

# Finding special factors of values of polynomials at integer points

Dzmitry Badziahin

November 26, 2014

## Abstract

We investigate the divisors  $d$  of the numbers  $P(n)$  for various polynomials  $P \in \mathbb{Z}[x]$  such that  $d \equiv 1 \pmod{n}$ . We managed to construct the complete classification of such divisors for some class of polynomials, in particular for  $P(x) = x^4 + 1$ . We also constructed a fast algorithm which provides all such factorizations up to a given limit for another class, for example for  $P(x) = 2x^4 + 1$ . We use these results to find all the divisors  $d = 2^m k + 1$  of numbers  $2^{4m} + 1$  and  $2^{4m+1} + 1$ . For the numbers  $2^{4m} + 1$  the complete classification of such divisors is provided while for the numbers  $2^{4m+1} + 1$  the given classification is proved to be exhaustive for  $m \leq 1000$  only.

## 1 Introduction

The motivation of this paper is to investigate the divisors of numbers like  $2^m + 1$ . The factorization of these numbers and in particular of the Fermat numbers  $F_n = 2^{2^n} + 1$  attracts an attention of communities from both Mathematics and Computer Science. For example the Cunningham project aims at finding the complete factorizations of numbers  $b^m \pm 1$  for small  $b \in \mathbb{N}$  and  $m$  as large as possible (see [3] and [4] for details).

The rapid increase of the computer power in the last 60 years contributed to a revolutionary improvement of the factoring algorithms. Many of them proved their efficiency by factoring various Fermat numbers. For example  $F_7$  was factored in 1970 with the continued fraction method, the first known factoring algorithm of subexponential complexity [2]. The fastest currently known algorithms, elliptic curve method and (special) number field sieve, were used to factor  $F_{10}$  and  $F_9$  respectively (see [1] and [6]). Unfortunately since 1999 no more Fermat numbers were completely factored and because of their rapid growth it seems that some dramatic development of factoring methods (or a big luck) is needed to factorize  $F_{12}$  and higher Fermat numbers.

In this paper instead of looking at general purpose factoring algorithms we use the algebraic structure of numbers to get some information about their divisors. It was already known by Euler that each divisor of  $F_m$  is of the form  $d = 2^{m+2} \cdot k + 1$ . We will show that on the other hand  $d - 1$  can not be divisible by a big power of two. For example Theorem 2 below states that if  $2^{4m} + 1$  is divisible by  $2^m \cdot k + 1$  then it must be a trivial algebraic divisor and in particular for any divisor  $d \mid F_m$  one must have  $2^{2^{m-2}} \nmid d - 1$ . Also Theorem 7 classifies all divisors  $d \mid 2^{4m+1} + 1$  of the form  $d = 2^{m+1} \cdot k + 1$  (which are also all algebraic). Furthermore it shows that  $2^{4m+1} + 1$  has only one extra pair of divisors of the form  $2^m \cdot k + 1$  for  $m \leq 1000$ . We believe that this exhausts all divisors of this type.

## 2 Numbers of the form $n^4 + 1$

The aim of this section is to classify all factors of  $n^4 + 1$  of the form  $kn + 1$ . They certainly exist, for example  $8 \cdot 30 + 1 \mid 30^4 + 1$ . Moreover one can easily get infinitely many of them by observing that

$$n^4 + 1 = n \cdot n^3 + 1 \mid (n^3)^4 + 1.$$

for all natural  $n$ . Define the set  $\mathcal{F}$  which is related to the factorizations of the given form:

$$\mathcal{F} := \{(k, n) \in \mathbb{Z}_{\geq 0}^2 : kn + 1 \mid n^4 + 1\}.$$

It appears that elements of  $\mathcal{F}$  are very well structured. We provide the classification of all elements of  $\mathcal{F}$  in the following theorem.

**Theorem 1** *Let  $f_k(x)$  be the sequence of rational functions from  $\mathbb{Z}(x)$  such that*

$$f_0(x) := 0; f_1(x) := x \quad \text{and} \quad f_{k+1}(x) := \frac{f_k(x)^3 - f_{k-1}(x)}{f_k(x)f_{k-1}(x) + 1}, \quad k \in \mathbb{N}.$$

*Then*

- $f_k(x) \in \mathbb{Z}[x]$  for all  $k \in \mathbb{N}$ ;
- the set  $\mathcal{F}$  can be described as follows:

$$\mathcal{F} = \{(f_{k-1}(n), f_k(n)), (f_k(n), f_{k-1}(n)) : n, k \in \mathbb{N}\}.$$

PROOF. We start with finding all possible factorizations of  $nk + 1 \mid n^4 + 1$  where the parameters  $n, k \in \mathbb{Z}$  are not necessarily nonnegative. Define

$$\mathcal{F}_{\mathbb{Z}} := \{(k, n) \in \mathbb{Z} : kn + 1 \mid n^4 + 1\}.$$

The proof is based on two observations. Firstly if the factor  $d$  of  $n^4 + 1$  is congruent to 1 modulo  $n$  then so is its cofactor  $(n^4 + 1)/d$ . Therefore the factorization  $n^4 + 1 = d \cdot ((n^4 + 1)/d)$  can be written in the following way:

$$n^4 + 1 = (an + 1)(bn + 1), \quad a, b \in \mathbb{Z}.$$

Hence if  $(a, n) \in \mathcal{F}_{\mathbb{Z}}$  then

$$(b, n) = \left( \frac{n^3 - a}{an + 1}, n \right) \in \mathcal{F}_{\mathbb{Z}}.$$

The second observation is that  $n \equiv -1/a \pmod{an + 1}$  and so  $a^4 + 1$  is also divisible by  $an + 1$  which gives us another factorization. I.e. if  $(a, n) \in \mathcal{F}_{\mathbb{Z}}$  then so is  $(n, a) \in \mathcal{F}_{\mathbb{Z}}$ .

These observations show that every pair  $(a_0, a_1) \in \mathcal{F}_{\mathbb{Z}}$  generates the chain of pairs  $\mathcal{C}_{\mathbb{N}}(a_0, a_1) := \{(a_i, a_{i+1})\}_{i \in \mathbb{N}}$  from  $\mathcal{F}_{\mathbb{Z}}$  where

$$a_2 = \frac{a_1^3 - a_0}{a_0 a_1 + 1}, \dots, \quad a_{i+1} = \frac{a_i^3 - a_{i-1}}{a_{i-1} a_i + 1}.$$

Moreover by the same formulas this chain can be defined for negative values  $i$  as well. So we can define  $\mathcal{C}(a_0, a_1) := \{(a_i, a_{i+1})\}_{i \in \mathbb{Z}} \subset \mathcal{F}_{\mathbb{Z}}$ . Note also that

$$\forall i_0 \in \mathbb{Z}, \quad \mathcal{C}(a_{i_0}, a_{i_0+1}) = \mathcal{C}(a_0, a_1) \quad \text{and} \quad \mathcal{C}(a_{i_0+1}, a_{i_0}) = \mathcal{C}(a_1, a_0) = \{(a_{i+1}, a_i)\}_{i \in \mathbb{Z}}. \quad (1)$$

Now consider the pair  $(a_0, a_1) \in \mathcal{F}$  with  $a_0 \geq a_1 \geq 0$ . Then from the formula

$$a_i^4 + 1 = (a_i a_{i-1} + 1)(a_i a_{i+1} + 1), \quad i \in \mathbb{N}$$

one can easily get that if  $a_1 > 0$  then  $a_1 > a_2 \geq 0$ . By continuing the same arguments further we get that  $a_1 > a_2 > \dots > a_t$  until the parameter  $a_t$  becomes non-positive. Moreover since  $a_t \geq 0$  then  $a_t$  must be equal to zero. The sequence of natural numbers can not decrease infinitely long therefore such value  $t$  must exist. Hence for every  $(a_0, a_1) \in \mathcal{F}$  with  $a_1 \leq a_0$  the chain  $\mathcal{C}(a_0, a_1)$  includes the pair of the form  $(n, 0)$ . By (1) in case  $a_1 \geq a_0$  we have that  $\mathcal{C}(a_0, a_1)$  contains the pair  $(0, n)$ . On the other hand for every  $n \in \mathbb{N}$  the pairs  $(n, 0)$  and  $(0, n)$  indeed lie in  $\mathcal{F}$ .

