Solving Some Diophantine Equations Involving Fibonacci Numbers, Catalan Numbers, Ramanujan Function and Factorials

by

Automan Sibusiso Mabaso

Thesis presented in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics

at

University of the Witwatersrand

School of Mathematics

Faculty of Science

Supervisor: Professor Florian Luca

June 2021

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the authorship owner thereof (unless to the extent explicitly otherwise stated) and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: 16 June 2021

Abstract

In this thesis we study some Diophantine equations involving Fibonacci numbers, Catalan numbers, Ramanujan τ-function and Factorials. Since there is no generic method or algorithm that can be used in solving all Diophantine equations, the arithmetic properties of Ramanujan τ-function, Catalan numbers and Fibonacci numbers will play an important role. For some Diophantine equations, we will compare the order at which some small prime, say 2, divides the left and right-hand side of the equation. In some cases, we will use lower bound for nonzero linear forms in logarithms due to Laurent Mignotte and Nesterenko.

Firstly, we solve some Diophantine equations of the form $|\tau(x)| = y$, where τ is the Ramanujan τ–function and x, y are integer variables restricted to values of factorials, Fibonacci numbers and Catalan numbers.

Our study in this thesis also includes an analysis of the Diophantine equation of the form $F_n = \pm\tau(m_1!) \pm \cdots \pm \tau(m_k!)$, where F_n is the nth Fibonacci number and τ is the Ramanujan τ–function. We find some bounds for k, m_k and show that when $k = 2$, the only positive integer solution of the Diophantine equation $F_n = \pm\tau(m_1!) \pm \tau(m_2!)$, where $m_1 \leq m_2$ is $(1, 1, 3)$.

Lastly, we do an analysis on the iterates of the Ramanujan τ–function and come up with some lemmas and propositions with respect to greatest prime factors and counting the number of solutions of some equations involving them.

Dedication

My late Mother and Father, oMbhulazi, Maqhoboza kaSketekete and

ALL 2020 MUT Statistics Tutors

Acknowledgements

I would like to take this opportunity to thank my supervisor, Prof. Florian Luca for his unwavering support in my journey towards finishing my thesis. I would also like to thank my colleagues Professor Alfred Mvunyelwa Msomi, Makhosonke Thabethe and my lady-friend Dudu Seme for their encouraging words, Mr Darlington Hove, for his help when I was stuck with LaTeX and my Statistics tutor Mthokozisi Gumede for his dedication to help my students when I was busy with my research project.

Ngaphezu kwakho konke ngibonga uMvelinqangi ngokungigcina ngesikhathi salolukhuvethe (Covid-19) nanaphakade!.

Contents

Chapter 1

Introduction

1.1 Historical background and recent innovation on Diophantine equations

A Diophantine equation is an algebraic equation for which integer solutions are sought. An algebraic equation is one that involves only polynomial expressions in one or more variables. The coefficients of the polynomial should be integers. Diophantine equations get their name from Diophantus of Alexandria. Diophantus was a well-known mathematician of the 3rd century. He wrote a highly regarded treatise called the Arithmetica. The mathematical study of Diophantine problems he initiated is called 'Diophantine Analysis'. The questions in Diophantine analysis we ask about a Diophantine equation include:

- are there any solutions?
- are there finitely or infinitely many solutions?
- can all the solutions be found in theory?
- can we find lower or upper bounds for the solutions?

These are some of the questions we will consider when we analyze or solve some Diophantine equations in the next chapters.

The number theory enthusiasts celebrated the news recently that: On September 6, 2019, Andrew R. Booker from Bristol and Andrew Sutherland from the Massachusetts Institute of Technology, found a sum of three cubes for 42 : $(-80538738812075974)^3 + (80435758145817515)^3 + (12602123297335631)^3$ and it said that this leaves 114 as the lowest unsolved case.

1.2 Motivation for studying some Diophantine equations with Catalan numbers, Fibonacci Numbers and Ramanujan numbers

We became fascinated with arithmetic properties of Ramanujan numbers (numbers which are in the image of the Ramanujan τ-function), Fibonacci numbers and Catalan numbers and the rate at which their absolute values increase and we had an interest to see where a Ramanujan number meets a Fibonacci number or a Catalan number or the absolute value of a Ramanujan τ–function of some other number.

1.3 Organisation of the Thesis

In this section, we give a mathematical introduction to various topics in the thesis. This thesis consists of five chapters. The material presented in this thesis covers the results that were published by the author and his supervisor in the following journal papers:

[LuMa] F. Luca, S. Mabaso, "Diophantine equations with the Ramanujan τ-function of factorials, Fibonacci numbers, and Catalan numbers", *The Fibonacci Quart.*, **57** (2019), 255–259.

[FLAS] F. Luca, S. Mabaso and P. Stănică , "On the prime factors of the iterates of the Ramanujan τ-function", *Proceedings of the Edinburgh Mathematical Society*, **63** (2020), 1031–1047.

Chapter 2 lays down the foundation for this thesis. It covers all the definitions, conjectures lemmas and theorems which will be applied in the next chapters and some of them may be restated as we deem it necessary to do so.

The work in Chapter 3 appears as a result in [LuMa]. In this chapter, we solve some Diophantine equations of the form $|\tau(x)| = y$, where τ is the Ramanujan τ-function and x, y are integer variables restricted to values of factorials, Fibonacci numbers and Catalan numbers.

In Chapter 4, we study a Diophantine equation of the form $F_n = \pm\tau(m_1!) \pm \cdots \pm \tau(m_k!)$, where F_n is the nth Fibonacci number and τ is the Ramanujan τ-function. We start by finding the lower bound for some k and upper bound for m_k. Lastly, we solve this Diophantine equation when $k = 2$. We apply a linear form in 2-adic logarithms and we develop Lemma 4.10 (on the 5-adic valuation of the Fibonacci numbers) as computational methods for reducing upper bounds for our solutions.

In concluding this thesis, Chapter 5 studies the iterates of the Ramanujan τ-function and from this we come up with some interesting results on the greatest prime factor of the Ramanujan τ–function and counting the numbers of solutions of some Diophantine equations involving the Ramanujan τ–function. The idea of primitive prime factor on Lucas sequence plays an important role here. The work in this chapter appears in [FLAS].

Chapter 2

Some Preliminary Results

In this chapter, we give some definitions and concepts which will be useful in the subsequent chapters. In Section 2.1, we define the Ramanujan τ-function which possesses many arithmetic properties and list some of them which will be used as we find it convenient to do so. In Section 2.2, we define Fibonacci sequence, Lucas sequence and Lehmer numbers and we state an inequality and an equation that relates Fibonacci numbers and Lucas numbers. We also recall the general definition of the primitive prime divisor in Section 2.3. In Section 2.4, we define a Catalan number and state and prove some inequalities involving a Catalan number. We conclude this chapter by defining when are the two algebraic numbers multiplicatively independent, stating without proof in Section 2.5 theorems on linear forms in p-adic algorithms and the ABC-conjecture which will help us in finding and reducing bounds for our solutions.

2.1 The Ramanujan τ-function

Definition 2.1 *The Ramanujan function $\tau(n)$, is defined as the coefficient of q^n of the following series:*

$$q\left(\prod_{k\geq 1}(1-q^k)\right)^{24} = \sum_{n\geq 1}\tau(n)q^n = \Delta \text{ for } |q|<1. \tag{2.1}$$

Some well-known properties of the Ramanujan τ-function are summarized in the lemma

below. They were conjectured by Ramanujan in 1916 in [44]. The first two were proved by Mordell in 1917 in [40]. The last was proved by Deligne in 1974 in [11].

Lemma 2.2 *(i) If m, n are coprime positive integers, then $\tau(mn) = \tau(m)\tau(n)$.*

(ii) For a prime p, the sequence $\{\tau(p^n)\}_{n\geq 0}$ satisfies

$$\tau(p^{n+2}) = \tau(p)\tau(p^{n+1}) - p^{11}\tau(p^n) \qquad n \geq 1.$$

(iii) By the famous result of Deligne we have:

$$|\tau(p)| < 2p^{11/2}.$$

More generally, for every positive integer n we have

$$|\tau(n)| \leq d(n)n^{11/2},$$

where $d(n)$ is the number of divisors of n.

Further, we will use the elementary fact that

$$d(n) \leq 2\sqrt{n}. \tag{2.2}$$

For the proof, we note that every divisor k of n either satisfies that $k \leq \sqrt{n}$, or its complimentary divisor n/k satisfies that $n/k \leq \sqrt{n}$ so there can be at most $2\sqrt{n}$ divisors of n altogether.

2.2 The Fibonacci sequence, Lucas sequence and nth Lehmer number

Let $\{F_n\}_{n\geq 0}$ be the Fibonacci sequence given by $F_0 = 0,\ F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$ and let $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$ be the roots of the characteristic polynomial $x^2 - x - 1 = 0$. It is well known that the Binet formula

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ holds for all } n \geq 0.$$

The sequence of Lucas numbers $\{L_n\}_{n\geq 0}$ starts with $L_0 = 2,\ L_1 = 1$ and satisfies $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$. From the Binet formula for F_n, we can by induction on n, deduce the fact that

$$\alpha^{n-2} < F_n < \alpha^{n-1}. \tag{2.3}$$

There are many formulas relating Fibonacci numbers and Lucas numbers, but the one we will use is

$$L_n^2 - 5F_n^2 = 4\,(-1)^n \text{ valid for all } n \geq 0. \tag{2.4}$$

Conversely, it is well-known that if (x, y) are positive integers such that $x^2 - 5y^2 = \pm 4$, then $(x, y) = (L_n, F_n)$ for some positive integer n. See section 10.14 in [22] for these are other properties of Fibonacci and Lucas numbers. The following is Lemma 2 in [37].

Lemma 2.3 *Let $m \geq n$ be two nonnegative integers such that $m \equiv n \pmod 2$. Let $\delta = (-1)^{(m-n)/2}$. Then, $F_m - F_n = F_{(m-\delta n)/2} L_{(m+\delta n)/2}$.*

Definition 2.4 *If α and β are algebraic integers such that $(\alpha + \beta)^2$ and $\alpha\beta$ are coprime, non-zero rational integers and α/β is not a root of unity then the nth Lehmer number with respect to α, β is defined to be*

$$\mu_n = \frac{\alpha^n - \beta^n}{\alpha^{\delta_n} - \beta^{\delta_n}}$$

where $\delta_n = 1$ if n is odd and $\delta_n = 2$ if n is even.

2.3 Primitive Prime Divisor

Definition 2.5 *Let $(\mu_n)_{n\geq o}$ be a sequence of integers. A prime p is said to be a primitive divisor of μ_n if $p|\mu_n$, but p does not divide $\mu_1\mu_2\ldots\mu_{n-1}$.*

For a positive real number x, we denote the number of primes $p \leq x$ by $\pi(x)$ and for a prime number p and a positive integer m, we let $\nu_p(m)$ denote the exponent of p in the factorisation of m.

2.4 The Catalan Numbers

Definition 2.6 *A Catalan number is a number in the form* $C_n := \dfrac{1}{n+1}\binom{2n}{n}$ *for some integer* $n \geq 0$.

We observe that a Catalan number is an integer since it can also be written in the form $C_n = \binom{2n}{n} - \binom{2n}{n+1}$, which is a difference of two integers. Hence a Catalan number is an integer.

Lemma 2.7 *The inequalities*

$$2^n < C_n < \frac{2^{2n}}{n+1} \quad \text{hold for all} \quad n > 3. \tag{2.5}$$

Proof The upper bound is easy since

$$\binom{2n}{n} < \sum_{k=0}^{2n} \binom{2n}{k} = 2^{2n}.$$

For the lower bound we prove by induction that

$$\binom{2n}{n} \geq \frac{2^{2n}}{n+1}$$

holds for all $n \geq 0$. We check it for $n = 0$ and $n = 1$. Assuming that it holds for n we get

$$\binom{2n+2}{n+1} = \frac{(2n+1)(2n+2)}{(n+1)^2}\binom{2n}{n} = \frac{4n+2}{n+1}\binom{2n}{n} \geq \frac{(2n+1)2^{2n+1}}{(n+1)^2}.$$

It suffices to check that

$$\frac{2^{2n+1}(2n+1)}{(n+1)^2} \geq \frac{2^{2n+2}}{n+2},$$

which is equivalent to

$$(2n+1)(n+2) \geq 2(n+1)^2,$$

so $2n^2 + 5n + 2 \geq 2n^2 + 4n + 2$, which obviously holds. To get the desired lower bound $C_n > 2^n$, we still need to show, via the lower bound we just proved, that $2^n > (n+1)^2$. This holds by induction on n for all $n \geq 6$. One can also check that $C_4 = 21 > 2^4 = 16$ and $C_5 = 42 > 32 = 2^5$.

We also recall (and it is easy to see from the definition) that C_n is divisible exactly once by all primes p such that $n + 1 < p \leq 2n$.

2.5 The p-adic algorithm

Definition 2.8 *Two algebraic numbers k and l are said to be multiplicatively dependent if there exist two integers m and n not both zero such that $k^m = l^n$. Otherwise k and l are multiplicatively independent.*

For an algebraic number η with minimal polynomial

$$f(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Z}[X] \quad \text{with} \quad \gcd(a_0, a_1, \ldots, a_d) = 1,$$

we put $H(\eta) := \max\{|a_i| : i = 0, 1, \ldots, d\}$. For example, if $\eta := m/n$ is a rational number written in reduced form; i.e., with coprime integers m and $n > 0$, then $H(\eta) = \max\{|m|, n\}$. Given a number field $\mathbb{K}$, a prime ideal π of its ring of algebraic integers $\mathcal{O}_{\mathbb{K}}$, and $\eta \in \mathbb{K}^*$, we write $\nu_\pi(\eta)$ for the exponent with which π appears in the prime ideal factorization of the principal fractional ideal $\eta\mathcal{O}_{\mathbb{K}}$ generated by η inside $\mathbb{K}$. The following result is due to Kunrui Yu [55].

Lemma 2.9 *Let $\mathbb{K}$ be an algebraic number field, π be a prime ideal of $\mathcal{O}_{\mathbb{K}}$, $\eta_1,\ \eta_2 \in \mathbb{K}^*$. Let $H_1,\ H_2$ be real numbers, $H_i \geq \max\{H(\eta_i), 3\},\ i = 1, 2$. Let $m_1,\ m_2$ be integers and put $M = \max\{|m_1|, |m_2|, 3\}$. Assume $\eta_1^{m_1}\eta_2^{m_2} - 1 \neq 0$. Then*

$$\nu_\pi(\eta_1^{m_1}\eta_2^{m_2} - 1) < c_1 \log H_1 \log H_2 \log M,$$

where $c_1 := c_1(\mathbb{K}, \pi)$ is a positive constant depending on $\mathbb{K}$ and π.

Bugeaud and Laurent proved the following result (see Corollary 1 of Theorem 3 in [10]).

Lemma 2.10 *Let p be a prime number. Let α_1 and α_2 be two algebraic numbers which are p-adic units. Denote by f the residual degree of the extension $\mathbb{Q}_p \hookrightarrow \mathbb{Q}_p(\alpha_1, \alpha_2)$ and put $D = [\mathbb{Q}(\alpha_1, \alpha_2) :\ \mathbb{Q}]/f$. Let b_1 and b_2 be two positive integers and put*

$$\Lambda = \alpha_1^{b_1} - \alpha_2^{b_2}.$$

Denote by $A_1 > 1$ and $A_2 > 1$ two real numbers such that

$$\log A_i \geq \max\left\{h(\alpha_i), \frac{\log p}{D}\right\}, \quad i = 1, 2,$$

and put

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

If α_1 and α_2 are multiplicatively independent, then we have the upper bound

$$\begin{aligned} \nu_p(\Lambda) &\leq \frac{18p(p^f-1)}{(p-1)(\log p)^4} \\ &\times D^4 \left(\max \left\{ \log b' + \log\log p + 0.4,\ \frac{15 \log p}{D}, 10 \right\} \right)^2 \log A_1 \log A_2. \end{aligned}$$

2.6 The ABC-conjecture

For a nonzero integer m, let

$$N(m) := \prod_{p|m} p,$$

be the *algebraic radical* of m.

Conjecture 2.11 *(The ABC-conjecture) For every $\varepsilon > 0$, there exists a constant $C := C_\varepsilon$ such that for all nonzero coprime integers a, b, c with $a + b = c$, we have*

$$\max\{|a|, |b|, |c|\} < C_\varepsilon N(abc)^{1+\varepsilon}.$$

In fact, we will use the following consequence of it which is Theorem 5 in [18].

Theorem 2.12 *Assume that the ABC-conjecture is true. Suppose that $f(x, y) \in \mathbb{Z}[x, y]$ is homogeneous without repeated factors. Fix $\varepsilon > 0$. Then for any coprime integers n, m*

$$N(f(m, n)) > c_{f,\varepsilon} \max\{|m|, |n|\}^{\deg(f)-2-\varepsilon}.$$

The constant $c_{f,\varepsilon}$ depends on f and ε.

2.7 Counting the solutions of a Thue–Mahler equation

We will use the following corollary, from [13], for bounding the number of solutions to a Thue–Mahler equation.

Corollary 2.13 *Let $F(x,y) \in \mathbb{Z}[x,y]$ be a binary form of degree $n \geq 3$ which is divisible by at least three pairwise linearly independent forms in some number field and let $\{p_1, p_2, p_3, \ldots, p_t\}$ be a (possibly empty) set of distinct prime numbers. Then the equation*

$$|F(x,y)| = {p_1}^{k_1} \cdot {p_2}^{k_2} \cdot {p_3}^{k_3} \cdots {p_t}^{k_t} \quad \text{in } x, y, k_1, \ldots, k_t \in \mathbb{Z} \text{ with } (x,y) = 1$$

has at most

$$2 \times 7^{n^3(2t+3)}$$

solutions.

Definition 2.14 *Let $\mathbb{K}$ be an algebraic number field and let $I(\mathbb{K})$ be the group of nonzero fractional ideal of $O_{\mathbb{K}}$. Let $P(\mathbb{K})$ be the subgroup of principal ideals of $I(\mathbb{K})$. Then the factor group $I(\mathbb{K})/P(\mathbb{K})$ is called the ideal class group of $\mathbb{K}$ and is denoted by $H(\mathbb{K})$.*

Definition 2.15 *Let $\mathbb{K}$ be an algebraic number field. The order of the ideal class group $H(\mathbb{K})$ is called the class number of $\mathbb{K}$ and is denoted by $h(\mathbb{K})$.*

2.8 Binary Recurrence Sequences

Let $\{u_n\}_{n\geq 0}$ be the binary recurrent sequence of integers given by

$$u_{n+2} = ru_{n+1} + su_n \quad \text{for all} \quad n \geq 0,$$

where $u_0, u_1 \in \mathbb{Z}$ and r, s are nonzero integers with $r^2 + 4s \neq 0$. It is well-known that

$$u_n = c\alpha^n + d\beta^n \tag{2.6}$$

where α, β are the two roots of the characteristic equation $x^2 - rx - s = 0$ and c, d can be computed in terms of α, β, u_0, u_1. In fact,

$$c = \frac{u_1 - u_0\beta}{\alpha - \beta} \qquad \text{and} \qquad d = \frac{u_0\alpha - u_1}{\alpha - \beta}.$$

When labelling the roots we make the convention that $|\alpha| \geq |\beta|$. The sequence $\{u_n\}_{n\geq 0}$ is called non-degenerate if $cd\alpha\beta \neq 0$ and α/β is not a root of 1. A famous example is the Fibonacci sequence $\{F_n\}_{n\geq 0}$ for which $r = s = 1$ (which has been defined in Section 2.2

above). In [21], it was shown that if $k \geq 1$ and $A \geq 1$ are fixed, then the Diophantine equation

$$|u_n| = a_1 m_1! + \cdots + a_k m_k! \quad \text{with} \quad a_i \in \mathbb{Z}, \quad |a_i| \in A, \quad (i = 1, \ldots, k)$$

has only finitely many positive integer solutions $(n, m_1, \ldots, m_k)$ with $1 \leq m_1 \leq \cdots \leq m_k$ and they are all effectively computable. When $A = 1$, $k = 2$ and $\{u_n\}_{n \geq 0}$ is the sequence of Fibonacci numbers, all such solutions are $F_1 = F_2 = 1! = -1! + 2!$, $F_3 = 2!$, $F_4 = 1! + 2!$, $F_5 = -1! + 3!$, $F_6 = 2! + 3!$, $F_{12} = 4! + 5!$.

