VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV MATEMATIKY

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF MATHEMATICS

O MODULÁRNÍ PERIODICITĚ KUBICKÉHO ZOBECNĚNÍ FIBONACCI ČÍSEL A SOUVISEJÍCÍCH PROBLÉMECH

ON THE MODULAR PERIODICITY OF A CUBIC GENERALIZATION OF THE FIBONACCI NUMBERS AND RELATED PROBLEMS

HABILITAČNÍ PRÁCE
HABILITATION DISSERTATION

AUTOR
AUTHOR

JIŘÍ KLAŠKA

BRNO 2018

Dedicated to the memory of my parents

CONTENTS

Contents **1**

Abstract **2**

Introduction **3**

Comments on the main results of habilitation dissertation **5**

Chapter 1 Donald Dines Wall's conjecture **28**

Chapter 2 Criteria for testing Wall's question **37**

Chapter 3 Short remark on Fibonacci-Wieferich primes **42**

Chapter 4 Tribonacci modulo p^t **47**

Chapter 5 Tribonacci modulo 2^t and 11^t **63**

Chapter 6 On Tribonacci-Wieferich primes **71**

Chapter 7 A search for Tribonacci-Wieferich primes **79**

Chapter 8 Tribonacci partition formulas modulo m **84**

Chapter 9 Further research of modular periodicity of Tribonacci sequence **95**

Chapter 10 The cubic character of the Tribonacci roots **102**

Chapter 11 Tribonacci sequence modulo a prime $p \equiv 1 (\mathrm{mod}\ 3)$ **110**

Chapter 12 A note on the cubic characters of Tribonacci roots **118**

Chapter 13 Mordell's equation and the Tribonacci family **121**

Chapter 14 Law of inertia for the factorization of cubic polynomials – the real case **131**

Chapter 15 Law of inertia for the factorization of cubic polynomials – the imaginary case **141**

Chapter 16 Law of inertia for the factorization of cubic polynomials – the case of discriminants divisible by three **149**

Chapter 17 Law of inertia for the factorization of cubic polynomials – the case of primes 2 and 3 **158**

Chapter 18 Applications of Fibonacci numbers and the golden ratio in physics, chemistry, biology and economy **169**

Chapter 19 Applications of sequences over finite fields **182**

Chapter 20 Real-world applications of number theory **186**

Appendix List of the author's papers **194**

Curriculum Vitae **196**

ABSTRACT

ON THE MODULAR PERIODICITY OF A CUBIC GENERALIZATION OF THE FIBONACCI NUMBERS AND RELATED PROBLEMS

The habilitation dissertation "*On the modular periodicity of a cubic generalization of the Fibonacci numbers and related problems* " deals with some special parts of the number theory a their applications. Primarily, this work is a contribution to the following fields: 11B39 – Fibonacci and Lucas numbers and polynomials and generalizations, 11B50 – Sequences (mod m), 11D25 – Cubic and quartic equations and 00A69 – General applied mathematics. Formally, the problems solved in this work can be partitioned into four basic parts as follows. First, we study the interesting problem concerning the modular periodicity of the Fibonacci sequence known as Wall's conjecture or as Wall-Sun-Sun prime conjecture. This problem first appeared in a paper by Donald Dines Wall published in American Mathematical Monthly in 1960. Second, we solve a number of problems concerning the cubic generalization of Fibonacci numbers. These numbers are often called the Tribonacci numbers. The modular periodicity of the Tribonacci numbers is examined in detail and many interesting results are established. For example, the combinatorial problem of Morgan Ward for the Tribonacci case will be completely solved. Third, we deal with the questions concerning the factorization of monic cubic polynomials with integer coefficients having the same discriminant. The problems of the factorization is studied over the Galois fields $\mathbb{F}_p$ where p is a prime. Above all, we focus on the question concerning the validity of the law of inertia for the factorization of cubic polynomials. Finally, an important part of this work is devoted to the practical applications of the number theory. In this part we show a whole range of examples which describe natural situations where the number theory problems can arise. In more detail, we will deal especially with the various applications of the Fibonacci numbers and with the use of the sequences over the finite fields. Some applications of Diophantine equations and the theory of partitions of positive integers into summands are also discussed. The habilitation dissertation is written in English in the form of twenty independent articles with commentaries. All the papers presented have already been published.

Mathematics Subject Classification:

11B39, 11B50, 11D25, 00A69, 11Axx, 05Axx, 01A60, 12E10, 11D45, 05A18, 11Y70.

INTRODUCTION

The following habilitation dissertation, "*On the modular periodicity of a cubic generalization of the Fibonacci numbers and related problems*", is a collection of twenty papers written by the author in the period 2007 – 2017. A majority of them has been published in reputable mathematical journals such as: The Fibonacci Quarterly, Acta Mathematica Sinica, Utilitas Mathematica, Mathematica Slovaca, Czechoslovak mathematical journal, Mathematica Bohemica and others. A complete list of the author's mathematical research papers can be found in the Appendix on pp. 194 – 195.

Primarily, by Mathematics Subject Classification (MSC 2010), the habilitation dissertation is a contribution to the following mathematical branches: 11B39 – Fibonacci and Lucas numbers and polynomials and generalizations, 11B50 - Sequences (mod m), 11D25 – Cubic and quartic equations, 00A69 – General applied mathematics. Secondarily, it is part of the following fields: 11Axx – Elementary number theory, 05Axx – Enumerative combinatorics, 12E10 – Special polynomials, 11D45 – Counting solutions of Diophantine equations, 05A18 – Partitions of sets, 11Y70 – Values of arithmetic function; tables, 01A60 History of mathematics and mathematicians - 20th century.

The habilitation dissertation consists of two basic parts. The first one lists the principal results achieved with comments and a short essay on the future of and outlooks for the studied field. The second part of the dissertation is formed by loosely related Chapters 1 – 20. The titles and contents of the chapters are identical with those of the published original papers. Thus, any chapter can be read and studied separately irrespective of the preceding text. At the beginning of each chapter, the exact reference can be found to the corresponding paper. The papers presented as Chapters 10 – 17 were written together with Professor Ladislav Skula as a co-author. Furthermore, it should be mentioned that some of our results have been obtained using the Maple and Pari GP computer programs.

The second part of the dissertation is organized as follows. Chapters 1 – 3 are devoted to an interesting, not yet resolved number-theory problem concerning the modular periodicity of a Fibonacci sequence. This problem is known as Wall's conjecture. Chapter 1 summarizes all important discoveries and known facts related to Wall's conjecture made over 56 years of its existence. The author's main results concerning Wall's conjecture are presented in Chapters 2 and 3.

In Chapters 4 – 12, we study some problems concerning the modular periodicity of a cubic generalization of Fibonacci numbers. These numbers are often called Tribonacci numbers. First, in Chapters 4 and 5, we find the fundamental relations between the primitive periods of sequences obtained by reducing a Tribonacci sequence by a given prime modulus p and by its powers p^t, $t \in \mathbb{N}$. Next, in Chapters 6 and 7, using the matrix formalism, we study an analogy to Wall's conjecture for the Tribonacci case. Consequently, the results of Chapters 4 to 7 enable us to resolve an interesting combinatorial problem. The exact formulation of this problem, together with its solution, can be found in Chapter 8. Next, in Chapter 9, we present some further results concerning the Tribonacci sequence. For example, we find the exact values of the periods of the Tribonacci sequence modulo p for any prime $p \leq 5000$. A detailed examination of these values leads us to a new hypothesis proved in Chapter 11. To prove it we need specific properties of the cubic character of Tribonacci roots. These properties are derived in Chapter 10 and some extension to this theory is given in Chapter 12.

A detailed study of the periods and their arithmetic properties in Chapters 4 – 12 points to the necessity of better understanding the problem of the factorization of monic cubic polynomials with integer coefficients over the Galois fields $\mathbb{F}_p$ where p is a prime. Let $D \in \mathbb{Z}$ and let $C_D = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = D\}$ where D_f is the discriminant of $f(x)$. In Chapter 13, we examine in detail the structure of the set C_D. We show, for example, that C_D is closely related to the problem of finding all integer solutions of Mordell's equation. Furthermore, we thoroughly examine the set C_{-44} containing the Tribonacci polynomial proving that all polynomials in C_{-44} have the same type of factorization over any Galois field $\mathbb{F}_p$ where p is a prime. This surprising property of the set C_{-44} suggests a fundamental question, namely, for which $D \in \mathbb{Z}$ the following theorem holds: *Let p be an arbitrary prime. Then, all polynomials in C_D have the same type of factorization over the Galois field $\mathbb{F}_p$.* In Chapters 14 – 17, an interesting sufficient condition is given. Moreover, work on this subject still continues and some new results have already been found.

An important part of the dissertation is devoted to the practical applications of the number theory. In particular, Chapter 18 is concerned with the applications of Fibonacci numbers and the golden ratio in physics, chemistry, biology and economy. An extensive list of chronological references is given. This chapter can be regarded as an introduction to the study of applications of Fibonacci numbers. Next, Chapter 19 is about applications of modular periodicity of the recurrent linear sequences defined over finite fields. Finally, Chapter 20 contains some further interesting examples of real-world applications of the number theory.

Brno, March 2018

COMMENTS ON THE MAIN RESULTS OF HABILITATION DISSERTATION

In the first part of the habilitation dissertation we summarize the main achieved results, which are detailed in Chapters 1 – 20. We begin with a section in which we focus on the most important applications of the studied subject.

1. Number theory and applications

German mathematician Johann Carl Friedrich Gauss (30 April 1777 – 23 February 1855), regarded as one of the greatest mathematicians of all time, claimed: "*Mathematics is the queen of the sciences and number theory is the queen of mathematics.*" However, for many years number theory had had only few practical applications. It is well known that the great English number theorist Godfrey Harold Hardy (7 February 1877 – 1 December 1947) believed that number theory had no practical applications. See his essay *"A Mathematician's Apology"* [18]. Over the 20th and 21st centuries, this situation has changed significantly. Contrary to Hardy's opinion, many practical and interesting applications of number theory have been discovered. Some of the major ones will be now presented.

The basic concepts studied in the number theory include primes and composite numbers. The properties of prime and composite numbers play an important role in modern cryptography and coding systems. The fundamental theorem of arithmetic says that every positive integer can be written uniquely as the product of primes. Although many various methods for the factorization of integers are known, it can take years for a supercomputer to find the prime factors of a large composite number. On the other hand, the multiplication of large integers lasts only a fraction of second on an ordinary computer. This salient difference is used by modern coding systems. In 1976, Whitfield Diffie and Martin E. Hellman [12] proposed a revolutionary cipher system, called a public-key cryptosystem. Subsequently, in 1978, Ronald L. Rivest, Adi Shamir, and Leonard Adleman [54] developed a practical way, based on Euler's Theorem, of implementing Diffie and Hellman's elegant concept. At present, this method is known as the RSA method where RSA is an acronym for Rivest, Shamir, and Adleman. Currently, the most important modern cryptographic systems are based on the RSA algorithm and its modifications. The RSA method found wide applications in banking transactions, electronic communication, digital signatures and data protection. In fact all global electronic economy is highly dependent on security of transactions and consequently, on the sophisticated methods of number theory.

Further branches of number theory with significant practical applications include the theory of the sequences defined over a finite fields $\mathbb{F}_{p^n}$. These fields are also called Galois fields, after the French mathematician Evariste Galois (25 October 1811 – 31 May 1832). It is well known that sequences over $\mathbb{F}_{p^n}$ are closely related to linear recursions modulo p [57]. Many remarkable and important examples of Galois sequences applications are known. Some of them will be now reminded [34].

One of the basic experiments corroborating the veracity of Einstein's general-relativity theory is called the Shapiro time delay. This experiment is based on the idea that radar signals passing a massive object will travel along a trajectory longer than the one taken with no massive object in the vicinity. Thus, by the relativity theory, a radar signal will travel for a longer time with this time lag being measurable. The radar signal used in the Shapiro experiment was structured as a Galois sequence with a period length of 63. For details of the experiment see [61] and [62]. Another remarkable application of Galois sequences is the measurement of ocean temperatures to monitor global warming [52]. Galois sequences were used to measure sound transmission delays between Heard Island in the Indian Ocean and Greenland, a distance exceeding 10000 km. In this case, the time delay of the sound is a function of the average ocean temperature.

Another important field of Galois sequences application is algebraic error correcting codes such as simplex and Hamming codes [79]. Error-correcting codes are part of the coding theory, which has recently seen major advances in view of the growing importance of data encryption and transfers on the Internet. Error-correcting codes are used in CD players, high speed modems, and mobile phones. Early space probes such as Mariner used a type of error-correcting code called a block code while more recent space probes use convolution codes.

Galois sequences have also been used in many other fields. In neuropsychology, for example, to measure brain–stem responses [14], in atmospheric physics [80], in the non-destructive evaluation of metallic materials [8] and in concert-hall acoustic [60]. Many other interesting applications of Galois sequences, such as the generation of pseudo-random numbers using linear feed-back shift registers, can be found in [57], [58] and [59]. The problems of applications of sequences defined over finite fields will be discussed in Chapter 19.

Further important applications of the number theory can be found in the theory of partition of natural numbers into summands [3]. This remarkable theory has a long history dating back to 1674. Recall, for example, that Hardy - Ramanujan formula [17] has been used, with great success, in quantum physics [6] and in solving various problems of statistical mechanics [4, 10, 48, 66]. The formula played an important role in the crucial breakthrough of Niels Henrik David Bohr (7 October 1885 – 18 November 1962) in the theory of decomposition of heavy atomic nuclei. The relationship between the basic problem of the theory of partitions and physics will be presented in Chapter 20. Some historical notes are also included in [39].

Other interesting applications of number theory include the use of the results and methods of Diophantine analysis. For example, many basic questions in chemistry and virology lead to some Diophantine equations [39]. In Chapter 20, several interesting examples will be shown. In particular, we focus on the problem of balancing chemical equations and the problem of determining the molecular formula. An example concerning the investigation of the virus structures will also be given.

There are many examples of other number theory applications [5]. Some of them have already become an integral part of our every day life. Recall, for example, that the number theory has been used in many ways to devise algorithms for efficient computer arithmetic and for computer operations with large integers. Many computers have preinstalled various internal programs that work thanks to the number theory. Next, a construction of barcodes, zip codes, International Serial Book Numbers (ISBN), International Bank Account Numbers (IBAN), International Standard Music Numbers (ISMN) and vehicle identification numbers are based on elementary number theory. In this sense the number theory affects our everyday life.

Finally, a very important part of the number theory having many practical applications is the theory of Fibonacci numbers and their generalizations. In the following section we will deal with this topic in more detail.

2. Fibonacci numbers and their applications

The Fibonacci sequence $(F_n)_{n=0}^{\infty}$ was introduced by Italian mathematician Leonardo Fibonacci (1175 – 1250) in 1202. It is defined recursively

$$F_0 = 0, F_1 = 1, \text{ and } F_{n+2} = F_{n+1} + F_n \text{ for all } \ n \geq 0.$$

The golden ratio (also known as golden mean, golden proportion or golden section) is an irrational number defined as $\varphi = (1+\sqrt{5})/2 = 1.618\cdots$. This number and $\overline{\varphi} = -1/\varphi = (1-\sqrt{5})/2 = 0.618\cdots$ are the solutions of the quadratic equation $x^2 - x - 1 = 0$. It is well known that Fibonacci numbers F_n can be computed using φ and $\overline{\varphi}$ as follows:

$$F_n = \frac{\varphi^n - \overline{\varphi}^{\,n}}{\varphi - \overline{\varphi}} = \frac{\varphi^n - (-\varphi^{-n})}{\sqrt{5}} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right], \text{ for all } n \geq 0.$$

This explicit formula for F_n is called Binet's formula, after the French mathematician Jacques-Phillipe-Marie Binet (1786 – 1856), who discovered it in 1843. In fact, it was first discovered in 1718 by Abraham De Moivre (1667 – 1754) using generating functions, and also arrived at independently in 1844 by Gabriel Lamé (1795 – 1870).

A comprehensive survey of discoveries concerning the number–theoretic properties of Fibonacci numbers through 1202 – 1919 can be found in *History of the Theory of Numbers* [11] written by Leonard Eugene Dicson (1874 – 1954). Tens of books and monographs as well as thousands of scholary papers have been published on Fibonacci numbers and the golden ratio. Note that the first known book devoted to the golden ratio is *De Divina Proportione* by Luca Pacioli (1445 – 1519). Published in 1509, this book was illustrated by Leonardo da Vinci. As a good introduction into the study of Fibonacci numbers, the book [71] by Nicolai Nicolaevich Vorobiev can be recommended together with the books by Thomas Koshy [44], Steven Vajda [67] and Richard A. Dunlap [13]. For advanced study, see the journal *The Fibonacci Quarterly* founded in 1963 by Alfred Brousseau (1907 – 1988) and Verner Emil Hoggatt (1921 – 1980). Further important facts on Fibonacci numbers can be found in the proceedings of international conferences *Applications of Fibonacci numbers*.

Fibonacci numbers appear in almost every branch of mathematics: in number theory obviously, but also in differential equations, probability, statistics, numerical analysis, and linear algebra. Recall, for example, that Fibonacci numbers played an important role in solving the tenth Hilbert problem (Matijasevich 1970 [49]) and that they are closely related to the Fermat Last Theorem (Sun–Sun 1992 [64]). In the first place, however, Fibonacci numbers and the golden ratio have many important and unexpected applications in physics, chemistry, biology economy, architecture, music, aesthetics and other fields. In physics, for example, they are used in the network analysis of electric transmission lines, help study the atomic structures of some materials and investigate the light reflection paths in optics. In chemistry, they can be found in the theory of aromatic hydrocarbons and in questions related to the periodic table of elements. In biology, they are used to derive formulas for form growth, and in economy, they are part of Elliott's wave principle. Recently, interesting applications have appeared of

Fibonacci numbers in the research of the human genome and cancer. In Chapter 18, we present an extensive list of chronological references to papers on applications of Fibonacci numbers. This chapter can be taken for an introduction to the study of the applications of Fibonacci numbers [32].

Applying the recurrence formula $F_{n+2} = F_{n+1} + F_n$ only to the last digits of the Fibonacci numbers (using modulo 10 arithmetic), we may be surprised to find that, after sixty terms, the sequence starts repeating itself:

0	1	1	2	3	5	8	3	1	4	5	9	4	3	7	0	7	7	4	1
5	6	1	7	8	5	3	8	1	9	0	9	9	8	7	5	2	7	9	6
5	1	6	7	3	0	3	3	6	9	5	4	9	3	2	5	7	2	9	1
0	1	1	.	.	.														

Table 1.

We may also notice further regularities. Applying to $(F_n)_{n=0}^{\infty}$ modulo 2 arithmetic, we obtain a period of length 3, while modulo 5 arithmetic will yield a length 20 period. This follows immediately from Table 1. Investigation of further cases leads to the discovery of the following general theorem: Let $m \in \mathbb{Z}$ and let $m \geq 2$. Then $(F_n \bmod m)_{n=0}^{\infty}$ is periodic. This remarkable property is called the modular periodicity of $(F_n)_{n=0}^{\infty}$. The first related discoveries concerning this property goes back to J. L. Lagrange [45, pp. 142 – 147]. See also Dickson's History [11, p. 393]. A positive integer $k(m)$ is called the period of Fibonacci sequence modulo m if it is the smallest positive integer for which $F_{k(m)} \equiv 0 \pmod{m}$ and $F_{k(m)+1} \equiv 1 \pmod{m}$. Various properties of $k(m)$ have been studied in great detail by many authors. For the basic properties of $k(m)$, see J. C. Kluyver [42], S. Täcklid [65], D. D. Wall [76], D. W. Robinson [55], J. Vinson [68], and A. Vince [69]. The following two properties of $k(m)$ belong certainly to all-important [76, pp. 526 – 527]. Let $m = p_1^{t_1} \cdots p_k^{t_k}$ be the prime factorization of m and let $\mathrm{lcm}(k(p_1^{t_k}), \ldots, k(p_k^{t_k}))$ is the least common multiple of $k(p_1^{t_k}), \ldots, k(p_k^{t_k})$. Then $k(m) = \mathrm{lcm}(k(p_1^{t_k}), \ldots, k(p_k^{t_k}))$. Furthermore, if p is an arbitrary prime and $k(p) = k(p^s) \neq k(p^{s+1})$, then $k(p^t) = p^{t-s}k(p)$ for any positive integers $t \geq s$. Consequently, if $k(p^2) \neq k(p)$, then $k(p^t) = p^{t-1}k(p)$ for all t. The relevance of the above statements is evident. They reduced the investigation of any period $k(m)$ to the periods $k(p)$ with p a prime.

Now we recall the exact formulation of a very interesting and difficult problem published by the American mathematician Donald Dines Wall (August 13, 1921 – November 28, 2000) in 1960. In his famous remark [76, p. 528] Wall poses a question that has so far remained unanswered:

The most perplexing problem we have met in this study concerns the hypothesis $k(p^2) \neq k(p)$. *We have run a test on a digital computer which shows that* $k(p^2) \neq k(p)$ *for all* p *up to* 10,000*; however, we cannot yet prove that* $k(p^2) = k(p)$ *is impossible. The question is closely related to another one, "can a number* x *have the same order* mod p *and* mod p^2*?", for which rare cases give an affirmative answer (e.g.,* $x = 3$, $p = 11$*;* $x = 2$, $p = 1093$*); hence, one might conjecture that equality may hold for some exceptional* p.

It is well known that $k(p^2) = k(p)$ if and only if $F_{p-(5|p)} \equiv 0 \pmod{p^2}$ where $(a|b)$ denotes the Legendere symbol of a and b. Crandal, Dilcher, and Pomerence [9] called primes $p > 5$ satisfying $F_{p-(5|p)} \equiv 0 \pmod{p^2}$ the Wall-Sun-Sun primes. These are sometimes called Fibonacci-Wieferich primes [43]. It has been conjectured that there are infinitely many Wall-Sun-Sun primes, but this conjecture remains unproven as well.

Chapters 1 – 3 are the author's contribution to Wall's problem. In Chapter 1, we begin with a detailed historical study [40] in which all related discoveries and known facts are summarized. Recall now at least the two most important ones. First, in 1992, Zhi-Hong Sun and Zhi-Wei Sun [64] proved that, if $k(p^2) \neq k(p)$ for all primes p, then $x^p + y^p = z^p$ has no integer solution with $p \nmid xyz$. Hence, the affirmative answer to the hypothesis that $k(p^2) \neq k(p)$ for all primes p implies the first case of Fermat's Last Theorem. For this reason, Wall's problem is also referred to as Wall-Sun-Sun prime conjecture in the literature. Further, recall that Wall's problem is closely related to the Fibonacci perfect power problem [7] which was resolved in 2006. Finally, note that in Chapter 1, the important milestones in computer search for Wall-Sun-Sun primes are also included. Thanks to extensive computations of many authors, we can state that there is no Wall-Sun-Sun prime less then 1.9×10^{17} [53].

In Chapter 2, as the main result, we give certain equivalent formulations of Wall's conjecture and derive two interesting criteria that can be used to resolve this conjecture for particular primes. Let K_p be the splitting field of the Fibonacci characteristic polynomial $f(x) = x^2 - x - 1$ over the field of p-adic numbers $\mathbb{Q}_p$ and α, β be the roots of $f(x)$ in K_p. Denote by R_p the ring of integers of K_p. Clearly $\alpha, \beta \in O_p$. Since the discriminant of $f(x)$ is equal to 5, it follows that, for $p \neq 5$, $K_p/\mathbb{Q}_p$ does not ramify and so the maximal ideal of R_p is generated by p. Moreover, if $K_p = \mathbb{Q}_p$, then $\alpha, \beta \in \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the ring of p-adic integers. For a unit $\varepsilon \in R_p$ we denote by $\mathrm{ord}_{p^t}(\varepsilon)$ the least positive rational integer h such that $\varepsilon^h \equiv 1 \pmod{p^t}$. Since $\varepsilon^h \equiv 1 \pmod{p}$ implies $\varepsilon^{ph} \equiv 1 \pmod{p^2}$, we have

$$\text{either} \quad \mathrm{ord}_{p^2}(\varepsilon) = \mathrm{ord}_p(\varepsilon) \quad \text{or} \quad \mathrm{ord}_{p^2}(\varepsilon) = p \cdot \mathrm{ord}_p(\varepsilon).$$

Furthermore, it is not difficult to prove that, if $p > 2$ and $\mathrm{ord}_p(\varepsilon) \neq \mathrm{ord}_{p^2}(\varepsilon)$, then, for any $t \in \mathbb{N}$, we have $\mathrm{ord}_{p^t}(\varepsilon) = p^{t-1}\mathrm{ord}_p(\varepsilon)$. More generally, if $\varepsilon \neq \pm 1$ and $s \in \mathbb{N}$ is the largest integer such that $\mathrm{ord}_{p^s}(\varepsilon) = \mathrm{ord}_p(\varepsilon)$, then, for any $t \geq s$, we have $\mathrm{ord}_{p^t}(\varepsilon) = p^{t-s}\mathrm{ord}_p(\varepsilon)$. Now we can formulate three main theorems proved in [21].

Theorem 2.1. *Let $p \neq 5$. Then $k(p^t) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta))$ for any $t \in \mathbb{N}$.*

Theorem 2.2. (i) *Let $p = 5$. Then $k(p^2) \neq k(p)$ and $k(5^t) = 4 \cdot 5^t$ for any $t \in \mathbb{N}$.*
(ii) *Let $p \neq 5$. Then $k(p^2) \neq k(p)$ if and only if*

$$\mathrm{ord}_{p^2}(\alpha) \equiv 0 \pmod{p} \quad \text{and} \quad \mathrm{ord}_{p^2}(\beta) \equiv 0 \pmod{p}.$$

Theorem 2.2 reduces Wall's question to solving the following equivalent problem. Is there at least one root $\alpha \in R_p$ of $f(x)$ for which $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ or is this never possible? Now we state two interesting criteria that can be used, without computing the roots of $f(x)$ in R_p, to decide whether $k(p^2) = k(p)$ or not. Let $p \neq 5$. Put $q = |R_p/(p)|$. Then $q = p^t$ where $t = [K_p : \mathbb{Q}_p] \in \{1, 2\}$. If $f(x)$ is irreducible over $\mathbb{Q}_p$, then $R_p/(p)$ is a field with p^2 elements. If $f(x)$ is not irreducible over $\mathbb{Q}_p$, then $f(x)$ has both roots in the ring $\mathbb{Z}_p$ and $R_p/(p)$ is a field with p elements.

Theorem 2.3. *Let $p \neq 5$, $u \in R_p$ be such that $f(u) \equiv 0 \pmod{p}$. Then, $k(p^2) = k(p)$ if and only if*

$$u^{2q} - u^q - 1 \equiv 0 \pmod{p^2} \quad \textit{or equivalently} \quad f(u) + (u^q - u)f'(u) \equiv 0 \pmod{p^2}$$

where f' is the derivative of the Fibonacci characteristic polynomial f.

In Chapter 3 we open an interesting question whether, for some primes, the chance that they are Wall-Sun-Sun is greater than for others. The conjecture that there are infinitely Wall-Sun-Sun primes is based on the assumption that the probability that a prime p is Wall-Sun-Sun is equal to $1/p$. Using the arguments presented in [20], we show that another form of probability can be assumed. Our consideration leads to an interesting conclusion that the probability of finding the first Wall-Sun-Sun prime is much greater for primes ending with the digits 1 or 9. Details are given in [20].

3. Cubic generalization of Fibonacci numbers

In 1961, Alwyn Francis Horadam (22 March 1923 – 22 July 2016) suggested that there are two main directions in which the Fibonacci sequence may be generalized [19, p. 458]. Namely, either the recurrence relation can be generalized and extended, or the recurrence relation is preserved, but the first two Fibonacci numbers are replaced by arbitrary integers. He further suggests that these two techniques could be combined. In fact, these generalizations were noted earlier by A. Tagiuri, R. Perrin, A. Agronomof and others. See Dickson's history [11, pp. 393 – 407].

In Chapters 4 – 12, Horadam's sugestion will follow. In particular, some problems concerning the modular periodicity of a cubic generalization of Fibonacci numbers will be studied. These numbers are often called Tribonacci numbers. The name Tribonacci was coined by a talented student, Mark Feinberg [15], in 1963. The Tribonacci sequence $(T_n)_{n=0}^{\infty}$ is defined by the third order linear recurrence $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ with the triple of initial values $[T_0, T_1, T_2] = [a, b, c]$ where a, b, c are integers. Tribonacci numbers T_n have been examined by many authors. First by A. Agronomof [1] in 1914 and, subsequently, by many others [65, 74, 75, 77]. It is well known [77] that $(T_n \bmod m)_{n=0}^{\infty}$ is periodic for any modulus $m > 1$. Let us denote the period of $(T_n \bmod m)_{n=0}^{\infty}$ by $h(m)[a, b, c]$. That is, $h(m)[a, b, c]$ is the least positive integer k for which we have $[T_k, T_{k+1}, T_{k+2}] \equiv [T_0, T_1, T_2] \pmod{m}$. Particularly, if $[T_0, T_1, T_2] = [0, 0, 1]$, then the period $h(m)[0, 0, 1]$ will be denoted by $h(m)$. It 1931, Morgan Ward (1901 – 1963) [77, p. 155] proved that, if $m = p_1^{t_1} \dots p_k^{t_k}$ is a prime factorization of m, then

$$h(m)[a, b, c] = \operatorname{lcm}(h(p_1^{t_1})[a, b, c], \dots, h(p_k^{t_k})[a, b, c]).$$

Consequently, $h(m) = \operatorname{lcm}(h(p_1^{t_1}), \dots, h(p_k^{t_k}))$ [75, p. 347]. Next, in 1978, Marcellus Emron Waddill (28 April 1930 – 24 August 2016) showed that, for any prime p and for any positive integers $r \le t$, the following implication holds.

$$\text{If} \quad h(p) = \cdots = h(p^r) \ne h(p^{r+1}) \quad \text{then} \quad h(p^t) = p^{t-r} h(p).$$

Particularly, if $r = 1$, then $h(p^t) = p^{t-1} h(p)$. See [75, pp. 349 – 351]. Up to the present, no instance of $h(p^2) = h(p)$ has been found and the question whether $h(p^2) = h(p)$ never appears is open. In [24], the primes p satisfying $h(p^2) = h(p)$ were called Tribonacci-Wieferich primes.

From the above it follows that the basic arithmetic properties of Fibonacci and Tribonacci numbers are very similar. However, many properties of Tribonacci numbers are quite different and new.

In Chapters 4 and 5, we generalize the implication by M. E. Waddill and the relationships between the numbers $h(p^t)[a, b, c]$ and $h(p)[a, b, c]$ will be established. Some basic properties of $h(p^t)[a, b, c]$ are summarized by the following lemma.

Lemma 3.1. *Let p be an arbitrary prime and let $[a, b, c]$ be an arbitrary triple of integers. Then, the following statements hold.*

(i) *For any $t \in \mathbb{N}$, we have $h(p^t)[a, b, c] | h(p^t)$.*
(ii) *For any $s, t \in \mathbb{N}$, $1 \le s \le t$, we have $h(p^t)[p^{t-s}a, p^{t-s}b, p^{t-s}c] = h(p^s)[a, b, c]$.*
(iii) *For any $s, t \in \mathbb{N}$, $1 \le s \le t$, we have $h(p^s)[a, b, c] | h(p^t)[a, b, c]$. In particular, we have $h(p)[a, b, c] | h(p^t)[a, b, c]$.*

It is evident that Lemma 3.1 restricts the form of the numbers $h(p^t)[a, b, c]$, which reduces the investigation of the periods $h(p)[a, b, c]$ for general triples $[a, b, c]$ to the case of $[a, b, c] \not\equiv [0, 0, 0] (\text{mod } p)$. As we will see in the sequel, the relations between $h(p^t)[a, b, c]$ and $h(p)[a, b, c]$ highly depend on the form of the factorization of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ over the Galois field $\mathbb{F}_p$ where p is a prime. In the investigation of the periods of Tribonacci sequences beginning with arbitrary triples $[a, b, c]$, the cubic form

$$D(a, b, c) = a^3 + 2b^3 + c^3 - 2abc + 2a^2b + 2ab^2 - 2bc^2 + a^2c - ac^2$$

plays an important role. In Chapter 4, the following theorem will be proved.

Theorem 3.2. *If a triple of initial values $[a, b, c]$ of a Tribonacci sequence $(T_n)_{n=0}^{\infty}$ satisfies $(D(a, b, c), m) = 1$, then $h(m)[a, b, c] = h(m)$.*

The form $D(a, b, c)$ will be also employed to prove the following Theorem 3.3.

Theorem 3.3. *Let p be an arbitrary prime such that $t(x)$ is irreducible over $\mathbb{F}_p$. If $[a, b, c] \not\equiv [0, 0, 0] (\text{mod } p)$ and $h(p) \neq h(p^2)$, then*

$$h(p^t)[a, b, c] = p^{t-1}\, h(p)[a, b, c] = p^{t-1} h(p)$$

for an arbitrary $t \in \mathbb{N}$.

However, if $t(x)$ is not irreducible, it is easy to find examples of triples $[a, b, c]$ for which $D(a, b, c) \equiv 0 \pmod p$ holds and $h(p^t)[a, b, c] = h(p^t)$. Consequently, the form $D(a, b, c)$ cannot be expected to enable us to describe the relationships between the primitive periods if $t(x)$ has at least one root over $\mathbb{F}_p$. In this case, the following concepts will be useful. For a $t \in \mathbb{N}$, denote by $\mathrm{S}_{p^t}(T)$ the set of roots of $t(x)$ in $\mathbb{Z}/p^t\mathbb{Z}$, that is, the spectrum of the Tribonacci matrix

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

over $\mathbb{Z}/p^t\mathbb{Z}$. Next, for $\lambda \in \mathrm{S}_{p^t}(T)$ denote by $\mathrm{E}_{p^t}(\lambda) = \{[a, a\lambda, a\lambda^2], a \in \mathbb{Z}/p^t\mathbb{Z}\}$ the eigenspace corresponding to the eigenvalue λ. Finally, let us denote by $\mathbb{Q}_p$ the field of p-adic numbers and by $\mathbb{Z}_p$ the ring of p-adic integers. The elements of the spectrum $\mathrm{S}_{p^t}(T)$ play an important role in our further considerations.

Let us now deal with the case of a Tribonacci polynom $t(x)$ having over $\mathbb{F}_p$ a factorization of the form $t(x) \equiv (x - \alpha_1)(x^2 - s_1x - r_1) \pmod p$, where the polynomial $u_1(x) = x^2 - s_1x - r_1$ is irreducible over $\mathbb{F}_p$. Since α_1 is a unique solution to $t(x) \equiv 0 \pmod p$, by Hensel's lemma, there is a unique solution α_t to the congruence $t(x) \equiv 0 \pmod{p^t}$. Moreover, for α_t we have $\alpha_t \equiv \alpha_1 \pmod p$. This implies $(x - \alpha_t) | t(x)$ and there is a unique polynomial $u_t(x) = x^2 - s_tx - r_t \in \mathbb{Z}/p^t\mathbb{Z}[x]$ such that $t(x) \equiv (x - \alpha_t)(x^2 - s_tx - r_t) \pmod{p^t}$ where α_t, r_t, s_t are units of the ring $\mathbb{Z}/p^t\mathbb{Z}$ for which $s_t \equiv 1 - \alpha_t \pmod{p^t}$, $r_t \equiv 1 + \alpha_t - \alpha_t^2 \pmod{p^t}$. Hence, the spectrum T

consists of a single element with $\mathrm{S}_{p^t}(T) = \{\alpha_t\}$. Let us denote by $\mathrm{ord}_{p^t}(\alpha_t)$ the order of α_t in the group of units of the ring $\mathbb{Z}/p^t\mathbb{Z}$. Now we are ready to formulate our main theorems.

Theorem 3.4. *Let p be an arbitrary prime such that $t(x)$ is factorized over $\mathbb{F}_p$ into the product of a linear factor and an irreducible quadratic factor. Further, let $h_0 = \mathrm{ord}_p(\alpha_t)$. Then, $h(p^t)[a,b,c]|p^{t-1}h_0$ if and only if $[a,b,c] \pmod{p^t} \in E_{p^t}(\alpha_t)$. Moreover, for $t>1$, $h(p^t)[a,b,c] = p^{t-1}h_0$ if and only if $[a,b,c] \pmod{p^t} \in E_{p^t}(\alpha_t)$, $[a,b,c] \not\equiv [0,0,0] \pmod{p}$ and $\mathrm{ord}_p(\alpha_t) \neq \mathrm{ord}_{p^2}(\alpha_t)$.*

Theorem 3.5. *Let p be an arbitrary prime such that $t(x)$ is factorized over $\mathbb{F}_p$ into the product of a linear factor and an irreducible quadratic factor. Further, let $h(p) \neq h(p^2)$, $\mathrm{ord}_p(\alpha_2) \neq \mathrm{ord}_{p^2}(\alpha_2)$ and $[a,b,c] \not\equiv [0,0,0] \pmod{p}$. Then, for any $t \in \mathbb{N}$, the following assertions are true.*

(i) *If $[a,b,c] \pmod{p^t} \in E_{p^t}(\alpha_t)$, then $h(p^t)[a,b,c] = \mathrm{ord}_{p^t}(\alpha_t) = p^{t-1}\mathrm{ord}_p(\alpha_t)$.*
(ii) *If $[a,b,c] \pmod{p} \notin E_p(\alpha_1)$, then $h(p^t)[a,b,c] = p^{t-1}h(p) = p^{t-1}h(p)[a,b,c]$.*
(iii) *If $[a,b,c] \pmod{p} \in E_p(\alpha_1)$ and $[a,b,c] \pmod{p^t} \notin E_{p^t}(\alpha_t)$, then $h(p^t)[a,b,c] = p^{t-1}h(p) \neq p^{t-1}h(p)[a,b,c]$.*

Let us now focus on the case of the Tribonacci polynomial $t(x)$ completely splitting over the Galois field $\mathbb{F}_p$ into linear factors, that is,

$$t(x) \equiv (x-\alpha_1)(x-\beta_1)(x-\gamma_1) \pmod{p} \quad \text{and} \quad \mathrm{S}_p(T) = \{\alpha_1, \beta_1, \gamma_1\}.$$

Since the discriminant of $t(x)$ is equal to $-44 = -2^2 \cdot 11$, the primes $p = 2, 11$ are the only primes for which $t(x)$ has multiple roots. The primes $p = 2, 11$ make an exception in our theory, which will be examined separately. The assumption $p \neq 2, 11$ implies that $\alpha_1, \beta_1, \gamma_1$ are distinct, thus $t(x)$ has nonzero first derivatives over $\mathbb{F}_p$ at these points. From Hensel's lemma, it follows that $t(x)$ can be factorized over $\mathbb{Q}_p$ as $t(x) = (x-\alpha)(x-\beta)(x-\gamma)$ where $\alpha, \beta, \gamma \in \mathbb{Z}_p$. Let us put $\alpha_t := \alpha \mod p^t$, $\beta_t := \beta \mod p^t$, $\gamma_t := \gamma \mod p^t$ for every $t \in \mathbb{N}$. Thus, over the ring $\mathbb{Z}/p^t\mathbb{Z}$, we have $t(x) \equiv (x-\alpha_t)(x-\beta_t)(x-\gamma_t) \pmod{p^t}$ and $\mathrm{S}_{p^t}(T) = \{\alpha_t, \beta_t, \gamma_t\}$. Our main results are as follows.

