ISSN 2220-5438

Moscow Journal of Combinatorics and Number Theory

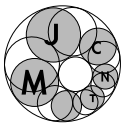
URSS

МФТИ

Volume 6 • Issue 2–3 2016

Moscow Journal of Combinatorics and Number Theory Volume 6 • Issue 2–3 2016 URSS

Moscow Journal
of Combinatorics
and Number Theory
2016, vol. 6, iss. 2–3,
pp. 38–55, [pp. 154–171]



Continuant Diophantine equations

Dzmitry Badziahin (Durham)

Abstract: We investigate a family of Diophantine polynomial equations which involve continuant functions. in particular, given a polynomial $P(x) \in \mathbb{Z}[x]$ and $n \in \mathbb{N}$, we consider the equation $P(K_n(x_1, \dots, x_n)) = K_{n+1}(x_0, \dots, x_n)K_{n+1}(x_1, \dots, x_{n+1})$. We show that with certain restrictions on $P(x)$ the set of its solutions has a rich structure. in particular, we provide several ways of generating new solutions from the existing ones.
in the last section we discuss the relation between the solutions of the above Diophantine equation for arbitrary values of n and factorisations $P(m) = d_1 d_2$ for integers m, d_1 and d_2.

Keywords: continuant, continuant Diophantine equation, integer factorisation

AMS Subject Classification: 11D72

Received: 20.05.2016

1. Introduction

We start by introducing the generalised continuants $K_n^{(t)}$. Given $t \in \mathbb{Z}\setminus\{0\}$, let $K_n^{(t)}$ be a polynomial of n variables which is defined by the recurrent formula

$$K_0^{(t)}() := 1; \quad K_1^{(t)}(x_1) := x_1;$$
$$K_{n+1}^{(t)}(x_1, \dots, x_{n+1}) = x_{n+1}K_n^{(t)}(x_1, \dots, x_n) + tK_{n-1}^{(t)}(x_1, \dots, x_{n-1}). \qquad (1)$$

To make the notation shorter, we denote

$$\mathbf{x}_{m,n} := (x_m, x_{m+1}, \dots, x_n), \quad m \leqslant n+1$$

and

$$\bar{\mathbf{x}}_{m,n} := (x_n, x_{n-1}, \ldots, x_m), \quad m \leqslant n+1.$$

For $t = 1$ the polynomial $K_n^{(t)}(\mathbf{x}_{1,n})$ is the standard continuant $K_n(\mathbf{x}_{1,n})$ which plays an important role in the theory of continued fractions. Indeed, a finite continued fraction $[a_0; a_1, \ldots, a_n]$ is a rational number which enumerator and denominator are $K_{n+1}(\mathbf{a}_{0,n})$ and $K_n(\mathbf{a}_{1,n})$ respectively. We refer the reader to [3, Chapter X] for details.

Fix $n \in \mathbb{N}$, $n \geqslant 2$ and $t \in \mathbb{Z}\backslash\{0\}$. Let $P(x) = c_0 + c_1 x + \ldots + c_d x^d$ be a polynomial with integer coefficients such that

$$c_0 = (-t)^n \quad \text{and} \quad x^d P((-t)^{n-1} x^{-1}) = C \cdot P(x), \tag{2}$$

where C is some non-zero constant. One can easily check that monic symmetric and antisymmetric polynomials are covered by this property. Indeed, for those polynomials the condition (2) is satisfied with $t = -1$. Many such polynomials also satisfy (2) with $t = 1$ and either an even or an odd value of n.

The central Diophantine equation of this paper is

$$P(K_{n-1}^{(t)}(\mathbf{x}_{1,n-1})) = K_n^{(t)}(\mathbf{x}_{0,n-1}) K_n^{(t)}(\mathbf{x}_{1,n}). \tag{3}$$

Since $\deg(P)$ can be arbitrarily high, so can be the degree of this equation. Despite this, we will show that it usually has infinitely many solutions and moreover the set of solutions has quite an interesting structure. In Section 3 we show that for $t = \pm 1$ every solution $\mathbf{x}_{0,n}$ of (3) generates a sequence $\mathcal{S} = \ldots, x_{-1}, x_0, \ldots, x_n, \ldots$ of integers such that any tuple $\mathbf{x}_{m,m+n}$ is also a solution of (3). In Section 4 we provide a different way of constructing infinitely many solutions $\mathbf{x}$ of the equation (3). We do it by noticing that $K_n^{(t)}(\mathbf{x}_{0,n-1}) = \pm 1$ implies that there exists $x_n \in \mathbb{Z}$ such that $\mathbf{x}_{0,n}$ is a solution of (3). We believe that in many cases different solutions $\mathbf{x}_{0,n}$ achieved in this way generate different sequences $\mathcal{S}$. We do not prove this statement formally, however we can see this in examples considered in the paper. Next, in Section 5 we show that, base on a solution of (3) for a particular value of n, we can construct new solutions of the equation for the same polynomial $P(x)$ and bigger values of n. That gives us the third method of generating solutions of (3). In the last section we notice the relation between the factorisations $P(m) = d_1 d_2$ for integer values of m, d_1, d_2 and the solutions of (3) where $t = 1$, $P(x)$ is fixed and n may

vary. At the end, by considering factorisations of the polynomial m^4+1 for small integer values m we conclude that in general the three methods for generating new solutions of (3) described above are still not sufficient to provide all solutions of this equation. Therefore the problem of classifying all the solutions of (3) still waits for its discoverer.

To the best of authors knowledge, equations of the form (3) are mostly uncovered in the literature. We can only refer to a paper [1] where the case $n=2$ and some particular types of the polynomials $P(x)$ were considered. On the other hand, continuants play an important role in the solutions of some Diophantine equations. The most classical example is Pell's equation $x^2-dy^2=\pm 1$ where d is not a perfect square. It is well known that all its solutions (x,y) are $(K_{kn}(\mathbf{a}_{0,kn-1}), K_{kn-1}(\mathbf{a}_{1,kn-1}))$, where $[a_0; a_1, a_2, \ldots]$ is a continued fraction of $\sqrt{d}$, n is the length of its period and k is any positive integer. We refer to [2, Section IV.11] for details. Also Schinzel recently used continuants to find all solutions of the equation $x^2+x+1=yz$ [4].