In [36], the authors replaced the sequence of factorials by the sequence of the number of divisors of the factorials; that is, the sequence of general term $d(n!)$, where $d(n)$ is the number of positive divisors of the positive integer n. They showed that $d((n+1)!) \leq 2d(n!)$. Thus, by the greedy algorithm, for any positive integer N, there are $1 \leq m_1 < m_2 < \cdots < m_k$ such that

$$N = d(m_1!) + \cdots + d(m_k!).$$

It was also shown that if $\{u_n\}_{n \geq 0}$ is a non-degenerate binary recurrent sequence with $\gcd(r, s) = 1$, then the number k in the above representation for $N = |u_n|$ with $n > n_0$ satisfies $k > c_0 \log n / \log \log n$, where c_0, n_0 are positive constants which are computable in terms of the sequence $\{u_n\}_{n \geq 0}$. They also found all such solutions with $k = 2$ for the case when $\{u_n\}_{n \geq 0}$ is the Fibonacci sequence. The largest one is $F_9 = 34 = 4 + 30 = d(3!) + d(6!)$.

Some authors use $\tau(n)$ instead of $d(n)$ for the number of divisors of n. With that notation, the results from [36] address the diophantine equation

$$u_n = \tau(m_1!) + \cdots + \tau(m_k!). \tag{2.7}$$

But there is another important function denoted $\tau(n)$, namely the Ramanujan τ-function which has been defined in Section 2.1 above.

Chapter 3

Some Diophantine Equations with Ramanujan τ-Function of Factorials, Fibonacci Numbers and Catalan Numbers

The work in this chapter has been published by the author and his supervisor, see [32]. In this chapter, we solve various Diophantine equations of the type $|\tau(x)| = y$, where τ is the Ramanujan τ–function and x, y are integer variables restricted to values of factorials, Fibonacci numbers and Catalan numbers.

3.1 Introduction

Various Diophantine equations of the form $f(x) = y$ have been solved in the literature, where f is some function defined on the set of positive integers, like the Euler function or the sum of divisors function, see for example, [30], [25], [31], [34]. We now prove the following theorem.

Theorem 3.1 *(1) The only positive integer solutions (m, n) of the Diophantine equation*

$$|\tau(m!)| = F_n$$

are $(1,1)$ *and* $(1,2)$.

(2) The only positive integer solution (m,n) *of the Diophantine equation*

$$|\tau(m!)| = C_n$$

is $(1,1)$.

(3) The only positive integer solutions (m,n) *of the Diophantine equation*

$$|\tau(C_m)| = F_n$$

are $(1,1)$ *and* $(1,2)$.

(4) The only positive integer solution (m,n) *of the Diophantine equation*

$$|\tau(C_m)| = C_n$$

is $(1,1)$.

In proving Theorem 3.1, we will mostly use the results in Sections 2.1 and 2.4 together with Lemma 3.2 below. Considering the 2–adic valuation, we come up with the following results:

Lemma 3.2 *The following properties hold:*

(i) $\nu_2(m!) > m/2$ *for all* $m \geq 4$.

(ii) $\nu_2(\tau(2^a)) \geq 3a$ *for all* $a \geq 0$.

(iii) $\nu_2(\tau(m!)) \geq 3m/2$ *for all* $m \geq 2$.

(iv) $\nu_2(F_n) \leq \log(4n/3)/\log 2$ *for all* $n \geq 1$.

(v) $\nu_2(C_m) \leq \log(2m)/\log 2$ *for all* $m \geq 1$.

(vi) $\pi(2m) - \pi(m+1) \geq m/(2\log m)$ *holds for all* $m \geq 19$.

Proof Part (i) follows from the well-known fact that

$$\nu_2(m!) = \left\lfloor \frac{m}{2} \right\rfloor + \left\lfloor \frac{m}{4} \right\rfloor + \cdots \geq \left\lfloor \frac{m}{2} \right\rfloor + 1 > \frac{m}{2}$$

for $m \geq 4$. Part (ii) follows by induction on a via the fact that $\tau(1) = 1$, $\tau(2) = -24$ and

$$\tau(2^{a+2}) = -24\tau(2^{a+1}) - 2048\tau(2^a) \quad \text{for all} \quad a \geq 0.$$

Part (iii) follows immediately from (i) and (ii) for $m \geq 4$ and one checks that it also holds for $m = 2, 3$ because $\tau(2) = -2^3 \cdot 3$ and $\tau(6) = -2^5 \cdot 3^3 \cdot 7$. For part (iv), one checks by induction on k, that for $k \geq 3$, we have that $2^k \mid F_n$ if and only if $3 \times 2^{k-2} \mid n$. Thus, if $k = \nu_2(F_n)$ and $k \geq 3$, then $3 \times 2^{k-2} \leq n$, so $k \leq \log(4n/3)/\log 2$. One checks that the inequality (iv) also holds for $k < 3$ by noting that k can never be 2, while for $k = 1$, inequality (iv) follows because in this case $3 \mid n$, so $n \geq 3$. Part (v) follows because

$$\nu_2(C_m) = \left(\left\lfloor \frac{2n}{2} \right\rfloor - 2 \left\lfloor \frac{n}{2} \right\rfloor \right) + \left(\left\lfloor \frac{2n}{4} \right\rfloor - 2 \left\lfloor \frac{n}{4} \right\rfloor \right) + \cdots + \left(\left\lfloor \frac{2n}{2^k} \right\rfloor - 2 \left\lfloor \frac{n}{2^k} \right\rfloor \right) + \cdots .$$

Furthermore, each of the above parentheses is in $\{0, 1\}$ and the largest k for which the parentheses is non-zero satisfies $2^k \leq 2n$, so $k \leq \log(2n)/\log 2$. For part (v), recall from [46] that the following estimates hold

$$\frac{x}{\log x - 0.5} < \pi(x) < \frac{x}{\log x - 1.5} \quad \text{for all} \quad x \geq 67.$$

In particular,

$$\pi(2m) - \pi(m+1) > \frac{2m}{\log(2m) - 0.5} - \frac{m+1}{\log(m+1) - 1.5}.$$

The right–hand side exceeds $m/(2\log m)$ for all $m \geq 160$. Now a quick computation shows that, in fact, $\pi(2m) - \pi(m+1) > m/(2\log m)$ for all $m \in [19, 160]$.

3.2 The proofs of Theorem 3.1

We start with part (1). First, we show that $n < 1000$. Assume $n \geq 1000$. Clearly, $m > 1$. Then

$$\alpha^{n-2} < F_n = |\tau(m!)| < d(m!)(m!)^{11/2} \leq 2\sqrt{m!} \left(\frac{m^m}{2} \right)^{11/2} < m^{6m}$$

by inequality (2.2), Lemma 2.2 (iii) and inequality (2.3). Suppose $m < n/(18\log n)$. We then get

$$\alpha^{n-2} < m^{6m} < \exp(6m\log m) < \exp(n/3),$$

which gives

$$(3\log\alpha)(n-2) < n, \qquad \text{so} \qquad n < \frac{6\log\alpha}{3\log\alpha - 1} < 7,$$

a contradiction. Thus, $m \geq n/(18\log n)$. Since $n > 438$, it follows that

$$m > \frac{n}{18\log n} > 4$$

and so

$$\nu_2(m!) > \frac{m}{2} > \frac{n}{36\log n} \tag{3.1}$$

by Lemma 3.2 (i). Thus,

$$\frac{\log(4n/3)}{\log 2} \geq \nu_2(F_n) = \nu_2(\tau(m!)) \geq 3\nu_2(m!) > \frac{n}{12\log n}$$

by Lemma 3.2 (i), (iii) and (iv). This gives $n \leq 809$, contradicting the fact that $n \geq 1000$. Thus, $n \leq 1000$. It then follows that

$$\nu_2(F_n) \leq \frac{\log(4n/3)}{\log 2} \leq 10.4,$$

so $\nu_2(|\tau(m!)|) \leq 10$, which shows that $\nu_2(m!) \leq 3$. Thus, $m \in \{1,2,3,4,5\}$, so

$$F_n \in \{1, 24, 6048, 21288960, 102825676800\},$$

and the only Fibonacci number in the above set is $1 = F_1 = F_2$.

For part (2), assume $n > 1000$. Note that

$$\alpha^{n-2} < \alpha^n < 2^n < C_n = |\tau(m!)| < m^{6m}$$

(see Lemma 2.7 for the middle inequality), and now the previous argument shows that $m \geq n/(18\log n)$. We thus get that

$$\frac{\log(2n)}{\log 2} \geq \nu_2(C_n) = \nu_2(\tau(m!)) > \frac{n}{12\log n}$$

by Lemma 3.2 (i), (iii) and (v). This gives $n \leq 876$, contradicting the fact that $n > 1000$. Thus, $n \leq 1000$. It then follows that

$$\nu_2(C_n) \leq \frac{\log(2n)}{\log 2} \leq 10.97,$$

so $\nu_2(|\tau(m!)|) \leq 10$, which shows that $\nu_2(m!) \leq 3$. Thus, $m \in \{1, 2, 3, 4, 5\}$, so

$$C_n \in \{1, 24, 6048, 21288960, 102825676800\},$$

and the only Catalan number in the above set is $1 = C_1$.

For part (3), we use Lemma 2.7 to deduce that assuming $m \geq 4$,

$$|\tau(C_m)| < 2C_m^6 < 2\left(\frac{2^{2m}}{m+1}\right)^6 < 2^{12m-2}.$$

Thus,

$$2^{12m-2} > F_n > \alpha^{n-2}, \quad \text{so} \quad 2^{12m} > \left(\frac{4}{\alpha^2}\right)\alpha^n > \alpha^n$$

giving

$$m > \frac{(\log \alpha)n}{12 \log 2} > \frac{n}{18}.$$

By Lemma 3.2 (vi), for $m \geq 19$, the interval $(m+1, 2m)$ contains at least $m/(2\log m)$ primes. For each one of such primes p, we have that $p \| C_m$ and $\tau(p)$ is even. Hence, by multiplicativity and Lemma 3.2 (vi),

$$\frac{\log(4n/3)}{\log 2} \geq \nu_2(F_n) = \nu_2(\tau(C_m)) \geq \pi(2m) - \pi(m+1) \geq \frac{m}{2\log m} > \frac{n}{36 \log n},$$

so $n \leq 4000$. This shows that

$$\nu_2(\tau(C_m)) \leq \nu_2(F_n) \leq \frac{\log(4n/3)}{\log 2} < 12.4,$$

so $\nu_2(\tau(C_m)) \leq 12$. Thus, there are at most 12 primes in the interval $(m+1, 2m)$, which gives $m \leq 63$. We now list all values of $|\tau(C_m)|$ for $m \in [1, 63]$ and all values of F_n for $n \in [1, 4000]$ and intersect these two sets and get the conclusion.

The same argument applies to part (4). Namely, assuming $n > 1000$, we have

$$2^{12m-2} > |\tau(C_m)| = C_n > 2^n \quad \text{therefore} \quad m > \frac{n}{12}.$$

We then get that

$$\frac{\log(2n)}{\log 2} \geq \nu_2(C_n) = \nu_2(\tau(C_m)) \geq \frac{m}{2\log m} > \frac{n}{24\log n},$$

giving $n \leq 2500$. Thus,

$$\nu_2(\tau(C_m)) \leq \frac{\log(2n)}{\log 2} \leq 12.3,$$

so again $\nu_2(\tau(C_m)) \leq 12$, which implies that $m \leq 63$. We now list all values of $|\tau(C_m)|$ for $m \in [1, 63]$ and all values of C_n for $n \in [1, 2500]$ and intersect these two sets and get the conclusion.

3.3 Conclusion

We did not get any interesting solutions for the equations studied in our main result. Allowing $|\tau(m!)|$ to be a product of more Fibonacci numbers, we got the following solutions:

$$\begin{aligned}
|\tau(1!)| &= F_1; \\
|\tau(2!)| &= F_4 F_6; \\
|\tau(3!)| &= F_3^5 F_4^2 F_8; \\
|\tau(4!)| &= F_3^{11} F_4^2 F_8 F_{10}; \\
|\tau(5!)| &= F_3^7 F_4 F_5 F_8 F_{10} F_{24}.
\end{aligned}$$

We suggest the following problem.

Problem 3.3 *Find all solutions of the equation*

$$|\tau(m!)| = F_{n_1} F_{n_2} \cdots F_{n_k}$$

in positive integers $m,\ n_1 \leq n_2 \leq \cdots \leq n_k$.

Without the Ramanujan τ-function, the largest solution of the equation $m! = F_{n_1} \cdots F_{n_k}$ is $11! = F_1 F_2 F_3 F_4 F_5 F_6 F_8 F_{10} F_{12}$ (see [35]).

Chapter 4

Some Diophantine Equations Involving Fibonacci Numbers and Ramanujan τ-Function of Factorials

4.1 Introduction

In this chapter, we look at the Diophantine equation $F_n = \pm\tau(m_1!) \pm \cdots \pm \tau(m_k!)$, where F_n is the nth Fibonacci number and τ is the Ramanujan τ-function. We study the same problem as before with the Ramanujan τ-function, which is equation (2.7). Since τ changes signs, we study in fact a slightly more general equation namely

$$u_n = \pm\tau(m_1!) \pm \cdots \pm \tau(m_k!). \tag{4.1}$$

Our results apply equally to the case where the signs $\pm$ are replaced by arbitrary coefficients a_i for $i = 1, \ldots, k$ with $|a_i| \leq A$, where A is fixed beforehand. We ignore such slight generalisation in order to simplify the presentation.

We start by finding the upper bound and lower bound of m_k in terms of n and k. We also show that $k \geq c_0 \log n / \log\log n$ for $n \geq n_0$. In the previous chapter and also [32], we solved $F_n = \pm\tau(m_1)$, which is the case $k = 1$.

Here, we will be treating the case $k = 2$, namely solving the Diophantine equation

$$F_n = \pm\tau(m_1!) \pm \tau(m_2!). \tag{4.2}$$

We also come up with the following main results:

Theorem 4.1 *Assume that $\{u_n\}_{n\geq 0}$ is non-degenerate. Then there are computable positive constants n_0, c_0 depending on $\{u_n\}_{n\geq 0}$ such that for $n > n_0$, any solution of equation (4.1) with $1 \leq m_1 \leq m_2 \leq \cdots \leq m_k$ has $k > c_0 \log n / \log\log n$.*

Theorem 4.2 *The only positive integer solution (m_1, m_2, n) of the equation (4.2) with $m_1 \leq m_2$ is $(m_1, m_2, n) = (1, 1, 3)$.*

In proving Theorem 4.2, we look at a case $m_1 = 1$ and $m_2 \geq 4$ and show that $n < 1000$ for this case. The other case we consider is when $m_1 \geq 2$ and $n \geq 1000$. In this case applying a linear form in 2-adic logarithms, we find that $n \leq 1.2 \times 10^{12}$. Using Mathematica, properties of the divisors of F_n and theory of 5-adic numbers, we eliminate some n and show that the given solutions are the only solutions.
In preparing to prove Lemmas 4.4 and 4.5, we first define the following:
For every prime q, let

$$\mathcal{P}_q = \{p \text{ prime} : p \equiv 1 \pmod{q},\ \tau(p) \equiv 2 \pmod{q}\}.$$

For a subset $\mathcal{A}$ of positive integers and a positive real number x, we put $\mathcal{A}(x) = \mathcal{A} \cap [1, x)$. We also need the following two results before proving Lemma 4.5:

Lemma 4.3 *For each prime q there is a computable positive constant $c_1 := c_1(q)$ depending on q such that for every $\varepsilon > 0$, we have*

$$\#\mathcal{P}_q(x) = (c_1 + \zeta)\pi(x) \quad \text{with} \quad |\zeta| < \varepsilon \quad \text{for} \quad x > x_{q,\varepsilon},$$

where $x_{q,\varepsilon}$ is also effectively computable.

Proof We mimic the hint for the solution of Exercise 6.9 on pages 227-260 in [47]. Let G_1 be the image subgroup of the q-adic representation attached to Δ, which is the modular form corresponding to τ. Then $\mathcal{P}_q$ is just the set of primes whose Frobenius with respect to the above representation corresponds to the identity element of G_1. Thus, by the Chebotarev density theorem, $c_1 = 1/\#G_1$. Serre's open mapping theorem says that $G_1 = \mathrm{GL}_2(\mathbb{F}_q)$ for large enough q, so $\#G_1 = (q^2 - 1)(q^2 - q)$ for such q. In fact, this is

so for all $q \notin \{2, 3, 5, 7, 23, 691\}$ by a result of Swinnerton-Dyer [51]. For $q = 2$, we have $c_1 = 1$ because $\tau(p)$ is always even. At any rate, $1/c_1$ is an integer smaller than q^4 for all $q \geq 2$. The fact that $x_{q,\varepsilon}$ is computable in terms of q and ε follows from the effective version of the Chebotarev density theorem due to Lagarias and Odlyzko [28].

Lemma 4.4 *If q is prime and $p \in \mathcal{P}_q$, then $q \mid \tau(p^{q-1})$.*

Proof This is clear if $q = 2$ since $\tau(n)$ is even unless n is a perfect square. So, we may assume that $q \geq 3$. Let $\alpha_p, \overline{\alpha}_p$ be the two roots of the quadratic equation $0 = x^2 - \tau(p)x + p^{11} := x^2 - rx - s$. Then

$$\alpha_p = \frac{\tau(p) + \sqrt{\tau(p)^2 - 4p^{11}}}{2} = \frac{r + \sqrt{\Delta}}{2} \qquad \text{where} \qquad \Delta := r^2 + 4s.$$

Since $p \in \mathcal{P}_q$, we have $r \equiv 2 \pmod{q}$ and $s \equiv -1 \pmod{q}$, so $\Delta \equiv 0 \pmod{q}$. Now

$$\begin{aligned} \tau(p^{q-1}) &= \frac{\alpha_p^q - \overline{\alpha}_p^q}{\alpha_p - \overline{\alpha}_p} = \frac{\left(\frac{r+\sqrt{\Delta}}{2}\right)^q - \left(\frac{r-\sqrt{\Delta}}{2}\right)^q}{\sqrt{\Delta}} \\ &= \frac{1}{2^{q-1}} \sum_{\substack{1 \leq k \leq q \\ k \equiv 1 \pmod 2}} \binom{q}{k} r^{q-k} \Delta^{(k-1)/2}. \end{aligned}$$

Thus,

$$2^{q-1}\tau(p^{q-1}) = \sum_{\substack{1 \leq k \leq q \\ k \equiv 1 \pmod 2}} \binom{q}{k} r^{q-k} \Delta^{(k-1)/2}.$$

The right–hand side above is an integer which is a multiple of q since for $k = 1$, we have $\binom{q}{k} = q$, while for $k \geq 3$ and odd, $q \mid \Delta^{(k-1)/2}$. Thus, $q \mid \tau(p^{q-1})$, as desired.