Consider the chain which includes  $(0, n)$ . Note that  $(0, n) = (f_0(n), f_1(n))$ . Then by construction

$$\mathcal{C}_{\mathbb{N}}(0, n) = \{(f_k(n), f_{k+1}(n))\}_{k \in \mathbb{N}}.$$

In particular it means that all values  $f_k(n)$  are integer. Since  $f_k(n) \in \mathbb{Z}$  for all  $n \in \mathbb{Z}$  then  $f_k(x) \in \mathbb{Z}[x]$ . Finally we have showed that every pair  $(a_0, a_1) \in \mathcal{F}$  must be in the chain generated by either  $(0, n)$  or  $(n, 0)$ . Therefore  $\exists k \in \mathbb{N}$  such that  $(a_0, a_1) = (f_{k-1}(n), f_k(n))$  or  $(a_0, a_1) = (f_k(n), f_{k-1}(n))$ .

□

## 2.1 Some properties and applications

Now we apply Theorem 1 for the numbers of the form  $2^{4m} + 1$ . At the end of this subsection we will classify all possible divisors of such numbers which are congruent to 1 modulo  $2^m$ . Surely there are infinitely many of them coming from the following algebraic factorization:

$$2^m \cdot 2^{3m} + 1 \mid 2^{12m} + 1.$$

We call factorizations of this form trivial.

Theorem 1 transforms the problem of finding the factorizations

$$2^{4m} + 1 = (a2^m + 1)(b2^m + 1)$$

to the following series of Diophantine equations:

$$f_k(n) = 2^m. \tag{2}$$

**Lemma 1** *The polynomial  $f_a(x)$  divides  $f_b(x)$  if and only if  $a$  divides  $b$ .*

Firstly note that by construction of  $f_k$ , the sequence of degrees of polynomials  $f_k$  is strictly increasing, therefore  $f_a$  can not divide  $f_b$  if  $a < b$ .

Consider the sequence  $\{f_k\}_{k \in \mathbb{N}}$  in the space  $\mathbb{Z}[x]/(f_a(x))$ . Then we have  $f_0 \equiv f_a \equiv 0$ . Note that the degree of polynomials  $f_k$  is strictly increasing therefore  $f_k$  can not be congruent to zero for  $0 < k < a$ .

Next, note that

$$f_{a+1} = \frac{f_a^3 - f_{a-1}}{f_{a-1}f_a + 1} \equiv -f_{a-1}.$$

We show by induction that for each  $k = \overline{1, a}$ ,  $f_{a+k} \equiv -f_{a-k}$ . The base of induction  $k = 0$  and  $k = 1$  has already been checked. Now assume that for all  $k$  from 0 to  $k_0$  this is true and prove it for  $k_0 + 1$ :

$$f_{a+k_0+1} = \frac{f_{a+k_0}^3 - f_{a+k_0-1}}{f_{a+k_0-1}f_{a+k_0} + 1} \equiv -\frac{f_{a-k_0}^3 - f_{a-k_0+1}}{f_{a-k_0+1}f_{a-k_0} + 1} \equiv -f_{a-k_0-1}.$$

This implies  $f_{2a} \equiv -f_0 \equiv 0$ . And since for all  $0 < k < a$ ,  $f_k \not\equiv 0$  then the same is true for all  $a < k < 2a$ .

Applying the same arguments for intervals  $2a < k \leq 3a, \dots, ma < k \leq (m+1)a$  finishes the proof.  $\square$

The straight corollary of Lemma 1 is that every term  $f_k(n)$  is divisible by  $n$ . So in order to satisfy equation (2)  $n$  has to be a power of two:

$$n = 2^d.$$

Then values  $k = 1, 2$  give us (trivial) solutions to (2):

$$f_1(2^d) = 2^d; \quad f_2(2^d) = 2^{3d}.$$

Now consider the values  $k \geq 3$ . Note that from the proof of Lemma 1 we have that for odd  $k$ ,  $f_k(2^d) \equiv \pm 2^d \pmod{2^{3d}}$  and since  $f_k(2^d) > f_2(2^d) = 2^{3d}$  it follows that  $f_k(2^d)$  is not a power of two for all odd values  $k$ .

Consider  $k = 2^t k_0$  where  $k_0$  is odd. If  $k_0 \geq 3$  then  $f_k(2^d)$  is divisible by  $f_{k_0}(2^d)$  which is not a power of two, so it can not be a solution of (2). Finally we get  $k = 2^t$ .

Let's firstly check  $k = 4$ :

$$f_3(n) = n(n^4 - 1); \quad f_4(n) = n^3(n^4 - 2).$$

One can easily check that  $2^{4d} - 2$  can not be a power of two for any natural  $d$  since it is never divisible by four.

Finally we get that for  $t > 2$ ,  $f_{2^t}(2^d)$  again is not a power of two since it is divisible by  $f_4(2^d)$ . So finally we prove the following fact:

**Theorem 2** *Every non-trivial divisor of a number  $2^{4n} + 1$  is not congruent to 1 modulo  $2^n$ .*

Concerning the divisors of the Fermat numbers to the best of the authors knowledge this result is new. It substantially improves the result presented in [5] where it was shown that any divisor  $d$  of a fermat number  $F_n$  is not of the form  $2^{\lfloor 2^n/3 \rfloor} k + 1$ .

At the end of this section we want to remark that Theorem 2 can easily be adopted to the divisors of numbers  $b^{4n} + 1$  for an arbitrary  $b \in \mathbb{N}$ .

### 3 Other polynomials

Here we continue considering the divisors of the form  $nk + 1$  of the values  $f(n)$  for various polynomials  $f$ . Define the set

$$\mathcal{F}_f := \{(k, n) \in \mathbb{Z}_{\geq 0} : kn + 1 \mid f(n)\}.$$

### 3.1 Monic polynomials of degree 4 with free coefficient 1

The technique discussed in the previous section can be applied to a bigger class of polynomials rather than just  $n^4 + 1$ . Consider the polynomial  $f(x) = x^4 + c_1x^3 + c_2x^2 + c_3x + 1$  with integer coefficients, i.e.  $c_1, c_2, c_3 \in \mathbb{Z}$ . We will look for the divisors of  $f(n)$  which are of the form  $an + 1$ .