2. Properties of generalised continuants

Continuants naturally arise from the following matrix identity which can easily be checked from the recurrent formula (1):

$$\begin{pmatrix} 0 & t \\ 1 & x_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & t \\ 1 & x_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & t \\ 1 & x_n \end{pmatrix} = \begin{pmatrix} tK^{(t)}_{n-2}(\mathbf{x}_{2,n-1}) & tK^{(t)}_{n-1}(\mathbf{x}_{2,n}) \\ K^{(t)}_{n-1}(\mathbf{x}_{1,n-1}) & K^{(t)}_{n}(\mathbf{x}_{1,n}) \end{pmatrix}.$$

It in turn provides the following properties of continuants which we will use later.

$$K^{(t)}_n(\mathbf{x}_{1,n})K^{(t)}_{n-2}(\mathbf{x}_{2,n-1}) - K^{(t)}_{n-1}(\mathbf{x}_{1,n-1})K^{(t)}_{n-1}(\mathbf{x}_{2,n}) = (-1)^n t^{n-1}. \tag{4}$$

$$\begin{aligned} K^{(t)}_{n+1}(\mathbf{x}_{1,n+1}) &= x_n K^{(t)}_n(\mathbf{x}_{1,n}) + tK^{(t)}_{n-1}(\mathbf{x}_{1,n-1}) \\ &= x_1 K^{(t)}_n(\mathbf{x}_{2,n+1}) + tK^{(t)}_{n-1}(\mathbf{x}_{3,n+1}). \end{aligned} \tag{5}$$

$$K^{(t)}_n(\mathbf{x}_{1,n}) = K^{(t)}_n(\overline{\mathbf{x}}_{1,n}). \tag{6}$$

The first two properties are trivial: (4) can be derived by considering the determinant of both hand sides and (5) is an application of the standard induction. To check (6)

one notices that

$$\begin{pmatrix} 0 & t \\ 1 & x_1 \end{pmatrix}^T = \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 0 & t \\ 1 & x_1 \end{pmatrix} \cdot \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}.$$

Then, by transposing the both sides of the matrix equation, multiplying by $\operatorname{diag}(t, 1)$ from the left and by $\operatorname{diag}(t, 1)^{-1}$ from the right we get

$$\begin{pmatrix} 0 & t \\ 1 & x_n \end{pmatrix} \cdot \begin{pmatrix} 0 & t \\ 1 & x_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & t \\ 1 & x_1 \end{pmatrix} = \begin{pmatrix} tK^{(t)}_{n-2}(\mathbf{x}_{2,n-1}) & tK^{(t)}_{n-1}(\mathbf{x}_{1,n-1}) \\ K^{(t)}_{n-1}(\mathbf{x}_{2,n}) & K^{(t)}_{n}(\mathbf{x}_{1,n}) \end{pmatrix}.$$

Now property (6) follows straightforwardly.

In the end of this section we provide another property of generalised continuants. From (5) we can derive that

$$K^{(t)}_n(\mathbf{x}_{1,n}) = K^{(t)}_{n+1}(1, x_1 - t, \mathbf{x}_{2,n}) = K^{(t)}_{n+2}(\mathbf{x}_{1,n-1}, x_n - t, 1). \tag{7}$$

3. Sequences of equation (3) solutions

Property (6) already reveals some symmetry of the solutions of (3): if $\mathbf{x}_{0,n}$ solves it then so does its "inverse" $\overline{\mathbf{x}}_{0,n}$. However one can say much more about their structure. The next theorem, which is one of the main results of this paper, says that every solution of (3) generates a chain of solutions.

THEOREM 1. *Let $P(x)$ be a polynomial with integer coefficients, which satisfies* (2). *Assume that $\mathbf{x}_{0,n} \in \mathbb{Z}^{n+1}$ is an integer solution of the equation* (3) *such that each term $x_0, \ldots, x_n$ is coprime with t. Then there exists $x_{n+1} \in \mathbb{Z}$ and $x_{-1} \in \mathbb{Z}$ such that $\mathbf{x}_{1,n+1}$ and $\mathbf{x}_{-1,n-1}$ are also solutions of* (3).

Moreover the value x_{n+1} (respectively x_{-1}) is uniquely defined by $\mathbf{x}_{0,n}$ unless $K^{(t)}_{n-1}(\mathbf{x}_{2,n}) = 0$ (respectively $K^{(t)}_{n-1}(\mathbf{x}_{0,n-2}) = 0$). In the latter case, $\mathbf{x}_{1,n+1}$ is a solution of (3) *for any integer x_{n+1}.*

PROOF. Firstly note that coprimeness conditions and recurrent formula (1) imply that for any $m, k \in \mathbb{Z}_{\geqslant 0}$ such that $0 \leqslant m \leqslant n-k+1$ the values $K^{(t)}_k(\mathbf{x}_{m,m+k-1})$ are coprime with t. Moreover, (4) implies that $K^{(t)}_{n-1}(\mathbf{x}_{2,n})$ and $K^{(t)}_n(\mathbf{x}_{1,n})$ are coprime.

Assume that $K_{n-1}^{(t)}(\mathbf{x}_{2,n}) \neq 0$. Then we can apply (4) to get

$$K_{n-1}^{(t)}(\mathbf{x}_{1,n-1}) \equiv (-t)^{n-1}(K_{n-1}^{(t)}(\mathbf{x}_{2,n}))^{-1} \pmod{K_n^{(t)}(\mathbf{x}_{1,n})}.$$

Substituting this into the equation (3) gives us

$$0 \equiv P(K_{n-1}^{(t)}(\mathbf{x}_{1,n-1})) \equiv P((-t)^{n-1}(K_{n-1}^{(t)}(\mathbf{x}_{2,n}))^{-1}) \overset{(2)}{\equiv}$$
$$\equiv P(K_{n-1}^{(t)}(\mathbf{x}_{2,n})) \pmod{K_n^{(t)}(\mathbf{x}_{1,n})}.$$

Therefore there is an integer T such that

$$P(K_{n-1}^{(t)}(\mathbf{x}_{2,n})) = T \cdot K_n^{(t)}(\mathbf{x}_{1,n}). \tag{8}$$

Look at equation (8) modulo $K_{n-1}^{(t)}(\mathbf{x}_{2,n})$ (recall that $K_{n-1}^{(t)}(\mathbf{x}_{2,n}) \neq 0$). by the first property in (2) the left hand side of (8) is congruent to $(-t)^n$. On the other hand, (5) implies that its right hand side is congruent to $tT \cdot K_{n-2}^{(t)}(\mathbf{x}_{3,n})$. Hence we have the following congruence

$$T \cdot K_{n-2}^{(t)}(\mathbf{x}_{3,n}) \equiv (-t)^{n-2} \cdot t \pmod{K_{n-1}^{(t)}(\mathbf{x}_{2,n})}.$$

Aditionally, (4) implies that

$$K_{n-2}^{(t)}(\mathbf{x}_{2,n-1})K_{n-2}^{(t)}(\mathbf{x}_{3,n}) \equiv (-t)^{n-2} \pmod{K_{n-1}^{(t)}(\mathbf{x}_{2,n})}.$$

by comparing the last two congruences and by cancelling $K_{n-2}^{(t)}(\mathbf{x}_{3,n})$ we get $T \equiv tK_{n-2}^{(t)}(\mathbf{x}_{2,n-1}) \pmod{K_{n-1}^{(t)}(\mathbf{x}_{2,n})}$ and therefore there exists $x_{n+1} \in \mathbb{Z}$ such that

$$T = x_{n+1}K_{n-1}^{(t)}(\mathbf{x}_{2,n}) + tK_{n-2}^{(t)}(\mathbf{x}_{2,n-1}) \quad \text{or}$$

$$T = K_n^{(t)}(\mathbf{x}_{2,n+1}). \tag{9}$$

Note that, since $K_{n-1}^{(t)}(\mathbf{x}_{2,n}) \neq 0$, x_{n+1} is defined uniquely (as a solution of linear equation).

