa\xi^2$ for some $\xi \in K$ then

$$\log|x| \le 8A_1^* \log(4A_1^*) + 8A_2^* + H^* + 20\log 2 + 13\,\mathrm{h}(\kappa) + 19\,\mathrm{h}(\alpha).$$

To obtain a lower bound for the possible unknown integer solutions we are going to use the so-called Mordell-Weil sieve. The Mordell-Weil sieve has been successfully applied to prove the non-existence of rational points on curves (see e.g. [29], [31], [54] and [111]).

Let $C/\mathbb{Q}$ be a smooth projective curve (in our case a hyperelliptic curve) of genus $g \ge 2$. Let J be its Jacobian. We assume the knowledge of some rational point on C, so let D be a fixed rational point on C and let $\jmath$ be the corresponding Abel-Jacobi map:

$$\jmath : C \to J, \qquad P \mapsto [P - D].$$

Let W be the image in J of the known rational points on C and $D_1, \ldots, D_r$ generators for the free part of $J(\mathbb{Q})$. By using the Mordell–Weil sieve we are going to obtain a very large and smooth integer B such that

$$\jmath(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q}).$$

Let

$$\varphi : \mathbb{Z}^r \to J(\mathbb{Q}), \qquad \varphi(a_1, \ldots, a_r) = \sum a_i D_i,$$

so that the image of φ is the free part of $J(\mathbb{Q})$. The variant of the Mordell-Weil sieve explained in [36] provides a method to obtain a very long decreasing sequence of lattices in $\mathbb{Z}^r$

$$B\mathbb{Z}^r = L_0 \supsetneq L_1 \supsetneq L_2 \supsetneq \cdots \supsetneq L_k$$

such that

$$\jmath(C(\mathbb{Q})) \subset W + \varphi(L_j)$$

for $j = 1, \ldots, k$.

The next lemma [36, Lemma 12.1] gives a lower bound for the size of rational points whose image are not in the set W.

Lemma 6.3

Let W be a finite subset of $J(\mathbb{Q})$ and L be a sublattice of $\mathbb{Z}^r$. Suppose that $\jmath(C(\mathbb{Q})) \subset W + \varphi(L)$. Let μ_1 be a lower bound for $h - \hat{h}$ and

$$\mu_2 = \max\left\{\sqrt{\hat{h}(w)} \ : \ w \in W\right\}.$$

Denote by M the height-pairing matrix for the Mordell–Weil basis $D_1, \ldots, D_r$ and let $\lambda_1, \ldots, \lambda_r$ be its eigenvalues. Let

$$\mu_3 = \min\left\{\sqrt{\lambda_j} \ : \ j = 1, \ldots, r\right\}$$

and $m(L)$ the Euclidean norm of the shortest non-zero vector of L. Then, for any $P \in C(\mathbb{Q})$, either $\jmath(P) \in W$ or

$$h(\jmath(P)) \geq (\mu_3 m(L) - \mu_2)^2 + \mu_1.$$

6.5.2 Proof of Theorem 6.4

In this section first we prove a lemma and than we use it to prove Theorem 6.4.

Lemma 6.4

(a) The integral solutions of the equation

$$\mathcal{C}^+ : Y^2 = X^2(X+15)^2(X+20) + 180000000 \tag{6.17}$$

are

$$(X, Y) \in \{(25, -15000), (25, 15000)\}.$$

(b) There are no integral solution of the equation

$$\mathcal{C}^- : Y^2 = X^2(X+15)^2(X+20) - 180000000. \tag{6.18}$$

Proof. [Proof of Lemma 6.4] We start with the proof of part (a). Let $J(\mathbb{Q})^+$ be the Jacobian of the genus two curve (6.17). Using MAGMA [23] we obtain that $J(\mathbb{Q})^+$ is free of rank 1 with

Mordell-Weil basis given by

$$D = (25, 15000) - \infty.$$

The MAGMA programs used to compute these data are based on Stoll's papers [123], [124], [125]. The rank of the Jacobian of $\mathcal{C}^+$ is 1, so classical Chabauty's method (see e.g. [38], [39], [46]) can be applied. The `Chabauty` procedure of MAGMA provides an upper bound for the number of rational points on the curve and in this case it is equal to the number of known points. Therefore

$$\mathcal{C}^+(\mathbb{Q}) = \{\infty, (25, \pm 15000)\}.$$

Now we deal with part (b). Let $J(\mathbb{Q})^-$ be the Jacobian of the genus two curve (6.18). Using MAGMA we determine a Mordell-Weil basis which is given by

$$D_1 = (\omega_1, -200\omega_1) + (\overline{\omega}_1, -200\overline{\omega}_1) - 2\infty,$$
$$D_2 = (\omega_2, 120000) + (\overline{\omega}_2, 120000) - 2\infty,$$

where ω_1 is a root of the polynomial $x^2 - 5x + 1500$ and ω_2 is a root of $x^2 + 195x + 13500$.