As before we extend  $\mathcal{F}_f$  to the set  $\mathcal{F}_{f,\mathbb{Z}}$  where the elements  $k, n$  are not necessarily non-negative. As before if  $(a_0, a_1) \in \mathcal{F}_{f,\mathbb{Z}}$  then we must have

$$f(a_1) = (a_0a_1 + 1) \cdot (a_2a_1 + 1), \quad \text{where } a_2 \in \mathbb{Z}. \quad (3)$$

So

$$(a_0, a_1) \in \mathcal{F}_{f,\mathbb{Z}} \Rightarrow (a_2, a_1) \in \mathcal{F}_{f,\mathbb{Z}} \quad \text{where} \quad a_2 = \frac{(f(a_1) - 1)/a_1 - a_0}{a_0a_1 + 1}. \quad (4)$$

We also have that  $a_1 \equiv -1/a_2 \pmod{a_2a_1 + 1}$  therefore by substituting that into  $f(a_1)$  and multiplying by  $a_2^4$  we get

$$a_2a_1 + 1 \mid a_2^4 \cdot f(-1/a_2) = a_2^4 - c_3a_2^3 + c_2a_2^2 - c_1a_2 + 1 =: f^*(a_2).$$

Therefore we have  $(a_1, a_2) \in \mathcal{F}_{f^*,\mathbb{Z}}$ . If  $c_1 = -c_3$  then  $f^* = f$  and we can create the chain in the same way as before. In any case we may proceed to get  $a_3 \in \mathbb{Z}$  calculated by the formula (4) with  $f^*$  instead of  $f$  such that  $(a_2, a_3) \in \mathcal{F}_{f^{**},\mathbb{Z}}$ . One can straightforwardly check that  $f^{**} = f$ .

The upshot of the above arguments is that every pair  $(a_0, a_1) \in \mathcal{F}_{f,\mathbb{Z}}$  defines the chain  $\mathcal{C}_f(a_0, a_1)$  of pairs in  $\mathcal{F}_{f,\mathbb{Z}}$  which can be defined as follows

$$\mathcal{C}_f(a_0, a_1) := \left\{ (a_i, a_{i+1}) : i \in \mathbb{Z}, a_{i+1} = \frac{(f(a_i) - 1)/a_i - a_{i-1}}{a_ia_{i-1} + 1} \right\} \quad \text{if } f^* = f$$

or

$$\mathcal{C}_f(a_0, a_1) := \left\{ (a_{2i}, a_{2i+1}) : i \in \mathbb{Z}, \begin{aligned} a_{2i+1} &= \frac{(f^*(a_{2i}) - 1)/a_{2i} - a_{2i-1}}{a_{2i}a_{2i-1} + 1}, \\ a_{2i+2} &= \frac{(f(a_{2i+1}) - 1)/a_{2i+1} - a_{2i}}{a_{2i+1}a_{2i} + 1} \end{aligned} \right\} \quad \text{otherwise.}$$

In the first case we have  $(a_1, a_0) \in \mathcal{F}_{f,\mathbb{Z}}$  and  $\mathcal{C}_f(a_1, a_0) = \{(a_{i+1}, a_i)\}_{i \in \mathbb{Z}}$ . In the second case  $(a_2, a_1) \in \mathcal{F}_{f,\mathbb{Z}}$  and  $\mathcal{C}_f(a_2, a_1) = \{(a_{2i}, a_{2i-1})\}_{i \in \mathbb{Z}}$ .

In the case of  $f(x) = x^4 + 1$  we showed that every chain  $\mathcal{C}(a_0, a_1)$  must contain  $a_k = 0$  which in turn allowed us to classify all the pairs in  $\mathcal{F}$ . In the case of general  $f$  of degree 4 unfortunately it is not always true. However we will show that a complete classification of elements of  $\mathcal{F}_f$  can still be constructed. It may contain several other infinite series of chains  $\mathcal{C}_f(a_0, a_1)$  together with finitely many exceptional chains.

Firstly if  $(a_0, a_1) \in \mathcal{F}_f$ ,  $a_0, a_1 > 0$  and  $f(a_1) > 0$  then by (3) we must have  $a_2 \geq 0$ . Further, if  $f^* \neq f$ ,  $a_2 > 0$  and  $f^*(a_2) > 0$  then by the same arguments we also have  $a_3 \geq 0$ . This observation leads to the following statement

**Lemma 2** *Let  $(a_0, a_1) \in \mathcal{F}_f$ . If the sequence  $\{a_i\}_{i \in \mathbb{Z}}$  from the chain  $\mathcal{C}_f(a_0, a_1)$  switches the sign then it must contain an element  $a \in \mathbb{N}$  such that either  $a = 0$ ,  $f(a) \leq 0$  or  $f^*(a) \leq 0$ .*

Both inequalities  $f(a) \leq 0$  and  $f^*(a) \leq 0$  have only finitely many natural solutions. By considering the factorizations of  $f(a)$  we can find all chains which contain  $a$ . There are

finitely many of them if  $f(a) < 0$ . Now consider the case  $f(a) = 0$ . Since  $f$  is a monic polynomial with free coefficient equal one, it may happen only for  $a = 1$ . In that case  $f(1) = 0$  and therefore for every  $b \in \mathbb{N}$  the pair  $(b, 1)$  is in  $\mathcal{F}_f$ .

It may also happen that the sequence  $\{a_i\}_{i \in \mathbb{Z}}$  from the chain  $\mathcal{C}_f(a_0, a_1)$  contains strictly positive elements only. In that case there must be  $k \in \mathbb{Z}$  such that  $a_{k-1} \geq a_k \leq a_{k+1}$ . To find all the solutions of this type we change the variables  $a_{k-1} = a_k + d_1, a_{k+1} = a_k + d_2$  where  $d_1, d_2 \in \mathbb{Z}_{\geq 0}$ . Then (3) is written as

$$((a_k + d_1)a_k + 1)((a_k + d_2)a_k + 1) = \begin{cases} f(a_k) & \text{if } k \text{ is odd;} \\ f^*(a_k) & \text{if } k \text{ is even} \end{cases}$$

which after simplifications appears to be

$$(d_1 + d_2)a_k^2 + (2 + d_1d_2)a_k + (d_1 + d_2) = \begin{cases} c_1a_k^2 + c_2a_k + c_3 & \text{if } k \text{ is odd;} \\ -c_3a_k^2 + c_2a_k - c_1 & \text{if } k \text{ is even.} \end{cases} \quad (5)$$

This equation can have solutions  $a_t \in \mathbb{N}$  only if one of the following inequalities is true:

$$\left[ \begin{array}{l} d_1 + d_2 \leq c_1; \\ d_1d_2 \leq c_2 - 2; \\ d_1 + d_2 \leq c_3. \end{array} \right] \quad \text{for } k \text{ odd or} \quad \left[ \begin{array}{l} d_1 + d_2 \leq -c_3; \\ d_1d_2 \leq c_2 - 2; \\ d_1 + d_2 \leq -c_1. \end{array} \right] \quad \text{for } k \text{ even.} \quad (6)$$

In both cases we have finitely many pairs  $d_1, d_2$  which satisfy one of these inequalities. For each of that pairs  $d_1, d_2$  we have either up to two solutions  $a_k$  of the equation (5) or infinitely many of them if it becomes an identity, i.e. if for some pair  $d_1, d_2$  we have  $d_1d_2 = c_2 - 2$  and  $d_1 + d_2 = c_1 = c_3$  or  $d_1 + d_2 = -c_1 = -c_3$ . In the last case we again have an infinite series of pairs  $(a_k + d_1, a_k) \in \mathcal{F}_f$  if  $k$  is odd or  $(a_k, a_k + d_1) \in \mathcal{F}_f$  if  $k$  is even.

Finally if non of the above happens then the chain must contain zero at some point.

Now we can provide the algorithm which finds all possible chains  $\mathcal{C}_f(a_0, a_1)$  with  $a_0, a_1 \in \mathbb{N}$ . It in turn classifies all pairs  $(a_0, a_1) \in \mathcal{F}_f$ .