We will now apply the above results in proving Lemma 4.5.

Lemma 4.5 *Let q be a prime. There exist positive constants c_2, c_3 depending on q such that for $m > c_2$,*

$$\nu_q(\tau(m!)) > c_3 \frac{m}{\log m}.$$

Proof For $m > q^2$, consider primes $p \in \mathcal{P}_q$ in the interval $(m/q, m/(q-1)]$. For such a prime p, we have that $p > m/q$, so $p^2 > (m/q)^2 > m$. Thus,

$$\nu_p(m!) = \left\lfloor \frac{m}{p} \right\rfloor = q - 1.$$

It thus follows that $p^{q-1} \| m!$ and by multiplicativity, we get that $\tau(p^{q-1}) \mid \tau(m!)$. By Lemma 4.4, $q \mid \tau(p^{q-1})$ for each such p, so

$$\begin{aligned} \nu_q(\tau(m!)) &\geq \#\left(\mathcal{P}_q \cap (m/q, m/(q-1)]\right) \\ &= \#\mathcal{P}_q(m/(q-1)) - \#\mathcal{P}_q(m/q) \\ &= (c_1+\zeta_1)\pi(m/(q-1)) - (c_1+\zeta_2)\pi(m/q), \end{aligned}$$

with $\max\{|\zeta_1|, |\zeta_2|\} < \varepsilon$ if $m > qx_{q,\varepsilon}$, where $c_1 := c_1(q)$ is the one from Lemma 4.3. Choosing $\varepsilon := 1/(4q^6)$, we get, by the prime number theorem, that

$$\nu_q(\tau(m!)) > \left(\frac{c_1}{q-1} - \frac{c_1}{q} - 3\varepsilon\right)\frac{m}{\log m} > c_3\frac{m}{\log m},$$

where we can take $c_3 := 1/(4q^6)$ and the above inequality holds in the range $m > c_2$, where c_2 depends on q.

4.1.1 Proof of Theorem 4.1

In proving Theorem 4.1, we follow the proof of the main result in [36]. We need a result from the theory of linear forms in p-adic logarithms (see Section 2.9) and also Lemma 4.6 which is due to Stewart [49]. Throughout this section, we label positive constants $c_1, c_2, \ldots$ in increasing order as they appear in our arguments. Recall that $\{u_n\}_{n\geq 0}$ is a binary recurrent sequence of integers of roots $\alpha,\ \beta$ such that $|\alpha| \geq |\beta|$.

Lemma 4.6 *There exist computable constants n_0 and c_2 such that*

$$|u_n| > |\alpha|^{n - c_2 \log n} \quad \textit{for all} \quad n \geq n_0.$$

Proof of Theorem 4.1 :

Throughout this proof, n_0 and m_0 are large numbers not necessarily the same at each occurrence. Consider the equation (4.1). Assume that $n > n_0$ so that $u_n \neq 0$. We may assume that $k < \log n$ otherwise we are done. Lemma 2.2 implies that $\tau(m) < d(m)m^{5.5} < m^6$ for $m > m_0$. Thus, $\tau(m!) < m!^6 < m^{6m}$ for $m > m_0$. So, by Lemma 4.6 and introducing log on both sides, we have

$$\begin{aligned} c_3 n - c_4 \log n &< \log|u_n| \leq \log(k \max_{1\leq i\leq k}\{|\tau(m_i!)|\}) \\ &\leq \log\log n + 6m_k \log m_k \qquad \text{for} \qquad m_k > m_0, \end{aligned} \tag{4.3}$$

where $c_3 := \log|\alpha|$ and where $c_4 := c_2 c_3$. It thus follows that

$$c_5 \frac{n}{\log n} < m_k \quad \text{holds whenever} \quad n > n_0, \tag{4.4}$$

where we can take $c_5 := c_3/7$. It remains to find an upper bound on m_k in terms of n and k, and then use (4.4) to extract a lower bound for k in terms of n.

Let q be the smallest prime exceeding s and let π be a prime ideal dividing q in $\mathbb{K} := \mathbb{Q}(\alpha)$. Note that since $q \nmid s$, it follows that π divides neither α nor β. Then

$$\begin{aligned} \nu_q(u_n) &\leq \nu_\pi(c\alpha^n + d\beta^n) = \nu_\pi(d\beta^n) + \nu_\pi((-c/d)(\alpha/\beta)^n - 1) \\ &\leq c_6 \log n + c_7, \end{aligned}$$

where $c_7 := \max\{\nu_\pi(d), 1\}$ and for the right–most inequality above we used Lemma 2.9 with $\eta_1 := -c/d$ and $\eta_2 := \alpha/\beta$. Lemma 4.5 implies that $\nu_q(\tau(m!)) \geq c_8 m/\log m$ for $m > c_9$. Here, $c_8 := c_1(q)$, where $c_1(q)$ is the constant from Lemma 4.5. Thus, assuming that $m_1 \geq m_0$, we have

$$\begin{aligned} c_6 \log n + c_7 &\geq \nu_q(u_n) = \nu_q(\pm\tau(m!) \pm \cdots \pm \tau(m_k!)) \geq \min_{1 \leq i \leq k} \{\nu_q(\tau(m_i!))\} \\ &\geq c_8 m_1/\log m_1, \end{aligned}$$

giving

$$m_1 \leq c_{10}(\log n)^2 \quad \text{for} \quad n \geq n_0. \tag{4.5}$$

We assume that $c_{10} \geq m_0$ so that the above inequality includes also the case when $m_1 \leq m_0$. Comparing (4.4) with (4.5), it follows that $k \geq 2$ once $n \geq n_0$, for if not, we would get that $c_5 n/\log n < m_1 < c_{10}(\log n)^2$, so $n < n_0$. We also assume that $c_{10}(\log n)^2 < n$ for $n > n_0$.

We will show, recursively, that the following holds:

Claim. *There exists a constant $c_{11} > 1$ such that if $j < k$ and both inequalities*

$$m_j < (c_{11} \log n)^{3j} \quad \textit{and} \quad (c_{11} \log n)^{3j+3} < n, \tag{4.6}$$

hold, then

$$m_{j+1} < (c_{11} \log n)^{3j+3}. \tag{4.7}$$

Let us see that once we have proved the above implication, we are through. Indeed, let $j \le k$ be maximal such that inequality (4.6) holds. If $j = k$, then, by (4.4),

$$c_5 \frac{n}{\log n} < m_k \le (c_{11} \log n)^{3k}. \tag{4.8}$$

If $j < k$, then inequality (4.7) holds. By the maximality of j, we must have

$$(c_{11} \log n)^{3k} \ge (c_{11} \log n)^{3j+3} \ge n. \tag{4.9}$$

Both inequalities (4.8) and (4.9) show that $k \ge c_0 \log n / \log\log n$ for $n \ge n_0$, which is the desired conclusion.

To prove the claim, notice that we have already proved it with $c_{11} := c_{10}^{1/3}$ for the case when $j = 1$. Assume now that (4.6) holds for some $j < k$ with some c_{11} to be determined later. We distinguish three cases.

Case 1. $\gcd(r, s) > 1$.

Let $q \mid \gcd(r, s)$. Then, by induction on n, we have $\nu_q(u_n) \ge n/2$. We rewrite equation (4.1) as

$$u_n - N_j := u_n - (\pm\tau(m_1!) \pm \cdots \pm \tau(m_j!)) = \pm\tau(m_{j+1}!) \pm \cdots \pm \tau(m_k!) \tag{4.10}$$

and study the exponent of q on both sides. On the right-hand side, it is at least

$$\min_{j+1 \le i \le k} \nu_q(\tau(m_i!)) \ge c_{12} \frac{m_{j+1}}{\log m_{j+1}}. \tag{4.11}$$

Here $c_{12} := c_1(q)$, where $c_1(q)$ is the one from Lemma 4.5. In the second term on the left-hand side is at most

$$\begin{aligned}
\frac{\log |N_j|}{\log q} &\le \frac{\log(|\tau(m_1! + \cdots + |\tau(m_j!)|)}{\log q} \\
&\le \frac{1}{\log 2}(\log k + 6 m_j \log m_j) \\
&< \frac{1}{\log 2}\left(\log\log n + 6(c_{11} \log n)^{3j}(3j)(\log c_{11} + \log\log n)\right) \\
&< \frac{42}{\log 2}(c_{11} \log n)^{3j} (\log\log n)^2 \\
&< c_{13}(c_{11} \log n)^{3j+1}
\end{aligned} \tag{4.12}$$

where $c_{13} := 42/\log 2$ and in the above chain of inequalities, we assume that $n > \exp(c_{11})$ and $\log n > (\log\log n)^2$. We assume that $c_{11} > 2c_{13}$, and further that

$$n > (c_{11}\log n)^{3j+3} > 2c_{13}(c_{11}\log n)^{3j+1}.$$

In this case,

$$\nu_q(u_n) \geq n/2 > c_{13}(c_{11}\log n)^{3j+1} > \nu_q(N_j),$$

so

$$\nu_q(u_n - N_j) = \nu_q(N_j) < c_{13}(c_{11}\log n)^{3j+1}.$$

Comparing this upper bound on the exponent of q on the left–hand side of (4.10) with the lower–bound from (4.11), we get

$$\frac{m_{j+1}}{\log m_{j+1}} \leq c_{14}(c_{11}\log n)^{3j+1} \qquad \text{where} \qquad c_{14} := c_{13}/c_{12}.$$

The inequality $x/\log x < y$ implies $x < 2y\log y$ for $y > e$. Hence,

$$\begin{aligned} m_{j+1} &< 2c_{14}(c_{11}\log n)^{3j+1}(\log c_{14} + (3j+1)(\log c_{11} + \log\log n)) \\ &< 2(6j+3)c_{14}(c_{11}\log n)^{3j+1}\log\log n \\ &< 20c_{14}(c_{11}\log n)^{3j+1}(\log\log n)^2 \\ &< (c_{11}\log n)^{3j+3}. \end{aligned}$$

In the above chain of inequalities, we assumed that $n > \max\{\exp(c_{11}, \exp(c_{14})\}$ and for the last inequality it suffices to assume that $c_{11} > 20c_{14}$. This is the induction step for this case.

Case 2. $\gcd(r, s) = 1$ and $s \neq \pm 1$.

In this case, there exists a prime ideal $\pi \in \mathcal{O}_{\mathbb{K}}$ dividing α, where $\mathbb{K} := \mathbb{Q}(\alpha)$. Indeed, this is true since if it were not, then α would be a unit. Since $|\alpha| > 1$, this unit cannot be rational because the only rational units are ± 1. Hence, α is a quadratic unit, β is its conjugate, and $s = -\alpha\beta = \pm 1$, which is not the case we are treating. Further, since π divides α and r and s are coprime, it follows that π does not divide β. Further, it is clear that π sits above a rational prime q dividing s. We write again

$$N_j := \pm\tau(m_1!) \pm \cdots \pm \tau(m_j!). \tag{4.13}$$

Rewrite again equation (4.1) as in (4.10),

$$c\alpha^n + (d\beta^n - N_j) = \pm\tau(m_{j+1}!) \pm \cdots \pm \tau(m_k!). \tag{4.14}$$

Suppose that

$$d\beta^n - N_j \neq 0. \tag{4.15}$$

We then compute an upper bound for the π-adic order of the above nonzero number using Lemma 4.6. Thus,

$$\begin{aligned} \nu_\pi(d\beta^n - N_j) &= \nu_\pi(d\beta^n) + \nu_\pi\left(\beta^{-n}(N_j d^{-1}) - 1\right) \\ &\leq c_{15} + c_{16}\log|N_j| \\ &\leq (2c_{13}\log q)(c_{11}\log n)^{3j+1} \end{aligned} \tag{4.16}$$

for $n \geq n_0$, where we applied Lemma 4.6 with

$$\eta_1 =: \beta, \quad \eta_2 = N_j d^{-1}, \quad m_1 := -n, \quad m_2 := 1,$$

and we also used the calculation (4.12) for an upper bound on $\log|N_j|$. Then, inequality (4.16) implies that

$$\nu_\pi(d\beta^n - N_j) < (c_{11}\log n)^{3j+2} < n - c_{17} \leq \nu_\pi(c\alpha^n)$$

for $n > n_0$, where $c_{17} := \max\{1, -\nu_\pi(c)\}$, which shows that

$$\begin{aligned} \nu_\pi(u_n - N_j) &= \nu_\pi(c\alpha^n + (d\beta^n - N_j)) \\ &= \nu_\pi(d\beta^n - N_j) \\ &< (c_{11}\log n)^{3j+2}. \end{aligned} \tag{4.17}$$

Comparing this with the lower bound on the exponent of q on the right–hand side of (5.6) estimated in (4.11), we get

$$c_{12}\frac{m_{j+1}}{\log m_{j+1}} \leq (c_{11}\log n)^{3j+2},$$

so

$$\begin{aligned} m_{j+1} &\leq (2/c_{12})(c_{11}\log n)^{3j+2}(\log(1/c_{12}) + (3j+2)(\log c_{11} + \log\log n)) \\ &\leq (2/c_{12})(6j+5)\log\log n(c_{11}\log n)^{3j+2} \\ &< (22/c_{12})(c_{11}\log n)^{3j+3} \end{aligned}$$

for $n > \max\{\exp(c_{11}), \exp(2/c_{12})\}$ and $\log n > (\log\log n)^2$. The right–hand side above is smaller than $(c_{11}\log n)^{3j+3}$ if $c_{11} > 22/c_{12}$. This is the induction step in this case,
This was however under the assumption (4.15). Let us see what happens if on the contrary $N_j = d\beta^n$. Then $d \in \mathbb{Q}^*$ and $\beta \in \mathbb{Z}$. If $|\beta| \geq 2$, we then have that

$$n\log 2 + \log|d| \leq \log|d\beta^n| = \log|N_j| < c_{13}(c_{11}\log n)^{3j}.$$

This implies $n < (c_{11}\log n)^{3j+3}$ for $n \geq n_0$, which implies the desired lower bound on k. Thus, we may assume that $\beta = \pm 1$. Treating separately the cases when n is even and when n is odd; i.e., replacing the sequence $\{u_n\}_{n\geq 0}$ by the two sequences $\{u_{2n}\}_{n\geq 0}$ and $\{u_{2n+1}\}_{n\geq 0}$, which has as effect of replacing the pair of roots (α, β) by the pair of roots (α^2, β^2), we may assume that $\beta = 1$. Then $d = N_j$, and so $j = j_0 \leq c_{18}$. We fix j_0 and work with the relation

$$a\alpha^n = \pm\tau(m_{j_0+1}!) \pm \cdots \pm \tau(m_k!).$$

Relabelling the indices in the right–hand side above, we may assume that they are $1 \leq m_1 \leq \cdots \leq m_k$. We let q be the smallest prime not dividing a. Then $m_1 < c_{19}$. We rewrite our equation as

$$a\alpha^n \pm \tau(m_1!) = \pm\tau(m_2!) \pm \cdots \pm \tau(m_k!).$$

We apply Lemma 4.6 to bound the q-adic valuation of the the left–hand side above getting $\nu_q(a\alpha^n \pm \tau(m_1!)) < c_{20}\log n$. This implies, by an argument similar to the one used before, that $m_2 < c_{21}\log n$. From now on, the proof proceeds in the same way as before and yields that (4.6) implies (4.7) with some appropriate constant $c_{11} > c_{21}$.

Case 3. $s = \pm 1$.

Here, α and β are quadratic units. As we already mentioned before, treating separately the cases n even and n odd amounts to replacing $\{u_n\}_{n\geq 0}$ by the two sequences $\{u_{2n}\}_{n\geq 0}$ and $\{u_{2n+1}\}_{n\geq 0}$. Thus, we replace (α, β) by (α^2, β^2), and therefore we may assume that $s = -1$, and $\beta = \alpha^{-1}$. We write

$$\begin{aligned} u_n - N_j &= c\alpha^n + d\beta^n - N_j \\ &= c\beta^n\left(\alpha^{2n} - c^{-1}N_j\alpha^n + dc^{-1}\right) \\ &= c\beta^n(\alpha^n - z_{1,j})(\alpha^n - z_{2,j}), \end{aligned}$$

where

$$z_{i,j} = \frac{c^{-1}N_j \pm \sqrt{c^{-2}N_j^2 - 4dc^{-1}}}{2} \quad \text{for} \quad i = 1, 2$$

are the roots of the quadratic equation $x^2 - c^{-1}N_j x + dc^{-1} = 0$. We let $\mathbb{L}_j := \mathbb{K}(z_{1,j})$ and π be some prime ideal of $\mathbb{L}_j$ sitting above the prime 2 (which is the smallest prime that does not divide $s = 1$). Then, by Lemma 4.6, we have

$$\nu_2(u_n - N_j) \leq \nu_\pi(u_n - N_j) = \nu_\pi(c\alpha^n) + \nu_\pi(\alpha^n - z_{1,j}) + \nu_\pi(\alpha^n - z_{2,j}).$$

Since $\mathbb{L}_j$ is of degree at most 4 and α is a unit, $\nu_\pi(c\alpha^n) = \nu_\pi(c) \leq c_{22}$, where we can take $c_{22} := 4\max\{\nu_\pi(c), 1\}$. The other two quantities can be bounded as

$$\max_{i=1,2}\{\nu_\pi(\alpha^n - z_{i,j})\} \leq c_{23}\log H(z_{i,j})\log n \leq c_{24}(c_{11}\log n)^{3j+1},$$

where we used (4.12), as well as the fact that

$$\log H(z_{i,j}) \leq c_{25}\log N_j \quad \text{for} \quad i = 1, 2$$

Hence,

$$\nu_2(u_n - N_j) < c_{22} + 2c_{24}(c_{12}\log n)^{3j+1} < 3c_{26}(\log n)^{2j+1} \quad \text{for} \quad n \geq n_0. \tag{4.18}$$

From now on, the argument continues as in the preceding case, by writing a lower bound for $\nu_2(u_n - N_j) = \nu_2(\pm\tau(m_{j+1}!) \pm \cdots \pm \tau(m_k!))$ as in (4.11) then comparing it with (4.18) to get

$$\frac{m_{j+1}}{\log m_{j+1}} < 3c_{26}(c_{11}\log n)^{3j+1}.$$

This leads to

$$\begin{aligned} m_{j+1} &< 6c_{26}(c_{11}\log n)^{3j+1}(\log(3c_{26}) + (3j+1)(\log(c_{11}) + \log\log n)) \\ &< 6c_{26}(6j+3)(c_{11}\log n)^{3j+1}\log\log n \\ &< 60c_{26}(c_{11}\log n)^{3j+3} \end{aligned}$$

assuming $n > \max\{\exp(c_{11}), \exp(3c_{26}\}$. This is the induction step for this case assuming $c_{11} > 60c_{26}$. The claim, and hence the theorem, is therefore proved.