Now suppose the contrary, $K_{n-1}^{(t)}(\mathbf{x}_{2,n}) = 0$. Then the value $K_n^{(t)}(\mathbf{x}_{1,n})$ equals either 1 or -1 because otherwise it is not coprime with $K_{n-1}^{(t)}(\mathbf{x}_{2,n}) = 0$. This fact implies (8) for some $T \in \mathbb{Z}$ because ± 1 divides every integer number.

By the first property in (2) the left hand side of (8) equals $(-t)^n$. On the other hand by (5) the right hand side equals $tT \cdot K_{n-2}^{(t)}(\mathbf{x}_{3,n})$. Property (4) implies that $K_{n-2}^{(t)}(\mathbf{x}_{2,n-1})K_{n-2}^{(t)}(\mathbf{x}_{3,n}) = (-t)^{n-2}$. Finally we get $T = tK_{n-2}^{(t)}(\mathbf{x}_{2,n-1})$. Since $K_{n-1}^{(t)}(\mathbf{x}_{2,n}) = 0$, the equation (9) is satisfied for any integer x_{n+1}.

To conclude, we have shown that for any integer solution $\mathbf{x}_{0,n}$ of (3) there exists $x_{n+1} \in \mathbb{Z}$ such that $\mathbf{x}_{1,n+1}$ is also a solution of (3). Analogous arguments allow us to find $x_{-1} \in \mathbb{Z}$ such that $\mathbf{x}_{-1,n-1}$ is a solution of (3). □

Note that from Theorem 1 we can extract the formula for x_{n+1}:

$$x_{n+1} = \frac{P(K_{n-1}^{(t)}(\mathbf{x}_{2,n})) - tK_{n-2}^{(t)}(\mathbf{x}_{2,n-1})K_n^{(t)}(\mathbf{x}_{1,n})}{K_{n-1}^{(t)}(\mathbf{x}_{2,n})K_n^{(t)}(\mathbf{x}_{1,n})}. \tag{10}$$

If $K_{n-1}^{(t)}(\mathbf{x}_{2,n}) = 0$ then any x_{n+1} gives a solution of (3). Finally if $K_n^{(t)}(\mathbf{x}_{1,n}) = 0$ then we necessarily have $P(K_{n-1}^{(t)}(\mathbf{x}_{2,n})) = 0$ and

$$x_{n+1} = -\frac{tK_{n-2}^{(t)}(\mathbf{x}_{2,n-1})}{K_{n-1}^{(t)}(\mathbf{x}_{2,n})}.$$

We can slightly modify Theorem 1 to show that the solution $\mathbf{x}_{0,n}$ is usually uniquely determined by its n first elements. In fact, we can prove

THEOREM 2. *Let $\mathbf{x}_{0,n-1}$ be an integer n-tuple such that all its terms are coprime with t. If the value $K_n^{(t)}(\mathbf{x}_{0,n-1})$ divides $P(K_{n-1}^{(t)}(\mathbf{x}_{1,n-1}))$ then there exists $x_n \in \mathbb{Z}$ such that $\mathbf{x}_{0,n}$ is a solution of (3). Moreover, this value is unique, provided that $K_{n-1}^{(t)}(\mathbf{x}_{1,n-1}) \neq 0$.*

PROOF. We have that there exists an integer T such that

$$P(K_{n-1}^{(t)}(\mathbf{x}_{1,n-1})) = T \cdot K_n^{(t)}(\mathbf{x}_{0,n-1}).$$

Then we repeat the arguments of Theorem 1 starting from (8) with $\mathbf{x}_{0,n-1}$ in place of $\mathbf{x}_{1,n}$. □

As before we can compute the value of x_n from Theorem 2. In this case it can be computed by formula (10) with all the scripts of x's shifted by one unit left.

Note that in both Theorems we assumed that all elements of $\mathbf{x}_{0,n}$ (respectively of $\mathbf{x}_{0,n-1}$ in Theorem 2) are coprime with t. Unfortunately, we can not guarantee

the same property for x_{-1} and x_{n+1} (respectively for x_n). However in two cases, $t = \pm 1$, the coprimality conditions for $\mathbf{x}_{0,n}$ become trivial and can be removed. For convenience, in further discussion we will always set t to one of these two values.

Theorem 1 shows that any solution $\mathbf{x}_{0,n}$ of the equation (3) comes with the sequence $\mathcal{S}$

$$\dots, x_{-2}, x_{-1}, x_0, \dots, x_n, x_{n+1}, \dots$$

of integer numbers such that any its $n+1$ consecutive elements form a solution of (3). It can be finite or infinite from either side. It terminates at the position m from the right if it encounters $K_{n-1}^{(t)}(\mathbf{x}_{m-n+2,m}) = 0$. The same is for the left side of the sequence: it terminates at the position m if $K_{n-1}^{(t)}(\mathbf{x}_{m,m+n-2}) = 0$. Furthermore, if $\mathbf{x}_{0,n-1}$ is not the utmost n-tuple of $\mathcal{S}$ then this sequence is uniquely defined by $\mathbf{x}_{0,n-1}$. We denote the set of all $(n+1)$-tuples of consecutive numbers from $\mathcal{S}$ by $\mathcal{L}(\mathbf{x}_{0,n})$ and call it *a chain*. As we will see later, in many cases chains $\mathcal{L}(\mathbf{x}_{0,n})$ are infinite and provide an infinite set of different solutions of (3). If $K_{n-1}^{(t)}(\mathbf{x}_{1,n-1}) \neq 0$ we will also use the notation $\mathcal{L}(\mathbf{x}_{0,n-1})$ for the chain $\mathcal{L}(\mathbf{x}_{0,n})$ to emphasize that it is uniquely defined by $\mathbf{x}_{0,n-1}$.

As we mentioned before, Property (6) suggests that the set of solutions of (3) is closed under inverting the terms in $(n+1)$-tuples $\mathbf{x}_{0,n}$. Moreover, careful investigation of the formula (10) shows that the chain $\mathcal{L}(\overline{\mathbf{x}}_{0,n})$ consists of all inverted $(n+1)$-tuples from $\mathcal{L}(\mathbf{x}_{0,n})$. We denote such a chain by $\overline{\mathcal{L}}(\mathbf{x}_{0,n})$, i. e.

$$\overline{\mathcal{L}}(\mathbf{x}_{0,n}) := \mathcal{L}(\overline{\mathbf{x}}_{0,n}).$$

It is quite straightforward to check that if $\mathbf{x} \in \mathcal{L}(\mathbf{x}_{0,n-1})$ then $\mathcal{L}(\mathbf{x}) = \mathcal{L}(\mathbf{x}_{0,n-1})$. In other words the sequences $\mathcal{L}(\mathbf{x}_{0,n-1})$ define the equivalence classes for the roots of (3): $\mathbf{x}$ is equivalent to $\mathbf{y}$ if $\mathcal{L}(\mathbf{x}) = \mathcal{L}(\mathbf{y})$.

We finish this section by the natural question:

PROBLEM A. Given $n \in \mathbb{N}$, $t = \pm 1$ and a polynomial $P(x)$ which satisfies (2), classify all chains $\mathcal{L}(\mathbf{x}_{0,n-1})$ of solutions of (3).