1. If  $f(1) = 0$  then there is an infinite series of chains  $\mathcal{C}_f(n, 1) \subset \mathcal{F}_{f, \mathbb{Z}}, n \in \mathbb{N}$ .
2. If  $f^*(1) = 0$  then there is another infinite series of chains  $\mathcal{C}_f(1, n) \in \mathcal{F}_{f, \mathbb{Z}}, n \in \mathbb{N}$ .
3. For each  $a_1 \in \mathbb{N}$  such that  $f(a_1) < 0$  find all possible pairs  $(a_0, a_1) \in \mathcal{F}_f$  by considering all the factorizations of  $f(a_1)$  as a product of two integers. there will be finitely many of them. Each of that pairs generates the chain  $\mathcal{C}_f(a_0, a_1) \subset \mathcal{F}_{f, \mathbb{Z}}$ .
4. Do the same for each  $a_1 \in \mathbb{N}$  such that  $f^*(a_1) < 0$ . It may give additional chains  $\mathcal{C}_f(a_1, a_0) \in \mathcal{F}_{f, \mathbb{Z}}$ .
5. For each of the pairs  $d_1, d_2 \in \mathbb{N}^2$  satisfying (6) solve the corresponding equation (5).
  - If for some  $d_1, d_2$  the equation becomes an identity then we have another infinite series of chains:  $\mathcal{C}_f(n+d_1, n), n \in \mathbb{N}$  for the first equation ( $k$  is odd) or  $\mathcal{C}_f(n, n+d_1), n \in \mathbb{N}$  for the second one ( $k$  is even).
  - For other solutions we get finitely many new pairs  $(a, a+d_1) \in \mathcal{F}_f$  or  $(a+d_1, a) \in \mathcal{F}_f$  depending on the equation. Both of them lead to the corresponding chains.
6. Finally we have the last infinite series of chains  $\mathcal{C}_f(0, n) \subset \mathcal{F}_{f, \mathbb{Z}}$  and  $\mathcal{C}_f(n, 0) \subset \mathcal{F}_{f, \mathbb{Z}}, n \in \mathbb{N}$ .

### 3.2 Monic polynomials of higher degrees

We still consider monic polynomials with free coefficient 1. As before in this case the elements of  $\mathcal{F}_f$  come in chains  $\mathcal{C}_f(a_0, a_1)$  where  $(a_0, a_1) \in \mathcal{F}_f$ . However if the degree of  $f$  is bigger than four then we only manage to classify some of the chains.

Here we restrict ourselves to the polynomials  $f_t(n) = n^{2^t} + 1$ . Since every divisor  $d$  of fermat number  $F_m$  is of the form  $d \equiv 1 \pmod{2^{m+2}}$  then the pair

$$\left(\frac{d-1}{2^{2^d}}, 2^{2^d}\right)$$

belongs to  $\mathcal{F}_{f_{m-d}}$  where  $2^d$  is the largest power of two not exceeding  $m+2$ . Therefore the sets  $\mathcal{F}_{f_t}$  are of the particular interest since they provide us with all the divisors of Fermat numbers. In particular, the pair  $(1071, 256) \in \mathcal{F}_{f_3}$  represents the divisor  $1071 \cdot 2^8 + 1$  of  $F_6$ .

By repeating the same arguments as in Section 2 one can check that any pair  $(a_0, a_1) \in \mathcal{F}_{f_t}$  generates the chain  $\mathcal{C}_{f_t}(a_0, a_1) = \{(a_k, a_{k+1})\}_{k \in \mathbb{Z}}$  of pairs from  $\mathcal{F}_{f_t, \mathbb{Z}}$  defined as follows

$$a_{k+1} := \frac{a_k^{2^t-1} - a_{k-1}}{a_{k-1}a_k + 1}. \quad (7)$$

There are chains which are generated by pairs  $(0, n)$  for any  $n \in \mathbb{N}$  (since any integer is divisible by one). However for  $t > 2$  there are many other chains which do not contain pairs  $(0, n)$ . In particular one can find that the chain generated by the pair  $(1071, 256) \in \mathcal{F}_{f_3}$  is

$$\dots, 5895155641970255, 1071, 256, 262814145745, \dots$$

with the smallest element 256 and monotonically increasing in both directions.

Easy checks show that the pairs  $(n^3, n^{2^t-3}), (n^5, n^{2^t-5}), \dots, (n^{2^t-1}, n^{2^t+1})$  also belong to  $\mathcal{F}_{f_t}$  and therefore generate the chains. We call all of these chains together with those generated by  $(0, n)$  standard. The following result shows that all nontrivial divisors  $2^m n + 1$  of  $2^{2^t \cdot m} + 1$  are associated with nonstandard chains.

**Theorem 3** *Consider the chain  $\mathcal{C}_{f_t}(a_0, a_1) = \{(a_k, a_k + 1)\}_{k \in \mathbb{Z}}$ . For  $a_0 = 0, a_1 = n$  all solutions to the Diophantine equation*

$$a_k = 2^m$$

*are as follows:*

$$n = 2^d, k = 1, m = d; \quad n = 2^d, k = 2, m = (2^t - 1)d.$$

*For  $a_0 = n^{2k+1}, a_1 = n^{2^t-2k-1}$  all solutions to the Diophantine equation*

$$a_k = 2^m$$

*are as follows:*

$$n = 2^d, k = 1, m = (2k + 1)d; \quad n = 2^d, k = 2, m = (2^t - 2k - 1)d.$$

**PROOF.** The first part of the theorem can be proven analogously to Theorem 2. Let  $a_0 = 0$  and  $a_1 = n$ . By considering  $f_0(x) = 0, f_1(x) = x$  and

$$f_{k+1}(x) := \frac{f_k^{2^t-1}(x) - f_{k-1}(x)}{f_{k-1}(x)f_k(x) + 1}$$

we show that  $f_a(x)|f_b(x)$  if and only if  $a|b$  (compare with Lemma 1). It implies that the solution  $a_k = 2^m$  can only exist if  $n$  is a power of two,  $n = 2^d$ . Next, by looking at  $a_k$  modulo  $2^{(2^t-1)d}$  we check that  $a_k$  can not be a power of two for odd  $k$ . Finally we show that  $a_4$  is not a power of two. By (7) we get that

$$a_3 \equiv -n \pmod{n^{2^t+1}}, a_4 \equiv -2n^{2^t-1} \pmod{n^{2^t+1}}$$

So the biggest power of two which divides  $a_4$  is  $2n^{2^t-1}$  which is certainly less than  $a_4$ . Therefore  $a_4$  can not be a power of two as well. By representing  $k$  as  $k = 2^u k_0$  with odd  $k_0$  we get that for  $k > 2$ ,  $a_k$  is divisible by either  $a_{k_0}$  for  $k_0 > 1$  or by  $a_4$ . In any case,  $a_k \neq 2^m$ .

For the chains generated by  $a_0 = n^{2k+1}$ ,  $a_1 = n^{2^t-2k-1}$  with  $1 \leq k \leq 2^{t-1}$ ,  $n > 1$  we firstly check that as  $i > 0$  the sequence  $a_i$  monotonically increases. This is easily verified from (7). By looking at the chain  $\mathcal{C}_{f_t}(a_1, a_0)$  we also get that for  $i < 0$  the sequence  $a_i$  monotonically decreases. Therefore the smallest term of the chain  $\mathcal{C}_{f_t}(a_0, a_1)$  is  $a_0$ . Moreover one can check that

$$a_{-1} = (n^{2^t \cdot 2k} + n^{2^t \cdot (2k-1)} + \dots + n^{2^t})/n^{2k+1}$$

is also bigger than  $a_1$ . So  $a_1$  is the second smallest term of the chain  $\mathcal{C}_{f_t}(a_0, a_1)$ .