Let $f = x^2(x+15)^2(x+20) - 180000000$ and α be a root of f. We will choose for coset representatives of $J(\mathbb{Q})^-/2J(\mathbb{Q})^-$ the linear combinations $\sum_{i=1}^{2} n_i D_i$, where $n_i \in \{0, 1\}$. Then

$$x - \alpha = \kappa\xi^2,$$

where $\kappa \in \mathcal{K}$ and $\mathcal{K}$ is constructed as described in Lemma 6.2. We have that $\mathcal{K} = \{1, \alpha^2 - 5\alpha + 1500, \alpha^2 + 195\alpha + 13500, \alpha^4 + 190\alpha^3 + 14025\alpha^2 + 225000\alpha + 20250000\}$. By local arguments it is possible to restrict the set $\mathcal{K}$ further (see e.g. [29], [30]). In our case one can eliminate

$$\alpha^2 - 5\alpha + 1500, \quad \alpha^2 + 195\alpha + 13500$$

by local computations in $\mathbb{Q}_2$ and

$$\alpha^4 + 190\alpha^3 + 14025\alpha^2 + 225000\alpha + 20250000$$

by local computations in $\mathbb{Q}_3$. It remains to deal with the case $\kappa = 1$. We apply Theorem 6.6 to get a large upper bound for $\log|x|$. A MAGMA code were written to obtain the bounds appeared in [36], it can be found at

`http://www.warwick.ac.uk/~maseap/progs/intpoint/bounds.m`. We used the above Magma functions to compute an upper bound corresponding to the case $\kappa = 1$. It turned out to be

$$1.58037 \times 10^{285}.$$

The set of known rational points on the curve (6.18) is $\{\infty\}$. Let W be the image of this set in $J(\mathbb{Q})^-$. Applying the Mordell-Weil implemented by Bruin and Stoll and explained in [36] we obtain that $\jmath(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q})^-$, where

$$B = 2^6 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 19 \cdot 23 \cdot 31 \cdot 41 \cdot \cdot 43 \cdot 47 \cdot 61 \cdot 67 \cdot 79 \cdot 83 \cdot 109 \cdot 113 \cdot 127,$$

that is

$$B = 678957252681082328769065398948800.$$

Now we use an extension of the Mordell-Weil sieve due to Samir Siksek to obtain a very long decreasing sequence of lattices in $\mathbb{Z}^2$. After that we apply Lemma 6.3 to obtain a lower bound for possible unknown rational points. We get that if (x, y) is an unknown integral point, then

$$\log|x| \geq 7.38833 \times 10^{1076}.$$

This contradicts the bound for $\log|x|$ we obtained by Baker's method.

Finally we prove Theorem 6.4.

Proof. [Proof of Theorem 6.4] We will use the following well known property of the sequences F_n and L_n :

$$L_n^2 - 5F_n^2 = 4(-1)^n.$$

We have that

$$\binom{X}{5}^2 \pm 4 = 5F_n^2.$$

The above equation can be reduced to two genus two curves given by (6.17) and (6.18), where $Y = 5^3 5! F_n$ and $X = 5x^2 - 20x$. By Lemma 6.4 we have that $X = 25$ and we also have that $X = 5x^2 - 20x$. That is it remains to solve a quadratic equation in x. We obtain that $x \in \{-1, 5\}$. Hence the only positive solution of equation (6.14) is $(n, x) = (1, 5)$, that is

$$1 = L_1 = \binom{5}{5}.$$

6.5.3 Proof of Theorem 6.5

Proof. In case of equation (6.15) by applying the identity (6.13) we obtain

$$5\binom{X}{5}^2 \pm 4 = L_n^2.$$

Hence we need to compute the integral solutions of the equations

$$C_\delta : \qquad y^2 = x^2(x+15)^2(x+20) + 4 \cdot 5^4 \cdot (5!)^2 \cdot \delta,$$

where $\delta \in \{-1, 1\}$ and $x = 5X^2 - 20X$. That is we deal with genus 2 curves. By using Magma [23] we can determine generators of the Mordell-Weil groups based on Stoll's papers [123], [124], [125]. Let us denote the Jacobians of the curves C_δ by J_δ, where $\delta \in \{-1, 1\}$. We get that J_{-1} is free of rank 2 with Mordell-Weil basis given by (in Mumford representation)

$$d_1 =< x - 25, 3000 >,$$
$$d_2 =< x^2 + 75x + 1500, 600x + 24000 >$$

and J_1 is free of rank 4 with Mordell-Weil basis given by

$$\begin{aligned} D_1 &=< x, 6000 >, \\ D_2 &=< x + 40, 4000 >, \\ D_3 &=< x^2 + 15x, 6000 >, \\ D_4 &=< x^2 + 15x - 1000, 200x + 4000 > . \end{aligned}$$