4.2 The proof of Theorem 4.2

In proving Theorem 4.2, we use some information from Lemma 3.2.

Lemma 4.7 *Assume that* $n \geq 1000$. *We have*

(i) $(n-2)\log\alpha < 6m_2 \log m_2$;

(ii) $m_2 > n/(18\log n)$;

(iii) $m_1 < 2\log(4n/3)/(3\log 2)$.

Proof Clearly, $m_2 \geq 2$. Then

$$\alpha^{n-2} < F_n \leq |\tau(m_1!)| + |\tau(m_2!)| \leq 2\max\{|\tau(m_1!)|, |\tau(m_2!)|\} < 4(m_2!)^6$$

(see page 182 in [10]). Hence,

$$\alpha^{n-2} < 4(m_2!)^6 \leq 4m_2^{6(m_2-1)} = \left(\frac{4}{m_2^6}\right) m_2^{6m_2} < \exp(6m_2 \log m_2).$$

In particular,

$$(n-2)\log\alpha < 6m_2 \log m_2, \tag{4.19}$$

which is (i). Suppose that $m_2 < n/(18\log n)$. We then get

$$(n-2)\log\alpha < 6m_2 \log m_2 < n/3,$$

which gives

$$(3\log\alpha)(n-2) < n \qquad \text{and so} \qquad n < \frac{6\log\alpha}{3\log\alpha - 1} < 7,$$

a contradiction. Thus, $m_2 \geq n/(18\log n)$. This proves (ii).

For (iii), assume that $m_1 \geq 4$, otherwise the stated inequality clearly holds because $n \geq 1000$. We then have $m_2 \geq m_1$, and so

$$\nu_2(\tau(m_1!)) \geq 3\nu_2(m_1!) \geq 3\left(\left\lfloor \frac{m_1}{2} \right\rfloor + \left\lfloor \frac{m_1}{4} \right\rfloor + \cdots\right) \geq 3\left(\left\lfloor \frac{m_1}{2} \right\rfloor + 1\right) > \frac{3m_1}{2},$$

and similarly

$$\nu_2(\tau(m_2!)) \geq 3\nu_2(m_2!) \geq 3\nu_2(m_1!) \geq \frac{3m_1}{2}.$$

Hence,

$$\nu_2(F_n) = \nu_2(\pm\tau(m_1!) \pm \tau(m_2!)) \geq \min\{\nu_2(\tau(m_1!)), \nu_2(\tau(m_2!))\} \geq \frac{3m_1}{2}.$$

The right-hand side above is at least 6 since we are assuming that $m_1 \geq 4$. Since for $k \geq 3$, we have $2^k \mid F_n$ if and only if $3 \times 2^{k-2} \mid n$, it follows that $k \leq \nu_2(F_n) \leq \log(4n/3)\log 2$. Putting these together, we have that

$$\frac{3m_1}{2} \leq \nu_2(F_n) \leq \frac{\log(4n/3)}{\log 2},$$

which implies the desired inequality (ii).

In proving Theorem 4.2, we now consider the following cases:

4.2.1 The case $m_1 = 1$

We assume $m_2 \geq 4$. In this case, the given equation is

$$F_n \pm 1 = |\tau(m_2)!|. \tag{4.20}$$

On the left–hand side, we use the fact that $F_n \pm 1 = F_{(n+\delta)/2}L_{(n-\delta)/2}$, for some suitable $\delta \in \{\pm 1, \pm 2\}$ which depends on the residue-class of n modulo 4 and on the sign of ± 1 (see, for example, [8]). Here, $\{L_m\}_{m\geq 0}$ is the Lucas companion of the Fibonacci sequence given by $L_0 = 2,\ L_1 = 1$ and $L_{m+2} = L_{m+1} + L_m$ for all $m \geq 0$. It thus follows, from the previous arguments, that for $m_2 \geq 2$, we have

$$\begin{aligned} \frac{3m_2}{2} &\leq 3\nu_2(m_2!) \leq \nu_2(\tau(m_2!)) = \nu_2(F_{(n+\delta)/2}L_{(n-\delta)/2}) \\ &\leq \nu_2(F_{(n+\delta)/2}) + \nu_2(L_{(n-\delta)/2}) \\ &\leq \frac{\log(4(n+2)/3)}{\log 2} + 2 = \frac{\log(16(n+2)/3)}{\log 2}. \end{aligned}$$

It thus follows that

$$m_2 \leq \frac{2\log(16(n+2)/3)}{3\log 2}, \tag{4.21}$$

so, using Lemma 4.7 (i),

$$(n-2)\log\alpha < 6m_2\log m_2 < \frac{4\log(16(n+2)/3)}{\log 2}\log\left(\frac{2\log(16(n+2)/3)}{3\log 2}\right),$$

which implies that $n < 160$, a contradiction with the fact that $n \geq 1000$. Let us record what we have proved.

Lemma 4.8 *If $m_1 = 1$, then $n < 1000$.*

4.2.2 The case $m_1 \geq 2$

For this case we apply a linear form in two 2-adic logarithms. We follow the proof of Case 3 of Theorem 4.1 by making all the estimates there explicit. The given equation is

$$\pm\tau(m_2!) = F_n \mp \tau(m_1!) = F_n - N, \qquad \text{where} \qquad N := \pm\tau(m_1!). \tag{4.22}$$

Writing

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} = \frac{\alpha^n - \varepsilon\alpha^{-n}}{\sqrt{5}}, \qquad \varepsilon = (-1)^n \in \{\pm 1\},$$

equation (4.22) becomes

$$\pm\tau(m_2!) = \frac{\alpha^{-n}}{\sqrt{5}}\left(\alpha^{2n} - \sqrt{5}N\alpha^n - \varepsilon\right) = \frac{\alpha^{-n}}{\sqrt{5}}(\alpha^n - z_1)(\alpha^n - z_2), \tag{4.23}$$

where

$$z_{1,2} = \frac{N\sqrt{5} \pm \sqrt{5N^2 + 4\varepsilon}}{2}.$$

We take a look at the number under the second square-root, namely $\triangle = 5N^2 + 4\varepsilon$ and we indicate it by $\square$ if it is a perfect square. It is coprime to 5 and not a square. Indeed if $5N^2 + 4\varepsilon = \square$, it follows that $\square - 5N^2 = \pm 4$. Associating this with identity $L_n^2 - 5F_n^2 = \pm 4$ implies that $N = F_k$ for some k (see identity (2.4) and the remarks following it). However, in our previous paper [32] and also Chapter 3 of this thesis, we showed that the only solution of the Diophantine equation $F_k = |\tau(m_1!)|$ has $m_1 = 1$ and in our case $m_1 \geq 2$. Thus, indeed $5N^2 + 4\varepsilon = d\square$, where $d \notin \{1, 5\}$. Note that d is positive. Further, write $N = 2^a N_1$ for some odd integer N_1. Clearly, $a \geq 3$. Hence $5N^2 + 4\varepsilon = 4(5 \cdot 2^{2a-2}N_1^2 + \varepsilon)$, showing that, in fact $5 \cdot 2^{2a-2}N_1^2 + \varepsilon = d\square$. It follows that $d \equiv \pm 1 \pmod 8$.

Let us write $\triangle = d\square$.

We now prove that α and $z_{1,2}$ are multiplicatively independent. On the contrary suppose α and one of z_1 or z_2 are multiplicatively dependent. Then by Definition 2.8, there exist integers u and v not both 0 such that $\alpha^u = z_i^v$ for some $i = 1, 2$. Replacing the pair (u, v) by the pair $(2u, 2v)$ if needed, we may assume that v is even. Note that

$$z_{1,2}^2 = \frac{(5N^2 + \triangle) \pm 2N\sqrt{\triangle}}{4} \in \mathbb{Q}[\sqrt{d}].$$

Thus $z_i^v = (z_i^2)^{v/2} = \alpha^u \in \mathbb{Q}[\sqrt{5}] \cap \mathbb{Q}[\sqrt{d}]$. Since $d \neq 1$ and coprime to 5 and squarefree, the above intersection is $\mathbb{Q}$. Thus $\alpha^u \in \mathbb{Q}$ which implies that $u = 0$. Thus $z_i^v = 1$, which implies $v = 0$, yielding a contradiction.

We next look at the biquadratic field $\mathbb{K} = \mathbb{Q}[\sqrt{5}, \sqrt{d}]$. It contains α as well as $z_1^2,\ z_2^2$. The prime 2 is inert in $\mathbb{Q}[\sqrt{5}]$, whereas the prime 2 is either the square of a prime or product of two distinct primes in $\mathbb{Q}[\sqrt{d}]$ according to whether $d \equiv -1 \pmod 8$ or $d \equiv 1 \pmod 8$. This shows that in $\mathbb{K}$, we have

$$2\mathcal{O}_{\mathbb{K}} = \pi_0^2 \text{ or } \pi_1\pi_2,$$

where in all cases $\mathcal{O}_{\mathbb{K}}/\pi_i$ for $i = 0, 1, 2$ has 2^2 elements. Thus, in classical notation, any prime ideal π of $\mathbb{K}$ sitting over 2 has $f = 2$ and hence putting $D := [\mathbb{K} : \mathbb{Q}]/f$, we have $D = 2$. Furthermore, taking $|x|_2 = 2^{-\nu(x)}$, where $\nu(x)$ is the exponent of 2 in the unique extension to $\mathbb{K}$ of the 2-adic valuation such that $|2|_2 = 2^{-1}$, it follows easily that $\nu(x) = \nu_{\pi_0}(x)/2$ or $(\nu_{\pi_1}(x) + \nu_{\pi_2}(x))/2$, according to whether $2\mathcal{O}_{\mathbb{K}} = \pi_0^2$ or $\pi_1\pi_2$, respectively. Note now that

$$\begin{aligned} z_{1,2}^2 &= \frac{5N^2 + (5N^2 + 4\varepsilon) \pm 2N\sqrt{5(5N^2 + 4\varepsilon)}}{4} \\ &= 5 \cdot 2^{2a-2}N_1^2 + (5 \cdot 2^{2a-2} + \varepsilon) + 2^a N_1\sqrt{5(5 \cdot 2^{2a-2}N_1^2 + \varepsilon)} \\ &\equiv 1 \pmod{\pi}. \end{aligned}$$

Furthermore,

$$\alpha^3 = \alpha^2 + \alpha = 2\alpha + 1 \equiv 1 \pmod{\pi}.$$

It thus follows that if we take $g := 3$, then $\alpha^g \equiv (z_{1,2}^2)^g \equiv 1 \pmod \pi$. Equation (4.23) together with the fact that α is a unit shows that

$$\tau(m_2!) \mid (\alpha^n - z_1)(\alpha^n - z_2) \mid (\alpha^{2n} - z_1^2)(\alpha^{2n} - z_2^2).$$

It thus follows that

$$\nu_\pi(\tau(m_2!)) \leq \nu_\pi((\alpha^{2n} - z_1^2)(\alpha^{2n} - z_2^2)).$$

On the left, we have that

$$\nu_\pi(\tau(m_2!)) \geq \nu_2(\tau(m_2!)) \geq 3\nu_2(m_2!) \geq 3m_2/2.$$

On the right, we have

$$\begin{aligned}\nu_\pi((\alpha^{2n}-z_1^2)(\alpha^{2n}-z_2^2)) &= \max\{\nu_\pi(\alpha^{2n}-z_1^2),\nu_\pi(\alpha^{2n}-z_2^2)\}\\ &+ \min\{\nu_\pi(\alpha^{2n}-z_1^2),\nu_\pi(\alpha^{2n}-z_2^2)\} \qquad (4.24)\\ &\le 2\max\{v_2(\alpha^{2n}-z_i^2); i=1,2\}+\nu_\pi(z_1^2-z_2^2).\end{aligned}$$

Note that $z_1^2 - z_2^2 = 2^{a+1}N_1\sqrt{5(5\cdot 2^{2a-2}N_1^2+\varepsilon)}$, so

$$\nu_\pi(z_1^2-z_2^2) \le \nu_\pi(2^{a+1}) = \nu_\pi(2\tau(m_1!)) \le 2\nu_2(2\tau(m_1!)).$$

Now

$$2\tau(m_1!) \le 4m_1!^6 \le 4m_1^{6m_1-6} = \left(\frac{4}{m_1^6}\right)m_1^{6m_1} < m_1^{6m_1},$$

so

$$\nu_2(2\tau(m_1!)) \le \frac{6m_1\log m_1}{\log 2}$$

and

$$\nu_\pi(z_1^2-z_2^2) < \frac{12m_1\log m_1}{\log 2} < 24m_1\log m_1. \qquad (4.25)$$

It remains to find an upper bound on $v_2(\alpha^{2n}-z_i^2)$. Since we have proved that α and $z_{1,2}$ are multiplicatively independent, we can use Lemma 2.10. In the notation of that lemma, we have

$$v_2(\alpha^{2n}-z_i^2) \le \frac{24\cdot 2\cdot 3}{(\log 2)^4}D^4\max\{\log b' + \log\log 2 + 0.4, 10\}^2\log A_1\log A_2,$$

where $\log A_j \ge \max\{h(\alpha_j), \log 2/D\}$, for $j=1,2$, where $\alpha_1 := \alpha$ and $\alpha_2 := z_i$ (and $i=1$ or 2). Here, $D=2$. Furthermore, for $j=1$, we can take $\log A_1 = 0.35 > \max\{h(\alpha), \log 2/2)$. As for $j=2$, considering z_1 to be such that $z_1^2 > 1$ (and $z_2^2 = 1/z_1^2$), we then have

$$\begin{aligned}z_1^2 &= \left(\frac{N\sqrt{5}+\sqrt{5N^2+4\varepsilon}}{2}\right)^2 < 5N^2+4 < 9N^2 < 9(2m_1!^6)^2\\ &< 9\cdot 4m_1^{12(m_1-1)} = \left(\frac{36}{m_1^{12}}\right)m_1^{12m_1} < m_1^{12m_1}\end{aligned}$$

showing that

$$h(z_1^2) = \frac{1}{2}\log(z_1^2) < 6m_1\log m_1.$$

So, we can take $\log A_2 := 6m_1 \log m_1$. Finally,

$$b' := \frac{2n}{D \log A_2} + \frac{1}{D \log A_1} = \frac{2n}{12 m_1 \log m_1} + \frac{1}{0.7} < \frac{n}{2},$$

where we used the fact that $m_1 \geq 2$ and $n \geq 1000$. In particular,

$$\log b' + \log\log 2 + 0.4 < \log(n/2) + \log\log 2 + 0.4 < \log n.$$

Thus,

$$v_2(\alpha^{2n} - z_i^2) \leq \frac{24 \cdot 2 \cdot 3}{(\log 2)^4} 2^4 (6 m_1 \log m_1) \cdot 0.35 \max\{\log n, 10\}^2.$$

It thus follows, by (4.24) and (4.25), that

$$\begin{aligned} \nu_\pi((\alpha^{2n} - z_1^2)(\alpha^{2n} - z_2^2)) &\leq \frac{24 \cdot 2 \cdot 3 \cdot 2^5 \cdot 0.35 \cdot 6}{(\log 2)^4} (m_1 \log m_1) \max\{\log n, 10\}^2 \\ &+ 24(m_1 \log m_1). \end{aligned}$$

Since $24 \cdot 2 \cdot 3 \cdot 2^5 \cdot 0.35 \cdot 6/(\log 2)^4 < 41950$, it follows that

$$\nu_\pi((\alpha^{2n} - z_1^2)(\alpha^{2n} - z_2^2)) < 50000 m_1 \log m_1 \left(\max\{\log n, 10\}\right)^2.$$

If $\log n < 10$, then $n < 23000$. So, assume $\log n \geq 10$. It thus follows that

$$\nu_\pi((\alpha^{2n} - z_1^2)(\alpha^{2n} - z_2^2)) < 50000 m_1 \log m_1 (\log n)^2.$$

We thus get that

$$3m_2/2 \leq \nu_2(3m_2!) \leq \nu_2(\tau(m_2!)) \leq \nu_\pi(\tau(m_2!)) \leq 50000 m_1 \log m_1 (\log n)^2. \tag{4.26}$$

Combining this with Lemma 4.7 (ii) and (iii), we get

$$\frac{n}{12 \log n} < 50000 \left(\frac{2\log(4n/3)}{3 \log 2}\right) \log \left(\frac{2\log(4n/3)}{3 \log 2}\right) (\log n)^2,$$

which gives $n < 1.2 \times 10^{12}$. Let us record what we have proved.

Lemma 4.9 *For $n \geq 1000$, we have $m_1 \geq 2$ and $n < 1.2 \times 10^{12}$.*

4.2.3 Final computations

Assume first that $m_1 = 1$. Then $n < 1000$ by Lemma 4.8. Inequality (4.21) tells us that $m_2 \leq 8$. We now generated the list of numbers $|\pm\tau(m_2!) \pm 1|$ for all $m_1 \in \{1, \ldots, 8\}$ and the only Fibonacci number F_n with positive n found in this list is $2 = F_3$.

Assume next that $m_1 > 1$. Then $n < 1.2 \times 10^{12}$. By Lemma 4.7 (iii), we get that $m_1 \leq 27$. Assume that $m_2 \leq 100$. Then Lemma 4.7 (i) shows that $n < 5500$. We generated the list of all numbers of the form $\pm\tau(m_1!) \pm \tau(m_2!)$ for $1 \leq m_1 \leq m_2 \leq 100$ and intersected it with the list of Fibonacci numbers F_n for $n \in [1, 5500]$ obtaining only the solutions from the statement of the theorem.

From now on, $m_2 > 100$. Assume $m_1 \geq 10$. We checked that in the range $m \in [10, 27]$, we have that

$$2^{27} \mid \tau(m!), \qquad 3^8 \mid \tau(m!), \qquad 5^2 \mid \tau(m!).$$

The above divisibilities persist even for $m \geq 28$. Indeed, for $m \geq 28$, we have that

$$\nu_2(\tau(m!)) \geq 3\nu_2(m!) \geq 3m/2 > m > 27.$$

Furthermore, since $3 \mid \tau(3)$, one proves by induction that $3^k \mid \tau(3^k)$ for all $k \geq 1$. Thus,

$$\nu_3(\tau(m!)) \geq \nu_3(m!) > m/3 > 8.$$

Similarly, since $5 \mid \tau(5)$, we deduce that $5^k \mid \tau(5^k)$ for all $k \geq 1$, so

$$\nu_5(\tau(m!)) \geq \nu_5(m!) > m/5 > 2.$$

Thus, for $m_1 \geq 10$, we have that $2^{27} \cdot 3^8 \cdot 5^2 \mid \pm\tau(m_1!) \pm \tau(m_2!)$, so $2^{27} \cdot 3^8 \cdot 5^2 \mid F_n$. This implies that $2^{25} \cdot 3^7 \cdot 5^2 \mid n$. Hence,

$$n \geq 2^{25} \cdot 3^7 \cdot 5^2 > 1.8 \times 10^{12},$$

a contradiction. Thus, $m_1 \leq 9$.