Next we show that for even  $i$ , the exact power of  $n$  which divides  $a_i$  is  $2k+1$ . Therefore for  $a_i$  to be a power of two,  $n$  has to be a power of two:  $n = 2^d$ . And since all other values  $a_i$  bigger than  $a_0 = n^{2k+1}$  the only power of two among them is  $a_0$ .

Similar observation works for odd  $i$  as well. In this case the exact power of  $n$  which divides  $a_i$  is  $2^t - 2k - 1$ . Since  $a_1 = n^{2^t-2k-1}$  is the smallest among other  $a_i$  it is the only possible power of two. □

Theorem 3 shows that the divisors of Fermat numbers should be searched among non-standard chains. Unfortunately we don't know how to classify all of them. From (3) one can get that for every non-standard chain  $\mathcal{C}_{f_t}(a_0, a_1)$  there exists  $k \in \mathbb{N}$  such that  $\dots > a_{k-2} > a_{k-1} > a_k \leq a_{k+1} < a_{k+2} \dots$ . Since  $\mathcal{C}_{f_t}(a_k, a_{k+1}) = \mathcal{C}_{f_t}(a_0, a_1)$  and  $\mathcal{C}_{f_t}(a_k, a_{k-1})$  contains the same elements as  $\mathcal{C}_{f_t}(a_0, a_1)$  but in reverse order then without loss of generality one can assume that  $a_0 \leq a_1$  and that these two elements are the smallest elements in the chain. In further discussion we will assume that this condition on  $(a_0, a_1) \in \mathcal{F}_{f_t}$  is satisfied.

For  $t = 3$  we conducted a search of all chains  $\mathcal{C}_{f_3}(a_0, a_1)$  for small  $a_0$  and  $a_1$ . By looking for the divisors  $a_0 a_1 + 1 \mid a_0^8 + 1$  we found all chains  $\mathcal{C}_{f_3}(a_0, a_1)$  with  $a_0 \leq 10^6$ . Additionally by noticing that  $a_0 \equiv -1/a_1 \pmod{a_0 a_1 + 1}$  one can get

$$0 \equiv a_0^4 + a_1^4 \equiv (a_0^2 + a_1^2)^2 - 2 \equiv ((a_0 + a_1)^2 + 2)^2 - 2 \pmod{a_0 a_1 + 1}.$$

Then by looking for the factors  $d$  of  $(s^2 + 2)^2 - 2$  such that  $d = kn + 1$  with  $k + n = s$  we found all the chains  $\mathcal{C}_{f_3}(a_0, a_1)$  with  $a_0 + a_1 \leq 10^7$ . In total we have got 201 different chains. The first three of them are

$$\begin{aligned} &\dots, 22787805757, 64, 3, 11, 573152, \dots \\ &\dots, 21620, 8, 12, 369400, \dots \\ &\dots, 418776, 16, 40, 255600624, \dots \end{aligned}$$

The only infinite collection of non-standard chains we were able to construct is generated as follows.

**Theorem 4** *Let positive integers  $t$  and  $d$  satisfy the Diophantine equation*

$$d^2 - 2t^2 = -7. \tag{8}$$

*Then  $\left(\frac{t(d-1)}{2}, \frac{t(d+1)}{2}\right) \in \mathcal{F}_{f_3}$ .*

For convenience we denote the chains  $\mathcal{C}_{f_3} \left( \frac{t(d-1)}{2}, \frac{t(d+1)}{2} \right)$  by  $\mathcal{C}_{t,d}$ .

PROOF. Firstly note that since  $a_0 \equiv -1/a_1 \pmod{a_0 a_1 + 1}$  we get

$$(a_0, a_1) \in \mathcal{F}_{f_3} \Leftrightarrow a_0 a_1 + 1 \mid a_0^4 + a_1^4.$$

Then by considering the equation  $d^2 - 2t^2 = -7$  modulo 8 one can get that  $2 \mid t$  and therefore both values  $t(d \pm 1)/2$  are integers. Next, we have

$$\frac{t(d-1)}{2} \cdot \frac{t(d+1)}{2} + 1 = \frac{t^2(d^2-1)}{4} + 1 = \frac{(d^2+7)(d^2-1)}{8} + 1 = \frac{d^4 + 6d^2 + 1}{8}.$$

and

$$\frac{t^4(d-1)^4}{16} + \frac{t^4(d+1)^4}{16} = t^4 \cdot \frac{d^4 + 6d^2 + 1}{8}.$$

So the first value always divides the second one. \(\square\)

Equation (8) is a Pell-type equation. One can check that its solutions can be found by one of the formulae:

$$(1 + 2\sqrt{2}) \cdot (3 + 2\sqrt{2})^n = d_{1,n} + \sqrt{2} \cdot t_{1,n}$$

or

$$(5 + 4\sqrt{2}) \cdot (3 + 2\sqrt{2})^n = d_{2,n} + \sqrt{2} \cdot t_{2,n}.$$

It seems that there are still infinitely many non-standard chains  $\mathcal{C}_{f_3}(a_0, a_1)$  which are not of the form  $\mathcal{C}_{t,d}$ . However we do not know the formal proof of that.

Consider the equation  $a_n = 2^m$  where  $a_n$  is associated to some chain  $\mathcal{C}_{f_3}(a_0, a_1) \subset \mathcal{F}_{f_3}$ . Every its integer solution  $(n, m)$  gives a factorization of  $2^{8m} + 1$  into the product of non-trivial factors. Among the 201 non-standard constructed chains there are 8 solutions to this equation with  $a_n < 2^{4000}$  which lead to the following factorizations:

$$\begin{array}{l|l} 2^{48} + 1 = (3 \cdot 2^6 + 1) \cdot (22787805757 \cdot 2^6 + 1) & 2^{24} + 1 = (12 \cdot 2^3 + 1) \cdot (369400 \cdot 2^3 + 1) \\ 2^{32} + 1 = (40 \cdot 2^4 + 1) \cdot (418776 \cdot 2^4 + 1) & 2^{24} + 1 = (84 \cdot 2^3 + 1) \cdot (3116 \cdot 2^3 + 1) \\ 2^{64} + 1 = (1071 \cdot 2^8 + 1) \cdot (262814145745 \cdot 2^8 + 1) & 2^{80} + 1 = (405 \cdot 2^{10} + 1) \cdot (2846712900280939 \cdot 2^{10} + 1) \\ 2^{48} + 1 = (197635 \cdot 2^6 + 1) \cdot (347709 \cdot 2^6 + 1) & 2^{80} + 1 = (26542549 \cdot 2^{10} + 1) \cdot (43436728875 \cdot 2^{10} + 1). \end{array}$$

The next theorem gives some necessary conditions for the chain  $\mathcal{C}_{f_3}(a_0, a_1)$  to contain a power of two.

**Theorem 5** *Let  $\mathcal{C}_{f_3}(a_0, a_1) = \{(a_k, a_{k+1})\}_{k \in \mathbb{N}}$ . Then the necessary conditions for  $a_k = 2^m$  to have a solution in integers  $k, m$  are*

1.  $\gcd(a_0, a_1) = 2^d$  for  $d \in \mathbb{Z}_{\geq 0}$ .
2. Let  $a_0 = 2^{d_0} a'_0$ ,  $a_1 = 2^{d_1} a'_1$  with odd  $a'_0, a'_1$ . Then one of the following must be true:
  - $d_1 \geq 7d_0$  or  $d_0 \geq 7d_1$ ;
  - $a'_0 = 1$  or  $a'_1 = 1$ . If additionally we have  $d_1/7 < d_0 < 7d_1$  then the only solutions to the equation above are  $a_0 = 2^{d_0}$  or  $a_1 = 2^{d_1}$ .