Theorem 3.6. Let $t(x)$ be factorized over $\mathbb{F}_p$ into the product of linear terms and let $p \neq 2, 11$. If $h(p) \neq h(p^2)$, then there is at most one eigenvalue $\lambda \in S_{p^t}(T)$ satisfying $\mathrm{ord}_p(\lambda) = \mathrm{ord}_{p^2}(\lambda)$.

Theorem 3.7. *Let $t(x)$ be factorized over $\mathbb{F}_p$, $p \neq 2, 11$, into the product of linear terms. Further, let $[a,b,c] \not\equiv [0,0,0] \pmod{p}$ and, for any $t \in \mathbb{N}$, let $S_{p^t}(T) = \{\alpha_t, \beta_t, \gamma_t\}$.*

(i) *If $\lambda \in S_{p^t}(T)$ and $[a,b,c] \pmod{p^t} \in E_{p^t}(\lambda)$, then $h(p^t)[a,b,c] = \mathrm{ord}_{p^t}(\lambda)$. Moreover, if, for $t > 1$, $\lambda \in S_{p^t}(T)$ fulfils the condition $\mathrm{ord}_p(\lambda) \neq \mathrm{ord}_{p^2}(\lambda)$, then $h(p^t)[a,b,c] = p^{t-1}\mathrm{ord}_p(\lambda) = p^{t-1}h(p)[a,b,c]$.*
(ii) *If $[a,b,c] \pmod{p^t} \notin E_{p^t}(\alpha_t) \cup E_{p^t}(\beta_t) \cup E_{p^t}(\gamma_t)$ and, for every $\lambda \in S_{p^t}(T)$, $t > 1$, $\mathrm{ord}_p(\lambda) \neq \mathrm{ord}_{p^2}(\lambda)$, then $h(p^t)[a,b,c] = h(p^t) = p^{t-1}h(p)$.*

We will now look more closely at the properties of the period $h(p)$. It is well known [70, p. 310] that the periods $h(p)$ highly depend on the form of the factorization of $t(x)$ modulo p. For $p \neq 2, 11$, we have:

$$\text{If } \left(\frac{p}{11}\right) = 1, \text{ then } \begin{cases} h(p)|p^2+p+1 \text{ if } t(x) \text{ is irreducible mod } p, \\ h(p)|p-1 \quad \text{otherwise.} \end{cases}$$

If $\left(\dfrac{p}{11}\right) = -1$, then $h(p)|p^2-1$. Here $\left(\dfrac{p}{11}\right)$ denotes the Legendre symbol.

The above statement is a consequence of a well known criterion for the factorability of cubics mod p, which can be formulated as follows:

Let N be the number of solutions of $x^3+ax^2+bx+c \equiv 0 \pmod p$ where $a,b,c \in \mathbb{Z}$ and let $D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$ be the discriminant of the cubic polynomial x^3+ax^2+bx+c. If p is a prime, $p>3$ and $p \nmid D$, we have:

(i) $N = 1$ *if and only if* $(D/p) = -1$,

(ii) $N = 0$ *or* $N = 3$ *if and only if* $(D/p) = 1$.

This theorem dates from 1894 originating in the thesis of G. F. Voronoï [72]. Consult also [73, p. 189]. On the other hand, this theorem follows from a more general Stickelberger Parity Theorem [63] published in 1897. See also Dickson's history [11, pp. 249 – 251]. Furthermore, recall that, if K is the splitting field of the Tribonacci polynomial $t(x)$ over the field $\mathbb{F}_p$, $p \neq 2, 11$ and α, β, γ are the roots of $t(x)$ in K, then

$$h(p) = \mathrm{lcm}(\mathrm{ord}_K(\alpha), \mathrm{ord}_K(\beta), \mathrm{ord}_K(\gamma))$$

where the numbers $\mathrm{ord}_K(\alpha)$, $\mathrm{ord}_K(\beta)$, $\mathrm{ord}_K(\gamma)$ are the orders of α, β, γ in the multiplicative group of K and lcm is their least common multiple [70].

Now we focus on our results proved in Chapter 4. Let $p \neq 2, 11$ be an arbitrary prime and let $\mathrm{S}_p(T) = \{\alpha_1, \beta_1, \gamma_1\}$, that is, $t(x)$ completely splits over $\mathbb{F}_p$ into linear factors. Further, let $\mathrm{ord}_p(\alpha_1) = h_1, \mathrm{ord}_p(\beta_1) = h_2$ and $\mathrm{ord}_p(\gamma_1) = h_3$. Then

$$\mathrm{lcm}(h_1,h_2) = \mathrm{lcm}(h_1,h_3) = \mathrm{lcm}(h_2,h_3) = \mathrm{lcm}(h_1,h_2,h_3) = h(p).$$

Investigating the orders h_1, h_2, h_3 for the first several hundreds of primes might lead to a hypothesis that there are always two of the orders h_1, h_2, h_3 that divide the third. The first counter-example that disproves this hypothesis is $p = 4481$. Over $\mathbb{F}_{4481}$, $t(x)$ can be written as $t(x) = (x-2661)(x-2677)(x-3625)$. Denoting $\alpha_1 = 2661$, $\beta_1 = 2677$, $\gamma_1 = 3625$, we arrive at $\mathrm{ord}_p(\alpha_1) = 2240$, $\mathrm{ord}_p(\beta_1) = 640$, $\mathrm{ord}_p(\gamma_1) = 896$ and $h(p) = \mathrm{lcm}(2240, 640, 896) = 4480$. Further, if two of the roots $\alpha_1, \beta_1, \gamma_1$ are of the same order in the multiplicative group of $\mathbb{F}_p$ different from the order of the third root, the following two situations may, theoretically, occur:

$$\mathrm{ord}_p(\alpha_1) < \mathrm{ord}_p(\beta_1) = \mathrm{ord}_p(\gamma_1) \qquad \text{and} \qquad \mathrm{ord}_p(\alpha_1) = \mathrm{ord}_p(\beta_1) < \mathrm{ord}_p(\gamma_1).$$

In [22, p. 286] we showed that the second case can never occur. That is, if $\mathrm{ord}_p(\alpha_1) = \mathrm{ord}_p(\beta_1) = h$, then $\mathrm{ord}_p(\gamma_1)|h$. Hence, without loss of generality we can denote the roots of $t(x)$ over $\mathbb{F}_p$ by α_1, β_1, γ_1 so that, for their orders h_1, h_2, h_3 and $h(p) = \mathrm{lcm}(h_1,h_2,h_3)$, exactly one of the four following events occurs:

$$\begin{aligned} &h_1 = h_2 = h_3 = h(p), \quad p = 103,\\ &h_1 < h_2 = h_3 = h(p), \quad p = 47,\\ &h_1 < h_2 < h_3 = h(p), \quad p = 311,\\ &h_1 < h_2 < h_3 < h(p), \quad p = 4481. \end{aligned}$$

The presented values of the primes p are the least values for which the corresponding relation occurs. Now we will shortly deal with the results of Chapter 5.

In Chapter 5 we determine the numbers $h(p^t)[a,b,c]$ for the case of the exceptional primes $p = 2, 11$. The methods used in proofs are mostly based on matrix algebra. The main results of Chapter 5 can be summarized as follows.

Theorem 3.8. *Let $t > 1$ and $[a,b,c] \not\equiv [0,0,0] \pmod 2$. Then, we have*

(i) *If $[a,b,c] \equiv [1,1,1] \pmod 2$, then $h(2^t)[a,b,c] = 2^t$.*
(ii) *If $[a,b,c] \not\equiv [1,1,1] \pmod 2$, then $h(2^t)[a,b,c] = 2^{t+1}$.*

Over the field $\mathbb{Q}_{11}$, $t(x)$ has only one root $\alpha = 9 + 2 \cdot 11 + 1 \cdot 11^2 + \cdots \in \mathbb{Z}_{11}$. Put $E(\alpha_t) = \{[q, q\alpha_t, q\alpha_t^2]; q \in \mathbb{Z}/11^t\mathbb{Z}\}$ where $\alpha_t = \alpha \bmod 11^t$. Then, for periods $h(11^t)[a,b,c]$, the following statements hold.

Theorem 3.9. *Let $t \geq 1$ and $[a,b,c] \not\equiv [0,0,0] \pmod{11}$. Then, we have*

(i) *If $[a,b,c] \notin E(\alpha_t)$ and $c \equiv 3a + 5b \pmod{11}$, then $h(11^t)[a,b,c] = 10 \cdot 11^{t-1}$.*
(ii) *If $[a,b,c] \notin E(\alpha_t)$ and $c \not\equiv 3a + 5b \pmod{11}$, then $h(11^t)[a,b,c] = 10 \cdot 11^t$.*
(iii) *If $[a,b,c] \in E(\alpha_t)$, then $h(11^t)[a,b,c] = \mathrm{ord}_{11^t}(\alpha_t) = 5 \cdot 11^{t-1}$.*

In Chapters 6 and 7, using the matrix formalism, we will study an analogy to Wall's conjecture for the Tribonacci case. Our considerations are placed in the following framework. Let L_p be the splitting field of the Tribonacci polynomial $t(x)$ over the field of p-adic numbers $\mathbb{Q}_p$ and let α, β, γ be the roots of $t(x)$ in L_p. Further, let O_p be the ring of integers of L_p. Clearly, $\alpha, \beta, \gamma \in O_p$. As the discriminant of $t(x)$ is equal to -44, the Galois extension $L_p/\mathbb{Q}_p$ does not ramify for $p \neq 2, 11$. For any unit $\xi \in O_p$ and for any $t \in \mathbb{N}$, we denote by $\mathrm{ord}_{p^t}(\xi)$ the least positive rational integer k such that $\xi^k \equiv 1 \pmod{p^t}$. In Chapter 6, the following theorem will be proved.

Theorem 3.10. *Let $p \neq 2, 11$. Then, for any $t \in \mathbb{N}$, we have*

$$h(p^t) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta), \mathrm{ord}_{p^t}(\gamma)).$$

Next, for any prime p, we define an integer matrix $A_p = [a_{ij}]$ such that

$$A_p = \frac{1}{p}(T^{h(p)} - E)$$

where E is the 3×3 identity matrix. In the investigation of the equality $h(p) = h(p^2)$ the matrix A_p plays an important role.

Theorem 3.11. The following statements are true.

(i) *For any prime p, we have $h(p) \neq h(p^2)$ if and only if $A_p \not\equiv 0 \pmod p$.*
(ii) *For any prime $p \neq 2, 11$, we have $A_p \equiv 0 \pmod p$ if and only if $\mathrm{ord}_{p^2}(\lambda) \not\equiv 0 \pmod p$ for each $\lambda \in \{\alpha, \beta, \gamma\}$.*
(iii) *Let $p \neq 2, 11$ and $A_p \not\equiv 0 \pmod p$. Then, $\det A_p \equiv 0 \pmod p$ if and only if there is a unique $\lambda \in \{\alpha, \beta, \gamma\}$ for which $\mathrm{ord}_{p^2}(\lambda) \not\equiv 0 \pmod p$. Moreover, for this λ, we have $\lambda \in \mathbb{Z}_p$ where $\mathbb{Z}_p$ is the ring of p-adic integers.*
(iv) *Let $t(x)$ be irreducible over $\mathbb{Q}_p$. Then, we have $A_p \equiv 0 \pmod p$ if and only if $\det A_p \equiv 0 \pmod p$.*
(v) *Let $p \neq 2, 11$. Then, $\det A_p \equiv 0 \pmod p$ if and only if there is at least one $\lambda \in \{\alpha, \beta, \gamma\}$ such that $\mathrm{ord}_{p^2}(\lambda) \not\equiv 0 \pmod p$.*

Our results can be summarized in the following theorem.

Theorem 3.12. *Let $p \neq 2, 11$ and let k be the number of roots α, β, γ of $t(x)$ in O_p whose order modulo p^2 is divisible by p. Then, the following cases may occur:*

Case $k = 0$: $h(p) = h(p^2)$, or equivalently $A_p \equiv 0 \pmod p$.
Case $k = 1$: This case is impossible.
Case $k = 2$: $h(p) \neq h(p^2)$ and $\det A_p \equiv 0 \pmod p$.
Case $k = 3$: $h(p) \neq h(p^2)$ and $\det A_p \not\equiv 0 \pmod p$.

A natural question arises whether there is a prime p satisfying $k = 2$. Since the solution of this question seems to be as difficult as the question whether $h(p) \neq h(p^2)$ for all primes p, we state it as a new problem:

Decide whether there is a prime p for which $h(p) \neq h(p^2)$ and $\operatorname{ord}_p(\alpha) = \operatorname{ord}_{p^2}(\alpha)$ where $\alpha \in \mathbb{Z}$ is a solution of $x^3 - x^2 - x - 1 \equiv 0 \pmod{p^2}$. The prime p satisfying these conditions may be called Tribonacci-Wieferich prime of the second kind.

Furthermore, in Chapter 6, we derive two interesting criteria that can be used, without computing the roots of $t(x)$ in O_p, to decide whether $h(p) = h(p^2)$ or not. For $p \neq 2, 11$ put $q = |O_p/(p)|$. Then, $q = p^t$ where $t = [L_p : \mathbb{Q}_p] \in \{1, 2, 3\}$.

Theorem 3.13. *Let $p \neq 2, 11$, $u \in O_p$ such that $t(u) \equiv 0 \pmod{p}$. Suppose that $t(x)$ is irreducible over $\mathbb{Q}_p$. Then the following statements are equivalent:*

(i) $h(p) = h(p^2)$,
(ii) $u^{3q} - u^{2q} - u^q - 1 \equiv 0 \pmod{p^2}$.
(iii) $t(u) + (u^q - u)t'(u) \equiv 0 \pmod{p^2}$,
(iv) $3u^{q+2} - 2u^{q+1} - u^q - 2u^3 + u^2 - 1 \equiv 0 \pmod{p^2}$.

In (iii) *t' is the derivative of the Tribonacci characteristic polynomial t.*

The case of $t(x)$ being reducible over $\mathbb{Q}_p$ is also solved in Chapter 6. By an extensive computer search, based on Theorem 3.13, we have obtained the following two results:

Theorem 3.14. (i) *There is no Tribonacci-Wieferich prime $p < 10^9$.*
(ii) *There is no Tribonacci-Wieferich prime of the second kind $p < 10^9$.*

By analogy with the problem of Tribonacci-Wieferich primes of the second kind, we can consider a similar problem for a Tetranacci sequence $(M_n)_{n=0}^{\infty}$ defined by $M_{n+4} = M_{n+3} + M_{n+2} + M_{n+1} + M_n$ with $M_0 = M_1 = M_2 = 0$ and $M_3 = 1$. Now, let $h(m)$ denote a period of $(M_n \bmod m)_{n=0}^{\infty}$. Is there a prime p for which $h(p) \neq h(p^2)$ and $\operatorname{ord}_p(\alpha) = \operatorname{ord}_{p^2}(\alpha)$ where $\alpha \in \mathbb{Z}$ is a solution of $x^4 - x^3 - x^2 - x - 1 \equiv 0 \pmod{p^2}$? To this problem we find the following solution. *For $p < 10^9$, there are exactly three Tetranacci-Wieferich primes of the second kind: $p_1 = 17$, $p_2 = 191$, and $p_3 = 11351$.*

In Chapter 7 we provide a method that can substantially extend the results presented in Theorem 3.14. Implementing this method in Pari GP, the following results have been obtained.

Theorem 3.15. (i) *There is no Tribonacci-Wieferich prime $p < 10^{11}$.*
(ii) *There is no Tribonacci-Wieferich prime of the second kind $p < 10^{11}$.*

More details related to our computer search for Tribonacci-Wieferich primes can be found in [25].

The results of Chapters 4 – 7 provide the necessary basis for solving the combinatorial problem originally formulated by Morgan Ward [78] in 1935. A solution for Fibonacci sequences was found by A. Andreassian [2] in 1974. In Chapter 8, we resolve Ward's problem for the case of Tribonacci sequences. Recall now some basic definitions needed for the formulation our main results. Let us consider a binary relation $\sim$ on the set $S = [\mathbb{Z}/m\mathbb{Z}]^3$ defined by

$$[a_1, b_1, c_1] \sim [a_2, b_2, c_2] \quad \text{if and only if} \quad h(m)[a_1, b_1, c_1] = h(m)[a_2, b_2, c_2].$$

Clearly, $\sim$ is an equivalence on S and $S/\sim$ is a partition of S. Let $N(h, m)$ denote the number of elements in the class $\{[a, b, c] \in S; h(m)[a, b, c] = h\}$ and let H denote the set of all possible periods $h(m)[a,b,c]$. Since, for a given modulus m, there are m^3 different initial conditions, we have

$$m^3 = \sum_{h \in H} N(h,m).$$

Further, for $[a_1,b_1,c_1],[a_2,b_2,c_2] \in S$, we put $[a_1,b_1,c_1] \approx [a_2,b_2,c_2]$ if and only if, in the sequence $(T_n \bmod m)_{n=1}^{\infty}$ that starts with a triple $[a_1,b_1,c_1]$, there is an index i such that $[T_i,T_{i+1},T_{i+2}] \equiv [a_2,b_2,c_2] \pmod{m}$. The relation $\approx$ is also an equivalence on S and the partition $S/\approx$ is a refinement of $S/\sim$. Let $n(h,m)$ denote the number of classes in $S/\approx$ that result from a refinement of the class $\{[a,b,c] \in S; h(m)[a,b,c] = h\}$. That is, $n(h,m)$ establishes the number of distinct Tribonacci sequences modulo m whose period is equal to h. Since we have $N(h,m) = n(h,m) \cdot h$, it follows that

$$m^3 = \sum_{h \in H} n(h,m) \cdot h = c_1 \cdot h_1 + \cdots + c_r \cdot h_r,$$

where $H = \{h_1,\ldots,h_r\}$ and $c_i = n(h_i,m)$ for $i \in \{1,\ldots,r\}$. This relation will be called a *Tribonacci partition formula modulo* m, and its left-hand side will be written as $[m]^3$. For example, if $m = 10$, then $H = \{1,2,4,31,62,124\}$ and the Tribonacci partition formula modulo 10 has the form

$$[10]^3 = 2 \cdot 1 + 1 \cdot 2 + 1 \cdot 4 + 8 \cdot 31 + 4 \cdot 62 + 4 \cdot 124.$$

By analogy, we can define a partition formula for any $\emptyset \neq R \subseteq S$. This formula will be denoted by $[m]^3_R$. The following special case will be useful in the sequel. Let $R = \{[a,b,c] \in [\mathbb{Z}/p^t\mathbb{Z}]^3; [a,b,c] \equiv [0,0,0] (\bmod p)\}$. Then $[p^t]^3_R = [p^{t-1}]^3$ for any $t > 1$.

In Chapter 8, we find two important methods that use known formulas to construct some others. These processess, together with the results obtained in [22], [23], and [24], enable us to establish the forms of Tribonacci formulas for any modulus $m > 1$.

Let $\emptyset \neq S_1, S_2 \subseteq S = [\mathbb{Z}/m\mathbb{Z}]^3$, and $S_1 \cap S_2 = \emptyset$. Further, let $[m]^3_{S_1} = c_1 \cdot h_1 + \cdots + c_r \cdot h_r$ and $[m]^3_{S_2} = c'_1 \cdot h'_1 + \cdots + c'_s \cdot h'_s$. We define the sum of $[m]^3_{S_1}$, $[m]^3_{S_2}$ as follows

$$[m]^3_{S_1} + [m]^3_{S_2} = c_1 \cdot h_1 + \cdots + c_r \cdot h_r + c'_1 \cdot h'_1 + \cdots + c'_s \cdot h'_s.$$

Clearly, if there is $1 \leq j \leq s$ such that $h_i = h'_j$ for some $1 \leq i \leq r$, then j is unique. In this case, we shall write $c_i h_i + c'_j h'_j$ as $(c_i + c'_j) \cdot h_i$ and Lemma 3.16 immediately follows.

Lemma 3.16. *Let $\emptyset \neq \{S_1, \cdots, S_k\}$ be an arbitrary system of nonempty and pairwise disjunct subsets of $S = [\mathbb{Z}/m\mathbb{Z}]^3$. Put $R = \cup_{i=1}^k S_i$. Then, we have*

$$[m]^3_R = \sum_{i=1}^{k} [m]^3_{S_i}.$$

Particulary, if $\{S_1,\ldots,S_k\}$ is a partition of S, then $[m]^3 = \sum_{i=1}^k [m]^3_{S_i}$.

Let $m_1, m_2 > 1$ be arbitrary modules such that $(m_1,m_2) = 1$. Further assume that the formulas $[m_1]^3 = c_1 \cdot h_1 + \cdots + c_r \cdot h_r$, and $[m_2]^3 = c'_1 \cdot h'_1 + \cdots + c'_s \cdot h'_s$ are known. We define the product of $[m_1]^3$ and $[m_2]^3$ by

$$[m_1]^3 \cdot [m_2]^3 = \sum_{i=1}^{r} \sum_{j=1}^{s} c_i c'_j \gcd(h_i, h'_j) \cdot \operatorname{lcm}(h_i, h'_j).$$

Thus, the product of the formulas can be computed as the obvious product of polynomials and the product of $c_i \cdot h_i$ and $c'_j \cdot h'_j$ will be interpreted as $c_i c'_j \gcd(h_i, h'_j) \cdot \mathrm{lcm}(h_i, h'_j)$. Finally, after this expansion, we group the terms with the same period.

Lemma 3.17. *Let $m = p_1^{t_1} \dots p_k^{t_k}$ be a prime factorization of m and let, for any $1 \le i \le k$, the formulas $[p_i^{t_i}]^3 = c_1^{(i)} \cdot h_1^{(i)} + \dots + c_{s_i}^{(i)} \cdot h_{s_i}^{(i)}$ be known. Then, we have*

$$[m]^3 = [p_1^{t_1}]^3 \dots [p_k^{t_k}]^3 = \sum_{i_1=1}^{s_1} \cdots \sum_{i_k=1}^{s_k} [c_{i_1}^{(1)} \dots c_{i_k}^{(k)} \gcd(h_{i_1}^{(1)}, \dots, h_{i_k}^{(k)})] \cdot \mathrm{lcm}(h_{i_1}^{(1)}, \dots, h_{i_k}^{(k)}).$$

Moreover,

$$n(h, m) = \frac{1}{h} \sum_{(h_1, \dots, h_k)} N(h_1, p_1^{t_1}) \cdots N(h_k, p_k^{t_k}),$$

where the sum extends over all k-tuples $(h_1, \dots, h_k)$ with $\mathrm{lcm}(h_1, \dots, h_k) = h$.

Lemma 3.17 has a practical meaning. If we know the partition formulas for the modulus of the form of powers of primes, then we can use them to construct the partition formulas for any composite modulus m. Hence, Lemma 3.17 reduced the investigation of Tribonacci partition formulas to those moduli that are powers of primes. We show some example. Using Lemma 3.17, we find the Tribonacci partition formula $[12]^3$. We assume that the formulas $[2^2]^3$ and $[3]^3$ are known. Since $[2^2]^3 = 2 \cdot 1 + 1 \cdot 2 + 3 \cdot 4 + 6 \cdot 8$, and $[3]^3 = 1 \cdot 1 + 2 \cdot 13$, Lemma 3.17 yields

$$\begin{aligned}[12]^3 = [2^2]^3 \cdot [3]^3 &= (2 \cdot 1 + 1 \cdot 2 + 3 \cdot 4 + 6 \cdot 8) \cdot (1 \cdot 1 + 2 \cdot 13) = \\ &= 2 \cdot 1 + 1 \cdot 2 + 3 \cdot 4 + 6 \cdot 8 + 4 \cdot 13 + 2 \cdot 26 + 6 \cdot 52 + 12 \cdot 104.\end{aligned}$$

Now we focus on the case of Tribonacci partition formulas for powers of primes. We begin with primes $p = 2$ and $p = 11$. By direct computation, we can establish that

$$[\,2\,]^3 = 2 \cdot 1 + 1 \cdot 2 + 1 \cdot 4,$$

$$[2^2]^3 = 2 \cdot 1 + 1 \cdot 2 + 3 \cdot 4 + 6 \cdot 8,$$

$$[2^3]^3 = 2 \cdot 1 + 1 \cdot 2 + 3 \cdot 4 + 14 \cdot 8 + 24 \cdot 16,$$

and

$$[\,11\,]^3 = 1 \cdot 1 + 2 \cdot 5 + 11 \cdot 10 + 11 \cdot 110,$$

$$[11^2]^3 = 1 \cdot 1 + 2 \cdot 5 + 11 \cdot 10 + 2 \cdot 55 + 1462 \cdot 110 + 1331 \cdot 1210,$$

$$[11^3]^3 = 1 \cdot 1 + 2 \cdot 5 + 11 \cdot 10 + 2 \cdot 55 + 1462 \cdot 110 + 2 \cdot 605 + 177022 \cdot 1210 + 161051 \cdot 13310.$$

In [28], the following general theorems have been proved.

Theorem 3.18. (i) *For any $t \ge 3$, the Tribonacci partition formula $[2^t]^3$ has the form*

$$[2^t]^3 = 2 \cdot 1 + 1 \cdot 2 + 3 \cdot 2^2 + (7 \cdot 2) \cdot 2^3 + (7 \cdot 2^3) \cdot 2^4 + \dots + (7 \cdot 2^{2t-5}) \cdot 2^t + (3 \cdot 2^{2t-3}) \cdot 2^{t+1}.$$

(ii) *For any $t \ge 2$, the Tribonacci partition formula $[11^t]^3$ has the form*

$$[11^t]^3 = 1 \cdot 1 + 11 \cdot 10 + \sum_{i=0}^{t-1} 2 \cdot (5 \cdot 11^i) + \sum_{i=1}^{t-2} (133 \cdot 11^{2i-1} - 1) \cdot (10 \cdot 11^i) + 11^{2t-1} \cdot (10 \cdot 11^t).$$

Theorem 3.19. *Let $t(x)$ have no root over the field of p-adic numbers $\mathbb{Q}_p$, $p \ne 2$. Let r be the largest positive integer such that $h(p^r) = h(p)$. Then, for any positive integers*

$r < t$, we have

$$[p^t]^3 = 1\cdot 1 + \frac{p^{3r}-1}{h}\cdot h + \sum_{i=1}^{t-r} \frac{p^{3r+2i} - p^{3r+2i-3}}{h}\cdot p^i h \quad \text{where} \quad h = h(p).$$

Particulary, if $r = 1$, we have

$$[p^t]^3 = 1\cdot 1 + \sum_{i=0}^{t-1} \frac{p^{2i}(p^3-1)}{h}\cdot p^i h.$$

Next we focus on the case of $t(x)$ having exactly one root over $\mathbb{Q}_p$. We have:

Theorem 3.20. *Let $t(x)$ have exactly one root α in the field of p-adic numbers $\mathbb{Q}_p$, $p \neq 11$. Let r be the largest positive integer satisfying $h(p) = h(p^r)$, and s be the largest positive integer satisfying $\mathrm{ord}_p(\alpha) = \mathrm{ord}_{p^s}(\alpha)$. If $r < s < t$, then we have*

$$[p^t]^3 = 1\cdot 1 + \frac{p^s-1}{h_1}\cdot h_1 + \frac{p^{3r}-p^r}{h}\cdot h + \sum_{i=1}^{t-s} \frac{p^s - p^{s-1}}{h_1}\cdot p^i h_1 + \sum_{i=1}^{t-r} \frac{p^{3r+2i} - p^{3r+2i-3} - p^r + p^{r-1}}{h}\cdot p^i h,$$

where $h_1 = \mathrm{ord}_p(\alpha)$ and $h = h(p)$. Particulary, for $r = s = 1$, we have

$$[p^t]^3 = 1\cdot 1 + \sum_{i=0}^{t-1} \frac{p-1}{h_1}\cdot p^i h_1 + \sum_{i=0}^{t-1} \frac{p^{2i+3} - p^{2i} - p + 1}{h}\cdot p^i h.$$

Some examples demonstrating the formulas presented in Theorem 3.19 and 3.20 are in [28] also included. The most interesting case is that of $t(x)$ having exactly three roots α, β, γ in $\mathbb{Q}_p$. In this case, the forms of the partition formulas heavily depend on the relationships between the orders of α, β, γ in the multiplicative group of the ring $\mathbb{Z}/p^t\mathbb{Z}$. Put $h_1 = \mathrm{ord}_p(\alpha), h_2 = \mathrm{ord}_p(\beta), h_3 = \mathrm{ord}_p(\gamma)$, and $h = h(p)$. By Chapter 4, exactly one of the four following events occurs

(I) $h_1 < h_2 < h_3 < h$, (II) $h_1 < h_2 < h_3 = h$, (III) $h_1 < h_2 = h_3 = h$, (IV) $h_1 = h_2 = h_3 = h$.

For (I), we have:

Theorem 3.21. *Let $t(x)$ have three roots α, β, γ in $\mathbb{Q}_p$, and assume that the numbers $h_1 = \mathrm{ord}_p(\alpha), h_2 = \mathrm{ord}_p(\beta), h_3 = \mathrm{ord}_p(\gamma)$, and $h = h(p)$ are distinct. Let r be the largest positive integer satisfying $h(p) = h(p^r)$, and let $s > r$ be the largest positive integer satisfying $\mathrm{ord}_p(\xi) = \mathrm{ord}_{p^s}(\xi)$ for a unique $\xi \in \{\alpha, \beta, \gamma\}$. Say, $\xi = \alpha$. Then, for any $t > s$, we have*

$$[p^t]^3 = 1\cdot 1 + \frac{p^s-1}{h_1}\cdot h_1 + \frac{p^r-1}{h_2}\cdot h_2 + \frac{p^r-1}{h_3}\cdot h_3 + \frac{p^{3r}-3p^r+2}{h}\cdot h + \sum_{i=1}^{t-s} \frac{p^s-p^{s-1}}{h_1}\cdot p^i h_1$$
$$+ \sum_{i=1}^{t-r} \frac{p^r-p^{r-1}}{h_2}\cdot p^i h_2 + \sum_{i=1}^{t-r} \frac{p^r-p^{r-1}}{h_3}\cdot p^i h_3 + \sum_{i=1}^{t-r} \frac{p^{3r+2i} - p^{3r+2i-3} - 3p^r + 3p^{r-1}}{h}\cdot p^i h.$$

Particulary, if $r = s = 1$, we have

$$[p^t]^3 = 1\cdot 1 + \sum_{i=0}^{t-1} \frac{p-1}{h_1}\cdot p^i h_1 + \sum_{i=0}^{t-1} \frac{p-1}{h_2}\cdot p^i h_2 + \sum_{i=0}^{t-1} \frac{p-1}{h_3}\cdot p^i h_3 + \sum_{i=0}^{t-1} \frac{p^{2i+3} - p^{2i} - 3p + 3}{h}\cdot p^i h.$$

For the remaining cases (II), (III) and (IV), the following theorems have been established:

Theorem 3.22. *If $h_1 < h_2 < h_3 = h$, then*

$$[p^t]^3 = 1\cdot1+\frac{p^s-1}{h_1}\cdot h_1+\frac{p^r-1}{h_2}\cdot h_2+\frac{p^{3r}-2p^r+1}{h}\cdot h+\sum_{i=1}^{t-s}\frac{p^s-p^{s-1}}{h_1}\cdot p^i h_1+\sum_{i=1}^{t-r}\frac{p^r-p^{r-1}}{h_2}\cdot p^i h_2$$

$$+\sum_{i=1}^{t-r}\frac{p^{3r+2i}-p^{3r+2i-3}-2p^r+2p^{r-1}}{h}\cdot p^i h.$$

If $h_1 < h_2 = h_3 = h$, then

$$[p^t]^3 = 1\cdot 1+\frac{p^s-1}{h_1}\cdot h_1+\frac{p^{3r}-p^r}{h}\cdot h+\sum_{i=1}^{t-s}\frac{p^s-p^{s-1}}{h_1}\cdot p^i h_1$$

$$+\sum_{i=1}^{t-r}\frac{p^{3r+2i}-p^{3r+2i-3}-p^r+p^{r-1}}{h}\cdot p^i h.$$

If $h_1 = h_2 = h_3 = h$, then

$$[p^t]^3 = 1\cdot 1+\frac{p^{3r}+p^s-p^r-1}{h}\cdot h+\sum_{i=1}^{t-s}\frac{p^{3r+2i}-p^{3r+2i-3}+p^s-p^r+p^{r-1}-p^{s-1}}{h}\cdot p^i h$$

$$+\sum_{i=t-s+1}^{t-r}\frac{p^{3r+2i}-p^{3r+2i-3}-p^r+p^{r-1}}{h}\cdot p^i h.$$

Specifically, if $r = s = 1$, then the above formulas have following simple forms:

$$[p^t]^3 = 1\cdot 1+\sum_{i=0}^{t-1}\frac{p-1}{h_1}\cdot p^i h_1+\sum_{i=0}^{t-1}\frac{p-1}{h_2}\cdot p^i h_2+\sum_{i=0}^{t-1}\frac{p^{2i+3}-p^{2i}-2p+2}{h}\cdot p^i h.$$

$$[p^t]^3 = 1\cdot 1+\sum_{i=0}^{t-1}\frac{p-1}{h_1}\cdot p^i h_1+\sum_{i=0}^{t-1}\frac{p^{2i+3}-p^{2i}-p+1}{h}\cdot p^i h.$$

$$[p^t]^3 = 1\cdot 1+\sum_{i=0}^{t-1}\frac{p^{2i}(p^3-1)}{h}\cdot p^i h.$$

In Chapter 9 we complete our preceding research of the modular periodicity of integer sequences defined by a Tribonacci recurrence [26]. Let $I = \{3, 5, 23, 31, \dots\}$ be the set of all primes p for which $t(x)$ is irreducible over $\mathbb{F}_p$, $Q = \{7, 13, 17, 19, \dots\}$ be the set of all primes for which $t(x)$ splits over $\mathbb{F}_p$ into the product of a linear factor and an irreducible quadratic factor and let $L = \{2, 11, 47, 53, \dots\}$ be the set of all primes for which $t(x)$ completely splits over $\mathbb{F}_p$ into linear factors. Recall now that a subset A of the set of all primes has a natural density $d(A)$ if

$$d(A) = \lim_{x\to\infty}\frac{|\{p \in A; p \le x\}|}{\pi(x)}.$$

Using the Frobenius density theorem, we proved that $d(I) = 1/3$, $d(Q) = 1/2$, and $d(L) = 1/6$. Hence, it follows:

Theorem 3.23. *For $d(I), d(Q), d(L)$ we have $d(I) : d(Q) : d(L) = 2 : 3 : 1$.*

Furthermore, in Chapter 9, the exact values can be found of the periods $h(p)$ for any prime $p \leq 5000$. A detailed examination of these values leads us to a new hypothesis proved in Chapter 11.

In Chapters 10 – 12, the cubic character of roots of Tribonacci polynomial $t(x)$ over the Galois fields $\mathbb{F}_p$ will be examined [29, 30, 31]. Our main result, proved in Chapter 10, is as follows:

Theorem 3.24. *Let p be an arbitrary prime such that $p \equiv 1 \pmod 3$ and let τ be any root of $t(x)$ in the field $\mathbb{F}_p$. Then,*

$$\tau^{\frac{p-1}{3}} \equiv 2^{\frac{2(p-1)}{3}} \pmod p.$$

Moreover, if τ is any root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$, then 2τ is a cubic residue of K, that is, there exists $\omega \in K$ such that $2\tau = \omega^3$.

Further, in Chapter 11 the following identity will be proved:

Theorem 3.25. *Let $p \in I$, $p \equiv 1 \pmod 3$ and let τ be an arbitrary root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$. Then,*

$$\tau^{\frac{p^2+p+1}{3}} = 1.$$

In proving the main results the following theorem is needed.

Theorem 3.26. *Let p be a prime, $p > 3$ and let $g(x) = x^3 + rx + s \in \mathbb{F}_p[x]$ with $r \neq 0$. Further let $d_g = r^3/27 + s^2/4$ and $\lambda \in \mathbb{F}_{p^2}$ such that $\lambda^2 = d_g$. Assume that $g(x)$ is irreducible over $\mathbb{F}_p$ or $g(x)$ has three distinct roots in $\mathbb{F}_p$. Then, the following statements are equivalent:*

(i) *$g(x)$ has three distinct roots in $\mathbb{F}_p$.*
(ii) *$g(x)$ has three distinct roots in $\mathbb{F}_{p^2}$.*
(iii) *$A = -s/2 - \lambda$ is a cubic residue of $\mathbb{F}_{p^2}$.*
(iv) *$B = -s/2 + \lambda$ is a cubic residue of $\mathbb{F}_{p^2}$.*

Note that Theorem 3.26 also holds in the case of $r = 0$ if we let $A = B = s$.