Going to (4.26) and using Lemma 4.7 (iii), we get

$$n/(12 \log n) < 50000 \cdot (9 \log 9)(\log n)^2,$$

which gives $n < 2.2 \times 10^{11}$. If $m_1 = 9$, then $2^{25} \cdot 3^{10} \cdot 5^2 \mid \tau(9!)$. By the previous argument, we have that for $m_2 \geq m_1 \geq 9$, we have $2^{25} \cdot 3^8 \cdot 5^2 \mid \pm\tau(m_1!) \pm \tau(m_2!)$. Thus, $2^{25} \cdot 3^8 \cdot 5^2 \mid F_n$, so $2^{23} \cdot 3^7 \cdot 5^2 \mid n$, giving $n \geq 2^{23} \cdot 3^7 \cdot 5^2 > 4 \times 10^{11}$, a contradiction. Thus, $m_1 \leq 8$.
If $m_1 = 8$, then $2^{25} \cdot 3^6 \cdot 5^2 \cdot 7^2 \mid \tau(8!)$. Since $7 \mid \tau(7)$, it follows that $7^k \mid \tau(7^k)$ for all $k \geq 1$. Thus, since $m_2 > 100$, then $\nu_7(\tau(m_2!)) \geq \nu_7(m_2!) > 2$. Thus, in this case $2^{25} \cdot 3^6 \cdot 5^2 \cdot 7^2 \mid \pm\tau(m_1!) \pm \tau(m_2!)$, so $2^{25} \cdot 3^6 \cdot 5^2 \cdot 7^2 \mid F_n$. This leads to $n \geq 2^{23} \cdot 3^5 \cdot 5^2 \cdot 7 > 3 \times 10^{11}$, a contradiction. Thus, $m_1 \leq 7$.
For the remaining values of m_1, we use a 5-adic argument. It is based on the following lemma.

Lemma 4.10 *Let $b \geq 0,\ k \geq 1,\ a \geq 1$ be integers with $5 \nmid a$. Put $M = 4 \cdot 5^b a$. The map $f : \mathbb{Z}/5^k\mathbb{Z} \mapsto \mathbb{Z}/5^k\mathbb{Z}$ given by $f(n \pmod{5^k}) = F_{Mn}/5^b \pmod{5^k}$ is well defined and bijective.*

Proof If $n_1 = n + 5^k m$ for some integer m, then $Mn_1 = Mn + 4 \cdot 5^{k+b}(am)$. Therefore $F_{Mn_1} \equiv F_{Mn} \pmod{5^{k+b}}$ because the Fibonacci sequence is periodic modulo 5^{k+b} with period $4 \cdot 5^{k+b}$. Since $5^b \mid F_{Mn}$ because $5^b \mid M$, it follows that $F_{Mn_1}/5^b \equiv F_{Mn}/5^b \pmod{5^k}$, showing that the map $f(n \pmod{5^k})$ is well-defined. To show that it is injective, assume $0 \leq n < n_1 \leq 5^k - 1$ are such that $F_{Mn_1}/5^b \equiv F_{Mn}/5^b \pmod{5^k}$. Thus, $5^{k+b} \mid F_{Mn_1} - F_{Mn}$. It is well-known that if u, v are integers congruent modulo 4, then using Lemma 2.3, we have $F_u - F_v = F_{(u-v)/2} L_{(u+v)/2}$. Thus, since $4 \mid M$, it follows that $F_{Mn_1} - F_{Mn} = F_{M(n_1-n)/2} L_{M(n_1+n)/2}$. Hence, $5^{k+b} \mid F_{M(n_1-n)/2} L_{(M(n_1+n)/2}$. Since the Lucas numbers are never multiples of 5, we deduce that $5^{b+k} \mid F_{M(n_1-n)/2}$. It then follows that $5^{b+k} \mid M(n_1 - n)/2$, and since $5^b \| M$, it follows that $5^k \mid n_1 - n$, a contradiction.

We are now ready to treat the remaining values.

(i) If $m_1 = 7$.
Then $\tau(7!) = 2^{16} \cdot 3^5 \cdot 5 \cdot 7^2 \cdot 13 \cdot 23^3 \cdot 61 \cdot 241$. Since $F_n = \pm\tau(m_1!) \pm \tau(m_2!)$ and $m_2 \geq 100$, it follows that $2^{17} \cdot 3^6 \cdot 5^{10} \cdot 7^3$ divides $\tau(m_2!)$. Hence, $\nu_2(F_n) = 16,\ \nu_3(F_n) = 5,\ \nu_5(F_n) = 1,\ \nu_7(F_n) = 2$. It follows that $n = M\ell$, where $M := 2^{14} \cdot 3^4 \cdot 5 \cdot 7$. We apply Lemma 4.10 for $k = 2, 3, \ldots, 9$ with $b = 1,\ a = 2^{12} \cdot 3^4 \cdot 7$. Then $M = 4 \cdot 5^b a$. That is, according to

Lemma 4.10, the value of

$$5(F_{M\ell}/5 \pm \tau(7!)/5) \equiv 0 \pmod{5^k} \tag{4.27}$$

determines uniquely the value of ℓ modulo 5^{k-1}. This allows us to find the first few "digits" of ℓ in base 5. For example, taking the sign $-$ in (4.27) for $\tau(7!)$ and $k = 2$, we get $\ell \equiv 2 \pmod 5$. Taking $k = 3$, we get $\ell \equiv 2 \pmod{5^2}$. Taking $k = 4$, we get $\ell \equiv 2 + 1 \cdot 25 \pmod{5^3}$. Continuing in this way with $k = 5, 6, 7$, we get that

$$\ell \equiv 2 \cdot 5^0 + 0 \cdot 5^1 + 1 \cdot 5^2 + 4 \cdot 5^3 + 1 \cdot 5^4 + 2 \cdot 5^5 \pmod{5^6}.$$

In particular, $n = M\ell \geq M(2 + 5^2 + 4 \times 5^3 + 5^4 + 2 \times 5^5) > 3 \times 10^{11}$, a contradiction. On the other hand, if we take the sign $+$ in (4.27), then using the fact that $F_{-M\ell} = -F_{M\ell}$ (because $M\ell$ is even), we conclude that the residue class modulo 5^6 of the ℓ corresponding to the sign $+$ is the negative modulo 5^6 of the value of ℓ corresponding to the sign $-$, namely

$$\ell \equiv 3 \cdot 5^0 + 4 \cdot 5^1 + 3 \cdot 5^2 + 0 \cdot 5^3 + 3 \cdot 5^4 + 2 \cdot 5^5 \pmod{5^6}.$$

In particular, $n \geq M(3 + 4 \cdot 5 + 3 \cdot 5^2 + 3 \cdot 5^4 + 2 \cdot 5^5) > 3 \times 10^{11}$, a contradiction.

(ii) If $m_1 = 6$.

Then $\tau(6!) = -2^{13} \cdot 3^5 \cdot 5 \cdot 7 \cdot 23^2 \cdot 61 \cdot 241$. Since $m_2 \geq 100$, it follows $\nu_2(F_n) = 13$, $\nu_3(F_n) = 5$, $\nu_5(F_n) = 1$. Thus, $2^{11} \cdot 3^4 \cdot 5 \mid n$. So, we take $a := 2^9 \cdot 3^4$, $b := 1$ so $M = 4 \cdot 5^b a$. We write $n = M\ell$. Then, by Lemma 4.10,

$$5(F_{M\ell}/5 \pm |\tau(6!)|/5) \equiv 0 \pmod{5^k}$$

determines ℓ uniquely modulo 5^{k-1} for $k = 2, 3, \ldots, 10$. Exploiting the above congruences for $k = 2, \ldots, 10$, we get

$$\begin{aligned} \ell &\equiv 3 + 4 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 + 3 \cdot 5^4 + 1 \cdot 5^5 + 4 \cdot 5^6 + 3 \cdot 5^7 + 3 \cdot 5^8 \pmod{5^9}; \\ \ell &\equiv 1 + 0 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + 1 \cdot 5^4 + 0 \cdot 5^5 + 0 \cdot 5^6 + 1 \cdot 5^7 + 1 \cdot 5^8 \pmod{5^9}, \end{aligned}$$

according to whether the sign of $|\tau(6!)|$ is $-$ or $+$. In particular, $\ell > 5^8$, so $n = M\ell > 3 \cdot 10^{11}$, a contradiction.

(iii) If $m_1 = 5$.

Then $\tau(5!) = 2^{12} \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 23$. Thus, $2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^2 \mid n$. We take $b := 2,\ a := 2^8 \cdot 3^3 \cdot 7$, so $M := 4 \cdot 5^b a$. We write $n = M\ell$ and exploit the relation

$$5^2(F_{M\ell}/5^2 \pm \tau(5!)/5^2) \equiv 0 \pmod{5^k} \tag{4.28}$$

for $k = 3, \ldots, 10$. We get

$$\begin{aligned} \ell &\equiv 1 \cdot 5^0 + 2 \cdot 5 + 0 \cdot 5^2 + 3 \cdot 5^3 + 2 \cdot 5^4 + 2 \cdot 5^5 + 4 \cdot 5^6 + 1 \cdot 5^7 \pmod{5^8}; \\ \ell &\equiv 4 \cdot 5^0 + 2 \cdot 5 + 4 \cdot 5^2 + 1 \cdot 5^3 + 2 \cdot 5^4 + 2 \cdot 5^5 + 0 \cdot 5^6 + 3 \cdot 5^7 \pmod{5^8}, \end{aligned}$$

according to whether the sign in (4.28) is $-$ or $+$. Hence, $\ell > 5^7$, giving $n = M\ell > 3 \times 10^{11}$, a contradiction.

(iv) If $m_1 = 4$.

We have $\tau(4!) = 2^{11} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$. Thus, $2^{11} \cdot 3^3 \cdot 5 \mid F_n$, so $2^9 \cdot 3^2 \cdot 5 \mid n$. We take $a := 2^7 \cdot 3^2,\ b := 1$ and $M = 4 \cdot 5^b a$. We write $n = M\ell$. We exploit the congruences

$$5(F_{M\ell}/5 \pm \tau(4!)/5) \equiv 0 \pmod{5^k}$$

for $k = 2, 3, \ldots, 13$. We get, according to the sign in the above congruence,

$$\begin{aligned} \ell &\equiv 2 + 1 \cdot 5 + 3 \cdot 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + 4 \cdot 5^5 + 3 \cdot 5^6 + 5^8 \\ &+ 4 \cdot 5^{11} \pmod{5^{12}}; \\ \ell &\equiv 2 + 4 \cdot 5 + 1 \cdot 5^2 + 1 \cdot 5^6 + 4 \cdot 5^7 + 3 \cdot 5^8 + 4 \cdot 5^9 + 4 \cdot 5^{10} \pmod{5^{12}}. \end{aligned}$$

Thus, $\ell > 4 \cdot 5^{10}$, giving that $n = M\ell > 4 \cdot 5^{10} M > 3 \cdot 10^{11}$.

(v) If $m_1 = 3$.

We first revisit inequality (4.26) together with $m_1 \leq 3$, and infer that $n < 3^{10}$. Next, $\tau(3!) = -2^5 \cdot 3^3 \cdot 7$. Thus, $2^5 \cdot 3^3 \mid F_n$, showing that $2^3 \cdot 3^2 \mid n$. So, we take $a := 2 \cdot 3^2,\ b := 0,\ M = 4a$. We write $n = M\ell$ and exploit the congruence

$$F_{M\ell} \pm |\tau(3!)| \equiv 0 \pmod{5^k}$$

for $k = 1, 2, \ldots, 13$. We get

$$\begin{aligned}
\ell &\equiv 2 + 2 \cdot 5 + 5^2 + 3 \cdot 5^3 + 2 \cdot 5^5 + 5^6 + 4 \cdot 5^7 + 4 \cdot 5^8 \\
&+ 5^{11} + 2 \cdot 5^{12} \pmod{5^{13}}; \\
\ell &\equiv 3 + 2 \cdot 5 + 3 \cdot 5^2 + 5^3 + 4 \cdot 5^4 + 2 \cdot 5^5 + 3 \cdot 5^6 + 4 \cdot 5^9 + 4 \cdot 5^{10} \\
&+ 3 \cdot 5^{11} + 2 \cdot 5^{12} \pmod{5^{13}},
\end{aligned}$$

again according to the sign of $|\tau(3!)|$. Thus, $\ell > 2 \cdot 5^{12}$, giving $n = M\ell > 2 \cdot 5^{12} M > 3 \cdot 10^{10}$, a contradiction.

(vi) If $m_1 = 2$.

The inequality (4.26) gives $n < 1.1 \cdot 10^{10}$. Now $\tau(2) = -24$. Since $24 \mid F_n$, it follows that $12 \mid n$. So, we take $a := 3,\ b := 0$, so $M = 12$. We write $n = M\ell$ and exploit the congruences

$$F_{M\ell} \pm |\tau(2!)| \equiv 0 \pmod{5^k}$$

for $k = 1, 2, \ldots, 14$. We get

$$\begin{aligned}
\ell &\equiv 1 + 4 \cdot 5 + 4 \cdot 5^2 + 3 \cdot 5^3 + 5^4 + 2 \cdot 5^5 + 2 \cdot 5^6 + 2 \cdot 5^7 + 4 \cdot 5^8 + 3 \cdot 5^9 \\
&+ 5^{10} + 5^{11} + 2 \cdot 5^{12} + 2 \cdot 5^{13} \pmod{5^{14}}; \\
\ell &\equiv 4 + 5^3 + 3 \cdot 5^4 + 2 \cdot 5^5 + 2 \cdot 5^6 + 2 \cdot 5^7 + 5^9 + 3 \cdot 5^{10} + 3 \cdot 5^{11} \\
&+ 2 \cdot 5^{12} + 2 \cdot 5^{13} \pmod{5^{14}},
\end{aligned}$$

again according to the sign of $|\tau(2!)|$. Thus, $\ell > 2 \cdot 5^{13}$, so $n = M\ell > 2 \cdot 5^{13} M > 2 \cdot 10^{10}$, a contradiction. The theorem is proved.

Chapter 5

On the Prime Factors of the Iterates of the Ramanujan τ-Function

The work in this chapter has been published by the author, his supervisor and P. Stănică, see [33]. The main aim for this chapter is to look at the dynamical system obtained by iteratively applying τ to a positive integer n and this resulted in the lemmas and propositions below. However, there are two obstructions to doing so. The first obvious one is that $\tau(n)$ is negative for some n. For example, $\tau(2) = -24$. To deal with this, we extend τ to negative numbers by putting $\tau(n) := \tau(|n|)$ for any nonzero integer n. A second more subtle obstruction appears if $\tau(n) = 0$ for some n.

This work was inspired by [42], where the authors studied the set of positive integers n such that $n \mid \tau(n)$ and on the way they derived congruences for the τ-function such as $\tau(1000n) \equiv 0 \pmod{64000}$ which holds for all positive integers n.

Independently, Balakrishnan, Craig and Ono showed in [1] that, for $n > 1$, $\tau(n) \notin \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 691\}$, which was further generalized in [2] (by the same authors along with Tsai) to additionally exclude $\tau(n) \notin \{\pm 13, \pm 17, -19, \pm 23, \pm 37\}$. Under the Generalized Riemann Hypothesis, it was also shown in [2] that

$$\tau(n) \notin \{\pm \ell : 41 \leq \ell \leq 97, \left(\frac{\ell}{5}\right) = -1\} \cup \{-11, -29, -31, -41, -59, -61, -71, -79, -89\},$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol.

5.1 Introduction

From the Definition 2.1 of the Ramanujan τ-function and its arithmetic properties stated in Lemma 2.2, we have that if α_p and β_p are the roots of the quadratic polynomial $x^2 - \tau(p)x + p^{11}$, the discriminant $(\alpha_p - \beta_p)^2 = \tau(p)^2 - 4p^{11}$ is negative, since $|\tau(p)| < 2p^{11/2}$. It then follows that α_p and β_p are complex conjugates. In particular, we have

$$\tau(p^a) = \frac{\alpha_p^{a+1} - \beta_p^{a+1}}{\alpha_p - \beta_p} \quad \text{holds for all} \quad a \geq 1.$$

It is a conjecture of Lehmer that $\tau(n) \neq 0$ for all n. This has not yet been proved. If it is false, then there exists a prime p such that $\tau(p) = 0$ and we have the following lemma.

Lemma 5.1 *Assume that the Lehmer conjecture is false, namely that $\tau(n) = 0$ for some integer n. Then for every prime q, there exist a_q such that $\tau(\tau(q^{a_q})) = 0$.*

To deal with this situation, we can also put, by definition $\tau(0) := 0$. One obvious question to ask is what happens with $\tau^{(k)}(n) = \tau\left(\tau(\cdots(\tau(n))\cdots)\right)$ (the composition of τ with itself, k times) for positive integers k and n. We conjecture that the set

$$\mathrm{Orb}_\tau(n) := \{\tau^{(k)}(n) : k \geq 0\} \tag{5.1}$$

is infinite for all $n > 1$. In what follows, we give some support to this conjecture. For a positive integer m, let $P(m)$ be the largest prime factor of m.

Proposition 5.2 *Assume the Lehmer conjecture holds. Then for integers $k \geq 1$ and n even, we have $P(\tau^{(k)}(n)) \geq 3^{k-1} + 2$.*

In particular, if the set $\mathrm{Orb}_\tau(n)$ contains an even element and the Lehmer conjecture holds, then $\mathrm{Orb}_\tau(n)$ is infinite. It remains to look at the situation when $\mathrm{Orb}_\tau(n)$ contains only odd numbers. The smallest odd number (in absolute value) is 1. We have the following proposition.

Proposition 5.3 *If $|\tau(n)| = 1$, then $n = 1$.*

From now on, we assume that $n > 1$, so $|\tau(n)| > 1$ and that $\tau(n)$ is odd. It is then well-known that n is a perfect square. Computations suggest that, in this case, $|\tau(n)|$ is much larger than n. If this was true for all perfect squares $n > 1$, then in case $\mathrm{Orb}_\tau(n)$ contains only odd numbers, the numbers

$$|n|,\ |\tau(n)|,\ |\tau^{(2)}(n)|,\ \ldots,$$

would form a strictly increasing sequence, so in particular $\mathrm{Orb}_\tau(n)$ would also be infinite. We cannot prove that this is indeed so, but we can almost prove it (up to finitely many putative exceptions) under the ABC-conjecture.

Proposition 5.4 *Assume the ABC-conjecture and the Lehmer conjecture. There exists n_0 such that if $n > n_0$ is a perfect square, then $|\tau(n)| > n$. In particular, if $\mathrm{Orb}_\tau(n)$ contains only odd numbers, then $\mathrm{Orb}_\tau(n)$ is infinite.*

Further, let n be such that $\mathrm{Orb}_\tau(n)$ has at least cardinality $k+1$ and assume the Lehmer conjecture. Put

$$\mathrm{Orb}_\tau(n,k) := \{|n|, |\tau(n)|, \ldots, |\tau^{(k)}(n)|\},$$

and assume that the elements in the above set are all distinct and nonzero. We ask whether we can say something about the prime factors of the above numbers. Let

$$P(\mathrm{Orb}_\tau(n,k)) := \max\{P(m), m \in \mathrm{Orb}_\tau(n,k)\}.$$

We have the following result.