PROOF. From (3) one gets

$$a_{k+1} = \frac{a_k^7 - a_{k-1}}{a_k a_{k-1} + 1}; \quad a_{k-1} = \frac{a_k^7 - a_{k+1}}{a_k a_{k+1} + 1}.$$

By that formulae if for some prime  $p > 2$ ,  $p \mid \gcd(a_0, a_1)$  then  $p$  divides every element  $a_k$  in the chain and therefore  $a_k$  is not a power of two.

Next, with help of the same formulae one can easily check that if  $d_0 < 7d_1$  and  $d_1 < 7d_0$  then the exact power of two which divides  $a_{2k}$  is  $2^{d_0}$  and the exact power of two which divides  $a_{2k+1}$  is  $2^{d_1}$ . Since  $a_0$  and  $a_1$  are two smallest elements of the chain  $\mathcal{C}_{f_3}(a_0, a_1)$  then the only possibility for the equation  $2^m = a_k$  to have integer solutions is if  $a_1$  or  $a_0$  are powers of two.  $\boxtimes$

Among 201 chains mentioned above only 62 of them satisfy the conditions of Theorem 5, so further investigation is needed to find all powers of two they contain.

In the end of this chapter we find all the solutions of the equation  $a_k = 2^m$  for the elements of the chains  $\mathcal{C}_{t,d}$  from the infinite collection mentioned above.

**Theorem 6** *Let  $\mathcal{C}_{t,d} = \{(a_k, a_{k+1})\}_{k \in \mathbb{Z}}$  where  $(a_0, a_1) = t(d \pm 1)/2$  and  $t, d$  satisfy (8). Then the only solution to  $a_k = 2^m$  in integers is  $a_0 = 8$  for  $\mathcal{C}_{4,5}$ .*

PROOF. Notice that for  $(a_0, a_1) \in \mathcal{C}_{t,d}$ ,  $t/2$  divides  $\gcd(a_0, a_1)$ . Therefore by Theorem 5 for  $a_k = 2^m$  to have solutions the parameter  $t$  must be a power of two:  $t = 2^u$ . This leads us to the variation of Ramanujan-Nagell equation:  $2^{2u+1} - 7 = d^2$ . Its solutions [7] are  $(t, d) = (4, 5), (8, 11)$  and  $(128, 181)$ . For each of these chains  $\mathcal{C}_{t,d}$  the parameters  $d_1$  and  $d_2$  from Theorem 5 satisfy  $d_0/7 < d_1 < 7d_0$ . So if there are solutions to  $a_k = 2^m$  they must be among  $a_0$  or  $a_1$ . Easy checks show that only the chain  $\mathcal{C}_{4,5}$  has  $a_0 = 8$ , so this is the only solution to the above equation for the elements of the chains  $\mathcal{C}_{t,d}$ .  $\boxtimes$

### 3.3 Non-monic polynomials or polynomials with free coefficient not equal to one

If we consider the polynomial  $f(x) \in \mathbb{Z}[x]$  in the most general form  $f(x) = c_0 + c_1x + \dots + c_dx^d$  with either  $c_0$  or  $c_d$  not equal to one then we can not construct the chain  $\mathcal{C}_f(a_0, a_1)$  containing the pairs from  $\mathcal{F}_f$  anymore. However we can still get some results. In this section we will stick our attention to one example  $f(x) = 2x^4 + 1$ , however similar arguments will work for many other polynomials  $f$ . We will show that the set  $\mathcal{F}_f$  is still infinite and we'll provide an efficient way to find all elements of  $\mathcal{F}_f$  up to a given limit.

Consider  $a_0, a_1 \in \mathbb{N}$  such that  $a_0a_1 + 1 \mid 2a_1^4 + 1$ . Then as before we have

$$2a_1^4 + 1 = (a_0a_1 + 1) \cdot (a_2a_1 + 1). \quad (9)$$

Since this equation is symmetric for  $a_0$  and  $a_2$ , without loss of generality one can assume that  $a_2 \leq a_0$ . By considering this equation modulo  $a_2a_1 + 1$  we get that  $a_1 \equiv -1/a_2$  and then  $a_1a_2 + 1 \mid a_2^4 + 2$ . This gives us another equation

$$a_2^4 + 2 = (a_1a_2 + 1) \cdot (a_2a_3 + 2)$$

which is different to (9). Now the situation splits in two cases. In the first case  $a_2$  is odd, this immediately implies that  $a_3$  is odd too and then we can write  $a_2 \equiv -2/a_3 \pmod{a_2a_3 + 2}$ . Another case  $a_2 \equiv 0 \pmod{2}$  will be considered later.

**Proposition 1** *Let  $a_0, a_1, a_2 \in \mathbb{Z}$  be such that  $2a_1^4 + 1 = (a_0a_1 + 1) \cdot (a_2a_1 + 1)$  and  $a_2$  is odd. Then there exists a sequence  $\mathcal{C}_f^*(a_0, a_1) = \{a_i\}_{i \in \mathbb{Z}_{\geq 0}} \subset \mathbb{Z}$  such that its elements satisfy the equalities*

$$a_k^4 + 2^{2k-3} = (a_{k-1}a_k + 2^{k-2}) \cdot (a_k a_{k+1} + 2^{k-1}), \quad a_k \equiv 1 \pmod{2} \quad \forall k \geq 2. \quad (10)$$

PROOF. One can prove it by induction. The case  $k = 2$  has already been shown. Now assume that  $a_{k-1}, a_k$  and  $a_{k+1}$  satisfy (10) and prove it for  $a_k, a_{k+1}, a_{k+2}$ . Firstly  $a_{k+1}$  must be odd since  $a_k a_{k+1} + 2^{k-1}$  is a factor of odd number  $a_k^4 + 2^{2k-3}$ . Secondly  $a_{k+1} \equiv -2^{k-1}/a_k \pmod{a_k a_{k+1} + 2^{k-1}}$  therefore

$$a_k^4 + 2^{2k-3} \equiv \frac{2^{4k-4} + 2^{2k-3} a_{k+1}^4}{a_{k+1}^4} \pmod{a_k a_{k+1} + 2^{k-1}}.$$

The last expression is zero modulo  $a_k a_{k+1} + 2^{k-1}$  if and only if  $a_{k+1}^4 + 2^{2k-1} \equiv 0 \pmod{a_k a_{k+1} + 2^{k-1}}$ . Therefore

$$a_{k+1}^4 + 2^{2k-1} = (a_k a_{k+1} + 2^{k-1}) \cdot d$$

for some integer  $d$ . Finally consider the last equation modulo  $a_{k+1}$  to get  $d \equiv 2^k \pmod{a_{k+1}}$  which finishes the proof.  $\square$

Note that every argument in the proposition works in both ways. So if one can construct the pair  $(a_k, a_{k+1})$  such that  $a_k a_{k+1} + 2^{k-1} \mid a_k^4 + 2^{2k-3}$  then it will give us the element  $(a_0, a_1) \in \mathcal{F}_f$ .