The following statement is due to John Andrew Vince [70, p. 310]. *Let $p \neq 2, 11$ be a prime. Then*

(i) *If $p \in L$, then $h(p)|p - 1$.*
(ii) *If $p \in Q$, then $h(p)|p^2 - 1$.*
(iii) *If $p \in I$, then $h(p)|p^2 + p + 1$.*

In Chapter 11, using the identity presented in Theorem 3.25, we strengthen Vince's result for $p \equiv 1 \pmod 3$ as follows:

Theorem 3.27. *Let p be an arbitrary prime, $p \equiv 1 \pmod 3$.*

(i) *If $p \in L$, then $h(p) | \frac{p-1}{3}$ if and only if 2 is a cubic residue of the field $\mathbb{F}_p$.*

(ii) *If $p \in Q$, then $h(p) | \frac{p^2-1}{3}$ if and only if 2 is a cubic residue of the field $\mathbb{F}_p$.*

(iii) *If $p \in I$, then $h(p) | \frac{p^2+p+1}{3}$.*

We also proved that part (iii) of Theorem 3.27 holds for any $h(p)[a, b, c]$. Some further extension to our theory studying the cubic character of Tribonacci roots is given in Chapter 12.

At the end of this section, note that the problems of modular periodicity of Fibonacci and Tribonacci sequences are parts of a more general theory of linear recurrence relations over finite fields. For this theory, see E. S. Selmer [57] and, for the theory of finite fields in general, consult [46, 51, 56].

4. Law of inertia for the factorization of cubic polynomials

A detailed study of the periods of Tribonacci sequences and their arithmetic properties points to the necessity of better understanding the problem of the factorization of cubic polynomials over the Galois fields $\mathbb{F}_p$ where p is a prime. In this section the main results related to our research of the factorization of monic cubic polynomials with integer coefficients having the same discriminant will be presented.

Let $D \in \mathbb{Z}$ and let

$$C_D = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = D\}$$

where $D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$ is the discriminant of $f(x)$. Put

$$V_1 = \{[u, v] \in \mathbb{Z}^2 : 4u^3 + 27v^2 = -D\} \text{ and } V_2 = \{[u, v] \in \mathbb{Z}^2 : 4u^3 + v^2 = -27D \text{ and } 3 \nmid u\}.$$

If $D \neq 0$, then V_1 and V_2 are finite sets and, by [35, p. 42], $V_1 \cap V_2 \neq \emptyset$ if and only if there exists $k \in \mathbb{Z}$ such that $3 \nmid k$ and $D = 7^2k^6$. Next, if $D \neq 0$, the sets V_1 and V_2 can be obtained by using the set of all integer solutions of Mordell's equation $y^2 = x^3 + k$ with $k = -432D$ [33, p. 313]. For theory of Mordell's equation see, for example, [50, 47, 16]. On the other hand, if $D = 0$, then V_1 and V_2 are infinite sets. This case is examined in detail in [36, pp. 107 – 108]. The sets V_1 and V_2 play an important role in our theory. As we see in Theorem 4.1, using V_1 and V_2, we can establish all polynomials in C_D. Before formulating Theorem 4.1, we recall one more important concept. For any $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$, we put $g_f(x) = f(x - a/3) = x^3 + rx + s \in \mathbb{Q}[x]$. Then, $r = b - a^2/3$, $s = 2a^3/27 - ab/3 + c$ and $D_{g_f} = D_f$. Sometimes the polynomial $g_f(x)$ will be called the reduced form of $f(x)$. Now we are ready to formulate the first important result of our theory.

Theorem 4.1. *Let $D \in \mathbb{Z}$ and let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.*

(i) *If $a \equiv 0 \pmod 3$, then $f(x) \in C_D$ if and only if there exist $[u, v] \in V_1$ and $w \in \mathbb{Z}$ such that*

$$a = 3w, \ b = 3w^2 + u, \ c = w^3 + uw + v.$$

(ii) *If $a \equiv e \pmod 3$ and $e \in \{1, 2\}$, then $f(x) \in C_D$ if and only if there exist $[u, v] \in V_2$, $w \in \mathbb{Z}$ such that $e^3 + 3eu + v \equiv 0 \pmod{27}$, and*

$$a = 3w + e, \ b = 3w^2 + 2ew + \frac{e^2 + u}{3}, c = w^3 + ew^2 + \frac{e^2 + u}{3}w + \frac{e^3 + 3eu + v}{27}.$$

Moreover, in (i), we have $g_f(x) = x^3 + ux + v$ and, in (ii), $g_f(x) = x^3 + (u/3)x + v/27$.

We show some example. Let $D = 5$. Then, Mordell's equation $Y^2 = X^3 - 2160$ has exactly six integer solutions $[X, Y] = [16, \pm 44], [24, \pm 108], [321, \pm 5751]$. Consequently, we have $V_1 = \{[-2, \pm 1]\}$ and $V_2 = \{[-4, \pm 11]\}$. Hence, using Theorem 4.1, we find that $f(x) \in C_5$ if and only if $f(x) = f_j(x, w)$ for some $j \in \{1, 2, 3, 4\}$ and $w \in \mathbb{Z}$ where

$$\begin{aligned}
f_1(x,w) &= x^3 + 3wx^2 + (3w^2 - 2)x + w^3 - 2w - 1,\\
f_2(x,w) &= x^3 + 3wx^2 + (3w^2 - 2)x + w^3 - 2w + 1,\\
f_3(x,w) &= x^3 + (3w+1)x^2 + (3w^2 + 2w - 1)x + w^3 + w^2 - w,\\
f_4(x,w) &= x^3 + (3w+2)x^2 + (3w^2 + 4w)x + w^3 + 2w^2 - 1.
\end{aligned}$$

Recall now that there exist five distinct types of factorization of $f(x)$ over the Galois field $\mathbb{F}_p$ where p is a prime. For these types, we adopted the notation found in M. Ward [77, p. 161]:

(i) $f(x)$ is of type $[1^3]$ if $f(x) = (x - \alpha)^3$ where $\alpha \in \mathbb{F}_p$.
(ii) $f(x)$ is of type $[1^2, 1]$ if $f(x) = (x - \alpha)^2 (x - \beta)$ where $\alpha, \beta \in \mathbb{F}_p$ and, $\alpha \neq \beta$.
(iii) $f(x)$ is of type $[1, 1, 1]$ if $f(x) = (x - \alpha)(x - \beta)(x - \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_p$ are distinct.
(iv) $f(x)$ is of type $[2, 1]$ if $f(x) = (x - \alpha)(x^2 + \beta x + \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_p$ and, $x^2 + \beta x + \gamma$ is irreducible over $\mathbb{F}_p$.
(v) $f(x)$ is of type $[3]$ if $f(x)$ is irreducible over $\mathbb{F}_p$ or, equivalently, $f(x)$ has no root in $\mathbb{F}_p$.

In Chapter 13, we thoroughly examined the set C_{-44} containing the well-known Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ and the following theorem was proved:

Theorem 4.2. *Let p be an arbitrary prime. Then, all polynomials in C_{-44} have the same type of factorization over the Galois field $\mathbb{F}_p$.*

Note, that the set C_{-44} has a nontrivial structure that can be described using Theorem 4.1 as follows:

$$C_{-44} = \bigcup_{j=1}^{8} \{t_j(x, w); w \in \mathbb{Z}\}$$

where $\{t_j(x, w); w \in \mathbb{Z}\}$, $j = 1, \cdots, 8$ are pairwise disjoint sets defined by

$$\begin{aligned}
t_1(x,w) &= x^3 + (3w+1)x^2 + (3w^2 + 2w + 1)x + w^3 + w^2 + w - 1,\\
t_2(x,w) &= x^3 + (3w+2)x^2 + (3w^2 + 4w + 2)x + w^3 + 2w^2 + 2w + 2,\\
t_3(x,w) &= x^3 + (3w+2)x^2 + (3w^2 + 4w)x + w^3 + 2w^2 - 2,\\
t_4(x,w) &= x^3 + (3w+1)x^2 + (3w^2 + 2w - 1)x + w^3 + w^2 - w + 1,\\
t_5(x,w) &= x^3 + (3w+2)x^2 + (3w^2 + 4w - 10)x + w^3 + 2w^2 - 10w - 22,\\
t_6(x,w) &= x^3 + (3w+1)x^2 + (3w^2 + 2w - 11)x + w^3 + w^2 - 11w + 11,\\
t_7(x,w) &= x^3 + (3w+1)x^2 + (3w^2 + 2w - 31281)x + w^3 + w^2 - 31281w - 2139919,\\
t_8(x,w) &= x^3 + (3w+2)x^2 + (3w^2 + 4w - 31280)x + w^3 + 2w^2 - 31280w + 2108638.
\end{aligned}$$

This surprising property of the set C_{-44} suggests a fundamental question [33, p. 318], namely, for which $D \in \mathbb{Z}$ the following theorem holds: *Let p be an arbitrary prime. Then, all polynomials in C_D have the same type of factorization over the Galois field $\mathbb{F}_p$*. In [35, p. 40], we called this property *the law inertia for the factorization in C_D*. Along the lines of papers [35, 36, 37, 38], the following implication has been proved:

Theorem 4.3. *Let $D \in \mathbb{Z}$ be square-free and let $3 \nmid h(-3D)$ where $h(-3D)$ is the class number of $\mathbb{Q}(\sqrt{-3D})$. Let p be an arbitrary prime. Then, all polynomials in C_D have the same type of factorization over $\mathbb{F}_p$.*

Clearly, for some $D \in \mathbb{Z}$, we have $C_D = \emptyset$. In this case, Theorem 4.3 holds trivially. On the other hand, Theorem 4.3 can be applied in many non-trivial cases. Consider, for example, C_{-31} and C_{-23}. Finally, it was proved by counterexamples that the inverse implication does not hold and that none of our assumptions, D is square-free and $3 \nmid h(-3D)$, can be omitted. In Chapter 14, we proved Theorem 4.3 for any prime $p > 3$ and any discriminant $D \in \mathbb{Z}$ satisfying the conditions

$$D < 0,\ D \text{ is square-free},\ 3 \nmid D,\ 3 \nmid h(-3D).$$

Next in Chapter 15, we extend our proof for any $p > 3$ and any $D \in \mathbb{Z}$ satisfying

$$D > 0,\ D \text{ is square-free},\ 3 \nmid D,\ 3 \nmid h(-3D).$$

Furthermore, in Chapter 16 we give the proof of Theorem 4.3 for any $p > 3$ and any $D \in \mathbb{Z}$ satisfying

$$D \text{ is square-free},\ 3 \nmid D,\ 3 \nmid h(-3D).$$

Finally in Chapter 17, we prove the validity of Theorem 4.3 also for primes 2 and 3.

In addition, in Chapter 17, some other statements related to the factorization of monic cubic polynomials over the fields $\mathbb{F}_2$ and $\mathbb{F}_3$ will be also established. Some of them are now listed as Proposition 4.4 and 4.5.

Proposition 4.4. *Let $D \in \mathbb{Z}$ be the discriminant of $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.*
(i) *$f(x)$ is of type $[1^3]$ or type $[1^2, 1]$ over $\mathbb{F}_2$ if and only if $D \equiv 0 \pmod 2$.*
(ii) *If $D \equiv 0 \pmod 2$, then $f(x)$ is of type $[1^3]$ if and only if $a \equiv b \equiv c \pmod 2$.*
(iii) *$f(x)$ is of type $[3]$ or type $[2, 1]$ over $\mathbb{F}_2$ if and only if $D \equiv 1 \pmod 2$.*
(iv) *If $D \equiv 1 \pmod 2$, then $f(x)$ is of type $[2, 1]$ if and only if $a \equiv b \not\equiv c \pmod 2$.*
(v) *If $D \equiv 0 \pmod 2$, then $D \equiv 0 \pmod 4$.*
(vi) *Let $D \in \mathbb{Z}$ be square-free and let $f(x), g(x) \in C_D$. Then, D is odd and the polynomials $f(x)$ and $g(x)$ have the same type of factorization over $\mathbb{F}_2$.*

Proposition 4.5. *Let $D \in \mathbb{Z}$ be the discriminant of $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.*
(i) *$f(x)$ is of type $[1^3]$ or type $[1^2, 1]$ over $\mathbb{F}_3$ if and only if $D \equiv 0 \pmod 3$.*
(ii) *If $D \equiv 0 \pmod 3$, then $f(x)$ is of type $[1^3]$ if and only if $a \equiv b \equiv 0 \pmod 3$.*
(iii) *If $f(x)$ is of type $[1^3]$ over $\mathbb{F}_3$, then $27|D$.*
(iv) *$f(x)$ is of type $[3]$ or type $[1, 1, 1]$ over $\mathbb{F}_3$ if and only if $D \equiv 1 \pmod 3$.*
(v) *If $D \equiv 1 \pmod 3$, then $f(x)$ is of type $[1, 1, 1]$ if and only if $c \equiv 0 \pmod 3$.*
(vi) *If $D \equiv 1 \pmod 3$ and $3 \nmid a$, then $f(x)$ is of type $[3]$ over $\mathbb{F}_3$.*
(vii) *$f(x)$ is of type $[2, 1]$ over $\mathbb{F}_3$ if and only if $D \equiv 2 \pmod 3$.*
(viii) *Let D be square-free, $D \not\equiv 1 \pmod 3$, and let $f(x), g(x) \in C_D$. Then, $f(x), g(x)$ have the same type of factorization over $\mathbb{F}_3$.*

Finally, we present one more surprising theorem proved in Chapters 15 and 16. With Theorem 4.6 we conclude this section.

Theorem 4.6. *Let $f(x) \in C_D$ and let D satisfy $D > 0$, D be square-free, and $3 \nmid h(-3D)$. Then, $f(x)$ has a rational integer root.*

In the last part of our comments, we summarize our work, briefly suggesting the future development of the studied subject.

5. Summary and expected development of the subject

The results presented in this work can be divided into four basic groups:

First, in Chapters 1 – 3, we deal with an interesting, not yet resolved number-theory problem on the Fibonacci sequence. In the literature, this problem is often referred to as Wall's conjecture or Wall-Sun-Sun prime conjecture. Chapters 1 – 3 are our contribution to this problem. In Chapter 1, we summarize all the previous main results related to this problem and describe their history. This survey is completed by an extensive list of bibliography.

Second, in Chapters 4 – 12 we solve a number of problems concerning the cubic generalization of Fibonacci numbers. These numbers are often called the Tribonacci numbers. In Chapters 4 – 7, the modular periodicity of Tribonacci numbers is examined in detail with many interesting results. Subsequently, the main theorems proved in Chapters 4 – 7 are applied to solving the combinatorial problem of Morgan Ward. In Chapter 8, the concept of the Tribonacci partition formula modulo m is introduced and Ward's problem for the Tribonacci case is completely resolved. In Chapters 9 – 12, some further properties of Tribonacci numbers are revealed and several previous results extended or strengthened. We also discover the remarkable properties of the cubic character of the Tribonacci roots and, subsequently, use them in the investigation of the periods of Tribonacci sequences. The table of the periods is also given.

Third, in Chapters 13 – 17 we deal with the basic questions about the factorization of monic cubic polynomials with integer coefficients having the same discriminant. The problems of the factorization is studied over the Galois fields $\mathbb{F}_p$ where p is a prime. Above all, we focused on the question concerning the validity of the law of inertia for the factorization of cubic polynomials. In spite of our results having quite an integrated form, new questions and problems arise.

Finally, an important part of this work is devoted to the practical applications of the number theory. In Chapters 18 – 20 we show a whole range of examples which describe natural situations where the number theory problems can arise. In more detail, we especially deal with applications of the Fibonacci numbers and with the use of sequences over finite fields. Some applications of Diophantine equations and the theory of partitions of positive integers into summands are also discussed. All the results presented in this work have already been published [20] – [40].

Now we attempt to describe the possible consequences of our work for further development of the branch. First, the historical survey in Chapter 1, together with the included bibliography, may be valuable for getting a better understanding of the subject and for further research. We also hope that our pessimistic opinion on the existence of Wall-Sun-Sun primes presented in [40, p. 49], will direct the attention of mathematicians to finding some comprehensive theory rather than to searching a counterexample on computer. Our alternative formulations of the problem can also be useful. In this sense, Chapters 1 – 3 can help to resolve Wall's problem.

We also hope that our results concerning the Tribonacci-Wieferich primes [24, 25] will attract the attention of other mathematicians who will continue our work and some new discoveries will soon be made. Next, our methodology described in Chapter 8, can easily be modified to find partition formulas in a general case. Hence, the use of our method by other authors can be presumably expected. Furthermore, the results deduced in Chapters 4 – 12 can stimulate an interest in the study of the modular periodicity of various generalizations of Fibonacci numbers. Moreover, our results evoke further relevant questions [24, p. 294].

Similarly, our theory [33, 35, 36, 37, 38] related to the law of inertia for the factorization of cubic polynomials over the Galois fields can be further developed and generalized. For example, we could ask under which conditions the law of inertia for the factorization of cubic polynomials holds in a Galois field $\mathbb{F}_q$ where q is a power of a prime. Another possible generalization is finding out whether this law also holds for polynomials of an order greater than three [36, p. 109]. Our work on this subject still continues and some new results have already been found [41].

Finally, our articles [27, 32, 34, 39] concerning the practical applications of the number theory can be an inspiration for a wide range of scientific and technician workers and stimulate a deeper interest in the field. This interest is the first step on the path that may change the results of the pure mathematics into a practical usable form.

Reference

[1] A. Agronomof, *Une série récurrente*, Mathesis **4** (1914), 125–126.

[2] Andreassian, A.: Fibonacci Sequences Modulo m, *Fibonacci Quarterly,* **12.1** (1974), 51–64.

[3] G. E. Andrews, *The Theory of Partitions*, Cambridge University Press (1998).

[4] F. C. Auluck, D. S. Kothari, *Statistical mechanics and the partitions of numbers*, Proc. Camb. Phil. Soc. **42** (1946), 272–277.

[5] J. C. A. Boeyens, D. C. Levendis, *Number Theory and the Periodicity of Matter*, Springer (2008).

[6] N. Bohr, F. Kalckar *On the transmutation of atomic nuclei by impact of material particles. I. General theoretical remarks*, Kgl. Danske Vid. Selskab. Math. Phys. Medd. **14.10** (1937), 1–40.

[7] Y. Bugeaud, M. Mignotte, S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Annals of Math. **163** (2006), 969–1018.

[8] P. Burrascano, M. Carpentieri, Pirani, M. Ricci, *Galois sequences in the non-destructive evaluation of metallic materials*, Meas. Sci. Technol. **17** (2006), 2973–2979.

[9] R. E. Crandall, K. Dilcher, C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433-449.

[10] L. Debnath, *Srinivasa Ramanujan (1887 – 1920) and the theory of partitions of numbers and statistical mechanics. A centennial tribute*, Internat. J. Math. and Mat. Sci. **10.4** (1987), 625–640.

[11] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York (1952).

[12] W. Diffie, M. E. Hellmann, *New directions in crypthigraphy*, IEEE Transaction on Information Theory **22.6** (1976), 644–654.

[13] R. A. Dunlap,*The Golden Ratio and Fibonacci numbers,* World Scientific, Singapore (1997).

[14] U. Eysholdt, C. E. Schreiner, *Maximum Length Sequences – A Fast Method for Measuring Brain–Stem–Evoked Responses*, Audiology **21** (1982), 242–250.

[15] M. Feinberg, *Fibonacci - Tribonacci*, The Fibonacci Quarterly **1.3** (1963), 70, 71–74.

[16] J. Gebel, A. Pethö, G. H. Zimmer, *On Mordell's equation*, Compositio Mathematica **110** (1998), 335–367.

[17] G. H. Hardy, S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. (2) **17** (1918), 75–115.

[18] G. H. Hardy, *A Mathematician's Apology*, Cambridge University Press (1940).

[19] A. F. Horadam *A generalized Fibonacci sequence*, Amer. Math. Monthly, **68** (1961), 455–459.

[20] J. Klaška, *Short remark on Fibonacci-Wieferich primes*, Acta Math. Univ. Ostrav. **15** (2007), 21–25.

[21] J. Klaška, *Criteria for testing Wall's question*, Czechoslovak Math. Journal, **58.4** (2008), 1241–1246.

[22] J. Klaška, *Tribonacci modulo p^t*, Math. Bohem. **133.3** (2008), 267–288.

[23] J. Klaška, *Tribonacci modulo 2^t and 11^t*, Math. Bohem. **133.4** (2008), 377–387.

[24] J. Klaška, *On Tribonacci-Wieferich primes*, The Fibonacci Quarterly **46/47** (2008/2009), 290–297.

[25] J. Klaška, *A search for Tribonacci-Wieferich primes*, Acta Math. Univ. Ostrav **16** (2008), 15–20.

[26] J. Klaška, *Further research of modular periodicity of Tribonacci sequence*, Univ. S. Boh. Dept. of Mathematics Report Series **16.1** (2008), 57–63.

[27] J. Klaška, *On the applications of ordered sets*, South Bohemia Mathematical Letters **17.1** (2009), 11–25.

[28] J. Klaška, *Tribonacci partition formulas modulo m*, Acta Mathematica Sinica, English Series, **26.3** (2010), 465–476.

[29] J. Klaška, L. Skula, *The cubic character of the Tribonacci roots*, The Fibonacci Quarterly **48.1** (2010), 21–28.

[30] J. Klaška, L. Skula, *Periods of the Tribonacci sequence modulo a prime* $p \equiv 1 (\mathrm{mod}\ 3)$, The Fibonacci Quarterly **48.3** (2010), 228–235.

[31] J. Klaška, L. Skula, *A note on the cubic characters of Tribonacci roots*, The Fibonacci Quarterly **48.4** (2010), 324–326.

[32] J. Klaška, *Applications of Fibonacci numbers and the golden ratio in physics, chemistry, biology and economy*, 7th Conference on Mathematics and Physics on Technical Universities, Brno (2011), 243–254.

[33] J. Klaška, L. Skula, *Mordell's equation and the Tribonacci family*, The Fibonacci Quarterly **49.4** (2011), 310–319.

[34] J. Klaška, *Applications of sequences over finite fields*, Mathematics Information Technologies and Applied Sciences, MITAV 2014, Brno (2014), p. 26.

[35] J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the real case*, Utilitas Mathematica, **102** (2017), 39–50.

[36] J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the imaginary case*, Utilitas Mathematica, **103** (2017), 99–109.

[37] J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the case of discriminants divisible by three*, Math. Slovaca **66.4** (2016), 1019–1027.

[38] J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the case of primes* 2 *and* 3, Math. Slovaca **67.1** (2017), 71–82.

[39] J. Klaška, *Real-world applications of number theory*, to appear in South Bohemia Mathematical Letters **25** (2017), 39–47.

[40] J. Klaška, *Donald Dines Wall's conjecture*, The Fibonacci Quarterly **56.1** (2018), 43–51.

[41] J. Klaška, L. Skula, *On the factorizations of cubic polynomials with the same discriminant modulo a prime*, to appear in Math. Slovaca **68** (2018).

[42] J. C. Kluyver, *Vraagstuk CXXXIX, CXL*, Wiskundige Opgaven **14** (1928), 278–281.

[43] J. Knauer, J. Richstein, *The continuing search for Wieferich primes*, Math. Comp. **74** (2005), 1559–1563.

[44] T. Koshy,*Fibonacci and Lucas Numbers with Applications,* Wiley, New York, (2001).

[45] J. L. Lagrange, *Oeuvres de LaGrange*, Vol. 7, §78-79, Gauthier Villars, Paris (1877).

[46] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, (1994).

[47] J. London, M. Finkelstein, *On Mordell's Equation* $y^2 - k = x^3$, Bowling Green, Ohio Bowling Green State University (1973).

[48] C. Van Lier, G. E. Uhlenbeck, *On the statistical calculation of the density of the energy levels of the nuclei*, Physica **4** (1937), 531–542.

[49] Y. V. Matiyasevich, *Hilbert's 10th Problem*, Cambridge, MIT Press (1993).

[50] L. J. Mordell,*The diophantine equation* $y^2 - k = x^3$, London Math. Soc. **13** (1913), 60–80.

[51] G. L. Mullen, C. Mummert, *Finite Fields and Applications*, American Mathematical Society, SML Volume **41**, (2007).

[52] W. Munk, *Acoustic monitoring of ocean gyres*, J. Fluid Mech. **173** (1986), 43–53.

[53] PrimeGrid, *Wall-Sun-Sun prime search*, `http://www.primegrid.com`

[54] R. L. Rivest, A. Shamir, L. M. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM **21** (1978), 120–126.

[55] D. W. Robinson, *The Fibonacci matrix modulo m*, The Fibonacci Quarterly **1.2** (1963), 29–36.

[56] S. Roman, *Field Theory*, Graduate Text in Mathematics **158**, Springer (2006).

[57] E. S. Selmer, *Linear Recurrence Relations over Finite Fields*, Department of Mathematics University of Bergen, Norway, (1966).

[58] M. R. Schroeder, *Number Theory in Science and Communication*, Springer, Berlin, (1997).
[59] M. R. Schroeder, *Sequences from Number Theory for Physics, Signal Processing, and Art*, Acoustical Physics, **49.1** (2003), 97–108.
[60] M. R. Schroeder, *Fractals, Chaos, Power Laws*, Dover Publications Inc., New York, (1992).
[61] I. I. Shapiro, *Fourth test of general relativity*, Physical Review Letters **13** (1964), 789–791.
[62] I. I. Shapiro, G. H. Pettengill, M. E. Ash, M. L. Stone, W. B. Smith, R. P. Ingalls, R. A. Brockelman, *Fourth test of general relativity: preliminary results*, Physical Review Letters **20** (1968), 1265–1269.
[63] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress (1897), 182–193.
[64] Zhi-Hong Sun, Zhi-Wei Sun, *Fibonacci Numbers and Fermat's Last Theorem*, Acta Arith. **60** (1992), 371–388.
[65] S. Täcklind, *Über die Periodiziät der Lösungen von Differenzenkongruenzen*, Ark. Math. Astr. Fys. **30A.22** (1944), 1–9.
[66] H. N. V. Temperley, *Statistical mechanics and the partition of numbers. I. The transition of liquid helium*, Proc. R. Soc. London, Series A **199** (1949), 361–375.
[67] S. Vajda,*Fibonacci and Lucas Numbers, and the Golden Section,* Horwood, Chichester (1989).
[68] J. Vinson, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence*, The Fibonacci Quarterly **1.2** (1963), 37–45.
[69] A. Vince, *The Fibonacci sequence modulo n*, The Fibonacci Quarterly **16.5** (1978), 403–407.
[70] A. Vince, *Period of a Linear Recurrence*, Acta Arith. **39** (1981), 303–311.
[71] N. N. Vorobiev, *Chisla Fibonacci,* Gosudarstv. Izdat. Tehn.-Teor. Lit., Moscow-Leningrad, (1951), (1th edition), *Fibonacci numbers,* Birkhäuser, (2002).
[72] G. F. Voronoï, *On integral algebraic numbers depending on a root of an irreducible equation of the third degree*, Master's dissertation 1894, (Russian).
[73] G. Voronoï, *Sur une propriété du discriminant des fonctions entirès*, Verhand. III. Internat. Math. Kongress, (1905), 186 – 189.
[74] M. E. Waddill, L. Sacks, *Another Generalized Fibonacci Sequence*, The Fibonacci Quarterly **5.3** (1967), 209–222.
[75] M. E. Waddill, *Some Properties of a Generalized Fibonacci Sequence Modulo m*, The Fibonacci Quarterly **16.4** (1978), 344–353.
[76] D. D. Wall, *Fibonacci Series Modulo m*, Amer. Math. Monthly **67.6** (1960), 525–532.
[77] M. Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. **33** (1931), 153–165.
[78] M. Ward, *An enumerative problem in the arithmetic of linear recurring series*, Trans. Amer. Math. Soc. **37** (1935), 435–440.
[79] F. J. MacWilliams, N. J. F. Sloane, *The Theory of Error–Correcting Codes*, North-Holland, Amsterdam, (1977).
[80] D. K. Wilson, D. W. Thomson, *Acoustic Tomographic Monitoring of the Atmospheric Surface Layer*, Atmos. Oceanic Technol. **11** (1994), 751–769.

CHAPTER 1

DONALD DINES WALL'S CONJECTURE★

Abstract. Wall's conjecture is an interesting, not yet resolved number-theory problem concerning a Fibonacci sequence. The problem took on a new significance after its connection was discovered with Fermat's Last Theorem. What follows is a summary of all important discoveries and known facts related to Wall's conjecture made over 56 years of its existence.

Dedicated to Ladislav Skula on the occasion of his 80th birthday.

1. Wall's question - state of problem

The Fibonacci sequence $(F_n)_{n=0}^{\infty}$ was introduced by Italian mathematician Leonardo Fibonacci (1175 – 1250) in 1202. It is defined recursively: $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. Fix a positive integer $m > 1$. It is well-known that, reducing $(F_n)_{n=0}^{\infty}$ modulo m and taking least positive residues, we obtain a sequence $(F_n \bmod m)_{n=0}^{\infty}$ which is periodic. The first related discovery concerning this property goes back to J. L. Lagrange [34, pp. 142–147]. See also Dickson's History [14, p. 393]. A positive integer $k(m)$ is called the period of Fibonacci sequence modulo m if it is the smallest positive integer for which $F_{k(m)} \equiv 0 \pmod{m}$ and $F_{k(m)+1} \equiv 1 \pmod{m}$. Various properties of $k(m)$ have been studied in great detail by many authors. For the basic properties of $k(m)$, see J. C. Kluyver [32], S. Täcklid [59], D. D. Wall [65], D. W. Robinson [49], and J. Vinson [61]. In 1928, J. C. Kluyver [32, p. 278] discovered that, if p is a prime, $p \equiv \pm 1 \pmod{10}$, then $k(p) | p - 1$. If $p \equiv \pm 3 \pmod{10}$, then $k(p) | 2(p+1)$ but $k(p) \nmid p + 1$. See also [65, p. 528]. In 1960, D. D. Wall [65, p. 527] proved that, if p is an arbitrary prime and $k(p) = k(p^s) \neq k(p^{s+1})$, then $k(p^t) = p^{t-s}k(p)$ for any positive integers $t \geq s$. Consequently, if $k(p^2) \neq k(p)$, then $k(p^t) = p^{t-1}k(p)$ for all t. Wall [65, p. 528] poses a question that has so far remained unanswered:

The most perplexing problem we have met in this study concerns the hypothesis $k(p^2) \neq k(p)$. We have run a test on a digital computer which shows that $k(p^2) \neq k(p)$ for all p up to $10,000$; however, we cannot yet prove that $k(p^2) = k(p)$ is impossible. The question is closely related to another one, "can a number x have the same order $\bmod\ p$ and $\bmod\ p^2$?", for which rare cases give an affirmative answer (e.g., $x = 3$, $p = 11$; $x = 2$, $p = 1093$); hence, one might conjecture that equality may hold for some exceptional p.

Note that the equality $k(m^2) = k(m)$ may be true if m is not a prime. For example, if $m = 12$, then $k(12^2) = k(12) = 24$, see [26, p. 347].

In 1997, R. E. Crandall, K. Dilcher and C. Pomerance [12] called primes p satisfying the equality $k(p^2) = k(p)$ the Wall-Sun-Sun primes. In the literature, these primes are

★ Published in J. Klaška, *Donald Dines Wall's Conjecture*, The Fibonacci Quarterly **56.1** (2018), 43–51.

also often referred to as Fibonacci-Wieferich primes. This name was first used in 2005 by J. Knauer and J. Richstein [33].

This paper aims to summarize all important discoveries concerning Wall's conjecture made in the period 1960–2016.

2. First partial answer of S. E. Mamangakis

In 1961, S. E. Mamangakis [39] furnished a proof of the hypothesis $k(p^2) \neq k(p)$ under the following assumptions: If p is an arbitrary prime and, for some n, $F_n = cp$ with $(c,p) = 1$, then $k(p^2) \neq k(p)$ [39, Theorem 1]. Next, if $(c,p) = 1$, $t \leq s$, and $F_j = cp^s$ is the first multiple of p to occur in $(F_n)_{n=0}^{\infty}$, then $k(p^t) = k(p)$ if and only if F_{j-1} has the same order modulo p and modulo p^t [39, Theorem 2]. Furthermore, in [39, p. 649], Mamangakis posed the question whether [39, Theorem 1] can be strengthened as follows: If c and p are relatively prime, then cp occurs in $(F_n)_{n=0}^{\infty}$ and $k(p^2) \neq k(p)$. The generalization of [39, Theorem 1] for sequences $(G_n)_{n=0}^{\infty}$ defined by $G_{n+2} = aG_{n+1} + bG_n$ with $G_0 = 0$, $G_1 = 1$ where a, b are integers is given by C. C. Yalavigi [73, p. 125]. Yalavigi also claims [72] that the answer to Mamangakis question is affirmative.

3. Rank of appearance and the Fibonacci quotient

In 1877, E. Lucas [35] discovered the following law of appearance of primes in the Fibonacci sequence: If p is a prime, $p \equiv \pm 1 \pmod{10}$, then $p|F_{p-1}$. If $p \equiv \pm 3 \pmod{10}$ then $p|F_{p+1}$. See also [14, p. 398]. Let (a/p) be the Legendere-Jacobi symbol. For $p \neq 2, 5$, using quadratic reciprocity law, we see that

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 5^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{10}. \end{cases}$$

Hence, for $p \neq 2$, we have $F_{p-(5/p)} \equiv 0 \pmod{p}$ and $F_{p-(5/p)}/p$ is a positive integer. Four different proofs of this fact have been given by G. H. Hardy and E. M. Wright [24], D. W. Robinson [49], J. H. Halton [22], and L. E. Sommer [55]. The number $F_{p-(5/p)}/p$ is called the Fibonacci quotient.

Next, a positive integer $z(m)$ is called the rank of appearance (or also the rank of apparition) of Fibonacci sequence modulo m if it is the smallest positive integer such that $F_{z(m)} \equiv 0 \pmod{m}$. As has been pointed out by P. Ribenboim [48, p. 45], the term *"apparition"* stems from a bad translation of the French *"loi d'apparition"*, which means "law of appearance", not "law of apparition". The number $z(m)$ is also often called Fibonacci entry point or restricted period in the literature. Many interesting properties of $z(m)$ are known [22, 61, 63]. For example, if p is an odd prime and $z(p^2) \neq z(p)$, then $z(p^t) = p^{t-1}z(p)$ for all positive integers t. Moreover, we have $z(p)|p - (5/p)$ for any odd prime p. See [22, p. 223] or [61, p. 43].

The relationship of rank of appearance $z(m)$ to the period $k(m)$ is also well-known. D. D. Wall [65, p. 526] showed that $z(m)|k(m)$ and J. Vinson [61, p. 39] proved that, if p is an odd prime and t any positive integer, then

$$\begin{aligned} k(p^t) &= 4z(p^t) \quad \text{if} \quad z(p^t) \not\equiv 0 \pmod{2}, \\ k(p^t) &= z(p^t) \quad \text{if} \quad z(p^t) \equiv 2 \pmod{4}, \\ k(p^t) &= 2z(p^t) \quad \text{if} \quad z(p^t) \equiv 0 \pmod{4}. \end{aligned}$$

Combining the above properties [23, pp. 347–348], it can be shown that the following statements (i)-(v) are equivalent:

$$\text{(i) } k(p^2) = k(p), \quad \text{(ii) } z(p^2) = z(p), \quad \text{(iii) } F_{z(p)} \equiv 0 \pmod{p^2},$$

$$\text{(iv) } F_{p-(5/p)} \equiv 0 \pmod{p^2}, \quad \text{and} \quad \text{(v) } F_{p-1}F_{p+1} \equiv 0 \pmod{p^2}.$$

Unfortunately, there is no known way to resolve $F_{p-(5/p)} \pmod{p^2}$, other than through explicit computations. A detailed study of the Fibonacci quotient $F_{p-(5/p)}/p$ has yielded the following results:

In 1969, G. H. Andrews [2] proved the following, rather complicated, formulas for the Fibonacci quotient: If $p \equiv \pm 1 \pmod 5$, then

$$\frac{F_{p-1}}{p} \equiv 2(-1)^{\frac{p-1}{2}} \sum_{\substack{|m|<p \\ m \equiv 5,7 \pmod{10}}} \frac{\binom{m+1}{5}\left(\frac{-1}{m}\right)}{p-m} \pmod p$$

and, if $p \equiv \pm 2 \pmod 5$, then

$$\frac{F_{p+1}}{p} \equiv 2(-1)^{\frac{p-1}{2}} \sum_{\substack{|m|<p \\ m \equiv 1,5 \pmod{10}}} \frac{\binom{m+1}{5}\left(\frac{-1}{m}\right)}{p-m} \pmod p.$$

In 1982, H. C. Williams [69] showed that, if $p \neq 2, 5$ is an arbitrary prime and $[p/5]$ denotes the greatest integer not exceeding $p/5$, then

$$\frac{F_{p-\left(\frac{5}{p}\right)}}{p} \equiv \frac{2}{5} \sum_{k=1}^{p-1-[p/5]} \frac{(-1)^k}{k} \pmod p.$$

In 1992, Z.-H. Sun and Z.-W. Sun [56, p. 381] proved for any $p \neq 2, 5$ the following simple and beautiful formula

$$\frac{F_{p-\left(\frac{5}{p}\right)}}{p} \equiv -2 \sum_{\substack{k=1 \\ k \equiv 2p \pmod 5}}^{p-1} \frac{1}{k} \equiv 2 \sum_{\substack{k=1 \\ 5 \mid p+k}}^{p-1} \frac{1}{k} \pmod p.$$

In 1996, A. Granville and Z.-W. Sun also discovered an interesting connection of Fibonacci quotient with Bernoulli numbers. See [20, p. 135].