Proposition 5.5 *Assume $k \geq 1$ is an integer. If the Lehmer conjecture holds and $\mathrm{Orb}_\tau(n,k)$ has cardinality $k+1$, then*

$$P(\mathrm{Orb}_\tau(n,k)) > \log(k/2). \tag{5.2}$$

Next, let $\mathcal{S} = \{p_1, \ldots, p_s\}$ be a finite set of odd primes arranged increasingly and let $P = p_s$ be the largest. We ask whether it is possible to compute the cardinality of the set of n such that

$$\tau(n) = \pm p_1^{a_1} \cdots p_s^{a_s} \quad \text{for some integer exponents} \quad a_1, \ldots, a_s. \tag{5.3}$$

By the multiplicativity of the function τ, it suffices to compute the number of solutions of the form p^a for some odd prime p and even positive integer a. If this number is denoted by Ω, then clearly the total number of solutions of (5.3) is at most 2^{Ω}.

Proposition 5.6 *The number of solutions $n = p^a$ with a prime p and a positive even integer a to the equation* (5.3) *is at most* $\max\{P, 11\}^{6500(s+4)}$.

Taking $S = \{3, 5, 7\}$, we have $s = 3,\ P = 7$ so equation (5.3) has at most 11^{45500} solutions of the form $n = p^a$ for an odd prime p and a positive even integer a. We end up with a computational result showing that in fact there is no such solution.

Proposition 5.7 *There is no $n > 1$ such that $\tau(n)$ is odd and $P(\tau(n)) \leq 10$.*

This last result shows that in Proposition 5.6, the bound $\max\{P, 11\}$ can be replaced by P. Indeed, either $P \geq 11$, in which case the maximum is P, or $P \leq 10$, in which case there is no solution to equation (5.3) so the stated inequality holds anyway.
We now prove the stated lemma and propositions above.

5.1.1 Proof of Lemma 5.1

Assume $\tau(n) = 0$ for some n. Then there is a prime p with $\tau(p) = 0$. For $q = p$, we take $a_q = 2$. Then $\tau(p^2) = (\tau(p))^2 - p^{11} = -p^{11}$. Since 11 is odd, $\tau(p^{11})$ is an integer multiple of $\tau(p)$, so it is zero. Hence, $\tau(\tau(p^2)) = 0$. Assume next that $q \neq p$. In particular, we may assume that $\tau(q) \neq 0$. The sequence $\{\tau(q^a)\}_{a\geq 0}$ is the shift of a Lucas sequence. To see this, recall that by putting $\alpha_q,\ \beta_q$ for the roots of the quadratic

$$x^2 - \tau(q)x + q^{11}, \tag{5.4}$$

we have

$$\tau(q^a) = \frac{\alpha_q^{a+1} - \beta_q^{a+1}}{\alpha_q - \beta_q}.$$

Using Definition 2.4, we show that $(\tau(q^a))_{a\geq 0}$ is a Lehmer sequence by showing that the ratio α_q/β_q is not a root of unity. Indeed, assume it is. Then since it is also a quadratic number, it follows that it is a root of unity of orders one of $1, 2, 3, 4, 6$. It is not possible

that $\alpha_q/\beta_q = 1$, since the discriminant $\tau(q)^2 - 4q^{11}$ of the quadratic (5.4) is negative so α_q and β_q are complex non-real and they are conjugates. It is also not possible that $\alpha_q/\beta_q = -1$, since we have assumed that $\tau(q) = \alpha_q + \beta_q \neq 0$. Thus, the order is one of $3, 4, 6$. Since

$$\tau(q^a) = \frac{\alpha_q^{a+1} - \beta_q^{a+1}}{\alpha_q - \beta_q},$$

it follows that $\tau(q^a) = 0$ for some $a \in \{2, 3, 5\}$. However,

$$\begin{aligned}
\tau(q^2) &= \frac{\alpha_q^3 - \beta_q^3}{\alpha_q - \beta_q} = \alpha_q^2 + \alpha_q\beta_q + \beta_q^2 = \tau(q)^2 - q^{11};\\
\tau(q^3) &= \frac{\alpha_q^4 - \beta_q^4}{\alpha_q - \beta_q} = (\alpha_q + \beta_q)(\alpha_q^2 + \beta_q^2) = \tau(q)(\tau(q)^2 - 2q^{11});\\
\tau(q^5) &= \frac{\alpha_q^6 - \beta_q^6}{\alpha_q - \beta_q} = (\alpha_q + \beta_q)(\alpha_q^2 + \alpha_q\beta_q + \beta_q^2)(\alpha_q^2 - \alpha_q\beta_a + \beta_q^2)\\
&= \tau(q)(\tau(q)^2 - q^{11})(\tau(q)^2 - 3q^{11}),
\end{aligned}$$

so we see that if one of the above expressions is zero but $\tau(q) \neq 0$, it follows that one of $\tau(q)^2 - bq^{11}$ is zero for some $b \in \{1, 2, 3\}$, this is impossible for $b = 1$ and for $b \in \{2, 3\}$, and hence it implies that $q = b$. So, $q \in \{2, 3\}$. However, one checks that α_2/β_2 is not a root of unity of order 4 and that α_3/β_3 is not a root of unity of order 6. Hence, $\{\tau(q^a)\}_{a\geq 0}$ is *almost* a Lucas sequence, except that it might be that $\tau(q)$ and q^{11} are not coprime. Put $d := \gcd(\tau(q), q^{11}) > 1$. Thus, $d = q^\lambda$. For $q = 2$, we have $\tau(2) = -24$, so $d = 8$ and $\lambda = 3$. For $q = 3$, we have $\tau(3) = 252 = 2^2 \cdot 3^2 \cdot 7$, so $d = 9$ and $\lambda = 2$. For $q \geq 5$, since $|\tau(q)| < 2q^{11/2}$, it follows that $q^\lambda \leq |\tau(q)| \leq 2q^{11/2} < q^6$, so $\lambda \in \{1, 2, 3, 4, 5\}$. Then writing $(\gamma_q, \delta_q) := (\alpha_q/q^\lambda, \beta_q/q^\lambda)$, we have

$$\tau(q^a) = q^{\lambda a}\left(\frac{\gamma_q^{a+1} - \delta_q^{a+1}}{\lambda_q - \delta_q}\right).$$

Further, (λ_q, δ_q) are the roots of the quadratic $x^2 - (\tau(q)/q^\lambda)x + q^{11-2\lambda}$ and $\tau(q)/q^\lambda$ and $q^{11-2\lambda}$ are coprime and $\gamma_q/\delta_q = \alpha_q/\beta_q$ is not a root of unity. Thus,

$$\tau(q^a) = q^{\lambda a}u_q(a + 1),$$

where $\{u_q(m)\}_{m\geq 0}$ is the Lucas sequence of roots (γ_q, δ_q).

Now let again p be such that $\tau(p) = 0$. Let b_p be the order of appearance of p in the sequence $\{u_q(m)\}_{m\geq 0}$. This is the smallest positive integer k such that $p \mid u_q(k)$, which

exists since p and q are coprime so the last coefficient of the characteristic equation for $\{u_q(m)\}_{m\geq 0}$ which is $q^{11-2\lambda}$ is coprime to p. It is known that b_p divides $p-e$, where $e=\left(\dfrac{\tau(p)^2-4p^{11}}{q}\right)$ and $\left(\dfrac{\bullet}{q}\right)$ is the Legendre symbol. Write

$$u_q(b_p)=p^{\nu_p}m_p,$$

where $\nu_p\geq 1$ and m_p is coprime to p. Let

$$c_p:=\begin{cases} b_p & \text{if} \quad \nu_p\equiv 1 \pmod 2;\\ pb_p & \text{if} \quad \nu_p\equiv 0 \pmod 2.\end{cases}$$

Since

$$u_q(pb_p)=p^{\nu_p+1}m_p'$$

for some integer m_p' coprime to p, it follows that the exponent of p in $u_q(c_p)$ is exactly $\mu_p:=2\lfloor \nu_p/2\rfloor+1$ so it is odd. Now compute

$$\tau(q^{c_p-1})=q^{\lambda(c_p-1)}u_q(c_p)=q^{\lambda(c_p-1)}p^{\mu_p}M_p,$$

where $M_p\in\{m_p,m_p'\}$ is coprime to p. Thus, by multiplicativity,

$$\tau(\tau(q^{c_p-1}))=\tau(p^{\mu_p})\tau(q^{\lambda(c_p-1)}|M_p|)$$

and $\tau(p^{\mu_p})$ is a multiple of $\tau(p)$ since μ_p is odd, so in particular $\tau(\tau(q^{c_p-1})=0$. This proves the lemma with $a_p:=c_p-1$. ∎

5.1.2 Proof of Proposition 5.2

Recall that for a prime p, we put $\nu_p(m)$ for the exponent of p in the factorization of m. We use the fact that $\nu_2(\tau(n))\geq 3\nu_2(n)$ (see Lemma 2.1 in [32]) and this also follows from Lemma 3.2 (ii). Thus, if $\nu_2(n)\geq 1$, then $\nu_2(\tau(n))\geq 3$ and by induction on k, we get that $\nu_2(\tau^{(k-1)}(n))\geq 3^{k-1}$. Write $|\tau^{(k-1)}(n)|=2^ab$, where $a\geq 3^{k-1}$ and b is odd. We look at the sequence $\{\tau(2^m)\}_{m\geq 0}$. With the notation from the proof of Lemma 5.1, we have $(\alpha_2,\beta_2)=4\left(-3+\sqrt{-119},3-\sqrt{-119}\right)$. Next, $d=\gcd(\tau(2),2^{11})=2^3$, so $(\gamma_2,\delta_2)=\left((-3+\sqrt{-119})/2,(-3-\sqrt{-119})/2\right)$. Further,

$$\tau(2^m)=2^{3m}u_2(m+1),\quad \text{where}\quad u_2(m+1)=\frac{\gamma_2^{m+1}-\delta_2^{m+1}}{\gamma_2-\delta_2}.$$

So for us, since τ is multiplicative, we have

$$\tau^{(k)}(n) = \tau(|\tau^{(k-1)}(n)|) = \tau(2^a b) = 2^{3a} u_2(a+1)\tau(b),$$

where $a + 1 \geq 3^{k-1} + 1$. The sequence $\{u_2(m)\}_{m \geq 0}$ is a Lucas sequence. Thus, by a celebrated result of Bilu, Hanrot and Voutier [5], $u_2(m)$ has a primitive prime factor for $m \geq 31$. This is a prime p which does not divide $u_2(\ell)$ for any positive integer $\ell < m$ and does not divide the discriminant $-119 = -7 \times 17$ either. This prime p has the property that $p \equiv \pm 1 \pmod{m}$. In particular, $p \geq m - 1$. Applying this to our situation, we get that $u_2(a+1)$ is divisible by a prime $p \geq a \geq 3^{k-1}$ provided $a + 1 \geq 31$. This last inequality holds for $k \geq 5$ since $a \geq 3^{k-1}$. For smaller values of k, we list $u_2(m)$ for all $m \in \{2, \ldots, 30\}$ and check that $u_2(m)$ has a primitive prime factor for all such values of m (note that $u_2(m)$ is odd for all $m \geq 1$). Thus, $\tau^{(k)}(n)$ is indeed divisible by a prime $p \geq 3^{k-1}$ for all $k \geq 1$. If $k \geq 3$, neither 3^{k-1} nor $3^{k-1} + 1$ can be primes so $p \geq 3^{k-1} + 2$. Thus, it suffices to prove that the inequality $p \geq 3^{k-1} + 2$ also holds for $k = 1, 2$. For $k = 1,\ 2$, since n is even (so, $a \geq 1$), it follows that the desired inequalities hold if $P(\tau(2^a)) \geq 3$ for all $a \geq 1$ and $P(\tau(2^a)) \geq 5$ for all $a \geq 3$. But these are equivalent to the fact that $P(u_2(a+1)) \geq 3$ for all $a \geq 1$ and $P(u_2(a+1)) \geq 5$ for all $a \geq 3$, which are consequences of the fact that the odd number $u_2(m)$ has primitive divisors for all $m \geq 2$ together with the fact that $u_2(2) = -3$. ∎

Remark. Stewart [50] showed that $P(u_2(n)) > n \exp(\log n/(104 \log\log n))$ holds once $n > n_0$. With this result, we get that the inequality $P(\tau^{(k)}(n)) > 3^{k-1} \exp(k/(104 \log k))$ holds under the same assumptions (that n is even and that the Lehmer conjecture holds) once $k > k_0$ is sufficiently large.

5.1.3 Proof of Proposition 5.3

Since $\tau(n)$ is odd, we may assume that n is an odd square. By the multiplicative property of τ, it follows that we can reduce the problem at a prime power $p^a \| n$. Then $\tau(p^a) = \pm 1$ and a is even. If $a = 2$, then $\tau(p^2) = \tau(p)^2 - p^{11}$. Thus, we get $x^2 - y^{11} = \pm 1$ with $(x, y) := (\tau(p), p)$, and this has no positive integer solutions (x, y) since, from the solution of Catalan's problem by Mihăilescu [38] we know that 3^2 and 2^3 are the only consecutive

perfect powers. Thus, $a \geq 4$. Further, p and $\tau(p)$ are coprime for if not then $p \mid \tau(p^a)$ for all $a \geq 1$, which is impossible. Thus,

$$\tau(p^a) = u_p(a+1) = \frac{\alpha_p^{a+1} - \beta_p^{a+1}}{\alpha_p - \beta_p} = \pm 1.$$

Since $\tau(p)$ and p are coprime, it follows that the above equation signals $u_p(a+1)$ as a member of a Lucas sequence without primitive divisors. Note that $a+1 \geq 5$ is odd. These are classified in Table 1 in [5]. If $(\alpha_p, \beta_p) = \varepsilon((u+\sqrt{v})/2, (u-\sqrt{v})/2)$, where $\varepsilon \in \{\pm 1\}$ and $u_n = (\alpha_p^n - \beta_p^n)/(\alpha_p - \beta_p)$ does not have a primitive divisor for some $n \geq 5$, which is odd, then $n \in \{5, 7, 13\}$. Further, if $b < 0$, then for $n = 5$, we have $(a,b) \in \{(1,-7),\ (2,-40),\ (1,-11),\ (1,-15),\ (12,-76),\ (12,-1364)\}$, while if $n = 7, 13$ then $(a,b) \in \{(1,-7),\ (1,-19)\}$. However, for us, $a = \pm\tau(p)$ and $b = \tau(p)^2 - 4p^{11}$. Thus, we get a certain number of equations for p^{11} which we check that they have no convenient solution. For example, $(a,b) = (1,-7)$ gives $\tau(p) = \pm 1$, $-7 = \tau(p)^2 - 4p^{11} = 1 - 4p^{11}$, so $4p^{11} = 8$, a contradiction. ∎

5.1.4 Proof of Proposition 5.4

Before proving Proposition 5.4, we start by analysing $\tau(p^a)$ for odd primes p and even exponents a. It turns out that if a is sufficiently large, then $|\tau(p^a)| > p^{2a}$. In proving this, we will consider the cases where $a > 10^{16}$ and $a \in [2, 10^{16}]$. To prove that this inequality holds for $a > 10^{16}$, amongst our arguments, we will use Lemma 2.9 and for $a \in [2, 10^{16}]$ will use the ABC–conjecture.

Lemma 5.8 *If $a > 10^{16}$ is even, then $|\tau(p^a)| > p^{2a}$.*

Proof We look again at the sequence $\{\tau(p^a)\}_{a \geq 0}$. Let $d := \gcd(\tau(p), p^{11})$. In the proof of Lemma 5.1, we saw that if $d > 1$, then $d = p^\lambda$ for some $\lambda \in \{1,2,3,4,5\}$. Then it is easy to prove by induction on a, via the recurrence formula

$$\tau(p^{a+2}) = \tau(p)\tau(p^{a+1}) - p^{11}\tau(p^a), \quad \text{valid for all} \quad a \geq 0,$$

that $p^{\lambda a} \mid \tau(p^a)$. Thus, if $\lambda \geq 3$, then $|\tau(p^a)| \geq p^{3a} > p^{2a}$ holds for all positive integers a. If $\lambda = 2$, then $p^{2a} \mid \tau(p^a)$ for all $a \geq 1$. Further, putting $(\gamma_p, \delta_p) := (\alpha_p/p^2, \beta_p/p^2)$, we get

$$\tau(p^a) = p^{2a} u_p(a+1) \quad \text{for all} \quad a \geq 1,$$

where μ_p is the Lucas sequence as in Lemma 5.1. Thus, $|\tau(p^a)| = p^{2a}$ leads to $u_p(a+1) = \pm 1$. If $a = 2$, we get

$$\pm 1 = u_p(3) = \gamma_p^2 + \gamma_p\delta_p + \delta_p^2 = (\gamma_p + \delta_p)^2 - \gamma_p\delta_p = (\tau(p)/p^2)^2 - p^7,$$

which leads to the integer solution $(x, y) := (\tau(p)/p^2, p)$ to the Diophantine equation

$$x^2 - y^7 = \pm 1,$$

which does not exist by Mihăilescu's result [38]. If $a \geq 4$, we get again that $u_p(a+1)$ is a member of a Lucas sequence without primitive divisors and an investigation of Table 1 in [5], as in the proof of Proposition 5.3, does not lead to any solutions. Thus, we may assume that $\lambda \in \{0, 1\}$. Write again $(\gamma_p, \delta_p) := (\alpha_p/p^\lambda, \beta_p/p^\lambda)$. Then we have

$$\tau(p^a) = p^{\lambda a} u_p(a+1) = p^{\lambda a}\left(\frac{\gamma_p^{a+1} - \delta_p^{a+1}}{\gamma_p - \delta_p}\right).$$

Thus introducing logs on both sides yields:

$$\log|\tau(p^a)| = \lambda a \log p + (a+1)\log|\delta_p| + \log|(\gamma_p/\delta_p)^{a+1} - 1| - \log|\gamma_p - \delta_p|.$$

We need a lower bound for $\log|\tau(p^a)|$. Since $|\gamma_p - \delta_p| \leq 2|\delta_p| = 2p^{11/2-\lambda}$, we get

$$\begin{aligned}\log|\tau(p^a)| &\geq \lambda a \log p + a\log|\delta_p| - \log 2 + \log|(\gamma_p/\delta_p)^{a+1} - 1| \\ &\geq 5.5a\log p - \log 2 + \log|\eta^{a+1} - 1|,\end{aligned}$$

where $\eta := \gamma_p/\delta_p$. We need a lower bound for $|\eta^{a+1} - 1|$. Corollary 4.2 in [6] shows that if we write D and $h(\eta)$ for the degree and logarithmic height of η, respectively, then the inequality

$$\log|\eta^{a+1} - 1| > -10^{12} D^4 (h(\eta) + 1)\log(a+2)$$

holds (since $|\eta| = 1$). A better (sharper) inequality can be found in Lemma 5 in [52]. For us, $D = 2$ and the minimal polynomial of γ_p/δ_p is

$$\gamma_p\delta_p(x - \gamma_p/\delta_p)(x - \delta_p/\gamma_p) = (\gamma_p\delta_p)x^2 - (\gamma_p^2 + \delta_p^2)x + (\gamma_p\delta_p),$$

and both η and its conjugate $\overline{\eta} = \eta^{-1}$ have absolute value 1, so

$$h(\eta) = \frac{1}{2}\log(\gamma_p\delta_p) = \left(\frac{11 - 2\lambda}{2}\right)\log p \leq 5.5\log p.$$

Thus,

$$\log|\eta^{a+1}-1| \geq -10^{12}\times 2^4(5.5\log p+1)\log(a+2) \geq -6.5\times 2^4\times 10^{12}\log p\log(a+2).$$

Hence,

$$\log|\tau(p^a)| \geq \log p\left(5.5a - 6.5\times 2^4\times 10^{12}\log(a+2) - \frac{\log 2}{\log p}\right) > 2a\log p,$$

where the last inequality holds for all $a > 10^{16}$.