Baker's method [9] can be applied to get large upper bounds B_δ for $\log |x|$. Using the improvements given in [36] and [56] we obtain that

$$B_{-1} = 2.26 \cdot 10^{493} \text{ and } B_1 = 1.11 \cdot 10^{503}.$$

Every integral point on the curves can be expressed in the forms

$$P - \infty = \sum_{i=1}^{2} m_i d_i \text{ and } P - \infty = \sum_{i=1}^{4} n_i D_i,$$

where m_1, m_2, n_1, n_2, n_3 and n_4 are integers. According to Proposition 6.2 in [56] we compute the period matrix and the hyperelliptic logarithms with 1200 digits of precision in case of both curves. The hyperelliptic logarithms of the divisors d_i are as follows

$$\begin{aligned} \varphi(d_1) &= (-0.018478\ldots + i0.009553\ldots, -0.397546\ldots + i0.372090\ldots) \in \mathbb{C}^2, \\ \varphi(d_2) &= (0.020606\ldots - i0.005882\ldots, -0.861905\ldots + i0.814915\ldots) \in \mathbb{C}^2. \end{aligned}$$

In case of the rank 4 curve we obtain

$$\begin{aligned} \varphi(D_1) &= (-0.020382\ldots + i0.004844\ldots, -1.182385\ldots - i0.446046\ldots) \in \mathbb{C}^2, \\ \varphi(D_2) &= (-0.013432\ldots - i0.004844\ldots, -1.326128\ldots - i0.446046\ldots) \in \mathbb{C}^2, \\ \varphi(D_3) &= (-0.011009\ldots + i0.004844\ldots, -0.854126\ldots - i0.446046\ldots) \in \mathbb{C}^2, \\ \varphi(D_4) &= (-0.007101\ldots - i0.004844\ldots, -1.160439\ldots - i0.446046\ldots) \in \mathbb{C}^2. \end{aligned}$$

Based on Proposition 6.2 in [56] we set $K := 10^{1000}$ for both curves and the reductions yield that

$$||(m_1, m_2)|| \leq 45.65 \quad \text{and} \quad ||(n_1, n_2, n_3, n_4)|| \leq 103.27.$$

Repeat reductions with $K := 10^{20}, 10^{14}, 10^{12}$ provide the following bounds

$$||(m_1, m_2)|| \leq 6.36 \quad \text{and} \quad ||(n_1, n_2, n_3, n_4)|| \leq 13.73.$$

Enumeration of possible linear combinations up to these bounds provide that

$$x \in \{-40, -20, -15, 0, 25, 105, 1425/4\}.$$

It remains to determine the corresponding values of X, these are as follows

$$X \in \{-3, -1, 0, 1, 2, 3, 4, 5, 7\}.$$

Therefore $X = 5, n = 1, 2$ and $X = 7, n = 8$ are the only non-trivial solutions.

dc_1892_21

Bibliography

[1] Aguirre, J., Dujella, A., and Peral, J. C. (2013). Arithmetic progressions and Pellian equations. *Publ. Math. Debrecen*, 83(4):683–695.

[2] Alfred, B. U. (1964). On square Lucas numbers. *Fibonacci Quart.*, 2:11–12.

[3] Allison, D. (1977). On certain simultaneous diophantine equations. *Math. Colloq. Univ. Cape Town*, 11:117–133.

[4] Alvarado, A. (2010). Arithmetic progressions on quartic elliptic curves. *Ann. Math. Inform.*, 37:3–6.

[5] Baer, C. and Rosenberger, G. (1998). The equation $ax^2 + by^2 + cz^2 = dxyz$ over quadratic imaginary fields. *Results Math.*, 33(1-2):30–39.

[6] Baker, A. (1967). Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228.

[7] Baker, A. (1968a). The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$. *J. London Math. Soc.*, 43:1–9.

[8] Baker, A. (1968b). Linear forms in the logarithms of algebraic numbers. IV. *Mathematika*, 15:204–216.