4. Ward's Last Theorem

In 1640 P. de Fermat stated that, if p is any prime and a is any integer not divisible by p, then $a^p - 1$ is divisible by p. See [14, p. 59]. The quotient $q_p(a) = (a^{p-1} - 1)/p$ is called the Fermat quotient of p with base a. Let $\Phi_n(x) = x + x^2/2 + \cdots + x^n/n$, and let p be an arbitrary odd prime greater then 5. Then,

$$F_{z(p)} \equiv 0 \pmod{p^2} \quad \text{if and only if} \quad \Phi_{\frac{p-1}{2}}\left(\frac{5}{9}\right) \equiv 2q_p\left(\frac{3}{2}\right) \pmod p.$$

This statement is often called Ward's Last Theorem in honour of Morgan Ward (1901-1963). It was posed by the late brilliant mathematician in [66]. For a proof, see the paper by L. Carlitz [9] and, for an alternative proof, consult the papers by J. H. Halton [23] and J. E. Desmond [13]. Since $F_{z(p)} \equiv 0 \pmod{p^2}$ if and only if $k(p^2) = k(p)$, Ward yields a new equivalent condition to Wall's question.

5. Further discoveries related to Wall's conjecture

In 1975, A. J. Vince [62] stated the following problem. Prove or disprove: if $m^2|F_n$, then $m|n$. In 1976, D. E. Penney and C. Pomerance [44] showed that Vince's statement is the equivalent to Wall's conjecture that $k(p^2) \neq k(p)$ for all primes p.

In 1998, S. Jakubec [27, p. 376] discovered the following connection of Wall's conjecture to cyclotomic fields: Let q be an odd prime and let l, p be primes such that $p = 2l + 1$, $l \equiv 3 \pmod 4$ and $p \equiv -5 \pmod q$. Suppose that the order of q modulo l is $(l-1)/2$. If q divides the class number of the real cyclotomic field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, then q is a Wall-Sun-Sun prime.

In 1999, Hua–Chieh Li [36, p. 83] showed that, if p is an odd prime satisfying $(5/p) = 1$ and α is a solution to $x^2 - x - 1 \equiv 0 \pmod p$, then $k(p^2) = k(p)$ if and only if $2\alpha^{p+1} - \alpha^p - \alpha^2 - 1 \equiv 0 \pmod{p^2}$. Next, if $p > 2$, $(5/p) = -1$ and α is a solution $x^2 - x - 1 \equiv 0 \pmod p$ in the ring $\mathbb{Z}[(1 + \sqrt{5})/2]$ modulo p, then $k(p^2) = k(p)$ if and only if $2\alpha^{p^2+1} - \alpha^{p^2} - \alpha^2 - 1 \equiv 0 \pmod{p^2}$.

In 2006, V. Andrejič [1, p. 42] proved that, if $(L_n)_{n=0}^{\infty}$ is the Lucas sequence defined by $L_0 = 2$, $L_1 = 1$, and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$, then p is a Wall-Sun-Sun prime if and only if $L_p \equiv 1 \pmod{p^2}$. Next, by [1],

$$k(p^2) = k(p) \quad \text{if and only if} \quad \sum_{k=1}^{(p-1)/2} \frac{5^k - 1}{k} \equiv 0 \pmod p.$$

Furthermore, it is well known [49] that the Fibonacci numbers can be computed by taking powers of a matrix. Namely, if

$$F = \begin{bmatrix} F_0 & F_1 \\ F_1 & F_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \text{then} \quad F^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}.$$

Let $Q_p = (F^{k(p)} - I)/p$, where I is a 2×2 identity matrix. In 2008, J. Klaška [28] proved that $k(p^2) = k(p)$ if and only if $Q_p \equiv 0 \pmod{p^2}$. Moreover, if $p \neq 5$, then $Q_p \equiv 0 \pmod{p^2}$ if and only if $\det Q_p \equiv 0 \pmod{p^2}$. Let K_p be the splitting field of $f(x) = x^2 - x - 1$ over the field of p-adic numbers $\mathbb{Q}_p$ and let α, β be the roots of $f(x)$ in K_p. Denote by O_p the ring of integers of K_p and, for a unit $\varepsilon \in O_p$, denote by $\mathrm{ord}_{p^t}(\varepsilon)$, $t \in \mathbb{N}$ the least positive rational integer h such that $\varepsilon^h \equiv 1 \pmod{p^t}$. If $p \neq 5$, then, by [28, p. 1244], $k(p^t) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta))$ for any $t \in \mathbb{N}$ and we have $k(p^2) \neq k(p)$ if and only if $\mathrm{ord}_{p^2}(\alpha) \equiv 0 \pmod p$ and $\mathrm{ord}_{p^2}(\beta) \equiv 0 \pmod p$. Furthermore, by [28, p. 1245] we have: if $p \neq 5$, $u \in O_p$ and $f(u) \equiv 0 \pmod p$, then $k(p^2) = k(p)$ if and only if $u^{2q} - u^q - 1 \equiv 0 \pmod{p^2}$.

Some further results related to Wall's conjecture can be found in [18, p. 208], [25, p. 117], [37, p. 348] and [50, p. 82].

6. Wall's conjecture and Fibonacci perfect power problem

The following interesting statement is closely related to Wall's question: The only perfect powers in the Fibonacci sequence are $F_0 = 0$, $F_1 = F_2 = 1$, $F_6 = 8$ and, $F_{12} = 144$. By definition, F_n is a perfect power if there exist integers x, q such that $q > 1$ and $F_n = x^q$. The first attempt to prove the theorem was made by F. Buchanan [6] in 1964. Unfortunately, the proof presented in [6] was incorrect being later retracted by the author [7]. A mistake in Buchanan's proof consists in the false assumption that a formula $z(p^t) = p^{t-1}z(p)$ holds for an arbitrary prime p. In fact, we have

$z(p^t) = p^{t-1}z(p)$ only for p satisfying $z(p^2) \neq z(p)$. Hence, if $k(p^2) \neq k(p)$ for all primes p, then the only perfect powers in the Fibonacci sequence are $0, 1, 8$ and, 144. A complete solution of $F_n = x^q$ was given for $q = 2$ by J. H. E. Cohn [10, 11] and by O. Wyler [71], and for $q = 3$ by H. London and R. Finkelstein [38]. The solution for $q = 5$ was found by A. Pethö [45] and for $q = 5, 7, 11, 13, 17$ by McLaughlin [41]. In general, the statement that 0, 1, 8 and, 144 are the only positive perfect powers in the Fibonacci sequence was proved in 2006 by Y. Bugeaud, M. Mignotte and S. Siksek [8]. An extensive list of references concerning the Fibonacci perfect powers can be found in [1, 8, 45] and, for short historical surveys, see [8, pp. 973–975] or [1, pp. 38–39].

7. Wall's conjecture and Fermat Last Theorem

Around 1637 Pierre de Fermat (1601–1665) stated that the Diophantine equation $x^n + y^n = z^n$ has no integer solution when $n > 2$ and $x, y, z \neq 0$. This proposition is known as Fermat's Last Theorem. In a marginal note, Fermat claimed to have discovered a truly remarkable proof. However, all the greatest mathematicians tried to find such proof without success over 350 years. The first accepted proof of Fermat's Last Theorem was published in 1995 by A. Wiles and R. Taylor [58, 68]. An extensive history of this problem can be found, for example, in [47]. It is well known that a solution of Fermat's problem can be reduced to the case of $n = p$ being an odd prime. Traditionally, two cases are then considered: case one if $p \nmid xyz$ and case two otherwise.

A central role in the study of the first case of Fermat's Last Theorem is played by Fermat quotients [1] $q_p(a)$ and the congruence $q_p(a) \equiv 0 \pmod{p}$, which can be written equivalently as $a^{p-1} \equiv 1 \pmod{p^2}$. In 1909, A. Wieferich [63] proved that, if there exists a solution of Fermat's equation $x^p + y^p = z^p$ such that $p \nmid xyz$ where p is an odd prime, then $a^{p-1} \equiv 1 \pmod{p^2}$ holds for $a = 2$. This implication is known as the Wieferich criterion and the primes p satisfying $2^{p-1} \equiv 1 \pmod{p^2}$ are called Wieferich primes. At present, only two Wieferich primes are known: 1093 was found by W. Meissner in 1913 and 3511 was found by N. Beeger in 1922. The Wieferich's result has been extended by many authors. See, for example, [19, 42, 57, 60]. The last result due to J. Suzuki [57] stated that, if there exists a prime p satisfying $x^p + y^p = z^p$ where $p \nmid xyz$, then $a^{p-1} \equiv 1 \pmod{p^2}$ for any prime $a \leq 113$.

The two following results connecting the first case of Fermat's Last Theorem with Wall's conjecture are known. In 1972, G. Brückner [5] stated that, if $k(p^2) \neq k(p)$ for all primes p, then the Diophantine equation $\alpha^p + \beta^p + \gamma^p = 0$ has no solution in integers α, β, γ of $\mathbb{Q}(\sqrt{5})$ such that $(\gamma, p) = 1$ and $\alpha = a_1 + a_2\sqrt{5}$, $\beta = b_1 + b_2\sqrt{5}$ satisfy the condition $a_1b_2 - a_2b_1 \not\equiv 0 \pmod{p}$. Brückner also stated that γ^p may be replaced by $\varepsilon\gamma^p$, where ε is a unit in $\mathbb{Q}(\sqrt{5})$.

In 1992, Zhi-Hong Sun and Zhi-Wei Sun [56] proved that, if $k(p^2) \neq k(p)$ for all primes p, then $x^p + y^p = z^p$ has no integer solution with $p \nmid xyz$. Hence, the affirmative answer to Wall's question implies the first case of Fermat's Last Theorem.

8. A Computer Search for Fibonacci-Wieferich primes

In this section we recall the most important historical milestones in a computer search for Fibonacci-Wieferich primes. First, D. D. Wall [65] showed that $k(p^2) \neq k(p)$ for any prime $p < 10.000$. In [23] J. H. Halton claims that $k(p^2) \neq k(p)$ has been verified

[1] Note that the connection of the first case of Fermat's Last Theorem with the Fermat quotients has been extensively studied also by Ladislav Skula, a Czechoslovak mathematician. See [51, 52, 53, 54].

thanks to Wunderlich's computations for $p \leq 28.837$. D. E. Penney and C. Pomerance [44] inform us that $k(p^2) \neq k(p)$ for $p \leq 177.409$. In [16] L. A. G. Dresel verified that $k(p^2) \neq k(p)$ for $p < 10^6$. According to H. C. Williams [69, 70], $k(p) \neq k(p^2)$ for every prime $p < 10^9$. By P. L. Montgomery [43], there is no Fibonacci-Wieferich prime less then 2^{32}. From a search conducted by R. J. McIntosh [12, p. 447], we learn that there are no Fibonacci-Wieferich primes $p < 2 \times 10^{12}$. An extensive computer search by A.-S. Elsenhans and J. Jahnel [17] leads to an extension of the bound up to 10^{14}. According to a report by R. J. McIntosh and E. L. Roettger [40], $k(p^2) \neq k(p)$ for $p < 2 \times 10^{14}$. F. G. Dorais and D. Klyve [15] proved that there exists no Fibonacci-Wieferich prime $p < 9.7 \times 10^{14}$.

Next, in December 2011, a PrimeGrid project [46] was started searching for Fibonacci-Wieferich primes. In 2011-2016 PrimeGrid extended the search limit to 1.9×10^{17} without finding any such primes. Finally, note that some computational results have been verified retrospectively. For example in [4, p. 228] for $p < 100.000$ and in [3, p. 62] for $p < 10^8$. Our short historical survey is summarized in Table 1.

Year	Author	Search limit
1960	D. D. Wall	$p < 10.000$
1967	J. H. Halton	$p \leq 28.837$
1976	D. E. Penny, C. Pomerance	$p \leq 177.409$
1977	L. A. G. Dresel	$p < 10^6$
1982	H. C. Williams	$p < 10^9$
1993	P. L. Montgomery	$p < 4.294.967.296 = 2^{32}$
1997	R. J. McIntosh	$p < 2 \times 10^{12}$
2004	A.– S. Elsenhans, J. Jahnel	$p < 10^{14}$
2007	R. J. McIntosh, E. L. Roettger	$p < 2 \times 10^{14}$
2011	F. G. Dorais, D. Klyve	$p < 9.7 \times 10^{14}$
2012	PrimeGrid	$p < 6 \times 10^{15}$
2014	PrimeGrid	$p < 2.8 \times 10^{16}$
2015	PrimeGrid	$p < 1.2 \times 10^{17}$
2016	PrimeGrid	$p < 1.9 \times 10^{17}$

Table 1

The computer search for Fibonacci-Wieferich primes is also closely related to the following statistical considerations. By the heuristic argument [12, pp. 446–447] and [40, p. 2091] the number N of Fibonacci-Wieferich primes in an interval $[x, y]$ is expected to be

$$N = \sum_{x \leq p \leq y} \frac{1}{p} \approx \sum_{n=x}^{y} \frac{1}{n \ln n} \approx \int_x^y \frac{dt}{t \ln t} = \ln(\ln y) - \ln(\ln x).$$

On the other hand, using the arguments presented in [29, p. 23], we have

$$N = \sum_{x \le p \le y} \frac{1}{q}, \quad \text{where} \quad \begin{cases} q = p^2, & \text{if } p \equiv 3, 7 \pmod{10}, \\ q = p, & \text{if } p \equiv 1, 9 \pmod{10}. \end{cases}$$

The mild conflict of these two heuristics is reconciled by G. Grell and W. Peng [21].

9. Some analogical problems

Analogies to the equality $k(p^2) = k(p)$ have also been examined for other linear recurrence sequences. Let $K(m)$ be the period of $(G_n \bmod m)_{n=0}^{\infty}$ where $G_0 = 0$, $G_1 = 1$, and $G_{n+2} = aG_{n+1} + bG_n$ for all $n \ge 0$, i.e. $K(m)$ is the least positive integer satisfying $[G_{K(m)}, G_{K(m)+1}] \equiv [0, 1] (\bmod m)$. For example, if $[a, b] = [2, 1]$ we get the Pell sequence. In this case, all primes $p \le 10^8$ for which $K(p^2) = K(p)$ are 13, 31, and 1546463. See [70, p. 86]. In general, $K(p^t) = K(p)$ can also be true for $t > 2$. If $[a, b] = [5, 1]$, then $K(3^3) = K(3^2) = K(3) = 8$. Consult [64, p. 305].

Similarly, let us denote by $h(m)$ the period of $(T_n \bmod m)_{n=0}^{\infty}$ where $T_0 = T_1 = 0$, $T_2 = 1$, and $T_{n+3} = T_{n+2} + T_{n+1} + T_n$, i.e. $h(m)$ is the least positive integer satisfying $[T_{h(m)}, T_{h(m)+1}, T_{h(m)+2}] \equiv [0, 0, 1] (\bmod m)$. A prime p is called Tribonacci-Wieferich [30] if $h(p^2) = h(p)$. By J. Klaška [31, p. 19], no Tribonacci-Wieferich prime exists below 10^{11}. Up to the present, no instance of $h(p^2) = h(p)$ has been found and it is an open question whether $h(p^2) = h(p)$ never appears. Finally, some results for Tetranacci-Wieferich primes are also known [30, p. 296].

10. Concluding remark

The long failure to find Wall-Sun-Sun primes supports the original conjecture of Donald Dines Wall, namely, that $k(p^2) \ne k(p)$ holds for all primes p. Therefore, the attention of the mathematicians should focus on finding a proof of this conjecture rather than on searching for a counterexample. However, it is evident that, until the proof of Wall's conjecture is found, the computer search for Wall-Sun-Sun primes will continue.

References

[1] V. Andrejič, *On Fibonacci powers*, Univ. Beograd. Publ. Elektroteh. Fak. Ser. Math. **17** (2006), 38–44.
[2] G. H. Andrews, *Some formulae for the Fibonacci sequence with generalizations*, The Fibonacci Quarterly **7.2** (1969), 113–130.
[3] H. Aydin, R. Dikici, G. C. Smith, *Wall and Vinson revisited*, Applications of Fibonacci Numbers **5** (1993), 61–68.
[4] R. A. Bateman, E. A. Clark, M. L. Hancock, C. A. Reiter, *The period of convergents modulo m of reduced quadratic irrationals*, The Fibonacci Quarterly **29.3** (1991), 220–229.
[5] G. Brückner, *Die Fermatsche Vermutung über $Q(\sqrt{5})$ und die Fibonacci-Folge*, Math. Nachr. **52** (1972), 255–257.
[6] F. Buchanan, *N-th powers in the Fibonacci series*, Amer. Math. Monthly **71** (1964), 647–649.
[7] F. Buchanan, *Retraction of "N-th powers in the Fibonacci series"*, Amer. Math. Monthly **71** (1964), 1112.
[8] Y. Bugeaud, M. Mignotte, S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Annals of Math. **163** (2006), 969–1018.
[9] L. Carlitz, *Solution of advanced problem* H-24, The Fibonacci Quarterly **2.3** (1964), 205–207.
[10] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. **39** (1964), 537–540.
[11] J. H. E. Cohn, *Square Fibonacci numbers, etc.*, The Fibonacci Quarterly **2.2** (1964), 109–113.

[12] R. E. Crandall, K. Dilcher, C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433-449.

[13] J. E. Desmond, *On the equality of periods of different moduli in the Fibonacci sequence*, The Fibonacci Quarterly **16.1** (1978), 86–87, 96.

[14] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York (1952).

[15] F. G. Dorais, D. Klyve, *A Wieferich prime search up to* 6.7×10^{15}, Journal of Integer Sequences **14** (2011), Article 11.9.2.

[16] L. A. G. Dresel, *Letter to the editor*, The Fibonacci Quarterly **15.4** (1977), 346.

[17] A.-S. Elsenhans, J. Jahnel, *The Fibonacci sequence modulo* p^2 *- An investigation by computer for* $p < 10^{14}$, The On-Line Encyclopedia of Integer Sequences (2004), 27 p.

[18] Ch. Guo, A. Koch, *Bounds for Fibonacci period growht*, Involve **2.2** (2009), 195–210.

[19] A. Granville, M. B. Monagan, *The first case of Fermat's Last Theorem is true for all prime exponents up to* 714.591.416.091.389, Trans. Amer. Math. Soc. **306** (1988), 329–359.

[20] A. Granville, Z.-W. Sun, *Values of Bernoulli polynomials*, Pacific J. Math. **172** (1996), 117–137.

[21] G. Grell, W. Peng, *Wall's conjecture and the ABC conjecture*, arXiv:1511.01210v1 [math. NT], (2015).

[22] J. H. Halton, *On the divisibility properties of Fibonacci numbers*, The Fibonacci Quarterly, **4.3** (1966), 217–240.

[23] J. H. Halton, *Some properties associated with square Fibonacci numbers*, The Fibonacci Quarterly, **5.4** (1967), 347–355.

[24] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, (1960), 148–150, 221–223.

[25] J. J. Heed, *Wieferichs and the problem* $z(p^2) = z(p)$, The Fibonacci Quarterly, **22.2** (1984), 116–118.

[26] V. E. Hoggatt, C. Smith *Primitive periods of generalized Fibonacci sequences*, The Fibonacci Quarterly, **14.4** (1976), 343–347.

[27] S. Jakubec, *On divisibility of the class number* h^+ *of the real cyclotomic fields of prime degree* l, Math. Comp., **67** (1998), 369–398.

[28] J. Klaška, *Criteria for testing Wall's question*, Czechoslovak Math. Journal, **58.4** (2008), 1241–1246.

[29] J. Klaška, *Short remark on Fibonacci-Wieferich primes*, Acta Math. Univ. Ostrav. **15** (2007), 21–25.

[30] J. Klaška, *On Tribonacci-Wieferich primes*, The Fibonacci Quarterly **46/47** (2008/2009), 290–297.

[31] J. Klaška, *A search for Tribonacci-Wieferich primes*, Acta Math. Univ. Ostrav **16** (2008), 15–20.

[32] J. C. Kluyver, *Vraagstuk CXXXIX, CXL*, Wiskundige Opgaven **14** (1928), 278–281.

[33] J. Knauer, J. Richstein, *The continuing search for Wieferich primes*, Math. Comp. **74** (2005), 1559–1563.

[34] J. L. Lagrange, *Oeuvres de LaGrange*, Vol. 7, §78-79, Gauthier Villars, Paris (1877).

[35] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.

[36] Hua-Chieh Li, *Fibonacci primitive roots and Wall's question*, The Fibonacci Quarterly **37.1** (1999), 77–84.

[37] Hua-Chieh Li, *On second-order linear recurrence sequences: Wall and Wyler revisited*, The Fibonacci Quarterly **37.4** (1999), 342–349.

[38] H. London, R. Finkelstein, *On Fibonacci and Lucas numbers which are perfect powers*, The Fibonacci Quarterly **7.5** (1969), 476–481 & 487 (errata ibid 8.3 (1970), p. 248.

[39] S. E. Mamangakis, *Remarks on the Fibonacci series modulo m*, Amer. Math. Monthly **68** (1961), 648–649.

[40] R. J. McIntosh, E. L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp. **76** (2007), 2087–2094.

[41] J. McLaughlin, *Small prime powers in the Fibonacci sequence*, arXiv:math.NT/0110150v2, (2002).

[42] D. Mirimanoff, *Zum letzter Fermat'schen Theorem*, J. Reine Angew. Math. **139** (1911), 309–324.

[43] P. L. Montgomery, *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. **61** (1993), 361–363.

[44] D. E. Penny, C. Pomerance, *Solution to problem* E 2539, Amer. Math. Monthly **83** (1976), 742–743.

[45] A. Pethö, *Perfect powers in second order recurrences*, Topics in Classical Number Theory, **2** (Budapest 1981), 1217–1227.

[46] PrimeGrid, *Wall-Sun-Sun prime search*, `http://www.primegrid.com`

[47] P. Ribenboim, 13 *Lectures on Fermat's Last Theorem*, Springer-Verlag, New York (1979).

[48] P. Ribenboim, *The Little Book of Big Primes*, Springer-Verlag, New York (1991).

[49] D. W. Robinson, *The Fibonacci matrix modulo m*, The Fibonacci Quarterly **1.2** (1963), 29–36.

[50] A. Saha, C. S. Karthik, *A few equivalences of Wall-Sun-Sun prime conjecture*, International Journal of Mathematics & Applications **4.1** (2011), 77–86.

[51] L. Skula, *A remark on Mirimanoff polynomials*, Commentarii Math. Univ. Sancti Pauli (Tokyo) **31** (1982), 89–97.

[52] L. Skula, *On the Kummer's system of congruences*, Commentarii Math. Univ. Sancti Pauli (Tokyo) **35** (1986), 137–163.

[53] L. Skula, *Some consequences of the Kummer system of congruences*, Commentarii Math. Univ. Sancti Pauli (Tokyo) **39** (1990), 19–40.

[54] L. Skula, *Fermat's Last Theorem and the Fermat quotients*, Commentarii Math. Univ. Sancti Pauli (Tokyo) **41** (1992), 35–54.

[55] L. E. Somer, *The Fibonacci group and a new proof that* $F_{p-(5/p)} \equiv 0 \pmod{p}$, The Fibonacci Quarterly **10.4** (1972), 345–348, 354.

[56] Zhi-Hong Sun, Zhi-Wei Sun, *Fibonacci Numbers and Fermat's Last Theorem*, Acta Arith. **60** (1992), 371–388.

[57] J. Suzuki, *On the generalized Wieferich criteria*, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), 230–234.

[58] R. L. Taylor, A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.

[59] S. Täcklind, *Über die Periodiziät der Lösungen von Differenzenkongruenzen*, Ark. Math. Astr. Fys. **30A.22** (1944), 1–9.

[60] H. S. Vandiver, *Extension of the criteria of Wieferich and Mirimanoff in connection with Fermat's last theorem*, J. Reine Angew. Math. **144** (1914), 314–318.

[61] J. Vinson, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence*, The Fibonacci Quarterly **1.2** (1963), 37–45.

[62] A. Vince, *Problem* E 2539, Amer. Math. Monthly **82** (1975), p. 521.

[63] A. Vince, *The Fibonacci sequence modulo n*, The Fibonacci Quarterly **16.5** (1978), 403–407.

[64] A. Vince, *Period of a Linear Recurrence*, Acta Arith. **39** (1981), 303–311.

[65] D. D. Wall, *Fibonacci Series Modulo m*, Amer. Math. Monthly **67.6** (1960), 525–532.

[66] M. Ward, *Advanced problem* H-24, The Fibonacci Quarterly **1.4** (1963), 47.

[67] A. Wieferich, *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math. **136.6** (1909), 293–302.

[68] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

[69] H. C. Williams, *A note on the Fibonacci quotient* $F_{p-\varepsilon}/p$, Canad. Math. Bull. **25.3** (1982), 366–370.

[70] H. C. Williams, *The influence of computers in the development of number theory*, Comput. Math. Appl. **8** (1982), 75–93.

[71] O. Wyler, *Solution of advanced problem* 5080, Amer. Math. Monthly **71** (1964), 220–222.

[72] C. C. Yalavigi, *A note on remarks of S. E. Mamangakis*, Math. Stud. **34** (1966) 37.

[73] C. C. Yalavigi, *A conjecture of J. H. Halton*, Math. Education, Ser. A **4.4** (1970), 125–126.

Keywords: Fibonacci numbers, Wall's conjecture, Fibonacci-Wieferich primes, Wall-Sun-Sun primes, history

MSC 2010: 11B50, 11B39, 01A60, 97A30

CHAPTER 2

CRITERIA FOR TESTING WALL'S QUESTION*

Abstract. In this paper we find certain equivalent formulations of Wall's question and derive two interesting criteria that can be used to resolve this question for particular primes.

1. Introduction

In 1960, D. D. Wall published a well-known paper [6] concerning the modular periodicity of a Fibonacci sequence. In this paper an interesting problem was formulated, often referred to as Wall's question (see [6, p. 528]), which has remained unsolved up to the present. Let us outline this problem.

Let $(F_n)_{n=0}^{\infty}$ denote the Fibonacci sequence defined by $F_{n+2} = F_{n+1} + F_n$ with $F_0 = 0$, $F_1 = 1$. Let $m > 0$ be an arbitrary integer. Reducing F_n modulo m and taking the least nonnegative residues, we obtain the sequence $(F_n \bmod m)_{n=0}^{\infty}$, which is periodic. A positive integer $k(m)$ is called the period of the Fibonacci sequence modulo m if it is the smallest positive integer for which $F_{k(m)} \equiv 0 \pmod{m}$ and $F_{k(m)+1} \equiv 1 \pmod{m}$. For a fixed prime p, Wall proved that, if $k(p) = k(p^s) \neq k(p^{s+1})$, then $k(p^t) = p^{t-s}k(p)$ for $t \geq s > 0$. Wall asked whether $k(p) = k(p^2)$ is possible. This is still an open question.

In [6] Wall noted that for $p < 10^4$, a counterexample of $k(p) \neq k(p^2)$ does not exist. According to [7], $k(p) \neq k(p^2)$ for $p < 10^9$. Using extensive search by computer, in [2] this result was extended to $p < 10^{14}$. Finally, according to the last report from 2007 (see [4]) there exists no such prime $p < 2 \times 10^{14}$. Finding the answer to Wall's question can be extremely difficult. In 1992, Zhi-Hong Sun and Zhi-Wei Sun [5] showed that, if $p \nmid xyz$ and $x^p + y^p = z^p$, then $k(p) = k(p^2)$. Consequently, an affirmative answer to Wall's question implies the first case of Fermat's last theorem.

It is well known that $k(p) = k(p^2)$ if and only if $F_{p-(5|p)} \equiv 0 \pmod{p^2}$ where $(a|b)$ denotes the Legendere symbol of a and b. Crandal, Dilcher, and Pomerence [1] called primes $p > 5$ satisfying $F_{p-(5|p)} \equiv 0 \pmod{p^2}$ the Wall-Sun-Sun primes. These are sometimes called Fibonacci-Wieferich primes. See [4] for example. It has been conjectured that there are infinitely many Wall-Sun-Sun primes, but the conjecture remains unproven.

2. Wall's question and its equivalent formulations

It is well known that F_n can be computed by taking the powers of a matrix. Namely, if

* Published in J. Klaška, *Criteria for testing Wall's question*, Czechoslovak Math. Journal, **58.4** (2008), 1241–1246.

$$F = \begin{bmatrix} F_0 & F_1 \\ F_1 & F_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \text{ then } F^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}. \tag{2.1}$$

Consequently, $k(p)$ is the period of $(F_n \bmod p)_{n=0}^{\infty}$ if and only if $k(p)$ is the smallest positive integer k for which $F^k \equiv E (\bmod p)$ and $k(p^2)$ is the period of $(F_n \bmod p^2)_{n=0}^{\infty}$ if and only if $k(p^2)$ is the smallest positive integer l satisfying $F^l \equiv E \pmod{p^2}$, where E is the 2×2 identity matrix. For any prime p, let us now define the integer matrix $A_p = [a_{ij}]$ such that

$$A_p = \frac{1}{p}(F^{k(p)} - E). \tag{2.2}$$

From (2.1) it follows that

$$A_p = \begin{bmatrix} a_{11} & a_{21} \\ a_{21} & a_{11} + a_{21} \end{bmatrix}. \tag{2.3}$$

Lemma 2.1. *For any prime p we have $k(p) \neq k(p^2)$ if and only if $A_p \not\equiv 0 \pmod{p}$.*

Proof. This follows from (2.2). □

Lemma 2.2. *Let $p \neq 5$. Then $A_p \equiv 0 \pmod{p}$ if and only if $\det A_p \equiv 0 \pmod{p}$.*

Proof. Let $p \neq 2$. Put $k = k(p)$. From (2.2) and (2.3), it follows that

$$\det F^k = 1 + p(2a_{11} + a_{21}) + p^2 \det A_p \quad \text{where} \quad \det A_p = a_{11}^2 + a_{11}a_{21} - a_{21}^2. \tag{2.4}$$

Since $\det F = -1$, (2.4) implies $2a_{11} + a_{21} \equiv 0 \pmod{p}$ and $\det A_p \equiv -5a_{11}^2 \pmod{p}$. Consequently, we have $a_{11} \equiv 0 \pmod{p}$ if and only if $a_{21} \equiv 0 \pmod{p}$, and thus, $\det A_p \equiv 0 \pmod{p}$ implies $A_p \equiv 0 \pmod{p}$. The validity of the converse implication is evident. On the other hand, for $p = 2$, we can easily verify that $A_2 \not\equiv 0 \pmod{2}$ and $\det A_2 \not\equiv 0 \pmod{2}$. □

Remark 2.3. For $p = 5$, we have $A_5 \not\equiv 0 \pmod{5}$ and $\det A_5 \equiv 0 \pmod{5}$.

Our next considerations will take place in the following framework. Let L_p be the splitting field of the Fibonacci characteristic polynomial $f(x) = x^2 - x - 1$ over the field of p-adic numbers $\mathbb{Q}_p$ and α, β be the roots of $f(x)$ in L_p. Denote by O_p the ring of integers of L_p. Clearly $\alpha, \beta \in O_p$. Since the discriminant of $f(x)$ is equal to 5, it follows that, for $p \neq 5$, $L_p/\mathbb{Q}_p$ does not ramify and so the maximal ideal of O_p is generated by p. Moreover, if $L_p = \mathbb{Q}_p$, then $\alpha, \beta \in \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the ring of p-adic integers.

For a unit $\varepsilon \in O_p$ we denote by $\operatorname{ord}_{p^t}(\varepsilon)$ the least positive rational integer h such that $\varepsilon^h \equiv 1 \pmod{p^t}$. Since $\varepsilon^h \equiv 1 \pmod{p}$ implies $\varepsilon^{ph} \equiv 1 \pmod{p^2}$, we have

$$\text{either} \quad \operatorname{ord}_{p^2}(\varepsilon) = \operatorname{ord}_p(\varepsilon) \quad \text{or} \quad \operatorname{ord}_{p^2}(\varepsilon) = p \cdot \operatorname{ord}_p(\varepsilon) \tag{2.5}$$

Furthermore, it is not difficult to prove that if $p > 2$ and $\operatorname{ord}_p(\varepsilon) \neq \operatorname{ord}_{p^2}(\varepsilon)$, then for any $t \in \mathbb{N}$ we have $\operatorname{ord}_{p^t}(\varepsilon) = p^{t-1}\operatorname{ord}_p(\varepsilon)$. More generally, if $\varepsilon \neq \pm 1$ and $s \in \mathbb{N}$ is the largest integer such that $\operatorname{ord}_{p^s}(\varepsilon) = \operatorname{ord}_p(\varepsilon)$, then, for any $t \geq s$, we have $\operatorname{ord}_{p^t}(\varepsilon) = p^{t-s}\operatorname{ord}_p(\varepsilon)$.

Lemma 2.4. *Let $p \neq 5$. We have either $\operatorname{ord}_{p^t}(\alpha) = \operatorname{ord}_{p^t}(\beta)$ or $\operatorname{ord}_{p^t}(\alpha) = 2\operatorname{ord}_{p^t}(\beta)$ or $2\operatorname{ord}_{p^t}(\alpha) = \operatorname{ord}_{p^t}(\beta)$.*

Proof. From Viète's equation $\alpha\beta = -1$ in L_p it follows that $\alpha = \pm 1$ if and only if $\beta = \pm 1$. Hence, if $\alpha^r = 1$, then $\beta^r = \pm 1$, and consequently, $\beta^{2r} = 1$. This implies $\mathrm{ord}_{p^t}(\beta) \mid 2\mathrm{ord}_{p^t}(\alpha)$. By analogy, we can obtain $\mathrm{ord}_{p^t}(\alpha) \mid 2\mathrm{ord}_{p^t}(\beta)$. □

Corollary 2.5. *For any prime $p \neq 5$ we have*

$$\mathrm{ord}_{p^2}(\alpha) \equiv 0 \pmod p \quad \textit{if and only if} \quad \mathrm{ord}_{p^2}(\beta) \equiv 0 \pmod p. \tag{2.6}$$

Proof. This is a consequence of Lemma 2.4 if $p \neq 2$. For $p = 2$, the polynomial $f(x)$ is irreducible over $\mathbb{Q}_2$ and so $\mathrm{ord}_{2^t}(\alpha) = \mathrm{ord}_{2^t}(\beta)$. □

In Theorem 2.6 we generalize [3, Lemma 2.4] also to the case of $f(x)$ being irreducible over $\mathbb{Q}_p$.

Theorem 2.6. *Let $p \neq 5$. Then $k(p^t) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta))$ for any $t \in \mathbb{N}$.*

Proof. Over L_p we can write $F_n = A\alpha^n + B\beta^n$ for suitable $A, B \in L_p$. The coefficients A, B are uniquely determined by the equations $A + B = 0$ and $A\alpha + B\beta = 1$ over L_p. The determinant of the matrix of this system is equal to $\beta - \alpha$. As $\alpha \not\equiv \beta \pmod p$, the Cramer rule gives $A = -(\beta - \alpha)^{-1}$, $B = (\beta - \alpha)^{-1}$. Moreover, A, B are units in O_p. Let $k = k(p^t)$. Then $[A\alpha^k + B\beta^k, A\alpha^{k+1} + B\beta^{k+1}] \equiv [A + B, A\alpha + B\beta] \pmod{p^t}$. This system can be reduced to an equivalent form

$$\begin{bmatrix} 1 & 1 \\ \alpha & \beta \end{bmatrix} \begin{bmatrix} A(\alpha^k - 1) \\ B(\beta^k - 1) \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{p^t}. \tag{2.7}$$

As the determinant of the matrix in (2.7) is not divisible by p, (2.7) has only one solution

$$A(\alpha^k - 1) \equiv 0 \pmod{p^t}, \; B(\beta^k - 1) \equiv 0 \pmod{p^t}.$$

This implies $\alpha^k \equiv 1 \pmod{p^t}$ and $\beta^k \equiv 1 \pmod{p^t}$. Thus, we have $\mathrm{ord}_{p^t}(\alpha) | k$ and $\mathrm{ord}_{p^t}(\beta) | k$, which implies $\mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta)) | k$. As A, B are not divisible by p, the periods of the sequences $(A\alpha^n \bmod p^t)_{n=0}^{\infty}$ and $(B\beta^n \bmod p^t)_{n=0}^{\infty}$ are $\mathrm{ord}_{p^t}(\alpha)$ and $\mathrm{ord}_{p^t}(\beta)$. Consequently, the period k of $(A\alpha^n + B\beta^n \bmod p^t)_{n=0}^{\infty}$ divides $\mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta))$ and the theorem follows. □

Theorem 2.7. *Let $p \neq 5$. Then $k(p) \neq k(p^2)$ if and only if*

$$\mathrm{ord}_{p^2}(\alpha) \equiv 0 \pmod p \quad \textit{and} \quad \mathrm{ord}_{p^2}(\beta) \equiv 0 \pmod p. \tag{2.8}$$

Proof. It follows from (2.8) that $\mathrm{lcm}(\mathrm{ord}_{p^2}(\alpha), \mathrm{ord}_{p^2}(\beta)) \equiv 0 \pmod p$ and, by Theorem 2.6, we have $k(p^2) \equiv 0 \pmod p$. Using Theorem 2.6 for $t = 1$ and recalling that (p) is the maximal ideal of O_p, we have $k(p) \not\equiv 0 \pmod p$, which, together with $k(p^2) \equiv 0 \pmod p$, gives $k(p) \neq k(p^2)$.

Conversely, if $k(p) \neq k(p^2)$, then $k(p^2) = p \cdot k(p)$. From Theorem 2.6 it now follows that $\mathrm{lcm}(\mathrm{ord}_{p^2}(\alpha), \mathrm{ord}_{p^2}(\beta)) \equiv 0 \pmod p$. This implies that $\mathrm{ord}_{p^2}(\alpha) \equiv 0 \pmod p$ or $\mathrm{ord}_{p^2}(\beta) \equiv 0 \pmod p$, which together with (2.6) proves (2.8). □

Remark 2.8. If $p = 5$, then $k(p) \neq k(p^2)$ and $k(5^t) = 4 \cdot 5^t$ for any $t \in \mathbb{N}$. See [6].