One can check that if  $a_{k-1} > a_k > 0$  then  $a_k > a_{k+1}$ . Moreover if  $a_{k+1} > 0$  then

$$a_{k-1}/a_k < a_k/a_{k+1}. \quad (11)$$

Indeed it follows from (10) that  $a_k^4 > a_k^2 a_{k-1} a_{k+1}$  which immediately implies (11). The last observation shows that if we have  $a_1 > a_2$  then sooner or later we must get  $a_{k+1} \leq 0$  for some  $k \in \mathbb{N}$ . It means that in (10) we will get

$$a_k^4 + 2^{2k-3} = (a_{k-1} a_k + 2^{k-2}) \cdot d \quad (12)$$

where  $d = a_k a_{k+1} + 2^{k-1}$  with  $1 \leq d \leq 2^{k-1}$ . One can easily make a search over all possible values  $d$  for small  $k$  to find all triples  $a_{k-1}, a_k, a_{k+1}$  which satisfy (10) with  $a_{k+1} \leq 0$ . At least one such a triple exists for every  $k$ . Indeed one can take  $d = 1$  and  $a_k = 2^{k-1} - 1, a_{k+1} = -1$ . This simple observation immediately shows that the set  $\mathcal{F}_f$  is infinite.

Let's turn back to the initial equation (9) and look at it from slightly different point of view. By  $a_2 \equiv -1/a_1 \pmod{a_1 a_2 + 1}$  one can get that

$$2a_1^2 + a_2^2 = c \cdot (a_1 a_2 + 1) \quad (13)$$

for some integer  $c$ . This equation becomes quadratic over  $a_1$  and  $a_2$ . By solving it for  $a_2$  we get the discriminant  $D = (c^2 - 8)a_1^2 + 4c$ . We are considering the case when  $a_2$  is odd therefore  $a_1$  in this case must be even  $a_1 = 2a_1^*$ . The equation (13) has a solution in integer  $a_2$  if and only if the discriminant  $D$  is a perfect square. This gives us another Diophantine equation

$$(c^2 - 8)a_1^{*2} + c = d^2. \quad (14)$$

A quick search shows that this equation does not have solutions in natural  $a_1^*$  if  $c^2 < 8$ . Also  $c^2 - 8$  can be a perfect square only for  $c = 3$  and the equation for  $c = 3$ :  $a_2^{*2} + 3 = d^2$  has only one solution  $a_1^* = 1$  which corresponds to  $(a_0, a_1) = (5, 2), (1, 2) \in \mathcal{F}_f$ . In further discussion we assume that  $c \geq 4$  and then the equation (14) is of Pell's type. For a fixed  $c \in \mathbb{N}$  it either has no solutions at all or has infinitely many solutions. Next, since for  $c > 3$

$$\left| d - \sqrt{c^2 - 8} \cdot a_1^* \right| = \frac{c}{d + \sqrt{c^2 - 8} \cdot a_1^*} < \frac{c}{2\sqrt{c^2 - 8}} \cdot \frac{1}{a_1^*} < \frac{1}{a_1^*}.$$

In other words  $\sqrt{c^2 - 8}$  is approximated by the fraction  $d/a_1^*$  very well. We can search for all such good rational approximations with help of the following theorem (see [8]):

**Theorem R** *Let  $\alpha \in \mathbb{R}$ . If a rational  $p/q$  satisfies inequality*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$$

*then  $p/q$  must be one of the following forms*

$$\frac{p_n}{q_n}, \quad \frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \quad \frac{p_n - p_{n-1}}{q_n - q_{n-1}}$$

*where  $p_n/q_n$  is  $n$ th convergent of  $\alpha$ .*

Since we can quickly compute the convergents of  $\sqrt{c^2 - 8}$ , Theorem R shows that for a fixed  $c$  one can find all the solutions of (14) up to a given limit very fast.

Consider the solution  $a_1, a_2$  of (13). Then we have  $2a_1^2 + a_2^2 > ca_1a_2$  and therefore

$$\frac{a_1}{a_2} \geq \frac{c + \sqrt{c^2 - 8}}{2} \quad \text{or} \quad \frac{a_1}{a_2} \leq \frac{c - \sqrt{c^2 - 8}}{2}.$$

Since  $c \geq 4$  those estimates in particular mean that either  $2a_2 < a_1$  or  $a_2 > 2a_1$ . However the second inequality  $a_2 > 2a_1$  is impossible because then the equation (9) with  $a_0 \geq a_2$  does not have solutions.

Now we are ready to present the efficient algorithm for finding all the elements  $(a_1, a_2) \in \mathcal{F}_f$  with the condition that  $a_2$  is odd. Assume that we want to find all such elements up to some limit  $L$ :  $a_1 \leq L$ .

1. We firstly find all the solutions of (14) for every  $c$  in the range  $4 \leq c \leq C$  and  $a_1^* \leq L/2$ .
2. All other pairs  $(a_1, a_2)$  not found in the previous step must satisfy

$$\frac{a_1}{a_2} \geq \delta := \frac{C + \sqrt{C^2 - 8}}{2}.$$

Further since  $a_{k-1}/a_k$  is monotonically decreasing as soon as  $a_k$  is positive, then there must be a natural number  $k \leq \lceil \log_\delta L \rceil$  for which  $a_k < 0$ . So for each  $k$  in that range we look for the solutions  $a_k$  of (12) with  $1 \leq d \leq 2^{k-1}$ .

To keep the balance between the complexity of the first and the second step of the algorithm one can choose  $C \asymp \exp(\sqrt{\log L})$ .

We conducted a search of the solutions  $(a_1, a_2)$  of the equation (14) with  $c \leq 2^{31}$  and  $a_1 \leq 2^{1000}$ . This gave us 2698 pairs  $(a_1, a_2) \in \mathcal{F}_f$ . For other pairs  $(a_1, a_2) \in \mathcal{F}_f$  we must have  $a_k < 0$  for some  $k \leq \lceil \log_\delta 2^{1000} \rceil = 33$ . Finally we also find all solutions of (12) with  $k \leq 33$ . This gave us extra 315 pairs  $(a_1, a_2)$ . Only one solution gives us  $a_1$  equal to a power of two. It corresponds to  $c = 3$  and  $(a_1, a_2) = (2, 1), (2, 5)$ . So the division

$$2^n \cdot a + 1 \mid 2^{4n+1} + 1, \quad a \equiv 1 \pmod{2}$$

has only one solution for  $n \leq 1000$ . It is  $2^5 + 1 = 3 \cdot 11$ .

Now we concentrate on the remaining case when  $a_2$  is odd,  $a_2 = 2a_2^*$ . For convenience from this point we will write  $a_2$  instead of  $a_2^*$ . Also notice that the reduction of (9) modulo  $2a_1$  gives us that  $a_0$  must be even as well. In this situation we can construct the chain very similar to that for monic polynomials with free coefficient equal to 1. Indeed this chain is constructed by the following procedure

$$\begin{aligned} 2a_1a_2 + 1 \mid 2a_1^4 + 1 &\Leftrightarrow 2a_1a_2 + 1 \mid 8a_2^4 + 1. \\ \Leftrightarrow 8a_2^4 + 1 = (2a_2a_1 + 1)(2a_2a_3 + 1) &\Leftrightarrow 2a_2a_3 + 1 \mid 2a_3^4 + 1. \end{aligned}$$

This observation leads to

**Proposition 2** Let  $a_0, a_1, a_2 \in \mathbb{Z}$  be such that  $2a_1^4 + 1 = (2a_0a_1 + 1) \cdot (2a_2a_1 + 1)$ . Then there exists a sequence  $\tilde{\mathcal{C}}_f(a_0, a_1) = \{a_i\}_{i \in \mathbb{Z}_{\geq 0}} \subset \mathbb{Z}$  such that its elements satisfy the equalities

$$2a_{2k+1}^4 + 1 = (2a_{2k}a_{2k+1} + 1) \cdot (2a_{2k+1}a_{2k+2} + 1), \quad \forall k \geq 1; \quad (15)$$

$$8a_{2k}^4 + 1 = (2a_{2k-1}a_{2k} + 1) \cdot (2a_{2k}a_{2k+1} + 1), \quad \forall k \geq 1. \quad (16)$$

If all terms in the equations (15) and (16) are positive then we have

$$a_{2k+1}^2 > 2a_{2k}a_{2k+2} \quad \text{and} \quad 2a_{2k}^2 > a_{2k-1}a_{2k+1}.$$

Therefore if  $a_0, a_1, a_2$  are positive then by possibly swapping  $a_0$  and  $a_2$  one guarantees that  $\sqrt{2}a_2 < a_1$  and then  $0 \leq a_3 < \sqrt{2}a_2 < a_1$ . By repeating the same arguments we get that if  $a_{2k-1}, a_{2k} > 0$  then  $0 \leq a_{2k+1} < \sqrt{2}a_{2k} < a_{2k-1}$  and if  $a_{2k}, a_{2k+1} > 0$  then  $0 \leq \sqrt{2}a_{2k+2} < a_{2k+1} < \sqrt{2}a_{2k}$ . Therefore  $a_1, a_3, \dots$  as well as  $a_2, a_4, \dots$  are strictly decreasing and sooner or later we must have  $a_k = 0$  for some  $k \in \mathbb{N}$ .