[9] Baker, A. (1969). Bounds for the solutions of the hyperelliptic equation. *Proc. Cambridge Philos. Soc.*, 65:439–444.

[10] Baker, A. and Coates, J. (1970). Integer points on curves of genus 1. *Proc. Cambridge Philos. Soc.*, 67:595–602.

[11] Bauer, M. and Bennett, M. A. (2007). On a question of Erdős and Graham. *Enseign. Math. (2)*, 53(3-4):259–264.

[12] Bazsó, A., Bérczes, A., Győry, K., and Pintér, A. (2010). On the resolution of equations $Ax^n - By^n = C$ in integers x, y and $n \geq 3$. II. *Publ. Math. Debrecen*, 76(1-2):227–250.

[13] Bazsó, A., Bérczes, A., Hajdu, L., and Luca, F. (2018). Polynomial values of sums of products of consecutive integers. *Monatsh. Math.*, 187(1):21–34.

[14] Bennett, M. A., Bruin, N., Győry, K., and Hajdu, L. (2006). Powers from products of consecutive terms in arithmetic progression. *Proc. London Math. Soc. (3)*, 92(2):273–306.

[15] Bennett, M. A., Pink, I., and Rábai, Z. (2013). On the number of solutions of binomial Thue inequalities. *Publ. Math. Debrecen*, 83(1-2):241–256.

[16] Bennett, M. A. and Van Luijk, R. (2012). Squares from blocks of consecutive integers: a problem of Erdős and Graham. *Indag. Math., New Ser.*, 23(1-2):123–127.

[17] Bérczes, A. and Pethő, A. (2004). On norm form equations with solutions forming arithmetic progressions. *Publ. Math. Debrecen*, 65(3-4):281–290.

[18] Bérczes, A. and Pethő, A. (2006). Computational experiences on norm form equations with solutions forming arithmetic progressions. *Glas. Mat. Ser. III*, 41(61)(1):1–8.

[19] Bérczes, A., Pethő, A., and Ziegler, V. (2006). Parameterized norm form equations with arithmetic progressions. *J. Symbolic Comput.*, 41(7):790–810.

[20] Bilu, Y. (1995). Effective analysis of integral points on algebraic curves. *Israel J. Math.*, 90(1-3):235–252.

[21] Bilu, Y. F. and Hanrot, G. (1998). Solving superelliptic Diophantine equations by Baker's method. *Compositio Math.*, 112(3):273–312.

[22] Blokhuis, A., Brouwer, A., and de Weger, B. (2017). Binomial collisions and near collisions. *Integers*, 17:Paper No. A64, 8.

[23] Bosma, W., Cannon, J., and Playoust, C. (1997). The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265. Computational algebra and number theory (London, 1993).

[24] Bosser, V. and Surroca, A. (2013). Upper bounds for the height of S-integral points on elliptic curves. *Ramanujan J.*, 32(1):125–141.

[25] Bremner, A. (1999). On arithmetic progressions on elliptic curves. *Experiment. Math.*, 8(4):409–413.

[26] Bremner, A. (2013). Arithmetic progressions on Edwards curves. *J. Integer Seq.*, 16(8):article 13.8.5, 5.

[27] Bremner, A., Silverman, J. H., and Tzanakis, N. (2000). Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$. *J. Number Theory*, 80(2):187–208.

[28] Brindza, B. (1984). On S-integral solutions of the equation $y^m = f(x)$. *Acta Math. Hungar.*, 44(1-2):133–139.

[29] Bruin, N. and Stoll, M. (2008). Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17(2):181–189.

[30] Bruin, N. and Stoll, M. (2009). Two-cover descent on hyperelliptic curves. *Math. Comp.*, 78(268):2347–2370.

[31] Bruin, N. and Stoll, M. (2010). The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306.

[32] Buchmann, J. and Pethő, A. (1989). Computation of independent units in number fields by Dirichlet's method. *Math. Comp.*, 52(185):149–159, S1–S14.

[33] Bugeaud, Y. (1997). Bounds for the solutions of superelliptic equations. *Compositio Math.*, 107(2):187–219.

[34] Bugeaud, Y. and Győry, K. (1996). Bounds for the solutions of unit equations. *Acta Arith.*, 74(1):67–80.

[35] Bugeaud, Y., Mignotte, M., and Siksek, S. (2006). Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers. *Ann. of Math. (2)*, 163(3):969–1018.

[36] Bugeaud, Y., Mignotte, M., Siksek, S., Stoll, M., and Tengely, S. (2008). Integral points on hyperelliptic curves. *Algebra Number Theory*, 2(8):859–885.