Our results can be summarized in the following theorem.

Theorem 2.9. *Let $p \neq 5$ and let s be the number of roots α, β of $f(x)$ in O_p whose order modulo p^2 is divisible by p. Then there are the following possibilities:*

Case $s = 0$: $k(p) = k(p^2)$, or equivalently $A_p \equiv 0 \pmod p$.
Case $s = 1$: This case is impossible.
Case $s = 2$: $k(p) \neq k(p^2)$, or equivalently $\det A_p \not\equiv 0 \pmod p$.

Proof. By Theorem 2.6 we have that $s = 0$ if and only if $k(p) = k(p^2)$. Lemma 2.1 states that $k(p) = k(p^2)$ if and only if $A_p \equiv 0 \pmod{p}$, which is equivalent to $\det A_p \equiv 0 \pmod{p}$ by Lemma 2.2. By Corollary 2.5 we see that the case of $s = 1$ is impossible. The proof is complete. □

Our results reduce Wall's question to solving the following equivalent problem. Is there at least one root $\alpha \in O_p$ of $f(x)$ for which $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ or is this never possible?

Now we derive two interesting criteria that can be used, without computing the roots of $f(x)$ in O_p, to decide whether $k(p) = k(p^2)$ or not. Let $p \neq 5$. Put $q = |O_p/(p)|$. Then $q = p^t$ where $t = [L_p : \mathbb{Q}_p] \in \{1, 2\}$. If $f(x)$ is irreducible over $\mathbb{Q}_p$, then $O_p/(p)$ is a field with p^2 elements. If $f(x)$ is not irreducible over $\mathbb{Q}_p$, then $f(x)$ has both roots in the ring $\mathbb{Z}_p$ and $O_p/(p)$ is a field with p elements. For a proof of our criteria, we shall need the following lemma.

Lemma 2.10. *We have* $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ *if and only if* $\alpha^{q-1} \equiv 1 \pmod{p^2}$.

Proof. Put $s = \mathrm{ord}_{p^2}(\alpha)$. Clearly, $[O_p/(p^2)]^\times$ has $q(q-1)$ elements and so $s | q(q-1)$. Let $p \nmid s$. As $q = p^t$, we have $s | q-1$ and $\alpha^{q-1} \equiv 1 \pmod{p^2}$ follows. On the other hand, let $\alpha^{q-1} \equiv 1 \pmod{p^2}$. Then $s | q-1$. As $p \nmid q-1$, we have $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$. □

Theorem 2.11. *Let* $p \neq 5$, $u \in O_p$ *be such that* $f(u) \equiv 0 \pmod{p}$. *Then* $k(p) = k(p^2)$ *if and only if*

$$u^{2q} - u^q - 1 \equiv 0 \pmod{p^2} \tag{2.9}$$

or equivalently

$$f(u) + (u^q - u)f'(u) \equiv 0 \pmod{p^2} \tag{2.10}$$

where f' *is the derivative of the Fibonacci characteristic polynomial* f.

Proof. Let $u \in O_p$, $u^2 - u - 1 \equiv 0 \pmod{p}$. Then we have $u \equiv \alpha \pmod{p}$ or $u \equiv \beta \pmod{p}$. We can assume $u \equiv \alpha \pmod{p}$. Then $u^q \equiv \alpha^q \pmod{p^2}$. If $k(p) = k(p^2)$, then $u^q \equiv \alpha^q \equiv \alpha \pmod{p^2}$ and $u^{2q} - u^q - 1 \equiv \alpha^2 - \alpha - 1 = 0 \pmod{p^2}$.

On the other hand, assume $u^{2q} - u^q - 1 \equiv 0 \pmod{p^2}$. Let $u^q = \alpha + pv$. Then $(\alpha+pv)^2 - (\alpha+pv) - 1 \equiv pv(2\alpha-1) \equiv 0 \pmod{p^2}$. Now $p \neq 5$ implies $2\alpha - 1 \not\equiv 0 \pmod{p}$ and so $v \equiv 0 \pmod{p}$. Consequently, $u^q \equiv \alpha \pmod{p^2}$ and $\alpha^{q-1} \equiv u^{q(q-1)} \equiv 1 \pmod{p^2}$. This, together with Lemma 2.10, yields $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ and $k(p) = k(p^2)$ follows by Theorem 2.7 and Corollary 2.5.

Furthermore, let $u = \alpha + pw$. Then (2.10) is equivalent to

$$(\alpha^q - \alpha)(2\alpha + 2pw - 1) \equiv 0 \pmod{p^2}. \tag{2.11}$$

If $k(p) = k(p^2)$, then $\alpha^q \equiv \alpha \pmod{p^2}$ and (2.11) follows.

Conversely, assume (2.11). As $p \neq 5$, we have $2\alpha + 2pw - 1 \equiv 2u - 1 \equiv f'(\alpha) \not\equiv 0 \pmod{p}$. Consequently, (2.11) gives $\alpha^q - \alpha \equiv 0 \pmod{p^2}$. This, together with Lemma 2.10, implies $k(p) = k(p^2)$ as required. □

References

[1] R. Crandall, K. Dilcher, C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 443–449.

[2] A. - S. Elsenhans, J. Jahnel, *The Fibonacci sequence modulo p^2 - An investigation by computer for $p < 10^{14}$*, The On-Line Encyclopedia of Integer Sequences (2004), 27 p.

[3] Hua-Chieh Li, *Fibonacci primitive roots and Wall's question*, The Fibonacci Quarterly **37** (1999), 77–84.
[4] R. J. McIntosh, E. L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp. **76** (2007), 2087–2094.
[5] Z.-H. Sun, Z.-W. Sun, *Fibonacci Numbers and Fermat's Last Theorem*, Acta Arith. **60** (1992), 371–388.
[6] D. D. Wall, *Fibonacci Series Modulo m*, Amer. Math. Monthly **67** (1960), 525–532.
[7] H. C. Williams, *A Note on the Fibonacci Quotient* $F_{p-\varepsilon}/p$, Canad. Math. Bull. **25** (1982), 366-370.

Keywords: Fibonacci numbers, Wall's question, Wall-Sun-Sun prime, Fibonacci-Wieferich prime, modular periodicity, periodic sequence

MSC 2000: 11B50, 11B39, 11A07

CHAPTER 3

SHORT REMARK ON FIBONACCI-WIEFERICH PRIMES★

Abstract. This paper has been inspired by the endeavour of a large number of mathematicians to discover a Fibonacci-Wieferich prime. An exhaustive computer search has not been successful up to the present even though there exists a conjecture that there are infinitely many such primes. This conjecture is based on the assumption that the probability that a prime p is Fibonacci-Wieferich is equal to $1/p$. According to our computational results and some theoretical considerations, another form of probability can be assumed. This observation leads us to interesting consequences.

1. Introduction

A prime p is called a Fibonacci-Wieferich prime if

$$F_{p-(p/5)} \equiv 0 \pmod{p^2} \tag{1.1}$$

where F_n denotes the n-th Fibonacci number defined by $F_{n+2} = F_{n+1} + F_n$ with $F_0 = 0$, $F_1 = 1$, and (a/b) denotes the Legendere symbol of a and b. Fibonacci-Wieferich primes are mostly studied in relation to the first case of Fermat's last theorem. In 1992, Zhi-Hong Sun and Zhi-Wei Sun [8] showed that, if $p \nmid xyz$ and $x^p + y^p = z^p$, then (1.1) is valid. Fibonacci-Wieferich primes are sometimes referred to as Wall-Sun-Sun primes. See [1].

Reducing F_n modulo m, we obtain the sequence $(F_n \bmod m)_{n=1}^{\infty}$, which is periodic. A positive integer $k(m)$ is called the period of a Fibonacci sequence modulo m if it is the smallest positive integer for which $F_{k(m)} \equiv 0 \pmod{m}$ and $F_{k(m)+1} \equiv 1 \pmod{m}$. For a fixed prime p, D. D. Wall [9, Theorem 5] has proved that, if $k(p) = k(p^s) \neq k(p^{s+1})$, then $k(p^t) = p^{t-s}k(p)$ for $t \geq s$. Wall asked whether $k(p) = k(p^2)$ is always impossible. This is still an open question. It is well known (see e.g. [3]) that $k(p) = k(p^2)$ if and only if p satisfies (1.1). Consequently, no Fibonacci-Wieferich prime p is known. Fibonacci-Wieferich primes were studied by many authors. From an extensive list of references let us recall at least the papers [3], [4], [7] and [10]. The problem of finding Fibonacci-Wieferich primes is in close analogy to the problem of finding Wieferich primes. See [1]. In 2007, R. McIntosh and E. L. Roettger [6] showed that there is no Fibonacci-Wieferich prime p for $p < 2 \times 10^{14}$. On the other hand, by statistical considerations [1, p. 447], in an interval $[x, y]$, there are expected to be

$$\sum_{x \leq p \leq y} \frac{1}{p} \approx \ln(\ln y / \ln x) \tag{1.2}$$

★ Published in J. Klaška, *Short remark on Fibonacci-Wieferich primes*, Acta Math. Univ. Ostrav. **15** (2007), 21–25.

Fibonacci-Wieferich primes. By (1.2), this means that, in the interval $[2, 2 \times 10^{14}]$, we can expected about 3.86 Fibonacci-Wieferich primes. The results presented in this paper suggest that, for the number of Fibonacci-Wieferich primes in an interval $[x, y]$, a formula different from (1.2) is more likely to be valid. As we see, there exist two kinds of primes and, for each of these, the estimate is principally different.

2. Basic observations

Let L_p be the splitting field of the Fibonacci characteristic polynomial $f(x)$ over the field of p-adic numbers $\mathbb{Q}_p$ and α, β be the roots of $f(x)$ in L_p. Denote by O_p the ring of integers of L_p. As the discriminant of $f(x)$ is equal to 5, it follows that, for $p \neq 5$, $L_p/\mathbb{Q}_p$ does not ramify and so the maximal ideal of O_p is generated by p. Put $q = |O_p/(p)|$. Then $q = p^t$ where $t = [L_p : \mathbb{Q}_p] \in \{1, 2\}$. If $f(x)$ is irreducible over $\mathbb{Q}_p$, then $O_p/(p)$ is a field with p^2 elements and $O_p/(p^2)$ is a ring with p^4 elements. If $f(x)$ is not irreducible over $\mathbb{Q}_p$, then $O_p/(p)$ is a field with p elements and $O_p/(p^2)$ has p^2 elements. For a unit $\xi \in O_p$, we denote by $\mathrm{ord}_{p^t}(\xi)$ the least positive rational integer h such that $\xi^h \equiv 1 \pmod{p^t}$. Let us now recall some results derived in [5].

Lemma 2.1. *For any prime $p \neq 5$, we have*
(i) $k(p^t) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta))$ *for any* $t \in \mathbb{N}$.
(ii) $\mathrm{ord}_{p^t}(\alpha) = \mathrm{ord}_{p^t}(\beta)$ *or* $\mathrm{ord}_{p^t}(\alpha) = 2 \cdot \mathrm{ord}_{p^t}(\beta)$ *or* $2 \cdot \mathrm{ord}_{p^t}(\alpha) = \mathrm{ord}_{p^t}(\beta)$.
(iii) $k(p) \neq k(p^2)$ *if and only if* $\mathrm{ord}_{p^2}(\alpha) \equiv 0 \pmod{p}$ *and* $\mathrm{ord}_{p^2}(\beta) \equiv 0 \pmod{p}$.
(iv) $\mathrm{ord}_{p^2}(\alpha) \equiv 0 \pmod{p}$ *if and only if* $\mathrm{ord}_{p^2}(\beta) \equiv 0 \pmod{p}$.

From (iii) and (iv), it now follows that p is a Fibonacci-Wieferich prime if and only if

$$\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p} \quad \text{and} \quad \mathrm{ord}_{p^2}(\beta) \not\equiv 0 \pmod{p}. \tag{2.1}$$

Let I denote the set of all primes for which $f(x)$ is irreducible over $\mathbb{Q}_p$ and $I(x)$ be the number of all $p \in I$, $p \leq x$. Similarly, let L denote the set of all primes p for which $f(x)$ is factorized over $\mathbb{Q}_p$ into linear factors and $L(x)$ be the number of all $p \in L$, $p \leq x$. Clearly, $I \cap L = \emptyset$ and $I \cup L$ is the set of all primes. Hence, $I(x) + L(x) = \pi(x)$ where $\pi(x)$ is the number of all primes p not exceeding x.

The following beautiful characterization of the sets I and L is known. See [9, Theorems 6 and 7].

Lemma 2.2. *For the sets I and L, we have:*
(i) $p \in I$ *if and only if* $p = 2, 5$ *or* $p \equiv 3 \pmod{10}$ *or* $p \equiv 7 \pmod{10}$.
(ii) $p \in L$ *if and only if* $p \equiv 1 \pmod{10}$ *or* $p \equiv 9 \pmod{10}$.

Theorem 2.3. *Let $q = p^{[L_p:\mathbb{Q}_p]}$. Then, in the multiplicative group $[O_p/(p^2)]^\times$, there exist exactly $q-1$ elements ξ satisfying $\xi^{q-1} \equiv 1 \pmod{p^2}$.*

Proof. If $\varepsilon_1, \dots, \varepsilon_q$ is a complete residue system of $O_p/(p)$, then $\varepsilon_i + p\varepsilon_j$ where $i, j \in \{1, \dots, q\}$ is a complete residue system of $O_p/(p^2)$. Clearly, $\varepsilon_i + p\varepsilon_j$ is a unit in $O_p/(p^2)$ if and only if $\varepsilon_i \neq 0$. It follows that $[O_p/(p^2)]^\times$ has $(q-1)q$ elements. Consequently, $[O_p/(p^2)]^\times \cong G \times H$ where G is a group of order $q-1$ and H is a group of order q. For any $[u, v] \in G \times H$, we have $[u, v]^{q-1} = [1, v^{-1}]$. This implies that $[u, v]^{q-1} = [1, 1]$ if and only if $v = 1$ and u is arbitrary. As u can be chosen in $q-1$ ways, there exist exactly $q-1$ elements $\xi \in [O_p/(p^2)]^\times$ satisfying $\xi^{q-1} \equiv 1 \pmod{p^2}$. □

By Theorem 2.3, the number of $\xi \in [O_p/(p^2)]^\times$ satisfying $\xi^{p-1} \equiv 1 \pmod{p^2}$ strongly depends on the form of the factorization of $f(x)$ over $\mathbb{Q}_p$. Put $Q(p) = \{\xi \in [O_p/(p^2)]^\times; \xi^{q-1} \equiv 1 \pmod{p^2}\}$. Clearly, $Q(p)$ is a subgroup of order $q-1$ of $[O_p/(p^2)]^\times$. Let α, β be the roots of $f(x)$ in O_p and let α_2, β_2 be the images of α, β in $[O_p/(p^2)]^\times$. By (2.1), we have $\alpha_2 \in Q(p)$ if and only if $\beta_2 \in Q(p)$. Moreover, the Viéte equation $\alpha_2\beta_2 = -1$ implies that $\beta_2 = -\alpha_2^{-1}$ in $[O_p/(p^2)]^\times$.

Remark 2.4. In my opinion, the results of Theorem 2.3 rather indicate that the probability P of inclusion $\{\alpha_2, \beta_2\} \subseteq Q(p)$ is equal to

$$P = \begin{cases} 1/p^2, & \text{if } p \in I, \\ 1/p, & \text{if } p \in L. \end{cases} \tag{2.2}$$

For this reason, the sum in (1.2) should be replaced by

$$\sum_{x \le p \le y} \frac{1}{q}, \quad \text{where} \quad \begin{cases} q = p^2, & \text{if } p \in I, \\ q = p, & \text{if } p \in L. \end{cases} \tag{2.3}$$

Of course, one knows in advance which of the cases $\{\alpha_2, \beta_2\} \subseteq Q(p)$ and $\{\alpha_2, \beta_2\} \nsubseteq Q(p)$ will occur as the roots α_2, β_2 are uniquely determined for any prime p.

3. Statistical consequences

Let us now consider the series

$$R = \sum_{p \in I} \frac{1}{p^2} = \frac{1}{4} + \frac{1}{9} + \frac{1}{25} + \frac{1}{49} + \frac{1}{169} + \frac{1}{289} + \cdots \tag{3.1}$$

and

$$S = \sum_{p \in L} \frac{1}{p} = \frac{1}{11} + \frac{1}{19} + \frac{1}{29} + \frac{1}{31} + \frac{1}{41} + \frac{1}{59} + \cdots . \tag{3.2}$$

Since $\sum_{p \in I} \frac{1}{p^2} < \sum_p \frac{1}{p^2} = \zeta_p(2)$, we have

Lemma 3.1. *The series R converges.*

Remark 3.2. The convergence of $\zeta_p(2) = \sum_p \frac{1}{p^2}$ is logarithmic and therefore extremely slow. The estimate $\zeta_p(2) = 0.45224\cdots$ comes from Euler (1748). On the other hand, we have $0.42151\cdots < \sum_{p \in I}^{p<10} \frac{1}{p^2}$. Computing yields

$$R = \sum_{p \in I} \frac{1}{p^2} = 0.43648\cdots \tag{3.3}$$

which is a good match with $0.42151\cdots < \sum_{p \in I} \frac{1}{p^2} < 0.45224\cdots$.

The probability P of finding a Fibonacci-Wieferich prime ending with digits 3 or 7 will virtually not increase as the search set becomes larger. Consequently, the existence of a Fibonacci-Wieferich prime $p \in I$, $p > 2 \times 10^{14}$ is very improbable. As the following lemma is valid by Dirichlet's theorem on primes in arithmetic progression, for a prime that ends with 1 or 9, the situation is more optimistic.

Lemma 3.3. *The series S diverges.*

Remark 3.4. It is well known (see e.g. [2, p. 57]) that

$$\sum_{p\equiv l \pmod k}^{p\le x} \frac{1}{p} = \frac{1}{\phi(k)} \ln\ln x + A(k,l) + O((\ln x)^{-1}) \tag{3.4}$$

where ϕ is the Euler function. From (3.4) it follows that

$$\sum_{p\in L\cap[x,y]} \frac{1}{p} \approx \frac{1}{2}\sum_{p\in[x,y]} \frac{1}{p} \approx \frac{1}{2}\ln(\ln y/\ln x). \tag{3.5}$$

Moreover, for $I(x)$ and $L(x)$, we have

$$\lim_{x\to\infty} \frac{I(x)}{L(x)} = 1. \tag{3.6}$$

Put $S(x) = \sum_{p\in L}^{p\le x} \frac{1}{p}$. A certain idea of the above functions can be obtained from Table 1.

x	$I(x)$	$L(x)$	$\pi(x)$	$I(x) : L(x)$	$S(x)$
10^2	15	10	25	1.50000	0.30599
10^3	90	78	168	1.15384	0.49500
10^4	620	609	1229	1.01806	0.63822
10^5	4815	4777	9592	1.00795	0.74875
10^6	39288	39210	78498	1.00198	0.83970
10^7	332443	332136	664579	1.00092	0.91673
10^8	2880971	2880484	5761455	1.00016	0.98342

Table 1.

From the results derived, it seems to be worthwile to direct attention only to the primes ending with the digits 1 or 9. In this case, to decide whether p is a Fibonacci-Wieferich prime, we can use some of the criteria derived in [5, Theorem 2.11]. The main advantage of such criteria is that they do not involve calculating with Fibonacci numbers but rather with the solution of the congruence $f(x) \equiv 0 \pmod p$. We have

Theorem 3.5. *Let* $p \equiv 1 \pmod{10}$ *or* $p \equiv 9 \pmod{10}$. *Further, let a be any solution of* $f(x) \equiv 0 \pmod p$ *and let* f' *be a derivative of the Fibonacci characteristic polynomial* f. *Then the following statements are equivalent:*

(i) p *is Fibonacci - Wieferich prime,*
(ii) $a^{2p} - a^p - 1 \equiv 0 \pmod{p^2}$,
(iii) $f(a) + (a^p - a)f'(a) \equiv 0 \pmod{p^2}$.

Proof. If $p \equiv 1 \pmod{10}$ or $p \equiv 9 \pmod{10}$, then by Lemma 2.2, part (ii), we have $p \in L$ and $|O_p/(p)| = p$. The equivalence of (i), (ii), and (iii) is now a straightforward consequence of [5, Theorem 2.11]. □

Anyone searching for a Fibonacci-Wieferich prime using a computer is facing an immediate problem of completing the search of the interval $[2 \times 10^{14}, 10^{15}]$. By (3.4), theoretically, there should be about 0.02 Fibonacci-Wieferich primes within this interval ending with 1 or 9. In the following interval $[10^{15}, 10^{16}]$ then, there should be about

0.03 primes. Even though the odds are not much favourable, there is still hope that a Fibonacci-Wieferich prime will be discovered.

References

[1] R. Crandall, K. Dilcher, C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 443–449.

[2] H. Davenport, *Multiplicative Number Theory*, Springer-Verlag, New York, 3rd ed. (2000).

[3] A. - S. Elsenhans, J. Jahnel, *The Fibonacci sequence modulo p^2 - An investigation by computer for $p < 10^{14}$*, The On-Line Encyclopedia of Integer Sequences (2004), 27 p.

[4] Hua-Chieh Li, *Fibonacci primitive roots and Wall's question*, The Fibonacci Quarterly, **37** (1999), 77–84.

[5] J. Klaška, *Criteria for testing Wall's question*, Czechoslovak Math. Journal, **58.4** (2008), 1241–1246.

[6] R. J. McIntosh, E. L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp. **76** (2007), 2087–2094.

[7] L. Skula, *A note on some relations among special sums of reciprocals modulo p*, Math. Slovaca **58.1** (2008), 5–10.

[8] Zhi-Hong Sun, Zhi-Wei Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), 371–388.

[9] D. D. Wall, *Fibonacci Series Modulo m*, Amer. Math. Monthly **67.6** (1960), 525–532.

[10] H. C. Williams, *A Note on the Fibonacci Quotient $F_{p-\varepsilon}/p$*, Canad. Math. Bull. **25** (1982), 366–370.

Keywords: Fibonacci numbers, Wall's question, Wall-Sun-Sun prime, Fibonacci-Wieferich prime, modular periodicity, periodic sequence

MSC 2000: 11B50, 11B39, 11A07, 11Y99.

CHAPTER 4

TRIBONACCI MODULO p^t ⋆

Abstract. Our research was inspired by the relations between the primitive periods of sequences obtained by reducing Tribonacci sequence by a given prime modulus p and by its powers p^t, which were deduced by M. E. Waddill. In this paper we derive similar results for the case of a Tribonacci sequence that starts with an arbitrary triple of integers.

1. Introduction - known results

Let $(g_n)_{n=1}^{\infty}$ be a Tribonacci sequence $0, 0, 1, 1, 2, 4, 7, 13, 24, 44, 81, \dots$ defined by the recurrence $g_{n+3} = g_{n+2} + g_{n+1} + g_n$ and the triple $[0, 0, 1]$ of initial values. Further, let $(G_n)_{n=1}^{\infty}$ be the Tribonacci sequence, defined by an arbitrary triple of integers $[a, b, c]$. It is well known that the sequences $(g_n \bmod m)_{n=1}^{\infty}$ and $(G_n \bmod m)_{n=1}^{\infty}$ are periodical for an arbitrary modulus $m > 1$. We denote by $h(m)$ and $h(m)[a, b, c]$ the primitive periods of these sequences. In this paper we derive a relationship between the numbers $h(p)[a, b, c]$ and $h(p^t)[a, b, c]$ where p is an arbitrary prime, $p \neq 2, 11$ and $t \in \mathbb{N} = \{1, 2, 3, \dots\}$. The case of the primes $p = 2, 11$ is solved in [2]. It can be proved that, if L is the splitting field of the Tribonacci polynomial $g(x) = x^3 - x^2 - x - 1$ over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $p \neq 2, 11$ and α, β, γ are the roots of $g(x)$ in L, then $h(p) = \operatorname{lcm}(\operatorname{ord}_L(\alpha), \operatorname{ord}_L(\beta), \operatorname{ord}_L(\gamma))$ where the numbers $\operatorname{ord}_L(\alpha)$, $\operatorname{ord}_L(\beta)$, $\operatorname{ord}_L(\gamma)$ are the orders of α, β, γ in the multiplicative group of L and lcm is their least common multiple. See [5]. Let T be a Tribonacci matrix where

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad T^n = \begin{bmatrix} g_n & g_{n-1} + g_n & g_{n+1} \\ g_{n+1} & g_n + g_{n+1} & g_{n+2} \\ g_{n+2} & g_{n+1} + g_{n+2} & g_{n+3} \end{bmatrix} \quad \text{for } n > 1. \tag{1.1}$$

Clearly, for an arbitrary $n \in \mathbb{N}$ and an arbitrary modulus m, T^n assumes a unique form $T^n = B + mA$ where $A = [a_{ij}]$, $B = [b_{ij}]$ are integer matrices such that $0 \le b_{ij} \le m - 1$ and a_{ij} are nonnegative integers. Specifically, if $n = h(m)$, then $T^{h(m)} \equiv E \pmod{m}$ where E is the identity matrix. Thus, we can express $T^{h(m)}$ as $T^{h(m)} = E + mA$. We will use this fact in an alternative proof of Theorem 1.1 published by M. E. Waddill in 1978, see [6, p. 349]. The proof that we will submit is based on matrix algebra. Its modification can also be used for the general case of linear recurrences of order k. This particularly applies to the case of Fibonacci sequences. For a proof of this, see [7, p. 527].

Theorem 1.1. *Let p be an arbitrary prime and $h(p) \neq h(p^2)$. Then*

$$h(p^t) = p^{t-1} h(p) \tag{1.2}$$

for all $t \in \mathbb{N}$.

⋆ Published in J. Klaška, *Tribonacci modulo p^t*, Mathematica Bohemica **133.3** (2008), 267–288.

Proof. We can write matrix $T^{h(p^t)}$ as $T^{h(p^t)} = E + p^t A$. Using binomial expansion, we have

$$T^{ph(p^t)} = (E + p^t A)^p = \sum_{i=0}^{p} \binom{p}{i} E^{p-i}(p^t A)^i.$$

Passing from equality to congruence by the modulus p^{t+1}, we get

$$T^{ph(p^t)} \equiv E \pmod{p^{t+1}}.$$

Since $h(p^{t+1})$ is the primitive period, we have $h(p^{t+1})|ph(p^t)$. Next, it is obvious that $h(p^t)|h(p^{t+1})$, which means that exactly one of the following equations is true:

$$h(p^{t+1}) = h(p^t) \quad \text{or} \quad h(p^{t+1}) = ph(p^t). \tag{1.3}$$

Now we use induction by t. For $t = 1$ the assertion is evident and for $t = 2$ it follows from the assumption. Assuming that $h(p^t) = ph(p^{t-1}) = p^{t-1}h(p)$ holds for a number $t \geq 1$, we will prove this equation for $t + 1$. The induction assumption $h(p^{t-1}) \neq h(p^t)$ implies $T^{h(p^{t-1})} = E + p^{t-1}A$ where $p \nmid A$. Thus we have

$$T^{ph(p^{t-1})} = (E + p^{t-1}A)^p = \sum_{i=0}^{p} \binom{p}{i} E^{p-i}(p^{t-1}A)^i.$$

Hence $T^{h(p^t)} = T^{ph(p^{t-1})} \not\equiv E \pmod{p^{t+1}}$ and $h(p^t) \neq h(p^{t+1})$. Next, from (1.3) we have $h(p^{t+1}) = ph(p^t)$ and $h(p^{t+1}) = p^t h(p)$. □

Remark 1.2. The congruence $T^{ph(p^{t-1})} \equiv E + p^t A \pmod{p^{t+1}}$ does not hold for $p = 2, t = 2$. This fact, however, is irrelevant for the proof of 1.1. We omit the details.

Theorem 1.3. *Let $s \in \mathbb{N}$ satisfy $h(p) = h(p^2) = \cdots = h(p^s) \neq h(p^{s+1})$. Then, for an arbitrary $t \geq s$, we have $h(p^t) = p^{t-s}h(p)$.*

Proof. We proceed by analogy with 1.1. □

Problem 1.4. The question of whether the assumption $h(p) \neq h(p^2)$ is necessary or whether the equality $h(p) = h(p^2)$ never occurs is open. Up to the present, no instance has been found of $h(p) = h(p^2)$. Neither is it proved that such an equality can never hold. However, for sequences defined by a general linear recurrence of order three, the condition analogous to $h(p) \neq h(p^2)$ need not be satisfied. For example, if $(f_n)_{n=1}^{\infty}$ is a sequence defined by the recurrence $f_{n+3} = 2f_{n+2} - f_{n+1} + f_n$ and the triple of initial values $[0, 0, 1]$, then $(f_n \bmod 2)_{n=1}^{\infty}$ and $(f_n \bmod 4)_{n=1}^{\infty}$ have the same period equal to 7. A similar problem is also discussed in the case of a Fibonacci sequence $(F_n)_{n=1}^{\infty}$ defined by $F_{n+2} = F_{n+1} + F_n$ with $F_1 = 1$ and $F_2 = 1$. In [4], it is proved that, if $(F_n \bmod p)_{n=1}^{\infty}$ and $(F_n \bmod p^2)_{n=1}^{\infty}$ have distinct primitive periods for all primes p, then the first case of Fermat's last theorem holds. However, questions related to the validity of the equation $h(p) = h(p^2)$ are not investigated in this paper. In the sequel, we will always assume $h(p) \neq h(p^2)$.

2. Elementary Observations

The primary aim of this paper is to prove theorems similar to 1.1 for the case of a Tribonacci sequence beginning with an arbitrary triple $[a, b, c]$ of integers. Evidently, the relation $h(p^t)[a, b, c] = p^{t-1}h(p)[a, b, c]$ is generally not valid. We have, for instance, $h(p)[0, 0, 0] = h(p^t)[0, 0, 0] = 1$ for arbitrary p, t. Put $x_0 = [a, b, c]^\tau$ and $x_n = [G_{n+1}, G_{n+2}, G_{n+3}]^\tau$ where τ is the transposition. Then x_n can be expressed in terms of x_0 using the equation $x_n = T^n x_0$. If a Tribonacci sequence is determined by the triple $[0, 0, 1]$, then $h(m)$ is the smallest number h for which $T^h \equiv E(\text{mod } m)$. In the following example, we will show that, to an arbitrary triple $[a, b, c]$, this rule need not apply.

Example 2.1. Let $p=7$ and $x_0=[1,3,2]^\tau$. We can verify easily that $T^6 \not\equiv E(\text{mod } 7)$ while $T^6 x_0 \equiv x_0 \ (\text{mod } 7)$. Since the congruence $T^h x_0 \equiv x_0 \ (\text{mod } 7)$ holds for no $h < 6$, we have $h(7)[1, 3, 2] = 6$. Assuming results analogous to 1.1, one could expect that $h(7^2)[1, 3, 2] = 42$. However, $h(7^2)[1, 3, 2] = 336$.

The relationships between the numbers $h(p^t)[a, b, c]$ and $h(p)[a, b, c]$ clearly seem to be more complex and are worth closer study. First we will prove two simple but important lemmas.

Lemma 2.2. *Let p be an arbitrary prime. Then, for every $t \in \mathbb{N}$ and $1 \le i \le t$, we have*

$$h(p^t)[p^{t-i}a, p^{t-i}b, p^{t-i}c] = h(p^i)[a, b, c]. \tag{2.1}$$

Proof. (2.1) follows from the equality

$$(p^{t-i}G_n \text{ mod } p^t)_{n=1}^{\infty} = p^{t-i} \cdot (G_n \text{ mod } p^i)_{n=1}^{\infty}.$$

□

Using (2.1), the investigation of the periods for general triples $[a, b, c]$ can be reduced to the case with $[a, b, c] \not\equiv [0, 0, 0](\text{mod } p)$. Particularly, for $i = 1$, (2.1) yields $h(p^t)[p^{t-1}a, p^{t-1}b, p^{t-1}c] = h(p)[a, b, c]$.

Lemma 2.3. *Let p be an arbitrary prime. For every triple $[a, b, c]$ and every $s, t \in \mathbb{N}$ where $s \le t$, we have $h(p^s)[a, b, c] | h(p^t)[a, b, c]$. In particular, we have*

$$h(p)[a, b, c] | h(p^t)[a, b, c]. \tag{2.2}$$

Proof. Put $h = h(p^s)[a, b, c]$, $k = h(p^t)[a, b, c]$ and $x_0 = [a, b, c]^\tau$. Then, from $T^k x_0 \equiv x_0(\text{mod } p^t)$, it follows that $T^k x_0 \equiv x_0(\text{mod } p^s)$. This means that k is a period of the Tribonacci sequence beginning with the triple $[a, b, c]$ reduced by the modulus p^s. Since the primitive period divides an arbitrary period, we have $h|k$. □

Moreover, $T^{h(p^t)} \equiv E \ (\text{mod } p^t)$ implies $T^{h(p^t)} x_0 \equiv x_0 \ (\text{mod } p^t)$ for any $x_0 = [a, b, c]^\tau$ and $t \in \mathbb{N}$ and therefore $x_{h(p^t)} \equiv x_0 \ (\text{mod } p^t)$. Consequently, we have

$$h(p^t)[a, b, c] | h(p^t). \tag{2.3}$$

Lemma 2.3 together with (2.3) restricts the form of the numbers $h(p^t)[a, b, c]$. As we will see in the sequel, the relations between $h(p^t)[a, b, c]$ and $h(p)[a, b, c]$ also depend on the form of the factorization of the polynomial $g(x)$ over the field $\mathbb{F}_p$.

3. Irreducible case

In the investigation of primitive periods of Tribonacci sequences beginning with arbitrary triples $[a, b, c]$, the cubic form

$$D(a, b, c) = a^3 + 2b^3 + c^3 - 2abc + 2a^2b + 2ab^2 - 2bc^2 + a^2c - ac^2 \tag{3.1}$$

plays an important role. By means of $D(a, b, c)$, we can prove a theorem similar to 1.1 for the case of $g(x)$ being irreducible over $\mathbb{F}_p$. (3.1) was studied in other circumstances as well. See [1].

Theorem 3.1. *If a triple of initial values $[a, b, c]$ of a Tribonacci sequence $(G_n)_{n=1}^{\infty}$ satisfies $(D(a, b, c), m) = 1$, then $h(m)[a, b, c] = h(m)$.*

Proof. For $n \geq 1$, the sequences $(g_n)_{n=1}^{\infty}$ and $(G_n)_{n=1}^{\infty}$ satisfy

$$G_{n+3} = bg_{n+1} + (a + b)g_{n+2} + cg_{n+3}. \tag{3.2}$$

If we put $h(m)[a, b, c] = h$, we have $[G_{h+1}, G_{h+2}, G_{h+3}] \equiv [a, b, c] \pmod m$. By substituting into (3.2) and after some simplification, we get

$$\begin{bmatrix} c-b-a & b-a & a \\ a & c-b & b \\ b & a+b & c \end{bmatrix} \cdot \begin{bmatrix} g_{h+1} \\ g_{h+2} \\ g_{h+3} \end{bmatrix} \equiv \begin{bmatrix} a \\ b \\ c \end{bmatrix} \pmod m. \tag{3.3}$$

The system of congruences (3.3) can be further modified to the form

$$\begin{bmatrix} c-b-a & b-a & a \\ a & c-b & b \\ b & a+b & c \end{bmatrix} \cdot \begin{bmatrix} g_{h+1} \\ g_{h+2} \\ g_{h+3}-1 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod m, \tag{3.4}$$

where the determinant of the matrix of system (3.4) depends only on a, b, c and is equal to $D(a, b, c)$. System (3.4) has only one solution if and only if the numbers $D(a, b, c), m$ are coprime. In this case, we have $[g_{h+1}, g_{h+2}, g_{h+3}] \equiv [0, 0, 1] \pmod m$ and thus $h(m)|h$. Since also $h|h(m)$, $h = h(m)$ follows. □

Corollary 3.2. *Let $u_1 = [a, b, c]$, $u_2 = [b, c, a + b + c]$, $u_3 = [c, a + b + c, a + 2b + 2c]$. Then u_1, u_2, u_3 are linearly independent over $\mathbb{F}_p$ if and only if $D(a, b, c) \not\equiv 0 \pmod p$. Moreover, the linear independence of u_1, u_2, u_3 implies $h(p)[a, b, c] = h(p)$.*

Proof. By elementary column transformations, the matrix of system (3.4) can be converted to the form

$$M = \begin{bmatrix} a & b & c \\ b & c & a+b+c \\ c & a+b+c & a+2b+2c \end{bmatrix} \text{ where } \det M = -D(a, b, c).$$

Hence, it follows that the rows of M are linearly independent over $\mathbb{F}_p$ if and only if $D(a, b, c) \not\equiv 0 \pmod p$. Now, from 3.1 it follows that $h(p)[a, b, c] = h(p)$. □

Remark 3.3. Generally, the equality of periods $h(p)[a, b, c] = h(p)$ does not imply linear independence of u_1, u_2, u_3 over $\mathbb{F}_p$.

Lemma 3.4. *A triple $[a, b, c]$ satisfies the congruence $D(a, b, c) \equiv 0 \pmod p$ if and only if the sequence $(G_n \bmod p)_{n=1}^{\infty}$ determined by $[a, b, c]$ can be defined by a first or second order recurrence formula.*

Proof. If $D(a, b, c) \equiv 0 \pmod p$, then it follows from 3.2 that u_1, u_2, u_3 are linearly dependent. Let first u_1, u_2 be linearly dependent. Then there is a $q \in \mathbb{Z}$ such that

$$q[a, b, c] \equiv [b, c, a + b + c] \pmod p. \tag{3.5}$$

Matching the terms, we obtain $G_n \equiv aq^{n-1} \pmod p$ from (3.5) by induction, which means that $(G_n \bmod p)_{n=1}^{\infty}$ can be defined over $\mathbb{F}_p$ by the first order recurrence $G_{n+1} \equiv qG_n \pmod p$ where $G_1 = a$. Suppose that u_1, u_2 are independent and u_1, u_2, u_3 dependent. This means that there are $q_1, q_2 \in \mathbb{Z}$ such that

$$q_1[a, b, c] + q_2[b, c, a + b + c] \equiv [c, a + b + c, a + 2b + 2c] \pmod p. \tag{3.6}$$

By analogy, it follows from (3.6) that $(G_n \bmod p)_{n=1}^{\infty}$ can be defined over $\mathbb{F}_p$ by a recurrence $G_{n+2} \equiv q_1 G_n + q_2 G_{n+1} \pmod{p}$ where $G_1 = a, G_2 = b$.