Since surely  $2 \cdot 0 \cdot n + 1 \mid 2n^4 + 1$  as well as  $2 \cdot 0 \cdot n + 1 \mid 8n^4 + 1$  we have  $(n, 0) \in \mathcal{F}_f$  and  $(n, 0) \in \mathcal{F}_{f^*}$  where  $f^*(x) = 8x^4 + 1$ . Define  $f_0(x) = f_0^*(x) = 0$ ,  $f_1(x) = f_1^*(x) = x$  and

$$f_{2k}(x) = \frac{f_{2k-1}(x)^3 - f_{2k-2}(x)}{2f_{2k-1}(x)f_{2k-2}(x) + 1}, \quad f_{2k+1}(x) = \frac{4f_{2k}(x)^3 - f_{2k-1}(x)}{2f_{2k}(x)f_{2k-1}(x) + 1}; \quad (17)$$

$$f_{2k}^*(x) = \frac{4f_{2k-1}^*(x)^3 - f_{2k-2}^*(x)}{2f_{2k-1}^*(x)f_{2k-2}^*(x) + 1}, \quad f_{2k+1}^*(x) = \frac{f_{2k}^*(x)^3 - f_{2k-1}^*(x)}{2f_{2k}^*(x)f_{2k-1}^*(x) + 1}; \quad (18)$$

Then by using formulae (16) and (15) in backward order we get:

- If  $a_{2k} = 0$  and  $a_{2k-1} = n$  then  $a_1 = f_{2k-1}(n)$ ;
- If  $a_{2k+1} = 0$  and  $a_{2k} = n$  then  $a_1 = f_{2k}^*(n)$ .

With help of this information we now can find all possible divisors of  $2^{4m+1} + 1$  of the form  $2^{m+1}k + 1$ .

**Proposition 3** The only solutions of the Diophantine equations  $f_k(n) = 2^m$  and  $f_k^*(n) = 2^m$  are

$$f_1(2^d) = 2^d, f_2(2^d) = 2^{3d}, f_1^*(2^d) = 2^d \text{ and } f_2^*(2^d) = 2^{3d+2}. \quad (19)$$

PROOF.

The arguments are very similar to that in Subsection 2.1. Analogously to Lemma 1 we show that  $f_a(n) \mid f_b(n) \Leftrightarrow a \mid b \Leftrightarrow f_a^*(n) \mid f_b^*(n)$ . It implies that  $n \mid f_k(n)$  and  $n \mid f_k^*(n)$  for every  $k$ . Therefore for  $f_k(n)$  or  $f_k^*(n)$  to be a power of two one must have  $n = 2^d$ .

If we consider  $f_k(n)$  modulo  $n^3$  we get

$$(f_1(n), f_2(n), f_3(n), \dots) \equiv (n, 0, -n, 0, n, 0, \dots) \pmod{n^3}.$$

The same is true for  $f_k^*(n)$ . Since for  $n \geq 2$  values of  $f_k(n)$  and  $f_k^*(n)$  are strictly growing then they can only be the powers of two if either  $k = 1$  or  $k$  is even. For  $k = 1$  and  $k = 2$  it gives us the solutions (19). The case  $f_k(1) = 2^m$  can be easily ruled out by the observation

$$f_1(1) = 1, f_2(1) = 1, f_3(1) = 1, f_4(1) = 0.$$

Finally if we consider  $f_k^*(1)$  modulo 2 we get

$$(f_1^*(1), f_2^*(1), \dots) \equiv (1, 0, 1, 0, \dots) \pmod{2}$$

Therefore in this case again we must have  $k$  to be even.

Finally we assume that  $k = 2^t k_0$  where  $k_0$  is odd. If  $k_0 \geq 3$  then  $f_{k_0}(n) \mid f_k(n)$  but  $f_{k_0}(n)$  is not a power of two therefore  $f_k(n) = 2^m$  does not have solutions. The same observation works for  $f_k^*(n) = 2^m$ . Thus we get  $k = 2^t$ .

Simple calculations give us

$$f_3(n) = 2n^5 - n, f_4(n) = 2n^3(n^4 - 1).$$

This shows that  $f_4(n)$  is never a power of two and so are  $f_{2^t}(n)$  for  $t \geq 2$ . Analogously

$$f_3^*(n) = n(8n^4 - 1), f_4^*(n) = 8n^3(4n^4 - 1).$$

So  $f_4^*(n)$  is also never a power of two.

⊠

We conclude this section with the following

**Theorem 7** *The only divisors  $2^{n+1}k + 1$  of  $2^{4n+1} + 1$  with  $k \geq 1$  come from the following factorization:*

$$2 \cdot 2^{4(3d+2)} + 1 = (2^{4d+3} + 1) \cdot (2 \cdot 2^{3d+2} \cdot (2^{5d+3} - 2^d) + 1).$$

*There is only one additional pair of divisors of the form  $2^n k + 1$  for  $n \leq 1000$  which comes from*

$$2^5 + 1 = 3 \cdot 11.$$

## References

- [1] R. P. Brent. Factorization of the tenth Fermat number. *Math. Comp.*, V. 68, N. 225, pp. 429 – 451, 1999.
- [2] J. Brillhart, M. Morrison. The factorization of  $F_7$ . *Bull. Amer. Math. Soc.*, V. 77, p. 264, 1971.
- [3] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, S. S. Wagstaff. Factorizations of  $b^n \pm 1$   $b = 2, 3, 5, 6, 7, 10, 11, 12$  Up to High Powers (3rd edition). *Contemporary Math.*, V. 22, 2002.
- [4] The Cunningham Project. <http://homes.cerias.purdue.edu/ssw/cun/index.html>
- [5] M. Křížek, F. Luca, L. Somer. 17 Lectures on Fermat Numbers. New York, Springer, 2001.
- [6] A. K. Lenstra, H. W. Lenstra, M. S. Manasse, J. M. Pollard. The factorization of the ninth Fermat number. *Math. Comp.* V. 61, N. 203, pp. 319 – 349, 1993.
- [7] T. Nagell. The Diophantine equation  $x^2 + 7 = 2^n$ . *Arkiv for Math.* V. 4, issue 2-3, pp. 185 – 187, 1961.
- [8] R. M. Robinson. The approximation of irrational numbers by fractions with odd or even terms. *Duke Math. J.* V. 7, N. 1, pp. 354 – 359, 1940.

Dzmitry A. Badziahin: Department of Mathematics, Durham University,  
Durham, DH1 3LE, England.  
e-mail: dzmitry.badziahin@durham.ac.uk