[37] Campbell, G. (2003). A note on arithmetic progressions on elliptic curves. *J. Integer Seq.*, 6(1):Article 03.1.3, 5 pp. (electronic).

[38] Cassels, J. W. S. and Flynn, E. V. (1996). *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge.

[39] Chabauty, C. (1941). Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885.

[40] Choudhry, A. (2015). Arithmetic progressions on Huff curves. *J. Integer Seq.*, 18(5):article 15.5.2, 9.

[41] Ciss, A. A. and Sow, D. (2011). On a new generalization of Huff curves. https://eprint.iacr.org/2011/580.pdf.

[42] Cohn, J. H. E. (1964a). On square Fibonacci numbers. *J. London Math. Soc.*, 39:537–540.

[43] Cohn, J. H. E. (1964b). Square Fibonacci numbers, etc. *Fibonacci Quart.*, 2:109–113.

[44] Cohn, J. H. E. (1965). Lucas and Fibonacci numbers and some Diophantine equations. *Proc. Glasgow Math. Assoc.*, 7:24–28 (1965).

[45] Cohn, J. H. E. (1996). Perfect Pell powers. *Glasgow Math. J.*, 38(1):19–20.

[46] Coleman, R. F. (1985). Effective Chabauty. *Duke Math. J.*, 52(3):765–770.

[47] Darmon, H. and Merel, L. (1997). Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100.

[48] Dickson, L. (1966). *History of the theory of numbers. Vol II: Diophantine analysis*. Chelsea Publishing Co., New York.

[49] Dilcher, K. and Stolarsky, K. B. (2005). Resultants and discriminants of chebyshev and related polynomials. *Trans. Amer. Math. Soc.*, 357:965–981.

[50] Dujella, A., Pethő, A., and Tadić, P. (2008). On arithmetic progressions on Pellian equations. *Acta Math. Hungar.*, 120(1-2):29–38.

[51] Erdős, P. and Graham, R. L. (1980). *Old and new problems and results in combinatorial number theory.* .

[52] Erdős, P. (1939). Note on the product of consecutive integers (II). *J. London Math. Soc.*, 14:245–249.

[53] Erdős, P. and Selfridge, J. L. (1975). The product of consecutive integers is never a power. *Illinois J. Math.*, 19:292–301.

[54] Flynn, E. V. (2004). The Hasse principle and the Brauer-Manin obstruction for curves. *Manuscripta Math.*, 115(4):437–466.

[55] Fujiwara, M. (1916). Über die obere Schranke des absoluten Betrages der Wurzeln einer algebraischen Gleichung. *Tôhoku Math. J.*, 10:167–171.

[56] Gallegos-Ruiz, H. R. (2019). Computing integral points on genus 2 curves estimating hyperelliptic logarithms. *Acta Arith.*, 187(4):329–344.

[57] Gallegos-Ruiz, H. R., Katsipis, N., Tengely, S., and Ulas, M. (2020). On the Diophantine equation $\binom{n}{k} = \binom{m}{l} + d$.

J. Number Theory, 208:418–440.

[58] Gebel, J., Pethő, A., and Zimmer, H. G. (1994). Computing integral points on elliptic curves. *Acta Arith.*, 68(2):171–192.

[59] González-Jiménez, E. (2014). Markoff-Rosenberger triples in geometric progression. *Acta Math. Hungar.*, 142(1):231–243.

[60] González-Jiménez, E. (2015a). Covering techniques and rational points on some genus 5 curves. In *Trends in number theory. Fifth Spanish meeting on number theory, Universidad de Sevilla, Sevilla, Spain, July 8–12, 2013. Proceedings*, pages 89–105. Providence, RI: American Mathematical Society (AMS); Madrid: Real Sociedad Matemática Española (RSME).

[61] González-Jiménez, E. (2015b). On arithmetic progressions on Edwards curves. *Acta Arith.*, 167(2):117–132.

[62] González-Jiménez, E. and Tornero, J. M. (2013). Markoff-Rosenberger triples in arithmetic progression. *J. Symbolic Comput.*, 53:53–63.

[63] González-Jiménez, E. and Xarles, X. (2011). On symmetric square values of quadratic polynomials. *Acta Arith.*, 149(2):145–159.

[64] Grytczuk, A. and Schinzel, A. (1992). On Runge's theorem about Diophantine equations. In *Sets, graphs and numbers (Budapest, 1991)*, volume 60 of *Colloq. Math. Soc. János Bolyai*, pages 329–356. North-Holland, Amsterdam.

[65] Guy, R. K. (1994). *Unsolved problems in number theory*. Problem Books in Mathematics. Springer-Verlag, New York, second edition. Unsolved Problems in Intuitive Mathematics, I.