In general this problem seems to be very difficult. The case $n = 2$ and $t = 1$ is considered in [1], where the complete classification of chains $\mathcal{L}(x_0, x_1)$ such that $x_0, x_1 \in \mathbb{Z}_{\geqslant 0}$ for polynomials P of degree four is provided. For certain polynomials of higher degrees [1] gives only a partial classification of chains. We will present the result for the polynomial $P(x) = x^4 + 1$ from that paper at the end of the next section.

4. Equation $K_n^{(t)}(x_1, \ldots, x_n) = 1$

Recall that now we only consider the cases $t = \pm 1$. Additionally, from now on we assume that the polynomial $P(x)$ is fixed and so is the equation (3). Therefore, whenever we mention the chain $\mathcal{L}(\mathbf{x})$, we mean the chain of solutions of that fixed equation.

Note that if $K_n^{(t)}(\mathbf{x}_{0,n-1}) = 1$ then the conditions of Theorem 2 are definitely satisfied. This fact allows us to construct many chains $\mathcal{L}(\mathbf{x}_{0,n-1})$. Indeed, it is not difficult to check that the equation $K_n^{(t)}(\mathbf{x}_{0,n-1}) = 1$ has infinitely many solutions for all $n \geqslant 2$ if $t = 1$ and for all $n \geqslant 3$ if $t = -1$. For example, the value $K_2^{(1)}(x_1, x_2) = x_1x_2 + 1$ equals one if and only if one of the terms x_1 or x_2 equals zero. Therefore we have an infinite collection of chains $\mathcal{L}(0, x_2)$ where x_2 is arbitrary. In general, any solution of $K_n^{(t)}(x_1, \ldots, x_n) = 1$ gives a chain $\mathcal{L}(\mathbf{x}_{1,n})$. Therefore the classification of all solutions $K_n^{(t)}(\mathbf{x}_{1,n}) = 1$ gives a family of chains $\mathcal{L}(\mathbf{x}_{1,n})$. Unfortunately, as we will see in Section 6 in the general case this family does not give us a full classification of equation (3) solutions.

Lets firstly concentrate on the case $t = 1$. A complete family of solutions of Diophantine equations $K_n(x_1, \ldots, x_n) = 1$ for small values n can be found with relatively standard elementary methods. A quick search of the literature did not reveal any research on the equations of this type. Therefore here we briefly consider these equations for $n = 2$, 3 and 4 to explain general ideas behind their solutions.

Because of the Property (6) we can restrict our search of the solutions to the case $(x_1, \ldots, x_n) \leqslant_l (x_n, x_{n-1}, \ldots, x_1)$ where by $\leqslant_l$ we mean being smaller or equal in the lexicographical order.

The case $n = 2$ is straightforward:

PROPOSITION 1. *The solutions of*

$$K_2(x_1, x_2) = 1$$

consist of one-parametric series $(0, a)$, $a \in \mathbb{Z}$ *together with its inverse* $(a, 0)$.

For higher values of n the number of different families of solutions grows quickly. However we still have a finite amount of them.

PROPOSITION 2. *The equation*

$$K_3(x_1, x_2, x_3) = 1$$

has

- *three one-parameter series of solutions* $(0, a, 1), (a, 0, 1-a), (1, -1, a),\ a \in \mathbb{Z}$ *together with their inverses and*
- *three extra solutions* $(-3, 1, -2), (-1, 3, -1), (-2, 2, -1)$ *together with their inverses.*

PROOF. The equation can be rewritten as follows

$$x_1x_2x_3 + x_1 + x_3 = 1.$$

Notice that at least one of the three values $|x_1|, |x_2|$ and $|x_3|$ must be less than two. Indeed, otherwise we have that $|x_1|, |x_3|$ are at most a quarter of $|x_1x_2x_3|$ and $1 \leqslant 1/8|x_1x_2x_3|$. Therefore

$$|x_1x_2x_3| > |x_1| + |x_3| + 1$$

which contradicts the equation.

Then we consider several cases.

- $x_1 = 0$. This gives a series of the solutions $(0, a, 1),\ a \in \mathbb{Z}$.
- $x_2 = 0$ gives solutions $(a, 0, 1-a),\ a \in \mathbb{Z}$.
- $x_3 = 0$ gives solutions $(1, a, 0),\ a \in \mathbb{Z}$.
- $x_1 = 1$ gives the equation $x_3(x_2 + 1) = 0$. The case $x_3 = 0$ has already been considered therefore $x_2 = -1$ which gives solutions $(1, -1, a),\ a \in \mathbb{Z}$.
- $x_2 = 1$ gives the equation $x_1x_3 + x_1 + x_3 = 1$. After rewriting it as $(x_1+1)(x_3+1) = 2$ and by taking all possible factorisations of 2 we get new solutions $(-2, 1, -3)$ and $(-3, 1, -2)$.
- $x_3 = 1$ gives solutions $(a, -1, 1),\ a \in \mathbb{Z}$.
- $x_1 = -1$ gives the equation $x_3(1 - x_2) = 2$. by taking all possible factorisations of 2 we get extra solutions $(-1, 3, -1)$ and $(-1, 2, -2)$.
- $x_2 = -1$ gives the equation $(x_1 - 1)(x_3 - 1) = 0$ with no new solutions.
- $x_3 = -1$ gives one more additional solution $(-2, 2, -1)$.

□

In the equation $K_4(\mathbf{x}_{1,4}) = 1$ for $n = 4$ we can also prove that at least one of the variables $|x_1|, \ldots, |x_4|$ is less than two. Then it again suffices to consider the finite amount of cases. Here we only provide the classification of the solutions of $K_4(\mathbf{x}_{1,4}) = 1$ and leave the rigorous proof to the interested reader.

THEOREM 3. *In total, the equation* $K_4(x_1, x_2, x_3, x_4) = 1$ *has*

- *three two-parameter series of solutions* $(0, a, b, 0), (0, a, 0, b), (a, 0, -a, b)$, $a, b \in \mathbb{Z}$ *together with their inverses*;
- *three one-parameter series of solutions* $(1, a, -1, 1), (-1, a, 1, -1), (a, -1, 1, a)$ *together with their inverses*;
- 15 *isolated solutions* $(-4, 1, -2, 2)$, $(-3, 1, -3, 1)$, $(-3, 1, -2, 3)$, $(-3, 2, -1, 3)$, $(-2, 1, -4, 1)$,$(-2, 1, -3, 2)$, $(-2, 2, -2, 1)$, $(-2, 2, -1, 4)$, $(-2, 3, -1, 2)$, $(-1, -1, -1, 1)$, $(-1, 2, -3, 1)$, $(-1, 2, -2, 2)$, $(-1, 3, -2, 1)$, $(-1, 3, -1, 3)$, $(-1, 4, -1, 2)$ *and their inverses.*

As we can see, the amount of different series of roots of the equation $K_n(x_1, \ldots, x_n) = 1$ grows rapidly with n. We expect that it will continue growing like that for bigger n too.

For higher values of n we only show that there are infinitely many solutions of the equation (11):

PROPOSITION 3. *Equation*

$$K_n(x_1, \ldots, x_n) = 1 \tag{11}$$

has infinitely many integer solutions for any $n \geqslant 2$.