So, we got that $|\tau(p^a)| > p^{2a}$ holds for all primes $p \geq 3$ and all $a > 10^{16}$. Here, we did not need the ABC-conjecture. We use the ABC-conjecture to deal with the low range $a \in [2, 10^{16}]$ to prove the following lemma.

Lemma 5.9 *The ABC-conjecture implies that for all even $a \in [2, 10^{16}]$ except for $a = 6$, the inequality $|\tau(p^a)| > p^{2a}$ holds for $p > P_a$ sufficiently large. For $a = 6$, the ABC-conjecture implies that $|\tau(p^6)| > p^9$ holds for all $p > P_6$ sufficiently large.*

Proof We start with $a = 2$. Then $\tau(p^a) = \tau(p)^2 - p^{11} = p^{2\lambda}(x_1^2 - p^{11-2\lambda})$, where we put again $p^\lambda = \gcd(\tau(p), p^{11})$, and $x_1 := \tau(p)/p^\lambda$. Recall that we only consider the case $\lambda \in \{0, 1\}$. If $|\tau(p^2)| \leq p^4$, we then get that $|x_1^2 - p^{11-2\lambda}| \leq p^{4-2\lambda}$. Consider the *abc*-equation $a + b = c$, where $a := x_1^2,\ b := -p^{11-2\lambda}$. Then $|c| \leq p^{4-\lambda}$, $a,\ b,\ c$ are coprime and $\max\{|a|, |b|, |c|\} = |b| = p^{11-2\lambda}$. We get

$$p^{11-2\lambda} \ll_\varepsilon N(abc)^{1+\varepsilon} \ll_\varepsilon (|x_1|p^{4-2\lambda})^{1+\varepsilon} \ll_\varepsilon (2p^{10.5-3\lambda})^{1+\varepsilon},$$

where we used the fact that $|x_1| = |\tau(p)|/p^\lambda \leq 2p^{5.5-\lambda}$. Choosing $\varepsilon := 0.01$, we get that $p \ll 1$. Thus, $p \leq P_2$ is bounded for $a = 2$.
Assume next that $a \in [4, 10^{16}]$ is even. Then

$$|\tau(p^a)| = p^{a\lambda}u_p(a+1) = p^{\lambda a}F_a(\gamma_p, \delta_p),$$

where

$$F_a(X, Y) = \frac{X^{a+1} - Y^{a+1}}{X - Y} = X^a + X^{a-1}Y + \cdots + XY^{a-1} + Y^a.$$

The polynomial $F_a(X, Y)$ is symmetric in X and Y so it is of the form $G_a(S, P)$ for some polynomial $G_a \in \mathbb{Z}[x, y]$, where we put $S := X+Y,\ P := XY$. In addition, as a polynomial

in S, it is concentrated only in even monomials. This can be seen by simultaneously changing the signs of X and Y (so, replacing (X,Y) by $(-X,-Y)$). This does not change $F_a(X,Y)$ since a is even and does not change P but changes the sign of S. Thus, $G_a(S,P) = G_a(-S,P)$ so $G_a(S,P) = H_a(S^2,P)$ for some polynomial $H_a(x,y) \in \mathbb{Z}[x,y]$. The polynomial H_a is homogenous of degree $a/2$. Let $a = 4$. Then one checks that

$$H_4(S^2,P) = S^4 - 3PS^2 + P^2 = (S^2 - 3P/2)^2 - (5/4)P^2.$$

So, assume that $|\tau(p^4)| \leq p^8$. Then putting again $x_1 := \tau(p)/p^\lambda$, we get

$$|\tau(p^4)| = p^{4\lambda}|F_4(\gamma_p,\delta_p)| = p^{4\lambda}|H_4(x_1^2,p^{11-2\lambda})| = p^{4\lambda}|(x_1^2 - 3p^{11-2\lambda}/2)^2 - (5/4)p^{2(11-2\lambda)}|.$$

We thus get that

$$|(2x_1^2 - 3p^{11-2\lambda})^2 - 5p^{2(11-2\lambda)}| \leq 4p^{8-4\lambda}.$$

We apply the ABC-conjecture to the equation $a+b=c$, where $a := (2x_1^2 - 3p^{11-2\lambda})^2$ and $b := -5p^{2(11-2\lambda)}$. The greatest common divisor D of these two numbers is either 1 or 5 because p does not divide a since p does not divide x_1. Thus, applying the ABC–conjecture to the equation $a_1 + b_1 = c_1$, where $a_1 := a/D,\ b_1 := b/D$, we get

$$\begin{aligned} p^{2(11-2\lambda)} &\leq \max\{|a_1|,|b_1|,|c_1|\} \\ &\ll_\varepsilon N(abc)^{1+\varepsilon} \leq (11p^{11-2\lambda} \times (5p) \times (4p^{8-\lambda}))^{1+\varepsilon} \\ &\ll_\varepsilon p^{(20-3\lambda)(1+\varepsilon)}, \end{aligned}$$

and taking $\varepsilon := 0.01$, we get again that $p \leq P_4$ (both when $\lambda = 0$ and $\lambda = 1$).
Now assume that $a \geq 6$. Then $H_a(x,y)$ has degree $a/2 \geq 3$. We apply Theorem 2.12 to it to infer that

$$\begin{aligned} |\tau(p^a)| &= p^{\lambda a}|F_a(\gamma_p,\delta_p)| = p^{\lambda a}|H_a(x_1^2,p^{11-2\lambda}| \\ &\gg_{a,\varepsilon} p^{\lambda a}(p^{11-2\lambda})^{a/2-2-\varepsilon} \\ &\gg_{a,\varepsilon} p^{5.5a-11(2+\varepsilon)+2\lambda(2+\varepsilon)}. \end{aligned}$$

We want that $|\tau(p^a)| > p^{2a}$. This will be so if

$$c_{H_a,\varepsilon} p^{5.5a-11(2+\varepsilon)+2\lambda(1+\varepsilon)} > p^{2a},$$

where $c_{H_a,\varepsilon}$ is the constant that comes from Theorem 2.12. This works for $a \geq 8$ since we can take $\varepsilon := 0.01$, and we see that it is enough that

$$p > c_{H_a,0.01}^{-1/(3.5a-(2.01\times 11)} := P_a,$$

and the denominator of the exponent of $c_{H_a,0.01}$ is positive for $a \geq 8$. It also works for $a = 6$ and $\lambda = 1$, but it fails for $a = 6$ and $\lambda = 0$, since then $3.5a + 2\lambda(2+\varepsilon) = 21 < 11(2+\varepsilon)$. However, for $a = 6$, we can replace the lower bound $|\tau(p^a)| > p^{2a}$ by $|\tau(p^a)| > p^{1.5a}$. This works if $4a > 11(2+\varepsilon)$ and this is satisfied with $a = 6$ and $\varepsilon = 0.01$. Thus, for $a = 6$, we get

$$p > c_{H_6,0.01}^{-1/(24-2.01\times 11)} := P_6,$$

which is what we wanted.

We are now ready to finish the proof of Proposition 5.4.

Proof of Proposition 5.4. For each $a \in [2, 10^{16}]$, we let P_a be such that if $|\tau(p^a)| > p^{1.5a}$ then $p \leq P_a$. Let

$$n_0 := \prod_{\substack{2\leq a\leq 10^{16}\\ 2|a}} P_a^a.$$

Let $n > n_0^3$ be an odd square. Write $n = n_1 n_2$ where $\gcd(n_1, n_2) = 1$, and n_1 is built up of prime powers p^{a_p} such that $|\tau(p^{a_p})| \leq p^{1.5a_p}$. Then $a_p \leq 10^{16}$ and $p \leq P_{a_p}$. In particular, $n_1 \leq n_0 < n^{1/3}$, so $n_2 > n^{2/3}$. Thus, since $|\tau(p^{a_p})| > p^{1.5a_p}$ for all prime powers p^{a_p} dividing n_2, we get

$$|\tau(n)| \geq |\tau(n_2)| > n_2^{1.5} > (n^{2/3})^{1.5} = n,$$

which completes the proof. ∎

5.1.5 Proof of Proposition 5.5

We may assume that $k > 10$, otherwise the left-hand side of (5.2) is smaller than 2 and the inequality trivially holds by Proposition 5.3. If among the elements of

$$L := \{n, \tau(n), \ldots, \tau^{(\lfloor k/2 \rfloor)}(n)\}, \tag{5.5}$$

there is an even number, then with $m := \tau^{(\lfloor k/2 \rfloor)}(n)$, we have that m is even and Proposition 5.2 shows that

$$P(\tau^{(k)}(n)) = P(\tau^{(k-\lfloor k/2 \rfloor)}(m)) \geq 3^{k-\lfloor k/2 \rfloor - 1} + 2 \geq 3^{k/2-1} + 2 > \log(k/2) \quad \text{for} \quad k > 10,$$

and therefore $P(\mathrm{Orb}_\tau(n,k)) \geq P(m) > \log(k/2)$. Thus, we may assume that all numbers in list L given at (5.5) are odd. We look at prime powers p^a, where $p^a \| s$ for some number s from list (5.5). Let ω be the number of such primes p and P be the largest. Then p's are odd, a's are even. Further, by the primitive divisor theorem and Table 1 in [5], each of $u_p(a+1)$ for $a \geq 4$, contains a primitive prime factor q which does not divide $u_p(b+1)$ for any even $b < a$. This together with the fact that $|\tau(p^2)| = p^{2\lambda} u_p(3)$ and $|u_p(3)| > 1$ is coprime to p, shows that for a fixed p, there can be at most ω values of a. This shows that

$$k/2 \leq \#L \leq \omega^\omega = e^{\omega \log \omega} \leq e^{p_\omega} < e^P,$$

where we use $p_1 < p_2 < \cdots$ for the sequence of all prime numbers and the fact that $P > p_\omega \geq \omega \log \omega$ (see (3.12) in [46]). Hence, $P \geq \log(k/2)$, as we wanted. ∎

5.1.6 Proof of Proposition 5.6

For technical reasons, we enlarge S and adjoin the primes $2, 5, 11$ to it. So, we work with s but in the final answer we need to replace s by $s+3$. We write

$$\mathbb{Z}_S^* = \{\pm p_1^{a_1} \cdots p_s^{a_s} : a_i \in \mathbb{Z}\}.$$

We want to count the solutions (p, a) where p is an odd prime and a is an even integer to $\tau(p^a) \in \mathbb{Z}_S^*$. Since $\tau(p^a) = p^{\lambda a} u_p(a+1)$ and $u_p(m)$ has primitive divisors for all even $m \geq 4$ (and $|u_p(2)| > 1$ is coprime to p), it follows that a can take at most s values and the largest one satisfies $a+1 \leq P-1$, so $a+1 \leq P-2$, since a is even and P is odd. Thus, there are at most P^s values of the form $\tau(p^a)$ with $p \in S$. From now on, we assume that $p \notin S$. In particular, $p \nmid \tau(p)$. Observe that

$$\tau(p^a) = u_p(a+1) = \frac{\alpha_p^{a+1} - \beta_p^{a+1}}{\alpha_p - \beta_p}.$$

Let $q := P(a+1)$ and then

$$\tau(p^a) = \left(\frac{(\alpha_p^{(a+1)/q})^q - (\beta_p^{(a+1)/q})^q}{\alpha_p^{(a+1)/q} - \beta_p^{(a+1)/q}} \right) u_p((a+1)/q).$$

Thus, putting $(\alpha_1, \beta_1) := (\alpha_p^{(a+1)/q}, \beta_p^{(a+1)/q})$, we have that

$$\tau(p^a) = F_{q-1}(\alpha_1, \beta_1) u_p((a+1)/q),$$

so we deduce that $F_{q-1}(\alpha_1, \beta_1) \in \mathbb{Z}_S^*$. If $q = 3$, then

$$F_2(\alpha_1, \beta_1) = \alpha_1^2 + \alpha_1\beta_1 + \beta_1^2 = S_1^2 - P_1,$$

where $S_1 := \alpha_1 + \beta_1$ and $P_1 := \alpha_1\beta_1$. Since $P_1 = p^{11(a+1)/q}$, we get with $(x, y) := (S_1, p^{(a+1)/q})$ that

$$x^2 - y^{11} \in \mathbb{Z}_S^*. \tag{5.6}$$

If $q = 5$, then

$$F_4(\alpha_1, \beta_1) = (\alpha_1 + \beta_1)^4 - 3(\alpha_1\beta_1)(\alpha_1 + \beta_1)^2 + \alpha_1\beta_1 = (S_1^2 - 3P_1/2)^2 - 5P_1^2/4.$$

Multiplying both sides above by 4×5^{10}, we get

$$4 \times 5^{10} F_5(\alpha_1, \beta_1) = (5^5(2S_1^2 - 3P_1))^2 - 5^{11}P_1^2.$$

Since $P_1 = p^{11(a+1)/q}$, we can take $(x, y) := (5^5 \times (2S_1^2 - 3P_1), 5p^{2(a+1)/q})$ and get that

$$4 \times 5^{10} F_5(\alpha_1, \beta_1) = x^2 - y^{11} \in \mathbb{Z}_S^*. \tag{5.7}$$

Next, we assume that $q \geq 7$. We then have

$$F_{q-1}(\alpha_1, \beta_1) = H_{q-1}(S_1^2, P_1),$$

and $H_{q-1}(x, y)$ is a homogeneous polynomial of degree $(q-1)/2 \geq 3$ which is irreducible (the polynomial $H_{q-1}(x, 1)$ is of degree $\phi(q)/2 = (q-1)/2$ and any of its roots spans the maximal real subfield of the cyclotomic field $\mathbb{Q}(e^{2\pi i/q})$). Thus, we get

$$H_{q-1}(x, y) \in \mathbb{Z}_S^*. \tag{5.8}$$

Any solution (x, y) of (5.6) or (5.8) which is convenient for us must have $y = p^{(a+1)/q}$, which a power of a prime p. Since q is known, so is a. Any solution (x, y) of (5.7) which is convenient for us must have $y = 5p^{2(a+1)/q}$, so again p and then a are known. Thus, it suffices to count the number of such solutions. For (5.6) and (5.7), we write

$$x^2 = y^{11} + A,$$

where $A = \pm p_1^{a_1} \cdots p_s^{a_s}$. In the case of (5.7), we must also allow factors of 4×5^{10}, which is why we enlarged S to contain 2 and 5. We may reduce a_i modulo 22 such as to write them as $a_i = 22b_i + r_i$ where $r_i \in \{0, 1, \ldots, 21\}$. Then we get that putting $z := \prod_{i=1}^{s} p_i^{b_i}$, $A' := \prod_{i=1}^{s} p_i^{r_i}$ and $x' := x/z^{11},\ y' := y/z^2$, we have

$$x'^2 = y'^{11} + A'. \tag{5.9}$$

The number of choices of A' is at most 2×22^s. Note that $(x', y') \in \mathbb{Z}_S^*$. Further, knowing y' we determine y uniquely since p is not in S. For each one of these, by Theorem 1 in [12] or Corollary 2.13, the number of solutions is at most

$$7^{11^2(4+9s)} h(\mathbb{L})^2,$$

where $\mathbb{L}$ is some extension of $\mathbb{Q}$ containing three of the roots of $f_{A'}(y) := y^{11} + A'$ and $h(\mathbb{L})$ is its class number. The above bound is valid provided that all primes dividing the discriminant of $f_{A'}(y)$ are in S, which is why we incorporated 11 into S. We can take $\mathbb{L}$ to be the field $\mathbb{Q}(A'^{1/11}, e^{2\pi i/11})$, where $A'^{1/11}$ is the real 11th root of A'. The absolute values of the discriminant of $\mathbb{K}_1 := \mathbb{Q}(A'^{1/11})$ is at most $(11|A'|)^{11}$ and of the discriminant of $\mathbb{K}_2 := \mathbb{Q}(e^{2\pi i/11})$ is at most 11^{11}, and the degrees of both fields are at most 11. So, the discriminant $\Delta_{\mathbb{L}}$ of $\mathbb{L}$ (which is the compositum of $\mathbb{K}_i$, for $i = 1, 2$) is in absolute value at most

$$(11A')^{11^2} \times 11^{11^2} \leq (11^2 A')^{11^2} \leq (P^{22s+2})^{11^2} = P^{2 \times 11^2 (11s+1)}.$$

Thus,

$$|\Delta_{\mathbb{L}}| < P^{2 \times 11^2 (11s+1)}. \tag{5.10}$$

From inequalities (3.6) and (3.7) in [4], we have that

$$h(\mathbb{L}) < 5 |\Delta_{\mathbb{L}}|^{1/2} (\log |\Delta_{\mathbb{L}}|)^{(11^2-1)/2}.$$

We show that the right-hand side above is smaller than the right–hand side of (5.10). Indeed, for that all we have to show is that

$$5(2 \times 11^2(11s+1)\log P)^{(11^2-1)/2} < P^{11^2(11s+1)}.$$

Since $5 < (11^2)^{1/2}$, we have that

$$5(2 \times 11^2(11s+1)\log P)^{(11^2-1)/2} < (2 \times 11^2(11s+1)\log P)^{11^2},$$

so taking 11^2 roots, it suffices to show that

$$2 \times 11^2(11s+1)\log P < P^{11s+1}.$$

Since $P > 2\log P$, it suffices to show that $P^{11s} > 11^2(11s+1)$, which is implied by $P^x > (x+1)^3$ with $x = 11s$, and further by, $2^x > (x+1)^3$, and this does indeed hold for all $x \geq 11$. Thus,

$$h(\mathbb{L}) \leq P^{2\times 11^2(11s+1)},$$

so the number of solutions of (5.9) is at most

$$7^{11^2(4+9s)} \times P^{4\times 11^2(11s+1)} < P^{11^2(4+9s+4+44s)} = P^{11^2(53s+8)},$$

where we use the fact that $P > 7$ (because 11 has been incorporated into S). This is for a fixed A' and there are at most $2 \times 22^s = 2^{s+1} \times 11^s < (1/2)P^{2s}$ such equations for each of $a = 2, 4$, which gives us a number of possibilities for p at most

$$P^{2s+1} \times P^{11^2(53s+8)} = P^{6415s+969}.$$

Now, we fix $q \geq 7$. In this case, we have the equation

$$H_{q-1}(x, y) \in \mathbb{Z}_S^*.$$

This is a Thue-Mahler equation of degree $(q-1)/2 \geq 3$ and $H_{q-1}(x, y)$ is irreducible. The number of equivalence classes of solutions $(x, y) \in (\mathbb{Z}_S^*)^2$ (where by equivalence classes we mean that $(x, y) \equiv (x', y')$ iff $(x, y) = \lambda(x', y')$ for some $\lambda \in \mathbb{Z}_S^*$) is, by a result of Evertse [13], at most

$$(5 \times 10^6(q-1)/2)^s \leq (10^7 P)^s < P^{8s}.$$

Our solutions for which y is a power of a prime p not in S are in inequivalent classes. Thus, the above bound bounds the acceptable number of primes p. This is for a q fixed and $q \leq P$. Each of these determines p and then we need to multiply by another factor of P to account for the number of possibilities for a. Thus, the total number is at most

$$P(P^{8s+1} + P^{6435s+969}) + P^s < P^{6500(s+1)}.$$

We replace s by $s+4$ (we need to add 3 for the primes $2, 5, 11$ and another 1 for the place at infinity which is always incorporated in both the results from [13] and [12]), and we get the desired result. ∎

5.1.7 Proof of Proposition 5.7

By the multiplicativity of τ, it suffices to show that there is no prime odd p and even positive integer a such that $P(\tau(p^a)) \leq 7$. We write again $d := \gcd(\tau(p), p^{11}) = p^\lambda$ and

$$\tau(p^a) = p^{\lambda a} u_p(a+1).$$

Then $\{u_p(m)\}_{m \geq 1}$ is a Lucas sequence. If $a \geq 8$, then, since $P(u_p(a+1)) \leq 7$, we conclude that $u_p(a+1)$ has no primitive divisors. As we saw, there are only finitely many possibilities for (a, γ_p, δ_p) and they can all be read from Table 1 in [5]. This gives no solutions. Assume next that $a = 6$. Then $P(u_p(7)) \leq 7$. Hence, the largest prime factor of $u_p(7)$ is either at most 5 (smaller than 7 and incongruent to ± 1 modulo 7), or 7. But if $7 \mid u_p(7)$, then 7 must divide the discriminant of the sequence (which is the same as the discriminant $(\gamma_p - \delta_p)^2$ of the characteristic polynomial) and such primes do not qualify as primitive primes, so these instances also appear in Table 1 in [5]. Similarly, if $a = 4$, then $u_p(a+1) = u_p(5)$. The only primes which can divide $u_p(q)$, with a prime q are either q itself (if q divides the discriminant of the sequence) or primes which are congruent to ± 1 modulo q. Thus, the only possibility is that $u_p(5)$ is a power of 5, so again $u_p(5)$ has no primitive prime factors and the possibilities can be read off from Table 1 in [5]. It remains to consider the case $a = 2$. Since each of $\tau(3^2),\ \tau(5^2),\ \tau(7^2)$ has a prime factor larger than 7, it follows that $p \geq 11$. Further, $p \nmid \tau(p)$. Now

$$\tau(p^2) = \tau(p)^2 - p^{11} = \pm 3^a 5^b 7^c.$$

We use congruences with the Ramanujan function to get information on the exponents a, b, c. Here are the congruences that we use. In what follows, $\sigma_k(n)$ is the sum of the kth powers of the divisors of n.