[66] Győry, K. (1998). On the diophantine equation $n(n+1)\dots(n+k-1) = bx^\ell$. *Acta Arith.*, 83(1):87–92.

[67] Győry, K. and Pintér, A. (2007). On the resolution of equations $Ax^n - By^n = C$ in integers x, y and $n \geq 3$. I. *Publ. Math. Debrecen*, 70(3-4):483–501.

[68] Győry, K., Hajdu, L., and Saradha, N. (2004). On the Diophantine equation $n(n+d)\cdots(n+(k-1)d) = by^l$. *Canad. Math. Bull.*, 47(3):373–388.

[69] Hajdu, L. and Herendi, T. (1998). Explicit bounds for the solutions of elliptic equations with rational coefficients. *J. Symb. Comput.*, 25(3):361–366, art. no. sy970181.

[70] Hajdu, L., Laishram, S., and Tengely, S. (2016). Power values of sums of products of consecutive integers. *Acta Arith.*, 172(4):333–349.

[71] Hajdu, L., Tengely, S., and Tijdeman, R. (2009). Cubes in products of terms in arithmetic progression. *Publ. Math. Debrecen*, 74(1-2):215–232.

[72] Hilliker, D. L. and Straus, E. G. (1983). Determination of bounds for the solutions to those binary Diophantine equations that satisfy the hypotheses of Runge's theorem. *Trans. Amer. Math. Soc.*, 280(2):637–657.

[73] Hirata-Kohno, N., Laishram, S., Shorey, T. N., and Tijdeman, R. (2007). An extension of a theorem of Euler. *Acta Arith.*, 129(1):71–102.

[74] Hopkins, B. and Tangboonduangjit, A. (2018). Fibonacci-producing rational polynomials. *The Fibonacci Quartely*, 56(4):303–312.

[75] Huff, G. B. (1948). Diophantine problems in geometry and elliptic ternary forms. *Duke Math. J.*, 15:443–453.

[76] Kedlaya, K. S. (1998). Solving constrained Pell equations. *Math. Comp.*, 67(222):833–842.

[77] Kovács, T. (2009). Combinatorial numbers in binary recurrences. *Period. Math. Hungar.*, 58(1):83–98.

[78] Laishram, S. and Shorey, T. N. (2007). The equation $n(n+d)\cdots(n+(k-1)d) = by^2$ with $\omega(d) \leq 6$ or $d \leq 10^{10}$. *Acta Arith.*, 129(3):249–305.

[79] Landau, E. (1918). Verallgemeinerung eines Pólyaschen satzes auf algebraische zahlkörper.

[80] Lang, S. (1978). *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York.

[81] Laurent, M. (2008). Linear forms in two logarithms and interpolation determinants. II. *Acta Arith.*, 133(4):325–348.

[82] Ljunggren, W. (1951). On the Diophantine equation $x^2 + 4 = Ay^4$. *Norske Vid. Selsk. Forh., Trondheim*,

24:82–84 (1952).

[83] London, H. and Finkelstein, R. (1970). On Fibonacci and Lucas numbers which are perfect powers. *Fibonacci Quart. 7 (1969), no. 5, 476-481, 487; errata, ibid.*, 8(3):248.

[84] Luca, F. and Srinivasan, A. (2018). Markov equation with Fibonacci components. *Fibonacci Quart.*, 56(2):126–129.

[85] Luca, F. and Walsh, P. (2007). On a diophantine equation related to a conjecture of Erdős and Graham. *Glas. Mat., III. Ser.*, 42(2):281–289.

[86] Luo, M. (1989). On triangular Fibonacci numbers. *Fibonacci Quart.*, 27(2):98–108.

[87] Luo, M. (1991). On triangular Lucas numbers. In *Applications of Fibonacci numbers, Vol. 4 (Winston-Salem, NC, 1990)*, pages 231–240. Kluwer Acad. Publ., Dordrecht.

[88] MacLeod, A. J. (2006). 14-term arithmetic progressions on quartic elliptic curves. *J. Integer Seq.*, 9(1):Article 06.1.2, 4 pp. (electronic).

[89] Markoff, A. (1880). Sur les formes quadratiques binaires indéfinies. *Math. Ann.*, 17(3):379–399.

[90] Matveev, E. M. (2000). An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. *Izv. Ross. Akad. Nauk Ser. Mat.*, 64(6):125–180.

[91] McDaniel, W. L. (1996). Triangular numbers in the Pell sequence. *Fibonacci Quart.*, 34(2):105–107.