PROOF. We have already showed this for $n \leqslant 4$. Now assume that $n \geqslant 5$. by using Property (5) of continuants we get that $(x_1, \ldots, x_{n-1}, 0)$ is a solution of (11) as soon as $(x_1, \ldots, x_{n-2})$ is a solution of $K_{n-2}(x_1, \ldots, x_{n-1}) = 1$. As we already know, the latter has infinitely many solutions. □

Theorem 2 and Proposition 3 together suggest the way of finding infinitely many different sequences $\mathcal{L}(\mathbf{x}_{0,n-1})$. We consider all n-tuples $\mathbf{x}_{0,n-1}$ such that $K_n(\mathbf{x}_{0,n-1}) = 1$ (Proposition 3 says that there are infinitely many of them) and then by Theorem 2 we construct $x_n \in \mathbb{Z}$ such that $\mathbf{x}_{0,n}$ is a solution of (3). Theoretically all $(n+1)$-tuples constructed in this way may belong to the same sequence $\mathcal{L}(\mathbf{x}_{0,n-1})$ but on practise this is usually not the case.

The case $t = -1$ can be considered in a similar way.

THEOREM 4. *The equation* $K_2^{(-1)}(x_1, x_2) = 1$ *has two solutions* $(1, 2)$ *and* $(-2, -1)$ *together with their inverses. The equation*

$$K_3^{(-1)}(x_1, x_2, x_3) = 1$$

has

- *three infinite series of solutions* $(0, a, -1), (a, 0, -1 - a), (-1, -1, a)$ *together with their inverses.*
- *four additional solutions* $(1, 2, 2), (1, 3, 1), (2, 1, 3)$ *together with their inverses.*

Finally for $n \geqslant 3$ *the equation* $K_n^{(-1)}(\mathbf{x}_{1,n}) = 1$ *has infinitely many solutions.*

PROOF. For $n = 2$ the equation can be rewritten as $x_1x_2 = 2$. By considering all factorisations of 2 we get the solutions $(-2, -1), (-1, -2), (1, 2), (2, 1)$.

For $n = 3$ we notice that $K_3^{(-1)}(x_1, x_2, x_3) = 1$ if and only if $K_3(-x_1, x_2, -x_3) = 1$. All solutions of the latter equation are provided by Proposition 2.

Finally, by (5) we have that $K_{n+2}^{(-1)}(\mathbf{x}_{1,n}, a, 0) = -K_n^{(-1)}(\mathbf{x}_{1,n})$ for any $a \in \mathbb{Z}$. Therefore if the equation $K_n^{(-1)}(\mathbf{x}_{1,n}) = -1$ has at least one solution then the equation $K_{n+2}^{(-1)}(\mathbf{x}_{1,n+2}) = 1$ has infinitely many solutions. By analogous reason, if $K_{n-2}^{(-1)}(\mathbf{x}_{1,n-2}) = 1$ has at least one solution then $K_{n+2}^{(-1)}(\mathbf{x}_{1,n+2})$ has infinitely many solutions.

By the definition of the generalised continuants, the equation $K_n^{(-1)}(\mathbf{x}_{1,n}) = 1$ has a solution for $n = 0$ and $n = 1$, we already know that it has solutions for $n = 2$ and $n = 3$ and basic induction finishes the proof for $n \geqslant 4$. □

To conclude, the solutions of $K_n^{(t)}(\mathbf{x}_{1,n}) = 1$ generate the chains $\mathcal{L}(\mathbf{x}_{1,n})$. By the same reason the solutions of the similar equation $K_n^{(t)}(\mathbf{x}_{1,n}) = -1$ may generate more chains $\mathcal{L}(\mathbf{x}_{1,n})$. by this method we can construct at least partial classification of chains. We call the chain $\mathcal{L}(\mathbf{x}_{1,n})$ nonstandard if $\forall\, \mathbf{x} \in \mathcal{L}(\mathbf{x}_{1,n})$ one has $K_n^{(t)}(\mathbf{x}) \neq \pm 1$. Then the Problem A can be speified a bit further.

PROBLEM B. Given $n \in \mathbb{N}$, $t = \pm 1$ and a polynomial $P(x)$ which satisfies (2), classify all nonstandard chains $\mathcal{L}(\mathbf{x}_{1,n})$.

4.1. The case $n = 2$ and $P(x) = x^4 + 1$

Let $n = 2$. The paper [1] contains a full classification of chains $\mathcal{L}(x_0, x_1)$ with nonnegative x_0 and x_1 for polynomials $P(x)$ of degree 4. With some efforts that

classification can be extended to all chains $\mathcal{L}(x_0, x_1)$. We demonstrate this statement for a model example $P(x) = x^4 + 1$.

In this case the result from [1] states

THEOREM (Bad). *The positive integer solutions of the equation*

$$x_1^4 + 1 = (x_0x_1 + 1)(x_1x_2 + 1) \tag{12}$$

are elements of chains $\mathcal{L}(0, a)$ *where* $a \in \mathbb{N}$

Firstly note that the solutions of (12) are close under changing the sign: (x_0, x_1, x_2) is a solution of (12) if and only if $(-x_0, -x_1, -x_2)$ is. This fact immediately gives us the classification of all negative solutions of (12): they are elements of the chains $\mathcal{L}(0, a)$ where $a < 0$.

Next, the solutions with at least one zero term can be easily found. If $x_0 = 0$ then $\mathbf{x}_{0,2}$ is an element of a chain $\mathcal{L}(0, a)$ for some $a \in \mathbb{Z}$. Similarly solutions with $x_2 = 0$ are elements of chains $\overline{\mathcal{L}}(0, a)$, $a \in \mathbb{Z}$. Finally, a straightforward check shows that any triple $(x_0, 0, x_2)$ is a solution of (12).

The remaining case is when the signs of the solutions (x_0, x_1, x_2) alternate. Without loss of generality assume that $x_0 > 0 > x_1$. Then from (12) we have that x_2 must also be positive. The chain $\mathcal{L}(x_0, x_1)$ can not contain zero since we already classified all chain with zeroes and none of them have terms with alternating signs. Therefore, by consecutive inspection of elements $x_3, x_4, \ldots$ from the chain $\mathcal{L}(x_0, x_1)$ we get that terms of any solution $\mathbf{x}_{k,k+2} \in \mathcal{L}(x_0, x_2)$ have alternating signs. By replacing $\mathbf{x}_{0,2}$ with its inverse $\overline{\mathbf{x}}_{0,2}$, if needed, we may guarantee that $|x_0| > |x_1|$. Therefore the chain $\mathcal{L}(x_0, x_1)$ must contain an element $\mathbf{x}_{k,k+2}$ such that $|x_k| \geqslant |x_{k+1}| \leqslant |x_{k+2}|$, otherwise it would contain zero, which is impossible. By rewriting (12) with

$$|x_{k+1}|^4 + 1 = (|x_kx_{k+1}| - 1)(|x_kx_{k+1}| - 1)$$

we can easily classify all such integer solutions. Up to a sign there is only one such a solution: $|x_k| = |x_{k+2}| = 2$ and $|x_{k+1}| = 1$. Hence $\mathbf{x}_{0,2}$ is an element of either $\mathcal{L}(2, -1, 2)$ or $\mathcal{L}(-2, 1, -2)$.

As a conclusion we end this section with the complete classification of integer solutions of (12).