(i) $\tau(n) \equiv n\sigma_9(n)$ if $n \equiv 0, 1, 2, 4 \pmod 7$;

(ii) $\tau(n) \equiv n^{-30}\sigma_{71}(n) \pmod{5^3}$ if $n \not\equiv 0 \pmod 5$;

(iii) $\tau(n) \equiv n^{-610}\sigma_{1231}(n) \pmod{3^6}$ if $n \equiv 1 \pmod 3$.

Assume now that $c \geq 1$. In particular, $p^{11} \equiv \tau(p)^2 \pmod 7$, so p is a quadratic residue modulo 7. Thus, we can apply congruence (i) above to $n = p^2$ to get that

$$0 \equiv \tau(p^2) \pmod 7 \equiv p^2\sigma_9(p^2) \pmod 7 \equiv p^2(1 + p^9 + p^{18}) \pmod 7 \equiv 3p^2 \pmod 7,$$

since $p^3 \equiv 1 \pmod 7$. Hence, $p = 7$, a contradiction. Thus, $c = 0$.
Assume next that $b \geq 1$. We use the congruence (ii) above for $n = p^2$. Note also that since $p^{11} \equiv \tau(p)^2 \pmod 5$, we get that p is a quadratic residue modulo 5. Thus, $p^2 \equiv 1 \pmod 5$. By (ii) above for $n = p^2$, we get

$$0 \equiv p^{-60}\sigma_{71}(p^2) \pmod 5 \equiv 1 + p^{71} + p^{142} \pmod 5 \equiv 2 + p \pmod 5,$$

so $p \equiv 3 \pmod 5$, which contradicts the fact that p is a quadratic residue modulo 5. Thus, $b = 0$.
Thus, the only possibility is

$$\tau(p)^2 - p^{11} = \pm 3^a,$$

and $a \neq 0$ since, otherwise we get again the Catalan equation. Hence, $a \geq 1$. Next, since $p^{11} \equiv \tau(p)^2 \pmod 3$, it follows that $p \equiv 1 \pmod 3$ so $p^3 \equiv 1 \pmod 9$ and $p^2 + p + 1 \equiv 3 \pmod 9$. We now apply (iii) to $n = p^2$ to get that

$$\begin{aligned} \pm 3^a &\equiv \tau(p^2) \pmod{3^6} \equiv p^{-1220}\sigma_{1231}(p^2) \pmod{3^6} \\ &\equiv p^{-1220}(1 + p^{1231} + p^{2432}) \pmod{3^6}. \end{aligned}$$

Since $p^3 \equiv 1 \pmod 9$, we get that $1 + p^{1231} + p^{2432} \equiv 1 + p + p^2 \pmod 9 \equiv 3 \pmod 9$. So, in the above congruence, we get

$$\pm 3^a \equiv 3p^{-1220} \pmod 9,$$

which shows that $a = 1$ and $\pm 1 \equiv p^{-1220} \pmod 3$. Since $p \equiv 1 \pmod 3$, we deduce that the sign is $+$. Hence, we get the equation

$$\tau(p^2) = \tau(p)^2 - p^{11} = 3.$$

With $(x, y) := (\tau(p), p)$, we get

$$x^2 - 3 = y^{11}. \tag{5.11}$$

This can be reduced to one of several Thue equations. Indeed, the left–hand side factors in the Euclidean ring $\mathbb{Z}[\sqrt{3}]$ as $(x - \sqrt{3})(x + \sqrt{3})$, and the two factors $x + \sqrt{3}$ and $x - \sqrt{3}$ are coprime since x is even. Thus, $y = (a + b\sqrt{3})(a - b\sqrt{3})$ for some integers $a,\ b$ and $(a + b\sqrt{3})^{11}$ is associated to one of $x \pm \sqrt{3}$. Up to changing b to $-b$, we may assume that $(a + b\sqrt{3})^{11}$ is associated to $x + \sqrt{3}$. Thus,

$$x + \sqrt{3} = (a + b\sqrt{3})^{11}\zeta,$$

where ζ is a unit. All units in $\mathbb{Z}[\sqrt{3}]$ are of the form $\pm(2 + \sqrt{3})^k$ for some integer k. We may reduce k modulo 11, so replace k by $11k_0 + r$, where $r \in \{0, 1, \ldots, 10\}$ and replace $a + b\sqrt{3}$ by $(a + b\sqrt{3})(2 + \sqrt{3})^{k_0}$. Thus, we get

$$x + \sqrt{3} = \pm(a + b\sqrt{3})^{11}(2 + \sqrt{3})^r \quad \text{for some} \quad r \in \{0, 1, \ldots, 10\}.$$

Conjugating and eliminating x, we get

$$\frac{(a + b\sqrt{3})^{11}(2 + \sqrt{3})^r - (a - b\sqrt{3})^{11}(2 - \sqrt{3})^r}{2\sqrt{3}} = \pm 3.$$

These are the Thue equations. For example, for $r = 2$, we get

$$\begin{aligned} \pm 3 \ &= \ 4a^{11} + 77a^{10}b + 660a^9b^2 + 3465a^8b^3 + 11880a^7b^4 + 29106a^6b^5 + 49896a^5b^6 \\ &+ \ 62370a^4b^7 + 53460a^3b^8 + 31185a^2b^9 + 10692ab^{10} + 1701b^{11}. \end{aligned}$$

At any rate, equation (5.11) (and several others of the type $x^2 - D = y^n$ for various $D \in [1, 100]$ and various exponents $n \geq 3$) have been solved in Carlos Barros' PhD. dissertation [3]. The only integer solutions are $(x, y) = (\pm 2, 1)$, which are not convenient for us. This completes the proof. ∎

5.1.8 Comments

One may wonder what happens if the Lehmer conjecture is false. Then we believe that for most n, $\tau^{(2)}(n) = 0$, and we provide some heuristics below. Indeed, it is known that there is a constant $c > 0$ such that on a set of n of asymptotic density 1, $\tau(n)$ is a multiple of all prime powers $p^a < c_1 \log n / \log\log n$. This was done in Proposition 1 in [19] for the nth coefficient of the modular form associated to an elliptic curve over $\mathbb{Q}$ without complex multiplication and the same argument works with the Ramanujan function $\tau(n)$. Let p be such that $\tau(p) = 0$ and for each prime q, let a_q be the minimal positive integer such that $\tau(q^{a_q})$ is divisible by p and the exponent $\nu_p(\tau(q^{a_q}))$ is odd. By the arguments from Lemma 5.1, we have that $a_q + 1$ is either the order of appearance of p in the Lucas sequence $\{u_q(m)\}_{m\geq 0}$, which we denote by $\ell_p(q)$, or $p\ell_p(q)$. Note that $\ell_p(q)$ is at most $q + 1$. Let $a_q(n)$ be the exponent of q in the factorization of $\tau(n)$. From what we have said, this is at least as large as $\lfloor (1/\log q) \log(c_1 \log n/\log\log n)\rfloor$ for most n. If $a_q(n)+1$ is an odd multiple of $a_q + 1$, then $\tau(q^{a_q(n)})$ is an integer multiple of $\tau(q^{a_q})$, so it is zero. So, we need to look at the situation when $a_q(n) + 1$ is not an odd multiple of $a_q + 1$. Assume that $a_q(n)$ behaves like a random large number with respect to being in a certain residue class modulo $2(a_q + 1)$. Thus, let us assume that the probability that $a_q(n) + 1$ is not an odd multiple of $a_q + 1$ is $1 - 1/(2(a_q + 1))$ and let us assume that these probabilities are independent as q ranges over small primes different than p. Then the probability that $\tau(\tau(n))$ is not zero would therefore be at most

$$\prod_{\substack{2\leq q<c\log n/\log\log n\\ 2\neq p}} \left(1 - \frac{1}{2(a_q + 1)}\right), \tag{5.12}$$

and since the sum

$$\sum_{\substack{q\geq 2\\ q\neq p}} \frac{1}{2(a_q + 1)} \geq \frac{1}{2p} \sum_{\substack{q\geq 2\\ q\neq p}} \frac{1}{\ell(q)} \geq \frac{1}{p} \sum_{q} \frac{1}{q + 1}$$

is divergent, it follows that the product shown at (5.12) tends to 0 with n.

References

[1] J. S. Balakrishnan, W. Craig, K. Ono, "Variations of Lehmer's conjecture for Ramanujan's τ-function", *Preprint*, arXiv **2005.10345**, 2020.

[2] J. S. Balakrishnan, W. Craig, K. Ono, and W.-L. Tsai, "Variants of Lehmer's speculation for newforms", *Preprint*, arXiv **2005.10354**, 2020.

[3] C. F. Barros, *On the Lebesgue-Nagell equation and related subjects*, Ph.D. thesis, The University of Warwick, 2010.

[4] A. Bérczes, J.-H. Evertse and K. Győry, "Effective results for hyper- and superelliptic equations over number fields", *Publ. Math. Debrecen* **82** (2013), 727–756.

[5] Yu. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, (with an appendix by M. Mignotte), *J. Reine Angew. Math.* **539** (2001), 75–122.

[6] Yu. Bilu and F. Luca, "Trinomials with given roots", *Indag. Math. (N.S.)* **31** (2020), 33–42.

[7] J. J. Bravo and F. Luca, "Factorials and the Ramanujan function", *Glasgow Math. J.* **58** (2016), 177–185.

[8] Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek, "Fibonacci numbers at most one away from a perfect power", *Elem. Math.* **63** (2008), 65–75.

[9] Y. Bugeaud, "On the Diophantine equation $x^2 - 2^m = \pm y^n$', *Proc. Amer. Math. Soc.* **125** (1997), 3203 –3208.

[10] Y. Bugeaud and M. Laurent, "Minoration effective de la distance p-adique entre puissances de nombres algébriques", *J. Number Theory* **61** (1996), 311–342.

[11] P. Deligne, "La conjecture de Weil", *Inst. Hautes udes Sci. Publ. Math.* **43** (1974), 273–307.

[12] J.-H. Evertse and J. H. Silverman, "Uniform bounds for the number of solutions to $Y^n = f(X)$", *Math. Proc. Camb. Phil. Soc.* **100** (1986), 237–248.

[13] J.-H. Evertse, "The number of solutions of the Thue-Mahler equation", *J. Reine Angew. Math.* **482** (1997), 121–149.

[14] Q. Fernado, Gouvêa, *p-adic Numbers*, Springer-Verlag, Berlin Heidelberg, USA, 1993.

[15] J. B. Fraleigh, *A First Course in Abstract Algebra*, Addison Wesley Longman, 2000.

[16] A. Gica, "The Diophantine equation $y^2 = 5^x + 11^x$", *Rev. Roumaine Math. Pure Appl.* **49** (2004), 455–459.

[17] A. Gica and L. Panaitopol, "On Obláth's problem", *J. Integer Sequences* **6** (2003) Art. 03.3.5.

[18] A. Granville, "ABC allows us to count squarefrees", *Internat. Math. Res. Notes* **19** (1998), 991–1009.

[19] A. Güloğlu, F. Luca and A. Yalçiner, "Arithmetic properties of coefficients of L-functions of elliptic curves", *Monatsh. Math.* **187** (2018), 247–273.

[20] Y. Guo and G. Le, "A note on the Diophantine equation $x^2 - 2^m = y^n$", *Proc. Amer. Math. Soc.* **123** (1995), 3627–3629.

[21] G. Grossman and F. Luca, "Sums of factorials in binary recurrence sequences", *J. Number Theory* **93** (2002), 87–107.

[22] G H. Hardy and E. M. Wright, *An introduction to the theory of numbers. Edited and revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. 6th ed.*, Oxford University Press, 2008.

[23] S. Hyyrö, "Über das Catalansche Problem", *Ann. Uni. Turku Ser A I* **79** (1964), 3–10.

[24] G. A. Jones and J. M. Jones, *Elementary Number Theory*, Springer-Verlag, Berlin Heidelberg London, 1998.

[25] D. E. Iannucci and F. Luca, "Catalan numbers, factorials and sums of aliquot parts", *The Fibonacci Quart.* **45** (2007), 327–336.

[26] N. Koblitz, *p-adic Numbers, p-adic Analysis and Zeta Functions*, Springer-Verlag, Berlin Heidelberg New York, 1977.

[27] S.V. Kotov, "Über die maximale Norm der Idealteiler des polynoms $\alpha x^m + \beta y^n$ mit den algebraischem Koeffizienten", *Acta Arith.* **31** (1976), 219 – 230.

[28] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem", in *Algebraic number fields: L-functions and Galois properties* (Proc. Sympos., Univ. Durham, Durham, 1975), 409–464. Academic Press, London, 1977.

[29] M. Laurent, M. Mignotte and Y. Nesterenko, "Formes linéaires en deux logarithmes et detérminants d'interpolation", *J. Number Theory* **55** (1995), 285–321.

[30] F. Luca, "Equations involving arithmetic functions of factorials", *Divulgaciones Math.* **8** (2000), 15–23.

[31] F. Luca and F. Nicolae, "$\phi(F_n) = F_m$", *Integers* **9** (2009), A30, 375–400.

[32] F. Luca and S. Mabaso, "Diophantine equations with the Ramanujan τ-function of factorials, Fibonacci numbers, and Catalan numbers", *The Fibonacci Quart.* **57** (2019), 255–259.

[33] F. Luca, S. Mabaso and P. Stănic ua, "On the prime factors of the iterates of the Ramanujan τ-function", *Proceedings of the Edinburgh Mathematical Society* **63** (2020), 1031– 1047.

[34] F. Luca and P. Stănică, "The Euler function of Fibonacci and Lucas numbers and factorials:", *Ann. Sci. Univ. Budapest, Sect. Comp.* **41** (2013), 119–124.

[35] F. Luca and P. Stănică, "$F_1F_2F_3F_4F_5F_6F_8F_{10}F_{12} = 11!$", *Port. Math. (N.S.)* **63** (2006), 251–260.

[36] F. Luca and A. O. Munagi, "Expansions of binary recurrences in the additive base formed by the number of divisors of the factorial", *Colloq. Math.* **134** (2014), 193–209.

[37] F. Luca and L. Szalay, "Fibonacci numbers of the form $p^a \pm p^b + 1$", *The Fibonacci Quart.* **98** (2007), 98–103.

[38] P. Mihăilescu, "Primary cyclotomic units and a proof of Catalan's conjecture", *J. Reine Angew. Math.* **572** (2004), 167–195.

[39] R. A. Mollin, *Advanced Number Theory with Applications*, CRS Press, 2009.

[40] L. J. Mordell, "On Mr. Ramanujan's empirical expansions of modular functions", *Proceedings of the Cambridge Philosophical Society* **19** (1917), 117–124.

[41] L. J. Mordell, *Diophantine Equations*, Academy Press, London, 1969.

[42] B. K. Moriya and C. J. Smyth, "Index–dependent divisors of coefficients of modular forms", *Internat. J. Number Theory* **9** (2003), 1841–1853.

[43] M. R. Murty, V. K. Murty and T. N. Shorey, "Odd values of the Ramanujan τ-function", *Bull. Soc. Math. France* **115** (1987), 391–395.

[44] S. Ramanujan, "On certain arithmetical functions", *Trans. Camb. Philos. Soc.* **22** (1916),159–184.

[45] A. Robert, *A course in p-adic Analysis*, Springer-Verlag, Berlin Heidelberg New York, 2000.

[46] J. B. Rosser and L. Schoenfeld, "Approximate formulas for some functions of prime numbers", *Illinois J. Math.* **6** (1962), 64–94.

[47] J.-P. Serre, "Divisibilité de certaines fonctions arithmétiques", *L'Enseignement Math. (2)* **22** (1976), 227–260.

[48] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, NY, 1986.

[49] C. L.Stewart, *Divisor Properties of Arithmetical Sequences*, Ph.D. Thesis, University of Cambridge, 1976.

[50] C. L. Stewart, "On prime factors of terms of linear recurrence sequences", in: J.M. Borwien, et al. (Eds.),*Number Theory and Related Fields: In memory of Alf van der Poorten*, Springer Proc. in Mathematics and Statistics **43** (2013), 341–359.

[51] H. P. F. Swinnerton-Dyer, "On l-adic representations and congruences for coefficients of modular forms, in Modular functions of one variable, III" in *Proc. Internat. Summer School, Univ. Antwerp.* Lecture Notes in Math. **350** (1972), 1–55.

[52] P. Voutier, "Primitive divisors of Lucas and Lehmer sequences, III," *Math. Proc. Cambridge Philos. Soc.* **123** (1998), 407–419.

[53] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups*, Springer-Verlag, Berlin Heidelberg, 2000.

[54] K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, USA, 2004.

[55] K. Yu: "p-adic logarithmic forms and group varieties II", *Acta Arith.* **89** (1999), 337–378.