[92] Moody, D. (2011a). Arithmetic progressions on Edwards curves. *J. Integer Seq.*, 14(1):Article 11.1.7, 4.

[93] Moody, D. (2011b). Arithmetic progressions on Huff curves. *Ann. Math. Inform.*, 38:111–116.

[94] Nemes, I. and Pethő, A. (1986). Polynomial values in linear recurrences. II. *J. Number Theory*, 24(1):47–53.

[95] Obláth, R. (1950). Über das Produkt fünf aufeinander folgender Zahlen in einer arithmetischen Reihe. *Publ. Math. Debrecen*, 1:222–226.

[96] Pethő, A. (2010). Fifteen problems in number theory. *Acta Univ. Sapientiae Math.*, 2(1):72–83.

[97] Pethő, A. (1983). Full cubes in the Fibonacci sequence. *Publ. Math. Debrecen*, 30(1-2):117–127.

[98] Pethő, A. (1984). Perfect powers in second order recurrences. In *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, volume 34 of *Colloq. Math. Soc. János Bolyai*, pages 1217–1227. North-Holland, Amsterdam.

[99] Pethő, A. (1992). The Pell sequence contains only trivial perfect powers. In *Sets, graphs and numbers (Budapest, 1991)*, volume 60 of *Colloq. Math. Soc. János Bolyai*, pages 561–568. North-Holland, Amsterdam.

[100] Pethő, A. and de Weger, B. M. M. (1986). Products of prime powers in binary recurrence sequences. I. The hyperbolic case, with an application to the generalized Ramanujan-Nagell equation. *Math. Comp.*, 47(176):713–727.

[101] Pethő, A. and Ziegler, V. (2008). Arithmetic progressions on Pell equations. *J. Number Theory*, 128(6):1389–1409.

[102] Pohst, M. and Zassenhaus, H. (1989). *Algorithmic Algebraic Number Theory*. Cambridge University Press, Cambridge.

[103] Poulakis, D. (1991). Solutions entières de l'équation $Y^m = f(X)$. *Sém. Théor. Nombres Bordeaux (2)*, 3(1):187–199.

[104] Poulakis, D. (1999). A simple method for solving the Diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$. *Elem. Math.*, 54(1):32–36.

[105] Rigge, O. (Helsingfors 1938). Über ein diophantisches problem. In *9th Congress Math. Scand.*, pages 155–160. Mercator 1939.

[106] Rosenberger, G. (1979). Über die diophantische Gleichung $ax^2 + by^2 + cz^2 = dxyz$. *J. Reine Angew. Math.*, 305:122–125.

[107] Runge, C. (1887). Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen. *J. Reine Angew. Math.*, 100:425–435.

[108] Sankaranarayanan, A. and Saradha, N. (2008). Estimates for the solutions of certain Diophantine equations by Runge's method. *Int. J. Number Theory*, 4(3):475–493.

[109] Saradha, N. (1997). On perfect powers in products with terms from arithmetic progressions. *Acta Arith.*,

82(2):147–172.

[110] Saradha, N. and Shorey, T. N. (2003). Almost squares in arithmetic progression. *Compositio Math.*, 138(1):73–111.

[111] Scharaschkin, V. (1999). *Local-global problems and the Brauer-Manin obstruction*. PhD thesis, University of Michigan.

[112] Schinzel, A. (1969). An improvement of Runge's theorem on Diophantine equations. *Comment. Pontificia Acad. Sci.*, 2(20):1–9.

[113] Schinzel, A. and Tijdeman, R. (1976). On the equation $y^m = P(x)$. *Acta Arith.*, 31(2):199–204.

[114] Schmidt, W. M. (1992). Integer points on curves of genus 1. *Compositio Math.*, 81(1):33–59.

[115] Sendra, J. R., Winkler, F., and Pérez-Díaz, S. (2008). *Rational Algebraic Curves, A Computer Algebra Approach*. Algorihms and Computation in Mathematics, Volume 22. Springer-Verlag Berlin Heidelberg.

[116] Siegel, C. L. (1926). The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \ldots + k$. *J. Lond. Math. Soc.*, 1:66–68.

[117] Siegel, C. L. (1929). Über einige Anwendungen diophantischer Approximationen. *Abh. Pr. Akad. Wiss.*, 1:41–69.

[118] Silverman, J. H. (1990). The Markoff equation $X^2 + Y^2 + Z^2 = aXYZ$ over quadratic imaginary fields. *J. Number Theory*, 35(1):72–104.

[119] Skałba, M. (2003). Products of disjoint blocks of consecutive integers which are powers. *Colloq. Math.*, 98(1):1–3.