Conversely, suppose that $(G_n \bmod p)_{n=1}^{\infty}$ can be defined by a recurrence of order at most two. This implies that u_1, u_2, u_3 are dependent over $\mathbb{F}_p$ and, by 3.2, we have $D(a,b,c) \equiv 0 \pmod{p}$. □

Remark 3.5. There are sequences $(G_n \bmod p)_{n=1}^{\infty}$ that can be defined over $\mathbb{F}_p$ by a recurrence formula of order at most two and $h(p)[a,b,c] = h(p)$.

Let us now investigate the number of all the solutions of the congruence

$$D(a,b,c) \equiv 0 \pmod{p}. \tag{3.7}$$

As we shall see in Lemmas 3.6 and 3.7, the number of solutions of (3.7) depends on the form of the factorization of $g(x) = x^3 - x^2 - x - 1$ over $\mathbb{F}_p$.

Lemma 3.6. *Let $g(x)$ be irreducible over $\mathbb{F}_p$. Then the only solution of* (3.7) *is* $[a,b,c] \equiv [0,0,0] \pmod{p}$.

Proof. Let L be the splitting field of $g(x)$ over $\mathbb{F}_p$. The irreducibility of $g(x)$ gives that $[L : \mathbb{F}_p] = 3$. The Galois group of $L/\mathbb{F}_p$ is generated by the Frobenius automorphism $\sigma : L \to L$ determined by $\sigma(t) = t^p$ for any $t \in L$. Let $\alpha \in L$ be a root of $g(x)$. Then $\beta = \sigma(\alpha)$ and $\gamma = \sigma(\beta)$ are the other roots of $g(x)$ and we have $\alpha^p = \beta$, $\beta^p = \gamma$, $\gamma^p = \alpha$. There are unique $A, B, C \in L$ such that

$$G_n \bmod p = A\alpha^n + B\beta^n + C\gamma^n \tag{3.8}$$

for each $n \in \mathbb{N}$. Moreover, $G_n \in \mathbb{Z}$, and so $A\alpha^n + B\beta^n + C\gamma^n = \sigma(A\alpha^n + B\beta^n + C\gamma^n)$ $= \sigma(A)\beta^n + \sigma(B)\gamma^n + \sigma(C)\alpha^n$, which gives

$$B = \sigma(A) = A^p, \quad C = \sigma(B) = B^p, \quad A = \sigma(C) = C^p. \tag{3.9}$$

It follows from (3.9) that A, B, C are either all non-zero or $A = B = C = 0$. Hence by (3.8), the sequence $(G_n \bmod p)_{n=1}^{\infty}$ cannot be, with the exception of the sequence beginning with $[0,0,0]$, defined by a recurrence formula of the first or second order. Lemma 3.6 now follows from 3.4. □

Lemma 3.7. *Let $g(x)$ be factorized over $\mathbb{F}_p$, $p \neq 2, 11$ into the product of a linear factor and an irreducible quadratic factor. Then* (3.7) *has exactly $p^2 + p - 1$ solutions. Let $g(x)$ be factorized over $\mathbb{F}_p$, $p \neq 2, 11$ into the product of linear factors. Then* (3.7) *has exactly $3p^2 - 3p + 1$ solutions.*

Proof. If $p \neq 2, 11$ then $g(x)$ has only simple roots in the splitting field L of $g(x)$ over $\mathbb{F}_p$, and so a Tribonacci sequence can be expressed in the form $G_n = c_1\alpha^n + c_2\beta^n + c_3\gamma^n$ where α, β, γ are the roots of $g(x)$ in L and $c_i \in L$. It is evident that $D(a,b,c) \equiv 0 \pmod{p}$ if and only if $c_i = 0$ for some $i = 1, 2, 3$. The assertion of the lemma can now be proved by a suitable use of the inclusion - exclusion principle. We leave the details to the reader. □

Corollary 3.8. *Let $p \neq 2, 11$. Then the number of all triples $[a,b,c]$ where $0 \leq a, b, c \leq p^t - 1$ such that $D(a,b,c) \not\equiv 0 \pmod{p}$ is equal to $p^{3(t-1)}(p^3 - 1)$ if $g(x)$ is irreducible over $\mathbb{F}_p$, $p^{3(t-1)}(p^3 - 3p^2 + 3p - 1)$ if $g(x)$ can be factorized over $\mathbb{F}_p$ into the product of linear factors, and $p^{3(t-1)}(p^3 - p^2 - p + 1)$ otherwise.*

Proof. Let $D(a_0, b_0, c_0) \not\equiv 0 \pmod p$ for $0 \le a_0, b_0, c_0 \le p-1$. Then also $D(a,b,c) \not\equiv 0 \pmod p$ for arbitrary $0 \le a,b,c \le p^t - 1$ such that $[a,b,c] \equiv [a_0, b_0, c_0] \pmod p$. The claim now follows from 3.6 and 3.7. □

Remark 3.9. The case of $g(x)$ having multiple roots over $\mathbb{F}_p$ leads to the investigation of the primes $p = 2, 11$ (see [2]). For $p = 2$, (3.7) has exactly 4 solutions and, for $p = 11$, it has exactly 231 solutions.

Theorem 3.10. *Let p be an arbitrary prime such that $g(x)$ is irreducible over $\mathbb{F}_p$. If $[a,b,c] \not\equiv [0,0,0] (\mathrm{mod}\ p)$ and $h(p) \neq h(p^2)$, then*

$$h(p^t)[a,b,c] = p^{t-1}\, h(p)[a,b,c] = p^{t-1} h(p) \tag{3.10}$$

for an arbitrary $t \in \mathbb{N}$.

Proof. The proof follows immediately from 1.1, 3.1 and 3.6. □

If $g(x)$ is not irreducible, it is easy to find examples of triples $[a,b,c]$ for which (3.7) holds and $h(p^t)[a,b,c] = h(p^t)$. Consequently, the form $D(a,b,c)$ cannot be expected to enable us to describe the relationships between the primitive periods if $g(x)$ has at least one root over $\mathbb{F}_p$.

4. The case of an irreducible quadratic factor

Let us now deal with the case of a Tribonacci polynom $g(x)$ having over $\mathbb{F}_p$ a factorization of the form

$$g(x) \equiv (x - \alpha_1)(x^2 - s_1 x - r_1) \pmod p, \tag{4.1}$$

where the polynomial $g_1(x) = x^2 - s_1 x - r_1$ is irreducible over $\mathbb{F}_p$. Since α_1 is a unique solution to $g(x) \equiv 0 \pmod p$, by Hensel's lemma there is a unique solution α_t to the congruence $g(x) \equiv 0 \pmod{p^t}$. Moreover, for α_t we have $\alpha_t \equiv \alpha_1 \pmod p$. This implies $(x - \alpha_t)|g(x)$ and there is a unique polynomial $g_t(x) = x^2 - s_t x - r_t \in \mathbb{Z}/p^t\mathbb{Z}[x]$ such that $g(x) \equiv (x - \alpha_t)(x^2 - s_t x - r_t) \pmod{p^t}$ where α_t, r_t, s_t are units of the ring $\mathbb{Z}/p^t\mathbb{Z}$ for which

$$s_t \equiv 1 - \alpha_t \pmod{p^t}, \quad r_t \equiv 1 + \alpha_t - \alpha_t^2 \pmod{p^t}. \tag{4.2}$$

Let us denote by $\mathrm{ord}_{p^t}(\alpha_t)$ the order of α_t in the group of units of the ring $\mathbb{Z}/p^t\mathbb{Z}$. Clearly, $\mathrm{ord}_{p^t}(\alpha_t) | p^{t-1}(p-1)$.

Lemma 4.1. *Let $(G_n)_{n=1}^{\infty}$ be the Tribonacci sequence determined by $[a, a\alpha_t, a\alpha_t^2]$. Then, for $(H_n)_{n=1}^{\infty}$ defined by $H_{n+1} = \alpha_t H_n$ and $H_1 = a$, we have $G_n \equiv H_n \pmod{p^t}$ for any $n \in \mathbb{N}$.*

Proof. Clearly, for $n = 1,2,3$, the claim holds. Let $n > 3$. Then $H_n = \alpha_t H_{n-1} \equiv \alpha_t^3 H_{n-3} \equiv (1 + \alpha_t + \alpha_t^2) H_{n-3} \equiv H_{n-3} + H_{n-2} + H_{n-1} \equiv G_n \pmod{p^t}$. □

Remark 4.2. Generally, the primitive period of a sequence $(a\alpha_t^n \bmod p^t)_{n=0}^{\infty}$ where $a \in \mathbb{N}$ does not depend only on the order of α_t in $\mathbb{Z}/p^t\mathbb{Z}$, but also on the coefficient a. If $p \nmid a$, then the primitive period of this sequence is equal to $\mathrm{ord}_{p^t}(\alpha_t)$. If $p^i || a$ where $0 \le i \le t-1$, then the primitive period equals $\mathrm{ord}_{p^{t-i}}(\alpha_{t-i})$.

Lemma 4.3. *Let $(G_n)_{n=1}^{\infty}$ be the Tribonacci sequence determined by $[a, b, r_t a + s_t b]$. Then for $(H_n)_{n=1}^{\infty}$ defined by $H_{n+2} = r_t H_n + s_t H_{n+1}$ with $H_1 = a$ and $H_2 = b$ we have $G_n \equiv H_n \pmod{p^t}$ for any $n \in \mathbb{N}$.*

Proof. For $n = 1, 2, 3$, the congruence $G_n \equiv H_n \pmod{p^t}$ holds. Let $n > 3$. Then

$$H_n \equiv r_t H_{n-2} + s_t H_{n-1} \equiv (r_t + s_t^2) H_{n-2} + r_t s_t H_{n-3} \pmod{p^t}. \quad (4.3)$$

The congruences (4.2) and $\alpha_t^3 \equiv \alpha_t^2 + \alpha_t + 1 \pmod{p^t}$ imply

$$r_t s_t \equiv 2 + \alpha_t - \alpha_t^2 \pmod{p^t}, \quad s_t^2 \equiv 1 - 2\alpha_t + \alpha_t^2 \pmod{p^t}. \quad (4.4)$$

By substituting (4.4) into (4.3) we obtain $H_n \equiv (2 - \alpha_t) H_{n-2} + (2 + \alpha_t - \alpha_t^2) H_{n-3} \equiv (1 + s_t) H_{n-2} + (1 + r_t) H_{n-3} \equiv H_{n-1} + H_{n-2} + H_{n-3} \equiv G_n \pmod{p^t}$. □

Remark 4.4. It is easy to find triples $[a, b, c]$ with $0 \leq a, b, c \leq p^t - 1$ and $t > 1$ such that $D(a, b, c) \equiv 0 \pmod{p^t}$ while $(G_n \bmod p^t)_{n=1}^{\infty}$ cannot be defined by a recurrence of order one or two. Thus, an analogue of Lemma 3.4 for the rings $\mathbb{Z}/p^t\mathbb{Z}$ cannot be proved. On the other hand, it is not difficult to prove that the sequences in 4.1 and 4.3 are the only ones that can be defined by lower order recurrences. In this case, of course, we have $D(a, b, c) \equiv 0 \pmod{p^t}$.

Theorem 4.5. *Let p be an arbitrary prime, $p \neq 2, 11$ and let $h = h(p) \neq h(p^2)$. Further, let $A = \frac{1}{p}(T^h - E)$. The system*

$$T^{p^{t-2}h} x \equiv x \pmod{p^t} \quad (4.5)$$

has $p^{3(t-1)}$ trivial solutions $[a, b, c] \equiv [0, 0, 0] \pmod{p}$. If $p \nmid \det A$ then (4.5) has no nontrivial solution. If $p | \det A$ then (4.5) has $(p-1)p^{3(t-1)}$ non-congruent nontrivial solutions.

Proof. From $h(p) \neq h(p^2)$ and 1.1 we can show by induction that, for an arbitrary $t > 1$, we have

$$T^{p^{t-2}h} \equiv E \pmod{p^{t-1}}, \quad T^{p^{t-2}h} \equiv E + p^{t-1} A \pmod{p^t} \quad (4.6)$$

and $p \nmid A$. By (4.6), the system (4.5) is equivalent to the system $(E + p^{t-1}A)x \equiv x \pmod{p^t}$ and thus to the system $Ax \equiv 0 \pmod{p}$. Clearly, this system has a unique solution $x \equiv 0 \pmod{p}$ if and only if $p \nmid \det A$. In this case, the solution of (4.5) is formed exactly by triples of the form $[a, b, c] \equiv [0, 0, 0] \pmod{p}$ and the number of non-congruent solutions of this form is equal to $p^{3(t-1)}$.

Let $A = [a_{ij}]$. It follows form (4.6) that $\det T^{p^{t-2}h}$ can be written as

$$\det T^{p^{t-2}h} \equiv 1 + p^{t-1}(a_{11} + a_{22} + a_{33}) + p^{2(t-1)} \sum_{i=1}^{3} \det A_i + p^{3(t-1)} \det A \pmod{p^t},$$

where A_i is a submatrix of A obtained by deleting the i-th row and i-th column in A. For $t > 1$, this implies

$$\det T^{p^{t-2}h} \equiv 1 + p^{t-1}(a_{11} + a_{22} + a_{33}) \pmod{p^t}. \quad (4.7)$$

Since $\det T = 1$, by the Cauchy theorem we have $\det T^n = 1$ for an arbitrary $n \in \mathbb{N}$. This yields $\det T^{p^{t-2}h} \equiv 1 \pmod{p^t}$. Combining this with (4.7), we get

$$a_{11} + a_{22} + a_{33} \equiv 0 \pmod{p}. \quad (4.8)$$

From (1.1) it follows that each of the entries of $A = [a_{ij}]$ reduced by modulus p can be expressed using only the three values a_{11}, a_{21}, a_{31} so that

$$A \equiv \begin{bmatrix} a_{11} & a_{31} - a_{21} & a_{21} \\ a_{21} & a_{11} + a_{21} & a_{31} \\ a_{31} & a_{21} + a_{31} & a_{11} + a_{21} + a_{31} \end{bmatrix} \pmod{p}. \tag{4.9}$$

Now it follows from (4.8) that

$$3a_{11} + 2a_{21} + a_{31} \equiv 0 \pmod{p}. \tag{4.10}$$

Using (4.10) we can simplify (4.9) to

$$A \equiv \begin{bmatrix} a_{11} & -3a_{11} - 3a_{21} & a_{21} \\ a_{21} & a_{11} + a_{21} & -3a_{11} - 2a_{21} \\ -3a_{11} - 2a_{21} & -3a_{11} - a_{21} & -2a_{11} - a_{21} \end{bmatrix} \pmod{p}. \tag{4.11}$$

Suppose that $p | \det A$. Then the rows of A are linearly dependent over $\mathbb{F}_p$. Suppose first that the first two rows of A are dependent. Then there is $q \in \mathbb{Z}$ such that

$$q[a_{11}, -3a_{11} - 3a_{21}, a_{21}] \equiv [a_{21}, a_{11} + a_{21}, -3a_{11} - 2a_{21}] \pmod{p}. \tag{4.12}$$

Matching the terms and using $p \nmid A$, we obtain

$$3q^2 + 4q + 1 \equiv 0 \pmod{p} \text{ and } \; q^2 + 2q + 3 \equiv 0 \pmod{p}. \tag{4.13}$$

It follows from (4.13) that $2q + 8 \equiv 0 \pmod{p}$. As $p \neq 2$, we have $q \equiv -4 \pmod{p}$. Substituting into the second congruence in (4.13) yields $11 \equiv 0 \pmod{p}$. Hence $p = 11$, and we get a contradiction.

Next suppose that the first two rows of A are independent and $p | \det A$. It follows from (4.11) and from $p \nmid A$ that at least one of the relations $p \nmid a_{11}$ and $p \nmid a_{21}$ is true. Suppose $p | a_{11}$ and $p \nmid a_{21}$. Then from (4.11) we have $\det A \equiv -14a_{21}^3 \pmod{p}$ and thus $14 \equiv 0 \pmod{p}$. As $p \neq 2$, we have $p = 7$. We can verify that $h(7) = 48$. Then for the corresponding matrix A we have

$$A \equiv \frac{1}{7}(T^{48} \text{mod } 7^2 - E) \equiv \begin{bmatrix} 4 & 2 & 0 \\ 0 & 4 & 2 \\ 2 & 2 & 6 \end{bmatrix} \pmod{7}.$$

Hence $a_{11} \equiv 4 \pmod{7}$, which is a contradiction with $p | a_{11}$. It follows now from the above that there is $\varepsilon \in \mathbb{Z}$ such that

$$a_{21} \equiv a_{11}\varepsilon \pmod{p}. \tag{4.14}$$

Substituting (4.14) into (4.11) then yields

$$\det A \equiv a_{11}^3(14\varepsilon^3 + 58\varepsilon^2 + 78\varepsilon + 38) \pmod{p}. \tag{4.15}$$

Since $p \nmid a_{11}$, $p \neq 2$ and $p | \det A$, it follows from (4.15) that

$$7\varepsilon^3 + 29\varepsilon^2 + 39\varepsilon + 19 \equiv 0 \pmod{p}. \tag{4.16}$$

The facts that $p | \det A$ and that the two rows of A are independent prove the existence of a linear combination of the first and second rows of A which can be used to eliminate the third row. Using (4.14), $Ax \equiv 0 \pmod{p}$ can now be reduced to

$$\begin{aligned} a \; - 3(1+\varepsilon)b + \quad \varepsilon c \quad &\equiv 0 \pmod{p}, \\ \varepsilon a + \; (1+\varepsilon)b \; - (3+2\varepsilon)c \; &\equiv 0 \pmod{p}. \end{aligned} \tag{4.17}$$

Substituting $a \equiv 3(1+\varepsilon)b - \varepsilon c$ into the second congruence of (4.17) we have $(3\varepsilon^2 + 4\varepsilon + 1)b \equiv (\varepsilon^2 + 2\varepsilon + 3)c$. Using (4.16) and $p \neq 2, 11$ it is easy to show that p divides neither $3\varepsilon^2 + 4\varepsilon + 1$ nor $\varepsilon^2 + 2\varepsilon + 3$. This means that every solution of (4.17) is congruent modulo p to a solution of the form

$$[q(5\varepsilon^2 + 14\varepsilon + 9), q(\varepsilon^2 + 2\varepsilon + 3), q(3\varepsilon^2 + 4\varepsilon + 1)], \text{ where } q \in \mathbb{Z}. \tag{4.18}$$

Thus, exactly $p - 1$ non-congruent solutions $[a, b, c]$ exists to system (4.17) that satisfy $[a, b, c] \not\equiv [0, 0, 0] \pmod{p}$ and therefore $(p - 1)p^{3(t-1)}$ noncongruent solutions satisfying $[a, b, c] \not\equiv [0, 0, 0] \pmod{p}$ exist to (4.5). □

For a $t \in \mathbb{N}$, denote by $\mathrm{S}_{p^t}(T)$ the set of roots of $g(x)$ in $\mathbb{Z}/p^t\mathbb{Z}$, i.e., the spectrum of the Tribonacci matrix T over $\mathbb{Z}/p^t\mathbb{Z}$. Next, for $\lambda \in \mathrm{S}_{p^t}(T)$ denote by $\mathrm{E}_{p^t}(\lambda) = \{[a, a\lambda, a\lambda^2], a \in \mathbb{Z}/p^t\mathbb{Z}\}$ the eigenspace corresponding to the eigenvalue λ. Specifically for this paragraph, due to Hensel's lemma, the spectrum T consists of a single element with $\mathrm{S}_{p^t}(T) = \{\alpha_t\}$. The elements of the spectrum $\mathrm{S}_{p^t}(T)$ play an important role in further considerations. Regarding their orders in the group of units of $\mathbb{Z}/p^t\mathbb{Z}$, the following lemma can easily be proved by modifying the proof of Theorem 1.1.

Lemma 4.6. *Let $p > 2$ be an arbitrary prime, $\lambda \in \mathbb{Z}$, $\lambda \neq \pm 1$ and $p \nmid \lambda$. If $\mathrm{ord}_p(\lambda) \neq \mathrm{ord}_{p^2}(\lambda)$, then, for any $t \in \mathbb{N}$,*

$$\mathrm{ord}_{p^t}(\lambda) = p^{t-1}\mathrm{ord}_p(\lambda). \tag{4.19}$$

More generally, if $s \in \mathbb{N}$ is the largest number such that $\mathrm{ord}_{p^s}(\lambda) = \mathrm{ord}_p(\lambda)$, then, for any $t \geq s$, $\mathrm{ord}_{p^t}(\lambda) = p^{t-s}\mathrm{ord}_p(\lambda)$.

Theorem 4.7. *Let p be an arbitrary prime, $p \neq 2, 11$ and $h = h(p) \neq h(p^2)$. The solution $[a, b, c]$ of the system $T^{p^{t-2}h}x \equiv x \pmod{p^t}$ for $t > 1$ satisfies $[a, b, c] \not\equiv [0, 0, 0] \pmod{p}$ if and only if $[a, b, c] \pmod{p} \in \mathrm{E}_p(\alpha_1)$ where $\alpha_1 \in \mathrm{S}_p(T)$.*

Proof. By 4.5 it is sufficient to prove that there exists a $q \in \mathbb{Z}$ such that $[q(5\varepsilon^2 + 14\varepsilon + 9), q(\varepsilon^2 + 2\varepsilon + 3), q(3\varepsilon^2 + 4\varepsilon + 1)] \equiv [1, \alpha_1, \alpha_1^2] \pmod{p}$, where $\alpha_1 \in \mathrm{S}_p(T)$. Using (4.16) and $p \neq 2, 11$, it is easy to show that $p \nmid 5\varepsilon^2 + 14\varepsilon + 9$. This implies $q = (5\varepsilon + 9)^{-1}(\varepsilon + 1)^{-1}$ and $\alpha_1 = (5\varepsilon + 9)^{-1}(\varepsilon + 1)^{-1}(\varepsilon^2 + 2\varepsilon + 3)$. Let us now prove that $\alpha_1^2 = q(3\varepsilon^2 + 4\varepsilon + 1)$. As $\alpha_1^2 = (5\varepsilon + 9)^{-2}(\varepsilon + 1)^{-2}(\varepsilon^2 + 2\varepsilon + 3)^2$, it is sufficient to prove that

$$(5\varepsilon + 9)^{-2}(\varepsilon + 1)^{-2}(\varepsilon^2 + 2\varepsilon + 3)^2 \equiv (5\varepsilon + 9)^{-1}(\varepsilon + 1)^{-1}(3\varepsilon^2 + 4\varepsilon + 1) \pmod{p}.$$

However, this congruence is equivalent to (4.16), which holds. What remains to be proved is that $\alpha_1 \in \mathrm{S}_p(T)$. Now α_1^3 can be expressed in terms of α_1 and α_1^2 to derive the congruence $(5\varepsilon + 9)^2(\varepsilon + 1)(\alpha_1^3 - \alpha_1^2 - \alpha_1 - 1) \equiv -6(7\varepsilon^3 + 29\varepsilon^2 + 39\varepsilon + 19) \pmod{p}$. Hence $\alpha_1^3 - \alpha_1^2 - \alpha_1 - 1 \equiv 0 \pmod{p}$ and thus $\alpha_1 \in \mathrm{S}_p(T)$. □

Let us denote by $\mathbb{Q}_p$ the field of p-adic numbers and by $\mathbb{Z}_p$ the ring of p-adic integers.

Theorem 4.8. *Let p be an arbitrary prime, $p \neq 2, 11$ and $h = h(p) \neq h(p^2)$. Further, let $g(x)$ be factorized over $\mathbb{F}_p$ into the product of a linear factor and an irreducible quadratic factor. Then $p | \det A$ if and only if $\mathrm{ord}_p(\alpha_2) = \mathrm{ord}_{p^2}(\alpha_2)$ where $\alpha_2 \in S_{p^2}(T)$.*

Proof. Let L_p be the splitting field of $g(x)$ over $\mathbb{Q}_p$ and let α, β, γ be the roots of $g(x)$ in L_p. Clearly, α, β, γ are in the ring O_p of integers of the field L_p. It follows from the form of the factorization of $g(x)$ over $\mathbb{F}_p$ that exactly one of the roots α, β, γ is in $\mathbb{Z}_p$. As the primes $p \neq 2, 11$ do not divide the discriminant $g(x)$, which is equal to -44, $L_p/\mathbb{Q}_p$ does not ramify and so the maximal ideal O_p is generated by p and α, β, γ are mutually different. Further, let $L = O_p/(p)$ be the residue field and $\alpha_1, \beta_1, \gamma_1$ be the images of α, β, γ in L. Over the field L_p the Tribonacci matrix T is similar to D, whose diagonal is formed by α, β, γ. Thus, there exists an invertible matrix H such that $T = HDH^{-1}$ and thus $T^h = HD^hH^{-1}$. Next, $h(p) \neq h(p^2)$ implies that $T^h = E + pA$ where $p \nmid A$. Thus, over L_p we have $E + pA = HD^hH^{-1}$, which yields $pH^{-1}AH = D^h - E$. By the Cauchy theorem and other known properties of determinants we obtain

$$p^3 \cdot \det A = (\alpha^h - 1)(\beta^h - 1)(\gamma^h - 1). \tag{4.20}$$

As $h = \operatorname{lcm}(\operatorname{ord}_L(\alpha_1), \operatorname{ord}_L(\beta_1), \operatorname{ord}_L(\gamma_1))$, we have $\alpha_1^h = 1, \beta_1^h = 1, \gamma_1^h = 1$, which implies that p divides each of the differences $\alpha^h - 1, \beta^h - 1, \gamma^h - 1$ in O_p. Now using $p|\det A$ and equality (4.20) we deduce that at least one of such differences is divisible by p^2. Suppose that $\alpha \in \mathbb{Z}_p$ and $p^2 \nmid \alpha^h - 1$. Then p^2 divides at least one of the differences $\beta^h - 1, \gamma^h - 1$. Assume, without loss of generality, that $p^2|\beta^h - 1$. Applying the Frobenius automorphism yields $p^2|\gamma^h - 1$. From this fact it follows that $p^2|\beta^h\gamma^h - 1$. Next, raising the Viète equation $\alpha\beta\gamma = 1$ to the h-th power in O_p yields $\alpha^h\beta^h\gamma^h = 1$. Since $p^2|\beta^h\gamma^h - 1$, we have $p^2|\alpha^h - 1$. Consequently, if $\alpha \in \mathbb{Z}_p$, then $p^2|\alpha^h - 1$. Let us now denote by α_2 the image of α in $O_p/(p^2)$. As $\alpha \in \mathbb{Z}_p$, we have that $\alpha_2 \in \mathbb{Z}/p^2\mathbb{Z}$, which means $\alpha_2 \in \mathrm{S}_{p^2}(T)$. It follows from $p^2|\alpha^h - 1$ in O_p that $p^2|\alpha_2^h - 1$ in $\mathbb{Z}/p^2\mathbb{Z}$ and so $\operatorname{ord}_{p^2}(\alpha_2)|h$. Next we prove that $\operatorname{ord}_p(\alpha_2) = \operatorname{ord}_{p^2}(\alpha_2)$. By 4.6, exactly one of the equations $\operatorname{ord}_{p^2}(\alpha_2) = p \cdot \operatorname{ord}_p(\alpha_2)$ and $\operatorname{ord}_{p^2}(\alpha_2) = \operatorname{ord}_p(\alpha_2)$ holds. Put $h_0 = \operatorname{ord}_p(\alpha_2)$ and suppose that $\operatorname{ord}_{p^2}(\alpha_2) = ph_0$. Then $ph_0|h$. However, this is not possible because $p \nmid h$ for $p \neq 2, 11$. In this case, $p \nmid h$ because of the fact that h divides the order of the multiplicative group of L, which is equal to $p^2 - 1$.

Conversely, suppose that $\operatorname{ord}_p(\alpha_2) = \operatorname{ord}_{p^2}(\alpha_2)$. Since $\alpha_1 \equiv \alpha_2 (\text{mod } p)$, we have $\operatorname{ord}_p(\alpha_1) = \operatorname{ord}_p(\alpha_2)$. Moreover, it is evident that $\operatorname{ord}_p(\alpha_1) = \operatorname{ord}_L(\alpha_1)$. Combining it with $\operatorname{ord}_p(\alpha_2) = \operatorname{ord}_{p^2}(\alpha_2)$ we find that $\operatorname{ord}_{p^2}(\alpha_2) = \operatorname{ord}_L(\alpha_1)$. Therefore from $h = \operatorname{lcm}(\operatorname{ord}_L(\alpha_1), \operatorname{ord}_L(\beta_1), \operatorname{ord}_L(\gamma_1))$ it follows that $\operatorname{ord}_{p^2}(\alpha_2)|h$. Thus $p^2|\alpha_2^h - 1$ in $O_p/(p^2)$ and $p^2|\alpha^h - 1$ in O_p. Next, $h = \operatorname{lcm}(\operatorname{ord}_L(\alpha_1), \operatorname{ord}_L(\beta_1), \operatorname{ord}_L(\gamma_1))$ yields that $p|\beta^h - 1$ and $p|\gamma^h - 1$ in O_p. Combining $p^2|\alpha^2 - 1$, $p|\beta^h - 1$, $p|\gamma^h - 1$ with (4.20) we get $p|\det A$, as required. □

Lemma 4.9. *Let $g(x)$ be factorized over $\mathbb{F}_p$, into the product of a linear factor and an irreducible quadratic factor. If $h(p) = h(p^2)$ then* $\operatorname{ord}_p(\alpha_2) = \operatorname{ord}_{p^2}(\alpha_2)$.

Proof. Put $h_0 = \operatorname{ord}_p(\alpha_2)$ and suppose that $\operatorname{ord}_p(\alpha_2) \neq \operatorname{ord}_{p^2}(\alpha_2)$. Then, by 4.6, we have $\operatorname{ord}_{p^2}(\alpha_2) = ph_0$. Consider now any triple of the form $[a, a\alpha_2, a\alpha_2^2]$ where $p \nmid a$. Obviously, $h(p^2)[a, a\alpha_2, a\alpha_2^2] = ph_0$ and, by (2.3), $ph_0|h(p^2)$. Hence, using the hypothesis $h(p) = h(p^2)$, we deduce that $p|h(p)$. However, this is not possible as $(h(p), p) = 1$. □

Problem 4.10. No prime p and $\lambda \in \mathrm{S}_{p^t}(T)$ where $t > 1$ are known such that (4.19) does not hold. Neither is there a proof of (4.19) holding for any $\lambda \in \mathrm{S}_{p^t}(T)$. However, 4.8 implies that (4.19) is not a consequence of $h(p) \neq h(p^2)$. It may be extremely difficult either to prove that (4.19) is generally true or find a counter-example. This means that we cannot even show a prime $p \neq 2, 11$ for which the system $Ax \equiv 0 \pmod p$ has a non-trivial solution. For $p = 2, 11$, however, $p|\det A$ and $Ax \equiv 0 \pmod p$ does have a non-trivial solution. Unfortunately, not even for $p = 2, 11$ there is a counter-example to

(4.19). In the remaining part of this paper we shall no longer deal with issues whether (4.19) holds in general and, when formulating assertions, we will assume that (4.19) is true for any $\lambda \in \mathrm{S}_{p^t}(T)$.

Theorem 4.11. *Let $g(x)$ be factorized over $\mathbb{F}_p$ as in* (4.1) *and let, for any $t \in \mathbb{N}$, $S_{p^t}(T) = \{\alpha_t\}$. Further, let $h_0 = \mathrm{ord}_p(\alpha_t)$. Then $h(p^t)[a,b,c] | p^{t-1}h_0$ if and only if $[a,b,c] \pmod{p^t} \in E_{p^t}(\alpha_t)$. Moreover, for $t > 1$, $h(p^t)[a,b,c] = p^{t-1}h_0$ if and only if $[a,b,c] \pmod{p^t} \in E_{p^t}(\alpha_t)$, $[a,b,c] \not\equiv [0,0,0] \pmod{p}$ and $\mathrm{ord}_p(\alpha_t) \neq \mathrm{ord}_{p^2}(\alpha_t)$.*

Proof. Let L be the splitting field of $g(x)$ over $\mathbb{F}_p$. Considering that $[L : \mathbb{F}_p] = 2$ and using the Frobenius automorphism we can prove, in a way similar to that used in 3.6, that the Tribonacci sequence $(G_n)_{n=1}^{\infty}$ defined by the initial conditions $[a,b,c]$ can be written over L as

$$G_n = A\alpha_1^n + B\beta_1^n + B^p(\beta_1^p)^n, \tag{4.21}$$

where $\alpha_1, \beta_1, \beta_1^p$ are different roots of $g(x)$ in L and the coefficients A, B are uniquely determined by $[a,b,c]$. Clearly, $A, \alpha_1 \in \mathbb{F}_p$ and $\beta_1 \in L$. Moreover, for the orders of $\alpha_1, \beta_1, \beta_1^p$ in the multiplicative group of L we have $\mathrm{ord}_L(\beta_1) = \mathrm{ord}_L(\beta_1^p)$ and $\mathrm{ord}_L(\alpha_1) | \mathrm{ord}_L(\beta_1)$ with $\mathrm{ord}_L(\alpha_1) < \mathrm{ord}_L(\beta_1)$ because the multiplicative group of L is cyclic. From $h(p) = \mathrm{lcm}(\mathrm{ord}_L(\alpha_1), \mathrm{ord}_L(\beta_1), \mathrm{ord}_L(\beta_1^p))$ it now follows that $h(p) = \mathrm{ord}_L(\beta_1)$. Further, we have from (4.21) that

$$h(p)[a,b,c] = \begin{cases} 1 & \text{if} \quad A = 0, B = 0, \\ h_0 = \mathrm{ord}_p(\alpha_1) & \text{if} \quad A \neq 0, B = 0, \\ h(p) = \mathrm{ord}_L(\beta_1) & \text{if} \qquad B \neq 0. \end{cases}. \tag{4.22}$$

Thus the only primitive periods $(G_n \bmod p)_{n=1}^{\infty}$ possible are $1, h_0$, and $h(p)$. From (4.21) and (4.22) we have that $h(p)[a,b,c] | h_0$ if and only if $[a,b,c] \equiv [0,0,0] \pmod{p}$ or $[a,b,c] \equiv [a, a\alpha_1, a\alpha_1^2] \pmod{p}$, i.e., if $[a,b,c] \pmod{p} \in E_p(\alpha_1)$.

Suppose now that the assertion is true for any $t \geq 1$ and let us prove it for $t+1$. Let $h(p^{t+1})[a,b,c] | p^t h_0$. By 4.2 and 4.6, $h(p^{t+1})[a, a\alpha_{t+1}, a\alpha_{t+1}^2] | p^t h_0$ and so

$$h(p^{t+1})[0, b - a\alpha_{t+1}, c - a\alpha_{t+1}^2] | p^t h_0. \tag{4.23}$$

It also follows from $h(p^{t+1})[a,b,c] | p^t h_0$ that $h(p)[a,b,c] | h_0$. Therefore we have $[a,b,c] \pmod{p} \in E_p(\alpha_1)$. This yields $[a,b,c] \equiv [a, a\alpha_{t+1}, a\alpha_{t+1}^2] \pmod{p}$ and thus $[0, b - a\alpha_{t+1}, c - a\alpha_{t+1}^2] \equiv [0,0,0] \pmod{p}$. Hence $[0, (b - a\alpha_{t+1})/p, (c - a\alpha_{t+1}^2)/p] \in \mathbb{Z}^3$. From (4.23) we have $h(p^t)[0, (b - a\alpha_{t+1})/p, (c - a\alpha_{t+1}^2)/p] | p^t h_0$. As $h(p^t)[0, (b - a\alpha_{t+1})/p, (c - a\alpha_{t+1}^2)/p] | h(p^t)$ and $h(p^t) | p^{t-1} h(p)$, where $p \nmid h(p)$, we obtain $h(p^t)[0, (b - a\alpha_{t+1})/p, (c - a\alpha_{t+1}^2)/p] | p^{t-1} h_0$. By the induction hypothesis, $[0, (b - a\alpha_{t+1})/p, (c - a\alpha_{t+1}^2)/p] \pmod{p^t} \in E_{p^t}(\alpha_t)$. Thus, there is a $q \in \mathbb{Z}$ such that

$$\left[0, \frac{b - a\alpha_{t+1}}{p}, \frac{c - a\alpha_{t+1}^2}{p}\right] \equiv q[1, \alpha_t, \alpha_t^2] \pmod{p^t}. \tag{4.24}$$

From (4.24) we obtain $q \equiv 0 \pmod{p^t}$ and so $(b - a\alpha_{t+1})/p \equiv (c - a\alpha_{t+1}^2)/p \equiv 0 \pmod{p^t}$. This yields $b \equiv a\alpha_{t+1} \pmod{p^{t+1}}$, $c \equiv a\alpha_t^2 \pmod{p^{t+1}}$ and therefore $[a,b,c] \pmod{p^{t+1}} \in E_{p^{t+1}}(\alpha_{t+1})$.

Conversely, let $[a,b,c] \pmod{p^t} \in E_{p^t}(\alpha_t)$ for any $t \geq 1$. Then $[a,b,c] \equiv [a, \alpha_t, a\alpha_t^2] \pmod{p^t}$ and, by 4.1, for the sequence defined by this triple we have $G_n \equiv a\alpha_t^{n-1} \pmod{p^t}$.

From 4.2, it follows that $h(p^t)[a,b,c]|\mathrm{ord}_{p^t}(\alpha_t)$ and, by 4.6, this means that $h(p^t)[a,b,c]|p^{t-1}h_0$.