THEOREM 5. *Every integer solution* (x_0, x_1, x_2) *of* (12) *falls into one of the following categories*:

- $\mathbf{x}_{0,2}$ *is an element of* $\mathcal{L}(0, a)$ *or* $\overline{\mathcal{L}}(0, a)$ *where* $a \in \mathbb{Z}\backslash\{0\}$;
- $\mathbf{x}_{0,2}$ *has* $x_1 = 0$;
- $\mathbf{x}_{0,2}$ *is an element of* $\mathcal{L}(-2, 1, -2)$ *or* $\mathcal{L}(2, -1, 2)$.

A trivial inspection of all three cases above shows that for $n = 2$ ad $P(x) = x^4+1$ all chains $\mathcal{L}(x_0, x_1)$ are standard.

5. Other ways of generating solutions of (3)

In this section we will show that each solution $\mathbf{x}_{0,n+1}$ of the equation (3) generates many other solutions of (3) for the same polynomial $P(x)$ but for different values of n. Fix a polynomial $P(x)$ and consider Condition (2) for various values n. Notice that for $t = 1$, if $P(x)$ satisfies (2) for some n then it satisfies the same condition for all values of n of the same parity. Furthermore, for $t = -1$ if $P(x)$ satisfies (2) for some n then it satisfies the same condition for all n. Based on this observation we denote by $\mathbf{A}^t(P)$ the set of all integer solutions of (3) for a given t and $P(x)$ and for any integer n such that $P(x)$ satisfies (2).

Further in this section we will always assume that $\mathbf{x}_{0,n+1}$ is a solutions of (3). To start with, assume that $t = 1$. We have $K_{n+1}(\mathbf{x}_{0,n}) \mid P(K_n(\mathbf{x}_{1,n}))$. Then we also have that for any $d \in \mathbb{Z}$,

$$K_{n+3}(0, a, \mathbf{x}_{0,n}) = K_{n+1}(\mathbf{x}_{0,n}) \mid P(K_n(\mathbf{x}_{1,n}) + aK_{n+1}(\mathbf{x}_{0,n})) = P(K_{n+2}(a, \mathbf{x}_{0,n})).$$

by applying Theorem 2 we find the value x'_{n+1} such that $(0, a, \mathbf{x}_{0,n}, x'_{n+1})$ is a new solution of (3) for the value $n + 2$. Since the parity of n and $n + 2$ coincide, we have that $(0, a, \mathbf{x}_{0,n}, x'_{n+1}) \in \mathbf{A}^1(P)$. Moreover if $K_n(\mathbf{x}_{1,n}) \neq 0$ then the value x'_{n+1} is unique and can be computed by formula (10). Otherwise $(0, a, \mathbf{x}_{0,n}, x'_{n+1})$ is a solution of the main equation for any integer x'_{n+1}. Therefore we can define the maps from $\mathbf{A}^1(P)$ to itself:

$$f_a \ : \ \{\mathbf{x}_{0,n+1} \in \mathbf{A}^1(P) \ : \ K_n(\mathbf{x}_{1,n}) \neq 0\} \to \mathbf{A}^1(P)$$

such that $f_a(\mathbf{x}_{0,n+1}) = (0, a, \mathbf{x}_{0,n}, x'_{n+1})$. Also define

$$f^*_{a,b} \ : \ \{\mathbf{x}_{0,n+1} \in \mathbf{A}^1(P) \ : \ K_n(\mathbf{x}_{1,n}) = 0\} \to \mathbf{A}^1(P)$$

by $f_a(\mathbf{x}_{0,n+1}) = (0, a, \mathbf{x}_{0,n}, b)$. These two functions f_a and $f^*_{a,b}$ provide a way of generating new solutions to (3) in addition to chains $\mathcal{L}(\mathbf{x}_{0,n})$.

From now on Let's assume that $P(x)$ is either even or odd (i. e. $P(-x) = \pm P(x)$). Then the same generating procedure will work for $t = -1$ too. Indeed,

$$K_{n+3}^{(-1)}(0,a,\mathbf{x}_{0,n}) = -K_{n+1}^{(-1)}(\mathbf{x}_{0,n}) \,|\, P(-K_n^{(-1)}(\mathbf{x}_{1,n}) + aK_{n+1}^{(-1)}(\mathbf{x}_{0,n})) = P(K_{n+2}^{(-1)}(a,\mathbf{x}_{0,n})).$$

Therefore in that case we can define two maps $f_a^{(-1)}$ and $f_{a,b}^{*(-1)}$ for $t=-1$ in the same way as f_a and $f_{a,b}^*$.

Finally, we provide one more way of generating new elements of $\mathbf{A}^t(P)$ for even and odd polynomials P. By (7) we have that $K_{n+2}^{(t)}(1,x_0-t,\mathbf{x}_{1,n}) = K_{n+1}^{(t)}(\mathbf{x}_{0,n})$. On the other hand, by Condition (5) we have

$$K_{n+1}^{(t)}(x_0-t,\mathbf{x}_{1,n}) = K_{n+1}^{(t)}(\mathbf{x}_{0,n}) - tK_n^{(t)}(\mathbf{x}_{1,n})$$

Therefore for $t=\pm 1$ a divisibility $K_{n+1}^{(t)}(\mathbf{x}_{0,n}) \,|\, P(K_n^{(t)}(\mathbf{x}_{1,n}))$ implies

$$K_{n+2}^{(t)}(1,x_0-t,\mathbf{x}_{1,n}) \,|\, P(K_{n+1}^{(t)}(x_0-t,\mathbf{x}_{1,n})).$$

For $t=-1$ this gives a new solution of the equation (3). Define a new map

$$g: \{\mathbf{x}_{0,n} \in \mathbb{Z}^{n+1} : n \in \mathbb{Z}_{\geqslant 0}\} \to \{\mathbf{x}_{0,n} \in \mathbb{Z}^{n+1} : n \in \mathbb{Z}_{\geqslant 0}\}$$

by $g(\mathbf{x}_{0,n}) = (1,x_0-t,\mathbf{x}_{1,n})$. Notice that in the case $x_0=1$ the inverse map g^{-1} is correctly defined. For $t=-1$, g maps $\mathbf{A}^{-1}(P)$ to itself. However, since g changes the parity of the length of $\mathbf{x}_{0,n}$, $g(\mathbf{A}^1(P))$ is not necessarily in $\mathbf{A}^1(P)$. On the other hand it can be fixed by introducing one more map

$$h: \{\mathbf{x}_{0,n} \in \mathbb{Z}^{n+1} : n \in \mathbb{Z}_{\geqslant 0}\} \to \{\mathbf{x}_{0,n} \in \mathbb{Z}^{n+1} : n \in \mathbb{Z}_{\geqslant 0}\}$$

by $h(\mathbf{x}_{0,n}) = (\mathbf{x}_{0,n-1}, x_n - t, 1)$. Notice that

$$K_{n+2}^{(t)}(\mathbf{x}_{0,n-1},x_n-t,1) = K_{n+1}^{(t)}(\mathbf{x}_{0,n}) \,|\, P(K_n^{(t)}(\mathbf{x}_{1,n})) = P(K_{n+1}^{(t)}(\mathbf{x}_{1,n},x_{n+1}-t)).$$

Again, as before, function h maps $\mathbf{A}^{-1}(P)$ to itself. On the other hand it also changes the parity of the size of vectors $\mathbf{x}$. Finally notice that $g \circ h = h \circ g$ does not change the parity of n, therefore $g \circ h$ maps $\mathbf{A}^1(P)$ to itself. Finally, if correctly defined, the maps $g^{\pm 1} \circ h^{\pm 1}$ also map $\mathbf{A}^1(P)$ to itself and therefore provide another way to generate new solutions of (3).