[120] Smart, N. P. (1998). *The algorithmic resolution of Diophantine equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge.

[121] Sprindžuk, V. G. (1977). The arithmetic structure of integer polynomials and class numbers. *Trudy Mat. Inst. Steklov.*, 143:152–174, 210. Analytic number theory, mathematical analysis and their applications (dedicated to I. M. Vinogradov on his 85th birthday).

[122] Stein, W. et al. (2020). *Sage Mathematics Software, version* `9.1`. The Sage Development Team. `http://www.sagemath.org`.

[123] Stoll, M. (1999). On the height constant for curves of genus two. *Acta Arith.*, 90(2):183–201.

[124] Stoll, M. (2001). Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277.

[125] Stoll, M. (2002). On the height constant for curves of genus two. II. *Acta Arith.*, 104(2):165–182.

[126] Stroeker, R. J. and Tzanakis, N. (1994). Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arith.*, 67(2):177–196.

[127] Stroeker, R. J. and Tzanakis, N. (2000). Computing all integer solutions of a general elliptic equation. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 551–561. Springer, Berlin.

[128] Stroeker, R. J. and Tzanakis, N. (2003). Computing all integer solutions of a genus 1 equation. *Math. Comp.*, 72(244):1917–1933.

[129] Szalay, L. (2001). Some polynomial values in binary recurrences. *Rev. Colombiana Mat.*, 35(2):99–106.

[130] Szalay, L. (2002). On the resolution of the equations $U_n = \binom{x}{3}$ and $V_n = \binom{x}{3}$. *Fibonacci Quart.*, 40(1):9–12.

[131] Tengely, S. (2003). On the Diophantine equation $F(x) = G(y)$. *Acta Arith.*, 110(2):185–200.

[132] Tengely, S. (2004). On the Diophantine equation $x^2 + a^2 = 2y^p$. *Indag. Math. (N.S.)*, 15(2):291–304.

[133] Tengely, S. (2008/09). Finding g-gonal numbers in recurrence sequences. *Fibonacci Quart.*, 46/47(3):235–240.

[134] Tengely, S. (2011). On the Diophantine equation $L_n = \binom{x}{5}$. *Publ. Math. Debrecen*, 79(3-4):749–758.

[135] Tengely, S. (2013). Balancing numbers which are products of consecutive integers. *Publ. Math. Debrecen*, 83(1-2):197–205.

[136] Tijdeman, R. (1976). Applications of the Gel′fond-Baker method to rational number theory. In *Topics in number theory (Proc. Colloq., Debrecen, 1974)*, pages 399–416. Colloq. Math. Soc. János Bolyai, Vol. 13.

[137] Tzanakis, N. (1996). Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms.

The case of quartic equations. *Acta Arith.*, 75(2):165–190.

[138] Tzanakis, N. (2002). Effective solution of two simultaneous Pell equations by the elliptic logarithm method. *Acta Arith.*, 103(2):119–135.

[139] Tzanakis, N. (2013). *Elliptic Diophantine equations. A concrete approach via the elliptic logarithm.* Berlin: de Gruyter.

[140] Ulas, M. (2005a). A note on arithmetic progressions on quartic elliptic curves. *J. Integer Seq.*, 8(3):Article 05.3.1, 5 pp. (electronic).

[141] Ulas, M. (2005b). On products of disjoint blocks of consecutive integers. *Enseign. Math. (2)*, 51(3-4):331–334.

[142] Ulas, M. (2009). A note on Sierpiński's question related to triangular numbers. *Coll. Math.*, 117(2):165–173.

[143] Voutier, P. (1996). An effective lower bound for the height of algebraic numbers. *Acta Arith.*, 74(1):81–95.

[144] Voutier, P. M. (1995). An upper bound for the size of integral solutions to $Y^m = f(X)$. *J. Number Theory*, 53(2):247–271.

[145] Walsh, P. G. (1992). A quantitative version of Runge's theorem on Diophantine equations. *Acta Arith.*, 62(2):157–172.

[146] Wu, H. and Feng, R. (2012). Elliptic curves in Huff's model. *Wuhan Univ. J. Nat. Sci.*, 17(6):473–480.

[147] Wyler, O. (1964). In the Fibonacci series $F_1 = 1, F_2 = 1, F_{n+1} = F_n + F_{n-1}$ the first, second and twelfth terms are squares. *Amer. Math. Monthly*, 71:221–222.

[148] Zhang, Y. and Cai, T. (2015). On products of consecutive arithmetic progressions. *Journal of Number Theory*, 147(0):287 – 299.