Let us now prove the second part of 4.11. Let $t>1$ and $h(p^t)[a,b,c]=p^{t-1}h_0$. Suppose first that $[a,b,c]\equiv[0,0,0] (\mathrm{mod}\ p)$. Then $[a/p,b/p,c/p]\in\mathbb{Z}^3$. From 2.2 and from $h(p^{t-1})[a,b,c]|p^{t-2}h(p)$ it follows that $h(p^t)[a,b,c]=h(p^{t-1})[a/p,b/p,c/p]|p^{t-2}h(p)$. Since $(h(p),p)=1$, we get a contradiction. Suppose next that $\mathrm{ord}_p(\alpha_t)=\mathrm{ord}_{p^2}(\alpha_t)$. From $h(p^t)[a,b,c]=p^{t-1}h_0$ we have that $[a,b,c]\ (\mathrm{mod}\ p^t)\in E_{p^t}(\alpha_t)$ and so, for any $n\in\mathbb{N}$, $G_n\equiv a\alpha_t^{n-1}\ (\mathrm{mod}\ p^t)$. By 4.2, for a primitive period of this sequence we have $h(p^t)[a,b,c]|\mathrm{ord}_{p^t}(\alpha_t)$. Next, from 4.6 and from $\mathrm{ord}_p(\alpha_t)=\mathrm{ord}_{p^2}(\alpha_t)$ it follows that $\mathrm{ord}_{p^t}(\alpha_t)|p^{t-2}\mathrm{ord}_p(\alpha_t)=p^{t-2}h_0$, contradiction.

Conversely, let $t>1$, $[a,b,c]\ (\mathrm{mod}\ p^t)\in E_{p^t}(\alpha_t)$, $[a,b,c]\not\equiv[0,0,0]\ (\mathrm{mod}\ p)$ and $\mathrm{ord}_p(\alpha_t)\neq\mathrm{ord}_{p^2}(\alpha_t)$. From the hypothesis $[a,b,c]\ (\mathrm{mod}\ p^t)\in E_{p^t}(\alpha_t)$ it follows that for the sequence determined by this triple, $G_n\equiv a\alpha_t^{n-1}\ (\mathrm{mod}\ p^t)$ and $[a,b,c]\not\equiv[0,0,0]\ (\mathrm{mod}\ p)$ implies $p\nmid a$. Thus, by 4.2, $h(p^t)[a,b,c]=\mathrm{ord}_{p^t}(\alpha_t)$. From 4.6 and from $\mathrm{ord}_p(\alpha_t)\neq\mathrm{ord}_{p^2}(\alpha_t)$ we now obtain $h(p^t)[a,b,c]=p^{t-1}h_0$. The proof is complete. □

Let us now formulate the main theorem of this section.

Theorem 4.12. *Let p be an arbitrary prime such that $g(x)$ is factorized over $\mathbb{F}_p$ into the product of a linear factor and an irreducible quadratic factor. Further, let $h(p)\neq h(p^2)$, $\mathrm{ord}_p(\alpha_2)\neq\mathrm{ord}_{p^2}(\alpha_2)$ and $[a,b,c]\not\equiv[0,0,0]\ (\mathrm{mod}\ p)$. Then, for any $t\in\mathbb{N}$, the following assertions are true.*

If $[a,b,c](\mathrm{mod}\ p^t)\in E_{p^t}(\alpha_t)$ then

$$h(p^t)[a,b,c]=\mathrm{ord}_{p^t}(\alpha_t)=p^{t-1}\mathrm{ord}_p(\alpha_t). \tag{4.25}$$

If $[a,b,c](\mathrm{mod}\ p)\notin E_p(\alpha_1)$ then

$$h(p^t)[a,b,c]=p^{t-1}h(p)=p^{t-1}h(p)[a,b,c]. \tag{4.26}$$

If $[a,b,c](\mathrm{mod}\ p)\in E_p(\alpha_1)$ and $[a,b,c](\mathrm{mod}\ p^t)\notin E_{p^t}(\alpha_t)$ then

$$h(p^t)[a,b,c]=p^{t-1}h(p)\neq p^{t-1}h(p)[a,b,c]. \tag{4.27}$$

Proof. The validity of (4.25) follows from 4.11.

Let $[a,b,c]\ (\mathrm{mod}\ p)\notin \mathrm{E}_p(\alpha_1)$. Then, by 4.11 and $[a,b,c]\not\equiv[0,0,0]\ (\mathrm{mod}\ p)$, we have $h(p)[a,b,c]=h(p)$ and, by (2.2), we have $h(p)|h(p^t)[a,b,c]$. Next, from $h(p)\neq h(p^2)$, 1.1 and (2.3) it follows that $h(p^t)[a,b,c]|p^{t-1}h(p)$. Combining these equations yields $h(p^t)[a,b,c]=p^ih(p)$ for some $i\in\{0,1,\dots t-1\}$. Next, from $\mathrm{ord}_p(\alpha_2)\neq\mathrm{ord}_{p^2}(\alpha_2)$ and 4.8 we have $p\nmid\det A$. Therefore, by 4.5, there exists no solution $[a,b,c]\not\equiv[0,0,0]\ (\mathrm{mod}\ p)$ of $T^{p^{t-2}h(p)}x\equiv x\ (\mathrm{mod}\ p^t)$ for $t>1$, which implies that $h(p^t)[a,b,c]\nmid p^{t-2}h(p)$. Thus we conclude that (4.26) holds.

Let $[a,b,c]\ (\mathrm{mod}\ p)\in\mathrm{E}_p(\alpha_1)$ and $[a,b,c](\mathrm{mod}\ p^t)\notin\mathrm{E}_{p^t}(\alpha_t)$. From 4.11 and $[a,b,c](\mathrm{mod}\ p^t)\notin\mathrm{E}_{p^t}(\alpha_t)$ it follows that $h(p^t)[a,b,c]\nmid p^{t-1}h_0$ where $h_0=\mathrm{ord}_p(\alpha_t)$. Moreover, by 4.11, for $[a,b,c]\not\equiv[0,0,0]\ (\mathrm{mod}\ p)$ exactly one of the equalities $h(p^t)[a,b,c]=p^ih(p)$ and $h(p^t)[a,b,c]=p^ih_0$ holds for some $i\in\{0,\dots,t-1\}$. Combining the above, we obtain $h(p^t)[a,b,c]=p^ih(p)$. We shall show that $h(p^t)[a,b,c]\nmid p^{t-2}h(p)$. Indeed, suppose that $h(p^t)[a,b,c]|p^{t-2}h(p)$. Theorem 4.5 and $[a,b,c]\not\equiv[0,0,0]\ (\mathrm{mod}\ p)$ then give $p|\det A$. By 4.8 we have $\mathrm{ord}_p(\alpha_2)=\mathrm{ord}_{p^2}(\alpha_2)$, a contradiction. Since $h(p^t)[a,b,c]|p^{t-1}h(p)$, we obtain $h(p^t)[a,b,c]=p^{t-1}h(p)$. In addition, it follows from 4.11 and from $[a, b, c] (\text{mod } p) \in E_p(\alpha_1)$ that $h(p)[a, b, c] = \text{ord}_L(\alpha_1) \neq \text{ord}_L(\beta_1) = h(p)$, which, together with the preceding facts, proves (4.27). □

5. The case of factorization into the product of linear terms

What remains to be investigated is the case of the Tribonacci polynomial $g(x)$ being factorized over $\mathbb{F}_p$ into the product of linear terms, i.e.,

$$g(x) \equiv (x - \alpha_1)(x - \beta_1)(x - \gamma_1) \pmod p \quad \text{and} \quad \mathrm{S}_p(T) = \{\alpha_1, \beta_1, \gamma_1\}. \tag{5.1}$$

The assumption $p \neq 2, 11$ implies that $\alpha_1, \beta_1, \gamma_1$ are distinct, thus $g(x)$ has nonzero first derivatives over $\mathbb{F}_p$ at these points. From Hensel's lemma it follows that $g(x)$ can be factorized over $\mathbb{Q}_p$ as $g(x) = (x - \alpha)(x - \beta)(x - \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{Z}_p$. Let us put $\alpha_t := \alpha \mod p^t$, $\beta_t := \beta \mod p^t$, $\gamma_t := \gamma \mod p^t$ for every $t \in \mathbb{N}$. Thus, over the ring $\mathbb{Z}/p^t\mathbb{Z}$, we have $g(x) \equiv (x - \alpha_t)(x - \beta_t)(x - \gamma_t) \pmod{p^t}$ and $\mathrm{S}_{p^t}(T) = \{\alpha_t, \beta_t, \gamma_t\}$. Since $\mathbb{Z} \subset \mathbb{Z}_p \subset \mathbb{Q}_p$, the terms of the triple $[a, b, c]$ can be viewed as elements of the field $\mathbb{Q}_p$. Thus, over $\mathbb{Q}_p$, the terms of the Tribonacci sequence $(G_n)_{n=1}^{\infty}$ can be uniquely written as

$$G_n = A\alpha^n + B\beta^n + C\gamma^n, \text{ where } A, B, C \in \mathbb{Q}_p. \tag{5.2}$$

The equation (5.2) defines a 1-1 correspondence between the triples of initial values $[a, b, c] \in \mathbb{Q}_p^3$ and the triples of p-adic numbers $[A, B, C] \in \mathbb{Q}_p^3$.

Lemma 5.1. *Let $g(x)$ be factorized over $\mathbb{F}_p$, $p \neq 2, 11$ into the product of linear terms. Then the terms of the sequence $(G_n \bmod p^t)_{n=1}^{\infty}$ defined by an arbitrary triple of initial values $[a, b, c]$ can be uniquely written as*

$$G_n \bmod p^t \equiv A_t\alpha_t^n + B_t\beta_t^n + C_t\gamma_t^n \pmod{p^t}, \tag{5.3}$$

where $0 \leq A_t, B_t, C_t \leq p^t - 1$ are nonnegative integers.

Proof. Let us first show that $[A, B, C] \in \mathbb{Z}_p^3$. By substituting $n = 1, 2, 3$ into (5.2) we obtain the system of equations over $\mathbb{Q}_p$

$$\begin{bmatrix} \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \\ \alpha^3 & \beta^3 & \gamma^3 \end{bmatrix} \begin{bmatrix} A \\ B \\ C \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}. \tag{5.4}$$

The determinant of the matrix M of the system (5.4) is the well-known Vandermonde determinant, for which we have $\det M = \alpha\beta\gamma(\alpha - \beta)(\alpha - \gamma)(\gamma - \beta)$. Since α, β, γ are pairwise incongruent modulo p, none of the differences $\alpha - \beta, \alpha - \gamma, \gamma - \beta$ is divisible by p. From this fact and from $\alpha\beta\gamma = 1$, it follows that $p \nmid \det M$. Thus, $\det M$ is an invertible element of the ring $\mathbb{Z}_p$ and matrix M is invertible over $\mathbb{Z}_p$. Multiplying (5.4) by M^{-1} we obtain $[A, B, C]$ as a $\mathbb{Z}_p$-linear combination of $[a, b, c]$ and so $[A, B, C] \in \mathbb{Z}_p^3$. Let us now put $A_t := A \bmod p^t$, $B_t := B \bmod p^t$, $C_t := C \bmod p^t$. It is not difficult to prove that $[A, B, C] \equiv [A', B', C'] \pmod{p^t}$ if and only if $[a, b, c] \equiv [a', b', c'] \pmod{p^t}$. Thus there exists a 1-1 correspondence between the triples $[a, b, c] \in (\mathbb{Z}/p^t\mathbb{Z})^3$ and the triples $[A_t, B_t, C_t] \in (\mathbb{Z}/p^t\mathbb{Z})^3$. Congruence (5.3) is now obtained by reducing (5.2) by p^t. □

Lemma 5.2. *Let the primitive periods of the sequences $(A_t\alpha_t^n \bmod p^t)_{n=1}^{\infty}$, $(B_t\beta_t^n \bmod p^t)_{n=1}^{\infty}$, $(C_t\gamma_t^n \bmod p^t)_{n=1}^{\infty}$ be k_1, k_2, k_3. Then the primitive period of the sequence $(A_t\alpha_t^n + B_t\beta_t^n + C_t\gamma_t^n \bmod p^t)_{n=1}^{\infty}$ is $\mathrm{lcm}(k_1, k_2, k_3)$.*

Proof. Clearly, $\operatorname{lcm}(k_1, k_2, k_3)$ is a period of $(A_t\alpha_t^n + B_t\beta_t^n + C_t\gamma_t^n \bmod p^t)_{n=1}^{\infty}$ and, therefore, it is sufficient to prove that this period is primitive. Suppose there is a primitive period $k < \operatorname{lcm}(k_1, k_2, k_3)$. Since k is a period, we have

$$[A_t\alpha_t^{k+1} + B_t\beta_t^{k+1} + C_t\gamma_t^{k+1}, A_t\alpha_t^{k+2} + B_t\beta_t^{k+2} + C_t\gamma_t^{k+2}, A_t\alpha_t^{k+3} + B_t\beta_t^{k+3} + C_t\gamma_t^{k+3}]$$
$$\equiv [A_t\alpha_t + B_t\beta_t + C_t\gamma_t, A_t\alpha_t^2 + B_t\beta_t^2 + C_t\gamma_t^2, A_t\alpha_t^3 + B_t\beta_t^3 + C_t\gamma_t^3] (\bmod\ p^t).$$

This system of congruences can be reduced to the equivalent form

$$\begin{bmatrix} \alpha_t & \beta_t & \gamma_t \\ \alpha_t^2 & \beta_t^2 & \gamma_t^2 \\ \alpha_t^3 & \beta_t^3 & \gamma_t^3 \end{bmatrix} \begin{bmatrix} A_t(\alpha_t^k - 1) \\ B_t(\beta_t^k - 1) \\ C_t(\gamma_t^k - 1) \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} (\bmod\ p^t). \tag{5.5}$$

As the determinant of the system matrix of (5.5) is not divisible by p, (5.5) has only one solution

$$A_t(\alpha_t^k - 1) \equiv 0 \ (\bmod\ p^t),\ B_t(\beta_t^k - 1) \equiv 0 \ (\bmod\ p^t),\ C_t(\gamma_t^k - 1) \equiv 0 \ (\bmod\ p^t). \tag{5.6}$$

Next, from (5.6) we have $A_t\alpha_t^{k+1} \equiv A_t\alpha_t \ (\bmod\ p^t)$, $B_t\beta_t^{k+1} \equiv B_t\beta_t \ (\bmod\ p^t)$, $C_t\gamma_t^{k+1} \equiv C_t\gamma_t \ (\bmod\ p^t)$. This implies that k is a period for each of the sequences $(A_t\alpha_t^n \bmod p^t)_{n=1}^{\infty}$, $(B_t\beta_t^n \bmod p^t)_{n=1}^{\infty}$, $(C_t\gamma_t^n \bmod p^t)_{n=1}^{\infty}$. Consequently, we have $k_1|k$, $k_2|k$, $k_3|k$, which contradicts the hypothesis $k < \operatorname{lcm}(k_1, k_2, k_3)$. □

Lemma 5.3. *Let* $p \neq 2, 11$ *be an arbitrary prime and let* $\mathrm{S}_p(T) = \{\alpha_1, \beta_1, \gamma_1\}$. *Further, let* $\operatorname{ord}_p(\alpha_1) = h_1, \operatorname{ord}_p(\beta_1) = h_2$ *and* $\operatorname{ord}_p(\gamma_1) = h_3$. *Then*

$$\operatorname{lcm}(h_1, h_2) = \operatorname{lcm}(h_1, h_3) = \operatorname{lcm}(h_2, h_3) = \operatorname{lcm}(h_1, h_2, h_3) = h(p). \tag{5.7}$$

Proof. Put $k = \gcd(h_1, h_2)$. Then there exist $r, s \in \mathbb{N}$ such that $h_1 = kr, h_2 = ks$ with $(r, s) = 1$. Thus, we have $\operatorname{lcm}(h_1, h_2) = krs$. Next, the Viète equation $\alpha_1\beta_1\gamma_1 \equiv 1 \ (\bmod\ p)$ yields $(\alpha_1\beta_1\gamma_1)^{krs} \equiv (\alpha_1^{kr})^s \cdot (\beta_1^{ks})^r \cdot \gamma_1^{krs} \equiv \gamma_1^{krs} \equiv 1 \ (\bmod\ p)$. Then we have $h_3|krs$, which implies $\operatorname{lcm}(h_1, h_2) = \operatorname{lcm}(h_1, h_2, h_3)$. By analogy, we can prove that $\operatorname{lcm}(h_1, h_3) = \operatorname{lcm}(h_1, h_2, h_3)$ and $\operatorname{lcm}(h_2, h_3) = \operatorname{lcm}(h_1, h_2, h_3)$. Next, using (5.4) and Cramer's rule, we can show that, for the coefficients A_t, B_t, C_t corresponding to $[0, 0, 1]$, $A_t \equiv \varepsilon \cdot \beta\gamma(\gamma - \beta)(\bmod\ p^t)$, $B_t \equiv \varepsilon \cdot \alpha\gamma(\alpha - \gamma)(\bmod\ p^t)$, $C_t \equiv \varepsilon \cdot \alpha\beta(\beta - \alpha)(\bmod\ p^t)$, where $\varepsilon \equiv (\det M)^{-1} \ (\bmod\ p^t)$. Hence none of the coefficients A_t, B_t, C_t is divisible by p. Applying now (5.3) to the module p and the triple $[0, 0, 1]$, we can use Lemma 5.2 to show that $h(p) = \operatorname{lcm}(h_1, h_2, h_3)$. This proves (5.7). □

Remark 5.4. Investigating the orders h_1, h_2, h_3 for the first several hundreds of primes might lead to a hypothesis that there are always two of the orders h_1, h_2, h_3 that divide the third. That is, if $h_1 < h_2 < h_3$, all the terms in (5.7) are equal to h_3. The first counter-example that disproves this hypothesis is $p = 4481$. Over $\mathbb{F}_{4481}$, $g(x)$ can be written as $g(x) = (x - 2661)(x - 2677)(x - 3625)$. Denoting $\alpha_1 = 2661$, $\beta_1 = 2677$, $\gamma_1 = 3625$, we arrive at $\operatorname{ord}_p(\alpha_1) = 2240$, $\operatorname{ord}_p(\beta_1) = 640$, $\operatorname{ord}_p(\gamma_1) = 896$ and $h(p) = \operatorname{lcm}(2240, 640, 896) = 4480$. Further, if two of the roots $\alpha_1, \beta_1, \gamma_1$ are of the same order in the multiplicative group of $\mathbb{F}_p$ different from the order of the third root, the following two situations may, theoretically, occur:

$$\operatorname{ord}_p(\alpha_1) < \operatorname{ord}_p(\beta_1) = \operatorname{ord}_p(\gamma_1) \qquad \text{and} \qquad \operatorname{ord}_p(\alpha_1) = \operatorname{ord}_p(\beta_1) < \operatorname{ord}_p(\gamma_1).$$

Let us prove that the second case can never occur.

Lemma 5.5. *If* $\operatorname{ord}_p(\alpha_1) = \operatorname{ord}_p(\beta_1) = h$, *then* $\operatorname{ord}_p(\gamma_1)|h$.

Proof. By raising the Viète equation $\alpha_1\beta_1\gamma_1 \equiv 1 \pmod p$ to the h-th power we obtain $\gamma_1^h \equiv \alpha_1^h\beta_1^h\gamma_1^h \equiv 1 \pmod p$ and so $\mathrm{ord}_p\gamma_1|h$. □

Remark 5.6. Without loss of generality we can denote the roots of $g(x)$ over $\mathbb{F}_p$ by α_1, β_1, γ_1 so that, for their orders h_1, h_2, h_3 and $h(p) = \mathrm{lcm}(h_1, h_2, h_3)$, exactly one of the four following events occurs:

$$\begin{array}{ll} h_1 = h_2 = h_3 = h(p), & p = 103, \\ h_1 < h_2 = h_3 = h(p), & p = 47, \\ h_1 < h_2 < h_3 = h(p), & p = 311, \\ h_1 < h_2 < h_3 < h(p), & p = 4481. \end{array} \tag{5.8}$$

The values of the primes p shown in (5.8) are the least values for which the situation in question occurs.

Theorem 5.7. *Let $g(x)$ be factorized over $\mathbb{F}_p$ into the product of linear terms and let $p \neq 2, 11$. If $h = h(p) \neq h(p^2)$, then there is at most one eigenvalue $\lambda \in S_{p^t}(T)$ satisfying*

$$\mathrm{ord}_p(\lambda) = \mathrm{ord}_{p^2}(\lambda). \tag{5.9}$$

Proof. Suppose that in $S_{p^t}(T)$ there are two eigenvalues satisfying (5.9). Without loss of generality, let $\mathrm{ord}_p(\alpha_t) = \mathrm{ord}_{p^2}(\alpha_t) = h_1$ and $\mathrm{ord}_p(\beta_t) = \mathrm{ord}_{p^2}(\beta_t) = h_2$. From (5.7) we obtain $\mathrm{lcm}(h_1, h_2) = h$ and thus $\mathrm{ord}_{p^2}(\alpha_2) = \mathrm{ord}_{p^2}(\beta_2)|h$. By raising the Viète equation $\alpha_2\beta_2\gamma_2 \equiv 1 \pmod{p^2}$ to the h-th power, we obtain $\alpha_2^h\beta_2^h\gamma_2^h \equiv 1 \pmod{p^2}$, which implies $\gamma_2^h \equiv 1 \pmod{p^2}$. Applying (5.3) to the triple $[0, 0, 1]$ and the module p^2, we obtain

$$[G_{h+1}, G_{h+2}, G_{h+3}] \equiv [A_2\alpha_2 + B_2\beta_2 + C_2\gamma_2, A_2\alpha_2^2 + B_2\beta_2^2 + C_2\gamma_2^2, A_2\alpha_2^3 + B_2\beta_2^3 + C_2\gamma_2^3]$$

$$\equiv [G_1, G_2, G_3] \pmod{p^2}. \tag{5.10}$$

From (5.10) we conclude $h(p^2)|h$. By (2.2), also $h|h(p^2)$, which yields $h = h(p^2)$. □

Remark 5.8. By slightly modifying the proof of Theorem 4.8 we can show that $\mathrm{ord}_p(\lambda) = \mathrm{ord}_{p^2}(\lambda)$ if and only if $p|\mathrm{det}A$. We can also prove that it is not possible that $h(p) = h(p^2)$ if there is a $\lambda \in S_{p^t}(T) = \{\alpha_t, \beta_t, \gamma_t\}$ such that $\mathrm{ord}_p(\lambda) \neq \mathrm{ord}_{p^2}(\lambda)$. Thus, $h(p) = h(p^2)$ implies $\mathrm{ord}_p(\lambda) = \mathrm{ord}_{p^2}(\lambda)$ for every $\lambda \in S_{p^t}(T)$. The proof can be done by analogy with 4.9.

Theorem 5.9. *Let $g(x)$ be factorized over $\mathbb{F}_p$, where $p \neq 2, 11$, into the product of linear terms. Further, let $[a, b, c] \not\equiv [0, 0, 0] \pmod p$ and, for any $t \in \mathbb{N}$, let $S_{p^t}(T) = \{\alpha_t, \beta_t, \gamma_t\}$. If $\lambda \in S_{p^t}(T)$ and $[a, b, c] \pmod{p^t} \in E_{p^t}(\lambda)$ then*

$$h(p^t)[a, b, c] = \mathrm{ord}_{p^t}(\lambda). \tag{5.11}$$

Moreover, if, for $t > 1$, $\lambda \in S_{p^t}(T)$ fulfils the condition $\mathrm{ord}_p(\lambda) \neq \mathrm{ord}_{p^2}(\lambda)$, then

$$h(p^t)[a, b, c] = p^{t-1}\mathrm{ord}_p(\lambda) = p^{t-1}h(p)[a, b, c]. \tag{5.12}$$

If $[a, b, c] \pmod{p^t} \notin E_{p^t}(\alpha_t) \cup E_{p^t}(\beta_t) \cup E_{p^t}(\gamma_t)$ and, for every $\lambda \in S_{p^t}(T)$, $t > 1$, $\mathrm{ord}_p(\lambda) \neq \mathrm{ord}_{p^2}(\lambda)$, then

$$h(p^t)[a, b, c] = h(p^t) = p^{t-1}h(p). \tag{5.13}$$

Proof. By (5.3) we have $[a, b, c] \equiv [0, 0, 0] \pmod p$ if and only if $[A_t, B_t, C_t] \equiv [0, 0, 0] \pmod p$. Thus $[a, b, c] \not\equiv [0, 0, 0] \pmod p$ implies that at least one of the coefficients A_t, B_t, C_t is not divisible by p. If $[a, b, c] (\text{mod } p^t) \in E_{p^t}(\lambda)$, for some $\lambda \in S_{p^t}(T)$, then exactly two of the coefficients A_t, B_t, C_t are divisible by p^t. Now, from (5.3) it follows that $h(p^t)[a, b, c] = \text{ord}_{p^t}(\lambda)$, which proves (5.11). Moreover, if $\text{ord}_p(\lambda) \neq \text{ord}_{p^2}(\lambda)$, then (4.19) implies (5.12).

Let $[a, b, c] (\text{mod } p^t) \notin E_{p^t}(\alpha_t) \cup E_{p^t}(\beta_t) \cup E_{p^t}(\gamma_t)$. Then at least two of the coefficients A_t, B_t, C_t in (5.3) are not divisible by p^t and at least one of them is not divisible by p. Without loss of generality we can denote $\alpha_t, \beta_t, \gamma_t$ so that $p \nmid A_t$ and $p^t \nmid B_t$. Hence (4.19) implies that that the primitive period of $(A_t \alpha_t^n \text{ mod } p^t)_{n=1}^{\infty}$ is $k_1 = \text{ord}_{p^t}(\alpha_t) = p^{t-1}\text{ord}_p(\alpha_t)$ and the primitive period of $(B_t \beta_t^n \text{ mod } p^t)_{n=1}^{\infty}$ is $k_2 = p^i \text{ord}_p(\beta_t)$ for some $i \in \{0, \dots, t-1\}$. If we put $h_1 = \text{ord}_p(\alpha_t)$, $h_2 = \text{ord}_p(\beta_t)$, then $\text{lcm}(k_1, k_2) = p^{t-1}\text{lcm}(h_1, h_2)$. By (5.7) we have $\text{lcm}(h_1, h_2) = h(p)$ and thus $\text{lcm}(k_1, k_2) = p^{t-1}h(p) = h(p^t)$. Now, from 5.2 we conclude that $h(p^t)[a, b, c] = \text{lcm}(k_1, k_2, k_3)$. As $\text{lcm}(k_1, k_2) | \text{lcm}(k_1, k_2, k_3)$ we have $h(p^t) | h(p^t)[a, b, c]$. This fact together with (2.3) yields (5.13). □

Remark 5.10. If $[a, b, c] (\text{mod } p) \notin E_p(\alpha_1) \cup E_p(\beta_1) \cup E_p(\gamma_1)$, then in (5.13) we have $h(p) = h(p)[a, b, c]$. In the opposite case, we have $h(p)[a, b, c] = \text{ord}_p(\lambda)$ for some $\lambda \in S_{p^t}(T)$ and the equality $h(p)[a, b, c] = h(p)$ may not hold in general. See (5.8).

We will use the results obtained in this paper along with the results proved in [2] to solve a problem in combinatorics which is closely related to the modular periodicity of Tribonacci sequences. See [3].

References

[1] M. Elia, *Derived sequences, the Tribonacci recurrence and cubic forms*, The Fibonacci Quarterly **39.2** (2001), 107–115.

[2] J. Klaška, *Tribonacci modulo* 2^t *and* 11^t, Math. Bohem. **133.4** (2008), 377–387.

[3] J. Klaška, *Tribonacci partition formulas modulo m*, Acta Mathematica Sinica, English Series, **26.3** (2010), 465–476.

[4] Zhi-Hong Sun, Zhi-Wei Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), 371–388.

[5] A. Vince, *Period of a Linear Recurrence*, Acta Arith. **39** (1981), 303–311.

[6] M. E. Waddill, *Some Properties of a Generalized Fibonacci Sequence Modulo m*, The Fibonacci Quarterly **16.4** (1978), 344–353.

[7] D. D. Wall, *Fibonacci Series Modulo m*, Amer. Math. Monthly **67.6** (1960), 525–532.

Keywords: Tribonacci, modular periodicity, periodic sequence

MSC 2000: 11B50, 11B39

CHAPTER 5

TRIBONACCI MODULO 2^t AND 11^t ⋆

Abstract. Our previous research was devoted to the problem of determining the primitive periods of the sequences $(G_n \bmod p^t)_{n=1}^{\infty}$ where $(G_n)_{n=1}^{\infty}$ is a Tribonacci sequence defined by an arbitrary triple of integers. The solution to this problem was found for the case of powers of an arbitrary prime $p \neq 2, 11$. In this paper, which could be seen as a completion of our preceding investigation, we find solution for the case of singular primes $p = 2, 11$.

1. Introduction

Having a linear recurrence formula of order k with integer coefficients we can construct the corresponding characteristic polynomial $f(x)$. If $f(x)$ has no multiple roots then its discriminant is a non zero integer and so it is divisible by only a finite number of prime divisors. When investigating modular periodicity of the sequences defined by these formulas, the primes that divide the discriminant of $f(x)$ form exceptions and have to be considered separately. The exceptional primes p correspond to the cases of $f(x)$ having multiple roots over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of residue classes modulo p. In this paper, which could be seen as an extension of our previous paper [1], we focus on the Tribonacci case. It is well known, see for example [2, p. 310], that the primes $p = 2, 11$ are the only primes for which the Tribonacci characteristic polynomial $g(x) = x^3 - x^2 - x - 1$ has multiple roots.

Let us now review the notations introduced in [1]. Let $(g_n)_{n=1}^{\infty}$ denote a Tribonacci sequence defined by the recurrence formula $g_{n+3} = g_{n+2} + g_{n+1} + g_n$ and the triple of initial values $[0, 0, 1]$. Let further $(G_n)_{n=1}^{\infty}$ denote the generalized Tribonacci sequence defined by an arbitrary triple $[a, b, c]$ of integers. We will denote the primitive periods of the sequences $(g_n \bmod m)_{n=1}^{\infty}$ and $(G_n \bmod m)_{n=1}^{\infty}$ by $h(m)$ and $h(m)[a, b, c]$ respectively. In 1978, M. E. Waddill [3, Theorem 8], proved that for any prime p and $t \in \mathbb{N} = \{1, 2, 3, \dots\}$, we have:

$$\text{If } \ h(p) \neq h(p^2), \text{ then } h(p^t) = p^{t-1}h(p). \tag{1.1}$$

This paper aims at determining the numbers $h(p^t)[a, b, c]$ and find the relationships between $h(p^t)[a, b, c]$ and $h(p)[a, b, c]$ for the primes $p = 2, 11$. The case of $p \neq 2, 11$ is solved in [1]. The methods used in proofs of this paper will mostly be based on matrix algebra. As usual, by T we will denote the Tribonacci matrix

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad T^n = \begin{bmatrix} g_n & g_{n-1} + g_n & g_{n+1} \\ g_{n+1} & g_n + g_{n+1} & g_{n+2} \\ g_{n+2} & g_{n+1} + g_{n+2} & g_{n+3} \end{bmatrix} \quad \text{for} \ \ n > 1. \tag{1.2}$$

⋆ Published in J. Klaška, *Tribonacci modulo* 2^t *and* 11^t, Mathematica Bohemica **133.4** (2008), 377–387.

Put $x_0 = [a, b, c]^\tau$ and $x_n = [G_{n+1}, G_{n+2}, G_{n+3}]^\tau$ where τ denotes the transposition. Then the triple x_n may be expressed by means of x_0 as follows: $x_n = T^n x_0$. Thus the primitive period of the sequence $(G_n \bmod m)_{n=1}^{\infty}$ defined by a triple $[a, b, c]$ for an arbitrary module $m > 1$ is equal to the smallest number h for which $T^h x_0 \equiv x_0 \pmod{m}$. By [1, Lemma 2.1], the investigation of the primitive periods of Tribonacci sequences modulo p^t is restricted to sequences beginning with the triples $[a, b, c] \not\equiv [0, 0, 0] \pmod{p}$. In the opposite case, for any $t \in \mathbb{N}$ and $1 \le i \le t$, we have $h(p^t)[p^{t-i}a, p^{t-i}b, p^{t-i}c] = h(p^i)[a, b, c]$. For this reason, we will investigate only the triples satisfying $[a, b, c] \not\equiv [0, 0, 0] \pmod{p}$.

2. Tribonacci modulo 2^t

We can easily calculate $h(2) = 4$ and $h(2^2) = 8$. By (1.1), we have $h(2^t) = 2^{t-1}h(2) = 2^{t+1}$ and so $h(2^t)[a, b, c] | 2^{t+1}$ for any $[a, b, c]$. For $p = 2$, the multiplicity of the root $\alpha = 1$ of the polynomial $g(x)$ is greater than $\mathrm{char}(\mathbb{F}_2) = 2$ and therefore $(G_n \bmod 2)_{n=1}^{\infty}$ cannot be expressed as $G_n \bmod 2 = c_1 + c_2 n + c_3 n^2$ as usual. The sequences $(1)_{n=1}^{\infty}, (n)_{n=1}^{\infty}, (n^2)_{n=1}^{\infty}$ are dependent over $\mathbb{F}_2$ and do not form a basis. Despite that, for some triples $[a, b, c] \not\equiv [0, 0, 0] \pmod{2}$, the numbers $h(2^t)[a, b, c]$ can be determined using the results derived in [1]. In the first place, it is proved in [1, Theorem 3.1], that, if $(D(a, b, c), m) = 1$ where $D(a, b, c)$ is a cubic form defined by

$$D(a, b, c) = a^3 + 2b^3 + c^3 - 2abc + 2a^2b + 2ab^2 - 2bc^2 + a^2c - ac^2, \tag{2.1}$$

then $h(m)[a, b, c] = h(m)$ for any modulus $m > 1$. The following theorem is an easy consequence of the above assertions.

Theorem 2.1. *If $D(a, b, c)$ is an odd number, then $h(2^t)[a, b, c] = h(2^t) = 2^{t+1}$. Hence, we have $h(2^t)[a, b, c] = 2^{t-1} \cdot h(2)[a, b, c]$.*

It is easy to verify that the premise of Theorem 2.1 is true if and only if $[a, b, c]$ is congruent modulo 2 with some of the triples $[0, 0, 1]$, $[1, 0, 0]$, $[1, 1, 0]$, $[0, 1, 1]$. Therefore it suffices to investigate the cases of the triple $[a, b, c]$ being congruent modulo 2 with some of the triples $[0, 1, 0], [1, 0, 1], [1, 1, 1]$. The following assertions will be important for the proofs of the main theorems 2.4, 2.5, and 2.6.

Lemma 2.2. *For any modulus of the form 2^t where $t \ge 5$, the following congruences hold:*

$$\begin{array}{llll} g_{2^{t-1}-1} \equiv -1 \pmod{2^t}, & & g_{2^{t-1}} \equiv 2^{t-2} + 1 \pmod{2^t}, & \\ g_{2^{t-1}+1} \equiv 0 \pmod{2^t}, & & g_{2^{t-1}+2} \equiv 2^{t-2} \pmod{2^t}, & \\ g_{2^{t-1}+3} \equiv 2^{t-1} + 1 \pmod{2^t}. & & & \end{array} \tag{2.2}$$

Proof. Using methods of matrix algebra, we will prove all the congruences in (2.2) simultaneously. Let us consider a Tribonacci matrix T. Due to (1.2), it suffices to prove that, for any $t \ge 5$, we have

$$T^{2^{t-1}} \equiv \begin{bmatrix} 2^{t-2}+1 & 2^{t-2} & 0 \\ 0 & 2^{t-2}+1 & 2^{t-2} \\ 2^{t-2} & 2^{t-2} & 2^{t-1}+1 \end{bmatrix} \equiv E + 2^{t-2}A \pmod{2^t}, \text{ where } A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix}$$

and E is an identity matrix. Let us first prove the congruence for $t = 5$. By direct calculation, we can verify that

$$T^{2^4} = \begin{bmatrix} 1705 & 2632 & 3136 \\ 3136 & 4841 & 5768 \\ 5768 & 8904 & 10609 \end{bmatrix} \equiv \begin{bmatrix} 2^3+1 & 2^3 & 0 \\ 0 & 2^3+1 & 2^3 \\ 2^3 & 2^3 & 2^4+1 \end{bmatrix} \pmod{2^5}.$$

Let us further assume that the congruence holds for $t \geq 5$. Since $AE = EA$, we have $T^{2^t} \equiv (E + 2^{t-2}A)^2 \equiv E + 2^{t-1}A \pmod{2^{t+1}}$, which proves (2.2). □

Consequence 2.3. For any modulus of the form 2^t where $t \geq 3$, the following congruences hold:

$$\begin{array}{ll} g_{2^t-1} \equiv -1 \pmod{2^t}, & g_{2^t} \equiv 2^{t-1}+1 \pmod{2^t}, \\ g_{2^t+1} \equiv 0 \pmod{2^t}, & g_{2^t+2} \equiv 2^{t-1} \pmod{2^t}, \\ g_{2^t+3} \equiv 1 \pmod{2^t}. & \end{array} \tag{2.3}$$

Proof. For $t = 3$, (2.3) can be verified by direct calculation. For $t \geq 4$, (2.3) follows from (2.2). □

Theorem 2.4. *If* $[a, b, c] \equiv [0, 1, 0] \pmod 2$, *then, for* $t > 1$ *we have*

$$h(2^t)[a, b, c] = 2^{t+1}. \tag{2.4}$$

Proof. Clearly, it is sufficient to prove that $x_{2^t} \not\equiv x_0 \pmod{2^t}$, that is, that 2^t is not a period. The triple $[a, b, c]$ can be written as $x_0 = [2a_1, 1+2b_1, 2c_1]^\tau$ where $a_1, b_1, c_1 \in \mathbb{Z}$. For $t = 2$ we have

$$T^{2^2}x_0 = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 3 & 4 \\ 4 & 6 & 7 \end{bmatrix} \begin{bmatrix} 2a_1 \\ 1+2b_1 \\ 2c_1 \end{bmatrix} \equiv \begin{bmatrix} 2+2a_1 \\ 3+2b_1 \\ 2+2c_1 \end{bmatrix} \pmod{2^2}.$$

Suppose that $T^{2^2}x_0 \equiv x_0 \pmod{2^2}$. Then we have

$$[2+2a_1, 3+2b_1, 2+2c_1] \equiv [2a_1, 1+2b_1, 2c_1] \pmod{2^2}.$$

Hence $[2, 3, 2] \equiv [0, 1, 0] \pmod{2^2}$, which is a contradiction. If $t \geq 3$, then by (2.3) we have

$$T^{2^t}x_0 \equiv \begin{bmatrix} 2^{t-1}+1 & 2^{t-1} & 0 \\ 0 & 2^{t-1}+1 & 2^{t-1} \\ 2^{t-1} & 2^{t-1} & 1 \end{bmatrix} \begin{bmatrix} 2a_1 \\ 1+2b_1 \\ 2c_1 \end{bmatrix} \equiv \begin{bmatrix} 2a_1+2^{t-1} \\ 1+2b_1+2^{t-1} \\ 2c_1+2^{t-1} \end{bmatrix} \pmod{2^t}.$$

Suppose that $T^{2^t}x_0 \equiv x_0 \pmod{2^t}$. Then we have

$$[2a_1+2^{t-1}, 2^{t-1}, 2c_1+2^{t-1}] \equiv [2a_1, 1+2b_1, 2c_1] \pmod{2^t}.$$

By matching terms, we obtain $2^{t-1} \equiv 0 \pmod{2^t}$ and thus a contradiction. □

It is not difficult to rephrase Theorem 2.4 to include the triples $[a, b, c] \equiv [1, 0, 1]$. Clearly, there is exactly one triple of the form $x_0 = [2(c_1 - a_1 - b_1), 1 + 2a_1, 2b_1]^\tau$ corresponding to each triple $x_1 = [1+2a_1, 2b_1, 1+2c_1]^\tau$. Since $Tx_0 = x_1$, the triples x_0 and x_1 define sequences with identical primitive periods. By 2.4, this primitive period equals 2^{t+1}. This proves the following theorem.