We conclude this section with the table which contains all maps discussed here. Given $\mathbf{x}_{0,n} \in \mathbf{A}^t(P)$ we can produce the following new elements of $\mathbf{x}_{0,n} \in \mathbf{A}^t(P)$:

$t = 1$	$t = -1$
$f_a(\mathbf{x}_{0,n})$ if $K_n(\mathbf{x}_{1,n}) \neq 0$	$f_a^{(-1)}(\mathbf{x}_{0,n})$ if $K_n^{-1}(\mathbf{x}_{1,n}) \neq 0$
$f_{a,b}(\mathbf{x}_{0,n})$ if $K_n(\mathbf{x}_{1,n}) = 0$	$f_{a,b}^{(-1)}(\mathbf{x}_{0,n})$ if $K_n^{-1}(\mathbf{x}_{1,n}) = 0$
$g \circ h(\mathbf{x}_{0,n})$	$g(\mathbf{x}_{0,n})$
$g \circ h^{-1}(\mathbf{x}_{0,n})$ if $x_n = 1$	$h(\mathbf{x}_{0,n})$
$g^{-1} \circ h(\mathbf{x}_{0,n})$ if $x_0 = 1$	$g^{-1}(\mathbf{x}_{0,n})$ if $x_0 = 1$
$g^{-1} \circ h^{-1}(\mathbf{x}_{0,n})$ if $x_0 = x_n = 1$	$h^{-1}(\mathbf{x}_{0,n})$ if $x_n = 1$

6. Relation with the factorisation of values $P(m)$

Fix $t = 1$ and a polynomial $P(x)$ which satisfies (2) for some integer value n_0. In the previous section we observed that $P(x)$ then satisfies conditions (2) for all n of the same parity as n_0.

Consider an arbitrary factorisation $P(m) = d_1 d_2$ of the value $P(m)$ at some positive integer value m into the product of two integer factors. Write d_1/m as a continued fraction:

$$\frac{d_1}{m} = [a_0; a_1, \dots, a_{n-1}]$$

where $a_0 \in \mathbb{Z}$ and $a_1, \dots, a_n \in \mathbb{N}$. Moreover, we can always choose such repesentation that $n - n_0$ is even. Since $t = 1$, conditions (2) imply that m and $P(m)$ are coprime, therefore d_1/m is irreducible continued fraction. From the theory of continued fractions we have

$$m = K_{n-1}(\mathbf{a}_{1,n-1}) \quad \text{and} \quad d_1 = K_n(\mathbf{a}_{0,n-1}) \tag{13}$$

Therefore the n-tuple $\mathbf{a}_{0,n-1}$ satisfies the conditions of Theorem 2. Moreover, $K_{n-1}(\mathbf{a}_{1,n-1}) = m \neq 0$ which implies that there exists unique value a_n such that $\mathbf{a}_{0,n}$ is a solution of (3).

To conclude, any factorisation of $P(m)$ for positive integer m generates a solution $\mathbf{a}_{0,n}$ of (3) with

$$a_0, a_n \in \mathbb{Z} \quad \text{and} \quad a_1, \dots, a_{n-1} \in \mathbb{N}. \tag{14}$$

Conversely, for any solution $\mathbf{a}_{0,n}$ which satisfies (14) we have

$$P(K_{n-1}(\mathbf{a}_{1,n-1})) = K_n(\mathbf{a}_{0,n-1}) \cdot K_n(\mathbf{a}_{1,n}).$$

Denote $m = K_{n-1}(\mathbf{a}_{1,n-1}) \in \mathbb{N}$, $d_1 = K_n(\mathbf{a}_{0,n-1})$ and $d_2 = K_n(\mathbf{a}_{1,n})$. Whence we have a bijection between all factorisations of $P(m)$ and the solutions $\mathbf{a}_{0,n}$ of (3) satisfying (14). Therefore if we understand the full structure of the set $\mathbf{A}^1(P)$ then we can generate factorisations of $P(m)$ in a constructive way. In particular, we will be able to construct values $P(m)$ which factorisation as a product of primes satisfies the prescribed properties. This is quite important for cryptosystems like RSA.

6.1. Example

For better understanding of the equation (3) and its link to the factorisations of $P(m)$ we look at our model example $P(x) = x^4 + 1$ and $t = 1$. It is easy to check that $P(x)$ satisfies (2) for any even value n.

As discussed in the previous chapters we have a number of ways to create new solutions in $\mathbf{A}^1(P)$ based on already known ones. For any given solution $\mathbf{x}_{0,n}$ we can create the chain $\mathcal{L}(\mathbf{x}_{0,n})$ of solutions, we can use maps f_a and $f^*_{a,b}$, finally we have maps $g^{\pm 1} \circ h^{\pm 1}$. The natural question is then as follows: *given all these maps and finitely many solutions of* (3), *can we generate all the set* $\mathbf{A}^1(P)$*?* We do not know the formal answer to this question, however, as we will see in a moment, it seems to be negative. In any case, with help of the described maps we can construct a subclass of $\mathbf{A}^1(P)$ and therefore the subclass of the factorisations of numbers like $m^4 + 1$.

We start with the table which covers the factorisations of m^4+1 for small values of m. In the "$\mathbf{x}$ and a sequence $\mathcal{S}$" column we write the solution $\mathbf{x}$ in brackets and then we write the sequence $\mathcal{S}$ around it.

m	factorisation	$\mathbf{x}$ and a sequence $\mathcal{S}$	notation
1	$1^4 + 1 = 1 \cdot 2$	$(\mathbf{0}, \mathbf{1}, \mathbf{1}), 0$	$\mathbf{x}^{(1)}$
2	$2^4 + 1 = 1 \cdot 17$	$(\mathbf{0}, \mathbf{2}, \mathbf{8}), 30, 112, \ldots$	$\mathbf{x}^{(2)}$
3	$3^4 + 1 = 1 \cdot 82$	$(\mathbf{0}, \mathbf{3}, \mathbf{27}), 240, 2133, \ldots$	$\mathbf{x}^{(3)}$
3	$3^4 + 1 = 2 \cdot 41$	$-1, (\mathbf{0}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{13}), 480, 23422307, \ldots$	$\mathbf{x}^{(4)} = f_1(\mathbf{x}^{(1)})$
4	$4^4 + 1 = 1 \cdot 257$	$(\mathbf{0}, \mathbf{4}, \mathbf{64}), 1020, \ldots$	$\mathbf{x}^{(5)}$
5	$5^4 + 1 = 1 \cdot 626$	$(\mathbf{0}, \mathbf{5}, \mathbf{125}), 3120, \ldots$	$\mathbf{x}^{(6)}$
5	$5^4 + 1 = 2 \cdot 313$	$-2, (\mathbf{0}, \mathbf{2}, \mathbf{1}, \mathbf{1}, \mathbf{62}), 6240, \ldots$	$\mathbf{x}^{(7)} = f_2(\mathbf{x}^{(1)})$
6	$6^4 + 1 = 1 \cdot 1297$	$(\mathbf{0}, \mathbf{6}, \mathbf{216}), 7770, \ldots$	$\mathbf{x}^{(8)}$
7	$7^4 + 1 = 1 \cdot 2402$	$(\mathbf{0}, \mathbf{7}, \mathbf{343}), 16800, \ldots$	$\mathbf{x}^{(9)}$
7	$7^4 + 1 = 2 \cdot 1201$	$-3, (\mathbf{0}, \mathbf{3}, \mathbf{1}, \mathbf{1}, \mathbf{171}), 33600, \ldots$	$\mathbf{x}^{(10)} = f_3(\mathbf{x}^{(1)})$

m	factorisation	$\mathbf{x}$ and a sequence $\mathcal{S}$	notation
8	$8^4+1 = 1\cdot 4097$	$(\mathbf{0}, \mathbf{8}, \mathbf{512})$, 32760, ...	$\mathbf{x}^{(11)}$
8	$8^4+1 = 17\cdot 241$	0, $(\mathbf{2}, \mathbf{8}, \mathbf{30})$, 112, ...	$\mathbf{x}^{(12)} \in \mathcal{L}(\mathbf{x}^{(2)})$
9	$9^4+1 = 1\cdot 6562$	$(\mathbf{0}, \mathbf{9}, \mathbf{729})$, 59040, ...	$\mathbf{x}^{(13)}$
9	$9^4+1 = 2\cdot 3281$	-4, $(\mathbf{0}, \mathbf{4}, \mathbf{1}, \mathbf{1}, \mathbf{364})$, 118080, ...	$\mathbf{x}^{(14)} = f_4(\mathbf{x}^{(1)})$
9	$9^4+1 = 17\cdot 386$	..., 21011, 198, $(\mathbf{1}, \mathbf{1}, \mathbf{7}, \mathbf{1}, \mathbf{42})$, 104543, ...	$\mathbf{x}^{(15)} = g\circ h(\mathbf{x}^{(12)})$
9	$9^4+1 = 34\cdot 193$	..., 42022, 99, $(\mathbf{3}, \mathbf{1}, \mathbf{3}, \mathbf{2}, \mathbf{21})$, 17487, ...	$\mathbf{x}^{(16)}$, new?
10	$10^4+1 = 1\cdot 10001$	$(\mathbf{0}, \mathbf{10}, \mathbf{1000})$, 99990, ...	$\mathbf{x}^{(17)}$
10	$10^4+1 = 73\cdot 137$	..., 1817, $(\mathbf{7}, \mathbf{3}, \mathbf{2}, \mathbf{1}, \mathbf{13})$, 503, ...	$\mathbf{x}^{(18)}$, new?

Based on this table, we make several observations. As we can see, all the factorisations of m^4+1 for $1 \leqslant m \leqslant 10$, except two, are generated by solutions $(0, a, a^3) \in \mathbf{A}^1(P)$ which in turn come from the solutions of $K_2(x_1, x_2) = 1$. However the remaining two products, namely $9^4+1 = 34\cdot 193$ and $10^4+1 = 73\cdot 137$, seem to generate new elements of $\mathbf{A}^1(P)$ which do not intersect with those generated by $(0, a, a^3)$. By considering larger values of m one can reveal more such elements. For example $\mathbf{x} = (7, 2, 2, 2, 19) \in \mathbf{A}^1(P)$, which comes from the factorisation $12^4+1 = 89\cdot 233$, is another example of this type. We believe that infinitely many generators $\mathbf{x}$ on top of $(0, a, a^3)$ are required to generate the whole set $\mathbf{A}^1(P)$. It will be interesting to see the formal proof of this statement.

Let's consider $\mathbf{x}^{(4)}$ and look at several first factorisations which are linked with elements of the chain $\mathcal{L}(\mathbf{x}^{(4)})$:

$$\begin{aligned}
\mathbf{x}_{0,4} &= (0, 1, 1, 1, 13) && : 3^4 = 2\cdot 41\\
\mathbf{x}_{1,5} &= (1, 1, 1, 13, 480) && : 27^4+1 = 41\cdot 12962\\
\mathbf{x}_{2,6} &= (1, 1, 13, 480, 23422307) && : 6721^4+1 = 12962\cdot 157421325361
\end{aligned}$$

The next solution $\mathbf{x}_{3,7}$ gives a factorisation of the number $(K_3(13, 480, 23422307))^4+$ $+ 1 = 146178618000^4+1$. This figures show that elements of $\mathbf{x}_{n,n+4}$ from $\mathcal{L}(\mathbf{x})$ provide non-trivial factorisations of values m^4+1 and that the numbers m grow very quickly as n grows. With help of the formula (10) we can estimate the rate of growth of x_n. Assuming that $0 < x_1 \leqslant x_2 \leqslant x_3 \leqslant x_4$ we have that $K_4(\mathbf{x}_{1,4}) = x_1K_3(\mathbf{x}_{2,4}) + K_2(\mathbf{x}_{3,4}) < (x_1+1)K_3(\mathbf{x}_{2,4})$, therefore

$$x_5 = \frac{(K_3(\mathbf{x}_{2,4}))^4 + 1 - K_2(\mathbf{x}_{2,3})K_4(\mathbf{x}_{1,4})}{K_3(\mathbf{x}_{2,4})K_4(\mathbf{x}_{1,4})} \geqslant \frac{K_3(\mathbf{x}_{2,4})^2}{x_1+1} - 1.$$

So definitely $x_5 > \frac{1}{2}x_4^2x_3^2x_2$.

Theorem 5 states that for $n = 2$ and $P(x) = x^4+1$ all chains $\mathcal{L}(x_0, x_1)$ are standard. However the table suggests that for the same polynomial $P(x)$ and for higher values n nonstandard chains do exist. For example, consider $\mathbf{x}^{(16)} = (3, 1, 3, 2, 21)$. Indeed, one can show that for $n \geqslant 4$ elements x_n in the chain are strictly increasing. Also for $n < 0$ elements x_n strictly decrease. We leave the rigorous proof of this statement to the reader. Therefore a quick inspection shows that $K_4(\mathbf{x}_{m,m+3}) > 1$ for any four consecutive elements from the chain $\mathcal{L}(3, 1, 3, 2, 21)$.

Bibliography

1. ***Badziahin D.,*** *Finding special factors of values of polynomials at integer points*, Int. J. of Numb. Theor., **13**:1 (2017), 209–228.
2. ***Davenport H.,*** *The Higher Arithmetic*, Fifth Edition, Cambridge University Press, 1982.
3. ***Hardy G., Wright E.,*** *An Introduction to the Theory of Numbers*, Sixth Edition, Oxford University Press, 2008.
4. ***Schinzel A.,*** *On the Diophantine equation* $x^2 + x + 1 = yz$, Colloq. Math. **141** (2015), 243–248.

Dzmitry Badziahin

Dept of Mathematical Sciences
Durham University
Lower Mountjoy
Stockton Road
Durham DH1 3LE
dzmitry.badziahin@durham.ac.uk