Theorem 2.5. *If* $[a, b, c] \equiv [1, 0, 1] \pmod 2$, *then, for* $t > 1$ *we have*

$$h(2^t)[a, b, c] = 2^{t+1}. \tag{2.5}$$

We can also use the procedure from 2.4 to prove the following theorem:

Theorem 2.6. *If* $[a,b,c] \equiv [1,1,1] \pmod 2$*, then for* $t > 1$ *we have*

$$h(2^t)[a,b,c] = 2^t. \tag{2.6}$$

Proof. The triple $[a,b,c]$ can be written as $x_0 = [1+2a_1, 1+2b_1, 1+2c_1]^\tau$ where $a_1, b_1, c_1 \in \mathbb{Z}$. Suppose $t \geq 5$. Then by Lemma 2.2 we have $T^{2^t}x_0 \equiv x_0 \pmod{2^t}$ and so $h(2^t)[a,b,c] | 2^t$. It is now sufficient to prove that $x_{2^{t-1}} \not\equiv x_0 \pmod{2^t}$, that is, that 2^{t-1} is not a period. By (2.2) we have

$$x_{2^{t-1}} \equiv T^{2^{t-1}}x_0 \equiv \begin{bmatrix} 2^{t-2}+1 & 2^{t-2} & 0 \\ 0 & 2^{t-2}+1 & 2^{t-2} \\ 2^{t-2} & 2^{t-2} & 2^{t-1}+1 \end{bmatrix} \begin{bmatrix} 1+2a_1 \\ 1+2b_1 \\ 1+2c_1 \end{bmatrix} \pmod{2^t}.$$

It follows that

$$x_{2^{t-1}} \equiv [1+2a_1+2^{t-1}(1+a_1+b_1), 1+2b_1+2^{t-1}(1+b_1+c_1), 1+2c_1+2^{t-1}(a_1+b_1)]^\tau.$$

Suppose $x_{2^{t-1}} \equiv x_0 \pmod{2^t}$. Matching the terms yields that

$$2^{t-1}(1+a_1+b_1) \equiv 0, \quad 2^{t-1}(1+b_1+c_1) \equiv 0, \quad 2^{t-1}(a_1+b_1) \equiv 0 \pmod{2^t}.$$

Hence $1 \equiv 0 \pmod 2$ and a contradiction follows. To prove the cases of $t = 2,3,4$ is easy and can be left to the reader. □

Remark 2.7. Theorems 2.4, 2.5, and 2.6 are true for $t > 1$. In particular, for $t = 1$, we have $h(2)[1,1,1] = 1$ and $h(2)[0,1,0] = h(2)[1,0,1] = 2$.

Corollary 2.8. *If a triple* $[a,b,c]$ *is congruent modulo* 2 *with some of the triples* $[0,1,0]$, $[1,0,1]$, $[1,1,1]$*, then for any* $t > 1$ *we have* $h(2^t)[a,b,c] = 2^t \cdot h(2)[a,b,c]$.

3. Tribonacci modulo 11^t

The determination of primitive periods modulo 11^t will be somewhat more complicated. We can directly verify that $h(11) = 110$ and $h(11^2) = 1210$. Now it follows from (1.1) that $h(11^t) = 10 \cdot 11^t$ for any $t \in \mathbb{N}$ and thus, for any triple $[a,b,c]$, we have $h(11^t)[a,b,c] | 10 \cdot 11^t$. As $x^3 - x^2 - x - 1 \equiv (x-9)(x-7)^2 \pmod{11}$ and $(9^n)_{n=1}^\infty$, $(7^n)_{n=1}^\infty$, $(n7^n)_{n=1}^\infty$ are linearly independent over $\mathbb{F}_{11}$, we have

$$G_n \equiv c_1 \cdot 9^n + (c_2 + c_3 n) \cdot 7^n \pmod{11}, \tag{3.1}$$

where the coefficients c_1, c_2, c_3 are uniquely determined by the triple $[a,b,c]$. Let $\mathrm{ord}_{11}(\varepsilon)$ denote the order of $\varepsilon \not\equiv 0 \pmod{11}$ in the multiplicative group of $\mathbb{F}_{11}$. It is easy to see that $\mathrm{ord}_{11}(9) = 5$ and $\mathrm{ord}_{11}(7) = 10$. Now yields (3.1) that for any $[a,b,c] \not\equiv [0,0,0] \pmod{11}$, $h(11)[a,b,c]$ is equal exactly one of the numbers $5, 10$ and 110. This, together with $h(11)[a,b,c] | h(11^t)[a,b,c]$, implies that for $[a,b,c] \not\equiv [0,0,0] \pmod{11}$, the only forms of the periods $h(11^t)[a,b,c]$ are $5 \cdot 11^i$ and $10 \cdot 11^i$ where $i \in \{0,1,\ldots,t\}$. Consequently, there exists no triple $[a,b,c]$ for which $h(11^t)[a,b,c] = 2 \cdot 11^i$. In some cases, $h(11^t)[a,b,c]$ can be determined using a form $D(a,b,c)$. However, there are triples for which $h(11^t)[a,b,c] = h(11^t)$ and also $D(a,b,c) \equiv 0 \pmod{11}$. Thus $D(a,b,c)$ cannot be used to determine all the triples for which $h(11^t)[a,b,c] = h(11^t)$.

Lemma 3.1. *Let* $t \geq 3$ *and* $h = 10 \cdot 11^{t-2}$*. Then we have the following congruences:*

$$\begin{aligned} g_{h-1} &\equiv 25\cdot 11^{t-2}-1 \pmod{11^t}, & g_h &\equiv 65\cdot 11^{t-2}+1 \pmod{11^t},\\ g_{h+1} &\equiv 26\cdot 11^{t-2} \pmod{11^t}, & g_{h+2} &\equiv 116\cdot 11^{t-2} \pmod{11^t},\\ g_{h+3} &\equiv 86\cdot 11^{t-2}+1 \pmod{11^t}. \end{aligned} \tag{3.2}$$

Proof. By (1.2), it is sufficient to prove that

$$T^{10\cdot 11^{t-2}} \equiv \begin{bmatrix} 65\cdot 11^{t-2}+1 & 90\cdot 11^{t-2} & 26\cdot 11^{t-2}\\ 26\cdot 11^{t-2} & 91\cdot 11^{t-2}+1 & 116\cdot 11^{t-2}\\ 116\cdot 11^{t-2} & 21\cdot 11^{t-2} & 86\cdot 11^{t-2}+1 \end{bmatrix} \pmod{11^t},$$

$$\text{i.e. } T^{10\cdot 11^{t-2}} \equiv E + 11^{t-2}A \pmod{11^t}, \quad \text{where } A = \begin{bmatrix} 65 & 90 & 26\\ 26 & 91 & 116\\ 116 & 21 & 86 \end{bmatrix}.$$

In the first induction step, we verify that the congruence is true for $t = 3$.

$$T^{10\cdot 11} \equiv \begin{bmatrix} 716 & 990 & 286\\ 286 & 1002 & 1276\\ 1276 & 231 & 947 \end{bmatrix} \equiv E + 11A \pmod{11^3}.$$

Suppose now that the assertion is true for a fixed $t \geq 3$ and let us prove it for $t+1$. Since A, E commute, using the binomial expansion, we obtain that $T^{10\cdot 11^{t-1}} \equiv$

$$\equiv (E + 11^{t-2}A)^{11} \equiv \sum_{i=0}^{11} \binom{11}{i} (11^{t-2}A)^i \equiv E + 11^{t-1}A + 5\cdot 11^{2t-3}A^2 \pmod{11^{t+1}}$$

and $A^2 \equiv 0 \pmod{11}$ proves (3.2). □

Consequence 3.2. Let $t \geq 1$ and $h = 10\cdot 11^{t-1}$. Then, for any modulus of the form 11^t, the following congruences hold:

$$\begin{aligned} g_{h-1} &\equiv 3\cdot 11^{t-1}-1 \pmod{11^t}, & g_h &\equiv 10\cdot 11^{t-1}+1 \pmod{11^t},\\ g_{h+1} &\equiv 4\cdot 11^{t-1} \pmod{11^t}, & g_{h+2} &\equiv 6\cdot 11^{t-1} \pmod{11^t},\\ g_{h+3} &\equiv 9\cdot 11^{t-1}+1 \pmod{11^t}. \end{aligned} \tag{3.3}$$

Proof. For $t = 1$, (3.3) can be easily verified by direct calculation. For $t \geq 2$, (3.3) follows from (3.2). □

Theorem 3.3. *For any $t \in \mathbb{N}$, we have $h(11^t)[a,b,c] | 10\cdot 11^{t-1}$ if and only if $c \equiv 3a + 5b \pmod{11}$. Moreover, for any $t > 1$, if $h(11^t)[a,b,c] | 10\cdot 11^{t-2}$ then $[a,b,c] \equiv [0,0,0] \pmod{11}$.*

Proof. Let $h(11^t)[a,b,c] | 10\cdot 11^{t-1}$. Then (3.3) implies

$$\begin{bmatrix} 10\cdot 11^{t-1}+1 & 2\cdot 11^{t-1} & 4\cdot 11^{t-1}\\ 4\cdot 11^{t-1} & 3\cdot 11^{t-1}+1 & 6\cdot 11^{t-1}\\ 6\cdot 11^{t-1} & 10\cdot 11^{t-1} & 9\cdot 11^{t-1}+1 \end{bmatrix} \begin{bmatrix} a\\ b\\ c \end{bmatrix} \equiv \begin{bmatrix} a\\ b\\ c \end{bmatrix} \pmod{11^t}.$$

A simple modification of the system yields

$$\begin{bmatrix} 10 & 2 & 4\\ 4 & 3 & 6\\ 6 & 10 & 9 \end{bmatrix} \begin{bmatrix} a\\ b\\ c \end{bmatrix} \equiv \begin{bmatrix} 0\\ 0\\ 0 \end{bmatrix} \pmod{11}.$$

The congruences of this system are linearly dependent over $\mathbb{F}_{11}$ with the entire system being equivalent to the single congruence $10a + 2b + 4c \equiv 0 \pmod{11}$. Hence, we have $c \equiv 3a + 5b \pmod{11}$.

Let $h(11^t)[a, b, c] | 10 \cdot 11^{t-2}$. The validity of the implication for $t = 2$ is not difficult to verify by direct calculation. If $t \geq 3$, then by (3.2), we have

$$\begin{bmatrix} 65 \cdot 11^{t-2} + 1 & 90 \cdot 11^{t-2} & 26 \cdot 11^{t-2} \\ 26 \cdot 11^{t-2} & 91 \cdot 11^{t-2} + 1 & 116 \cdot 11^{t-2} \\ 116 \cdot 11^{t-2} & 21 \cdot 11^{t-2} & 86 \cdot 11^{t-2} + 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \equiv \begin{bmatrix} a \\ b \\ c \end{bmatrix} \pmod{11^t}.$$

This system is equivalent to

$$\begin{bmatrix} 65 & 90 & 26 \\ 26 & 91 & 116 \\ 116 & 21 & 86 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod{11^2}.$$

The last system has exactly 121 non-congruent solutions over $\mathbb{Z}/11^2\mathbb{Z}$ that can be written as $[11r, 11s, 11(3r + 5s)]$ where r, s are integers. □

Remark 3.4. It follows from 3.3 that, if $t \geq 1$ and $[a, b, c] \not\equiv [0, 0, 0] \pmod{11}$, then $h(11^t)[a, b, c]$ is equal to some of the numbers $5 \cdot 11^{t-1}, 10 \cdot 11^{t-1}, 5 \cdot 11^t, 10 \cdot 11^t$. The following lemmas will help us determine which of the cases will occur for a given $[a, b, c]$. We will also prove that there exists no triple for which $h(11^t)[a, b, c] = 5 \cdot 11^t$.

Lemma 3.5. *For any $t \in \mathbb{N}$ we have*

$$T^{5 \cdot 11^t} \equiv A \pmod{11} \quad \textit{where} \quad A = \begin{bmatrix} 7 & 4 & 6 \\ 6 & 2 & 10 \\ 10 & 5 & 1 \end{bmatrix}. \tag{3.4}$$

Moreover, $A^{2t} \equiv E \pmod{11}$.

Proof. For $t = 1$, (3.4) is true since

$$T^{55} = \begin{bmatrix} 35731770264967 & 55158741162067 & 65720971788709 \\ 65720971788709 & 101452742053676 & 120879712950776 \\ 120879712950776 & 186600684739485 & 222332455004452 \end{bmatrix} \equiv \begin{bmatrix} 7 & 4 & 6 \\ 6 & 2 & 10 \\ 10 & 5 & 1 \end{bmatrix}.$$

Let now (3.4) be true for a fixed $t \geq 1$. Then $T^{5 \cdot 11^{t+1}} = (T^{5 \cdot 11^t})^{11} \equiv A^{11} \pmod{11}$ and it suffices to prove that $A^{11} \equiv A \pmod{11}$. Since $A^2 \equiv E \pmod{11}$, we have $A^{2t} \equiv (A^2)^t \equiv E^t \equiv E \pmod{11}$ for any $t \in \mathbb{N}$. Consequently, $A^{11} \equiv A \pmod{11}$, which proves 3.5. □

Lemma 3.6. *For any $t \in \mathbb{N}$ we have* $\det(T^{5 \cdot 11^t} - E) \equiv 0 \pmod{11^{t+1}}$.

Proof. If $t = 1$, then

$$\det(T^{55} - E) = 2 \cdot 11^2 \cdot 397 \cdot 3742083511 \equiv 0 \pmod{11^2}.$$

Let the assertion be true for a fixed $t \geq 1$. First, it is evident that $T^{5 \cdot 11^{t+1}} - E$ can be written as

$$T^{5 \cdot 11^{t+1}} - E = (T^{5 \cdot 11^t} - E) \cdot (E + T^{5 \cdot 11^t} + T^{2 \cdot 5 \cdot 11^t} + \cdots + T^{10 \cdot 5 \cdot 11^t}). \tag{3.5}$$

Now it follows from the induction hypothesis, from (3.5) and from Cauchy's theorem that it suffices to prove that

$$\det(E + T^{5 \cdot 11^t} + T^{2 \cdot 5 \cdot 11^t} + \cdots + T^{10 \cdot 5 \cdot 11^t}) \equiv 0 \pmod{11}.$$

From (3.4), it follows that

$$E + T^{5\cdot 11^t} + T^{2\cdot 5\cdot 11^t} + \cdots + T^{10\cdot 5\cdot 11^t} \equiv E + A + A^2 + \cdots + A^{10} \equiv 6E + 5A \pmod{11}.$$

As congruent matrices have congruent determinants, we have

$$\det(E + T^{5\cdot 11^t} + T^{2\cdot 5\cdot 11^t} + \cdots + T^{10\cdot 5\cdot 11^t}) \equiv \det(6E + 5A) = 132 \equiv 0 \pmod{11}.$$

This proves 3.6. □

Theorem 3.7. *For any $t \in \mathbb{N}$, the system of congruences*

$$(T^{5\cdot 11^t} - E)x \equiv 0 \pmod{11^{t+1}} \tag{3.6}$$

has exactly 11^{t+1} solutions and the number of solutions satisfying $x \not\equiv 0 \pmod{11}$ is equal to $10 \cdot 11^t$. Moreover, if α_{t+1} is a solution of $g(x) \equiv 0 \pmod{11^{t+1}}$, then each solution of (3.6) can be expressed as $[q, q\alpha_{t+1}, q\alpha_{t+1}^2]$, where $q \in \mathbb{Z}$.

Proof. Put $W = T^{5\cdot 11^t} - E \pmod{11^{t+1}}$. From (3.4) it follows that all the entries of W, except for w_{33}, are units of the ring $\mathbb{Z}/11^{t+1}\mathbb{Z}$. Since $11 \nmid \det \begin{bmatrix} 6 & 4 \\ 6 & 1 \end{bmatrix}$, there are coefficients r, s, that are also units of the ring $\mathbb{Z}/11^{t+1}\mathbb{Z}$, for which

$$r(w_{11}, w_{12}) + s(w_{21}, w_{22}) \equiv (w_{31}, w_{32}) \pmod{11^{t+1}}.$$

Thus there is a linear combination of the first and second rows of W transforming $Wx \equiv 0 \pmod{11^{t+1}}$ to an equivalent form

$$\begin{bmatrix} w_{11} & w_{12} & w_{13} \\ w_{21} & w_{22} & w_{23} \\ 0 & 0 & w'_{33} \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod{11^{t+1}}. \tag{3.7}$$

Let us now prove that $w'_{33} \equiv 0 \pmod{11^{t+1}}$. Multiplying the first row in (3.7) by a suitable unit and, subsequently, adding it to the second row yields

$$\begin{bmatrix} w_{11} & w_{12} & w_{13} \\ 0 & w'_{22} & w'_{23} \\ 0 & 0 & w'_{33} \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod{11^{t+1}}. \tag{3.8}$$

The determinant of the matrix of (3.8) is $w_{11}w'_{22}w'_{33}$ and, by Lemma 3.6, we have $w_{11}w'_{22}w'_{33} \equiv 0 \pmod{11^{t+1}}$. Now it follows from (3.4) that w_{11} and w'_{22} are units of $\mathbb{Z}/p^{t+1}\mathbb{Z}$ and thus $w'_{33} \equiv 0 \pmod{11^{t+1}}$. This implies that the system $Wx \equiv 0 \pmod{11^{t+1}}$ is equivalent to the system

$$\begin{aligned} w_{11}a + w_{12}b + w_{13}c &\equiv 0 \pmod{11^{t+1}}, \\ w_{21}a + w_{22}b + w_{23}c &\equiv 0 \pmod{11^{t+1}}, \end{aligned} \tag{3.9}$$

in which all the coefficients are units of $\mathbb{Z}/p^{t+1}\mathbb{Z}$. As no subdeterminant of the system matrix of (3.9) is divisible by 11, any of the unknowns a, b, c can be chosen as a parameter to express the other unknowns in a unique manner. Thus, each solution of $Wx \equiv 0 \pmod{11^{t+1}}$ can be written as $[qu_1, qu_2, qu_3]$ for a fixed triple of units u_1, u_2, u_3 and a parameter $q \in \mathbb{Z}$. Therefore the number of non-congruent solutions to (3.6) is equal to the number of elements of the ring $\mathbb{Z}/11^{t+1}\mathbb{Z}$, which is 11^{t+1}, and the number of solutions of the form $x \not\equiv 0 \pmod{11}$ is equal to the number of units of this ring, which is $10 \cdot 11^t$.

Let us now prove that the solutions to (3.6) are exactly the triples $[q, q\alpha_{t+1}, q\alpha_{t+1}^2]$ where $q \in \mathbb{Z}$. As the number of non-congruent triples $[q, q\alpha_{t+1}, q\alpha_{t+1}^2]$ is equal to 11^{t+1}, it suffices to show that $h(11^{t+1})[q, q\alpha_{t+1}, q\alpha_{t+1}^2] | 5 \cdot 11^t$. As $\alpha = 9$ is a simple root of $g(x) \equiv 0 \pmod{11}$, we obtain by Hensel's lemma, that for each $t \in \mathbb{N}$ there is α_t, which is uniquely determined modulo 11^t, satisfying $g(x) \equiv 0 \pmod{11^t}$ such that $\alpha_1 = \alpha$ and $\alpha_t \equiv \alpha_{t-1} \pmod{11^{t-1}}$. Let $\mathrm{ord}_{11^t}(\varepsilon)$ for $\varepsilon \not\equiv 0 \pmod{11}$ denote the order of ε in the multiplicative group of $\mathbb{Z}/11^t\mathbb{Z}$. Clearly, $h(11^{t+1})[q, q\alpha_{t+1}, q\alpha_{t+1}^2] = \mathrm{ord}_{11^{t+1}}(\alpha_{t+1})$ for any $q \in \mathbb{Z}$ where $q \not\equiv 0 \pmod{11}$. From $\mathrm{ord}_{11}(\alpha_1) = 5$ and $\alpha_{t+1} \equiv \alpha_1 \pmod{11}$ it now follows $\alpha_{t+1}^5 \equiv 1 \pmod{11}$ for any $t \in \mathbb{N}$ and thus $\alpha_{t+1}^{5\cdot 11^t} \equiv 1 \pmod{11^{t+1}}$. Hence $\mathrm{ord}_{11^{t+1}}(\alpha_{t+1}) | 5 \cdot 11^t$. □

According to Theorem 3.7, the set of all non-congruent solutions to (3.6) can be written as $E(\alpha_{t+1}) = \{[q, q\alpha_{t+1}, q\alpha_{t+1}^2], q \in \mathbb{Z}/p^{t+1}\mathbb{Z}\}$ and viewed as the eigenspace associated with the eigenvalue α_{t+1}.

Remark 3.8. The equality $\mathrm{ord}_{11^t}(\alpha_t) = 5 \cdot 11^{t-1}$ is a non-trivial consequence of 3.3 and 3.7 for each $t \in \mathbb{N}$. See also Lemma 4.6 in [1].

Lemma 3.9. *There exists no triple $[a, b, c]$ for which $h(11^t)[a, b, c] = 5 \cdot 11^t$.*

Proof. It suffices to prove that the systems $(T^{5\cdot 11^{t-1}} - E)x \equiv 0 \pmod{11^t}$ and $(T^{5\cdot 11^t} - E)x \equiv 0 \pmod{11^t}$ have identical solution sets for any $t \geq 1$. Denote by X the set of all solutions of $(T^{5\cdot 11^{t-1}} - E)x \equiv 0 \pmod{11^t}$ and by Y the set of all solutions of $(T^{5\cdot 11^t} - E)x \equiv 0 \pmod{11^t}$. The inclusion $X \subseteq Y$ follows immediately from the equality

$$T^{5\cdot 11^t} - E = (E + T^{5\cdot 11^{t-1}} + T^{2\cdot 5\cdot 11^{t-1}} + \cdots + T^{10\cdot 5\cdot 11^{t-1}}) \cdot (T^{5\cdot 11^{t-1}} - E).$$

Modifying the proof of 3.7, we can determine that $(T^{5\cdot 11^t} - E)x \equiv 0 \pmod{11^t}$ has 11^t solutions, thus the same number as $(T^{5\cdot 11^{t-1}} - E)x \equiv 0 \pmod{11^t}$. The equality of the sets X and Y follows from their finiteness. □

Now we can summarize our results in the main theorem:

Theorem 3.10. *For any triple* $[a, b, c] \not\equiv [0, 0, 0] \pmod{11}$*, we have:*
If $[a, b, c] \notin E(\alpha_t)$ *and* $c \equiv 3a + 5b \pmod{11}$*, then* $h(11^t)[a, b, c] = 10 \cdot 11^{t-1}$.
If $[a, b, c] \notin E(\alpha_t)$ *and* $c \not\equiv 3a + 5b \pmod{11}$*, then* $h(11^t)[a, b, c] = 10 \cdot 11^t$.
If $[a, b, c] \in E(\alpha_t)$*, then* $h(11^t)[a, b, c] = \mathrm{ord}_{11^t}(\alpha_t) = 5 \cdot 11^{t-1}$.

References

[1] J. Klaška, *Tribonacci modulo p^t*, Mathematica Bohemica **133.3** (2008), 267–288.
[2] A. Vince, *Period of a linear recurrence*, Acta Arithmetica **39** (1981), 303–311.
[3] M. E. Waddill, *Some Properties of a generalized Fibonacci sequence modulo m*, The Fibonacci Quarterly **16.4** (1978), 344–353.

Keywords: Tribonacci, modular periodicity, periodic sequence

MSC 2000: 11B50, 11B39

CHAPTER 6

ON TRIBONACCI-WIEFERICH PRIMES ⋆

Abstract. The problem of the existence of Fibonacci-Wieferich primes has already been investigated by many authors. In this paper we shall study a similar problem for the sequence of Tribonacci numbers. Using matrix algebra, we find certain equivalent formulations of this problem and also derive some criteria that can be used to effectively test particular primes. A computer search showed that the problem has no solution for primes $p \leq 10^9$.

1. Introduction

Let $(F_n)_{n=0}^{\infty}$ be the Fibonacci sequence defined by $F_{n+2} = F_{n+1} + F_n$ with $F_0 = 0$ and $F_1 = 1$. It is well known [9, p. 525] that $(F_n \bmod m)_{n=0}^{\infty}$ is periodic for any modulus $m > 1$. Let $k(m)$ denote the period of $(F_n \bmod m)_{n=0}^{\infty}$. That is, $k(m)$ is the least positive integer such that $F_{k(m)} \equiv 0$ and $F_{k(m)+1} \equiv 1 \pmod{m}$. In 1960, D. D. Wall [9, Theorem 5] proved that for any prime p, we have: if $k(p) = k(p^s) \neq k(p^{s+1})$, then $k(p^t) = p^{t-s}k(p)$ for $t \geq s$. Wall [9, p. 528] asked whether $k(p) = k(p^2)$ is always impossible. This problem has not yet been resolved. The primes p satisfying the relation $k(p) = k(p^2)$ are often referred to as Wall-Sun-Sun primes [1] or as Fibonacci-Wieferich primes [5].

Finding an answer to Wall's question can be extremely difficult. In 1992, Zhi-Hong Sun and Zhi-Wei Sun [6] showed that, if $p \nmid xyz$ and $x^p + y^p = z^p$, then $k(p) = k(p^2)$. Consequently, an affirmative answer to Wall's question implies the first case of Fermat's last theorem. From this point of view, there is a similarity to the well-known Wieferich primes. Recall that an odd prime p is called Wieferich if $2^{p-1} \equiv 1 \pmod{p^2}$. In 1909, A. Wieferich [10] proved that, if $p \nmid xyz$ and $x^p + y^p = z^p$, then $2^{p-1} \equiv 1 \pmod{p^2}$. The only Wieferich primes known are 1093 and 3511; this has been verified up to 1.25×10^{15} [3].

In this paper we focus on a similar problem related to the Tribonacci sequence. Recall that the Tribonacci sequence $(T_n)_{n=0}^{\infty}$ is defined by $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ with $T_0 = 0$, $T_1 = 0, T_2 = 1$. It is well known [8, Theorem 1] that $(T_n \bmod m)_{n=0}^{\infty}$ is periodic. Let $h(m)$ denote the period of $(T_n \bmod m)_{n=0}^{\infty}$. In [8, pp. 349–351], M. E. Waddill proved that, if $h(p) = h(p^s) \neq h(p^{s+1})$, then $h(p^t) = p^{t-s}h(p)$ for $t \geq s$. By analogy with the Fibonacci case, the primes p satisfying $h(p) = h(p^2)$ may be called Tribonacci-Wieferich primes. Up to the present, no instance of $h(p) = h(p^2)$ has been found, and it is an open question whether $h(p) = h(p^2)$ never appears.

⋆ Published in J. Klaška, *On Tribonacci-Wieferich primes*, The Fibonacci Quarterly **46/47** (2008/2009), 290–297.

2. Matrix characterization of $h(p) = h(p^2)$

The Tribonacci numbers T_n can be computed by taking the powers of the Tribonacci companion matrix T. If

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \quad \text{then} \quad T^n = \begin{bmatrix} T_{n-1} & T_{n-2} + T_{n-1} & T_n \\ T_n & T_{n-1} + T_n & T_{n+1} \\ T_{n+1} & T_n + T_{n+1} & T_{n+2} \end{bmatrix} \quad \text{for } n > 1. \tag{2.1}$$

Clearly, $h(p)$ is the period of $(T_n \bmod p)_{n=0}^{\infty}$ if and only if $h(p)$ is the smallest positive integer h for which $T^h \equiv E \pmod p$ and $h(p^2)$ is the period of $(T_n \bmod p^2)_{n=0}^{\infty}$ if and only if $h(p^2)$ is the smallest positive integer k satisfying $T^k \equiv E \pmod{p^2}$ where E is the 3×3 identity matrix. For any prime p we define an integer matrix $A_p = [a_{ij}]$ such that

$$A_p = \frac{1}{p}(T^{h(p)} - E). \tag{2.2}$$

From (2.1) it follows now that

$$A_p = \begin{bmatrix} a_{11} & a_{31} - a_{21} & a_{21} \\ a_{21} & a_{11} + a_{21} & a_{31} \\ a_{31} & a_{21} + a_{31} & a_{11} + a_{21} + a_{31} \end{bmatrix}. \tag{2.3}$$

Lemma 2.1. *For any prime p, we have $h(p) \neq h(p^2)$ if and only if $A_p \not\equiv 0 \pmod p$.*

Proof. This follows from (2.2). ☐

Lemma 2.2. *For any prime p, the elements a_{11}, a_{21}, a_{31} in (2.3) satisfy*

$$3a_{11} + 2a_{21} + a_{31} \equiv 0 \pmod p. \tag{2.4}$$

Proof. From (2.2) and (2.3), we obtain that

$$\det T^{h(p)} \equiv 1 + p(3a_{11} + 2a_{21} + a_{31}) \pmod{p^2}$$

and the lemma follows from $\det T = 1$. ☐

From (2.3) and (2.4) it follows that the elements of A_p mod p can be expressed by means of a_{11}, a_{21} alone. Of course, if $A_p \equiv 0 \pmod p$, then $\det A_p \equiv 0 \pmod p$. On the other hand, we have the following proposition.

Proposition 2.3. *Let $p \neq 2$. If $\det A_p \equiv 0 \pmod p$ and $A_p \not\equiv 0 \pmod p$, then there is an $\varepsilon \in \mathbb{Z}$ such that*

$$7\varepsilon^3 + 29\varepsilon^2 + 39\varepsilon + 19 \equiv 0 \pmod p \quad \text{and} \quad a_{21} \equiv a_{11}\varepsilon \pmod p.$$

Proof. Using (2.3) and (2.4), we obtain after some simplification

$$\det A_p \equiv -(38a_{11}^3 + 78a_{11}^2 a_{21} + 58a_{11}a_{21}^2 + 14a_{21}^3) \pmod p. \tag{2.5}$$

Suppose $p | a_{11}$ and $p \nmid a_{21}$. Then, from (2.5), we have $\det A_p \equiv -14a_{21}^3 \pmod p$ and thus $14 \equiv 0 \pmod p$. As $p \neq 2$, we have $p = 7$. We can verify that $h(7) = 48$. Then, for A_7, we have

$$A_7 = \frac{1}{7}(T^{48} - E) \equiv \begin{bmatrix} 4 & 2 & 0 \\ 0 & 4 & 2 \\ 2 & 2 & 6 \end{bmatrix} \pmod 7.$$

Hence, $a_{11} \equiv 4 \pmod 7$, which is a contradiction to $p|a_{11}$. Consequently, there is an $\varepsilon \in \mathbb{Z}$ such that $a_{21} \equiv a_{11}\varepsilon \pmod p$. From (2.5) it now follows that

$$\det A_p \equiv -a_{11}^3(14\varepsilon^3 + 58\varepsilon^2 + 78\varepsilon + 38) \pmod p. \tag{2.6}$$

Since $p \nmid a_{11}$, $p \neq 2$ and $p|\det A_p$, it follows from (2.6) that

$$7\varepsilon^3 + 29\varepsilon^2 + 39\varepsilon + 19 \equiv 0 \pmod p.$$

□

Let L_p be the splitting field of the Tribonacci characteristic polynomial $t(x) = x^3 - x^2 - x - 1$ over the field of p-adic numbers $\mathbb{Q}_p$ and let α, β, γ be the roots of $t(x)$ in L_p. Clearly, α, β, γ are in the ring O_p of integers of the field L_p. By a simple calculation we find that the discriminant of $t(x)$ is $\triangle t(x) = -44$. See also [7, p. 310]. This implies that $L_p/\mathbb{Q}_p$ does not ramify for $p \neq 2, 11$ and so the maximal ideal of O_p is generated by p. Finally, for a unit $u \in O_p$, we denote by $\mathrm{ord}_{p^t}(u)$ the least positive rational integer k such that $u^k \equiv 1 (\mathrm{mod}\ p^t)$. As $u^k \equiv 1 \pmod p$ implies $u^{pk} \equiv 1 \pmod{p^2}$, we have either $\mathrm{ord}_{p^2}(u) = \mathrm{ord}_p(u)$ or $\mathrm{ord}_{p^2}(u) = p \cdot \mathrm{ord}_p(u)$.

Theorem 2.4. *Let $p \neq 2, 11$. Then, for any $t \in \mathbb{N}$, we have*

$$h(p^t) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta), \mathrm{ord}_{p^t}(\gamma)). \tag{2.7}$$

Proof. Over L_p, we can write $T_n = A\alpha^n + B\beta^n + C\gamma^n$ for suitable $A, B, C \in L_p$. The coefficients A, B, C are uniquely determined by the system of equations $A + B + C = 0$, $A\alpha + B\beta + C\gamma = 0$ and $A\alpha^2 + B\beta^2 + C\gamma^2 = 1$ over L_p. The determinant of the matrix of this system is equal to $(\alpha - \beta)(\alpha - \gamma)(\gamma - \beta)$. As $\alpha \not\equiv \beta (\mathrm{mod}\ p)$, $\alpha \not\equiv \gamma (\mathrm{mod}\ p)$ and $\beta \not\equiv \gamma (\mathrm{mod}\ p)$, Cramer's rule gives $A = [(\alpha - \beta)(\alpha - \gamma)]^{-1}$, $B = [(\alpha - \beta)(\gamma - \beta)]^{-1}$, $C = -[(\alpha - \gamma)(\gamma - \beta)]^{-1}$. Moreover, A, B, C are units in O_p. Let $k = h(p^t)$. Then $[A\alpha^k + B\beta^k + C\gamma^k, A\alpha^{k+1} + B\beta^{k+1} + C\gamma^{k+1}, A\alpha^{k+2} + B\beta^{k+2} + C\gamma^{k+2}] \equiv [A + B + C, A\alpha + B\beta + C\gamma, A\alpha^2 + B\beta^2 + C\gamma^2] (\mathrm{mod}\ p^t)$. This system can be reduced to the equivalent form

$$\begin{bmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{bmatrix} \begin{bmatrix} A(\alpha^k - 1) \\ B(\beta^k - 1) \\ C(\gamma^k - 1) \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod{p^t}. \tag{2.8}$$

As the determinant of the matrix in (2.8) is not divisible by p, (2.10) has only one solution

$$A(\alpha^k - 1) \equiv 0 \pmod{p^t},\ B(\beta^k - 1) \equiv 0 \pmod{p^t},\ C(\gamma^k - 1) \equiv 0 \pmod{p^t}.$$

This implies $\alpha^k \equiv 1 \pmod{p^t}$, $\beta^k \equiv 1 \pmod{p^t}$ and $\gamma^k \equiv 1 \pmod{p^t}$. Thus, we have $\mathrm{ord}_{p^t}(\alpha)|k$, $\mathrm{ord}_{p^t}(\beta)|k$ and $\mathrm{ord}_{p^t}(\gamma)|k$, which implies

$$\mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta), \mathrm{ord}_{p^t}(\gamma))|k.$$

As A, B, C are not divisible by p, the periods of $(A\alpha^n \bmod p^t)_{n=0}^\infty$, $(B\beta^n \bmod p^t)_{n=0}^\infty$ and $(C\gamma^n \bmod p^t)_{n=0}^\infty$ are $\mathrm{ord}_{p^t}(\alpha)$, $\mathrm{ord}_{p^t}(\beta)$ and $\mathrm{ord}_{p^t}(\gamma)$. Consequently, the period k of $(A\alpha^n + B\beta^n + C\gamma^n \bmod p^t)_{n=0}^\infty$ divides $\mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta), \mathrm{ord}_{p^t}(\gamma))$ and the theorem follows. □

Remark 2.5. If $p \neq 2, 11$ then $O_p/(p)$ is the field with $p^{[L_p:\mathbb{Q}_p]}$ elements where $[L_p : \mathbb{Q}_p] \in \{1, 2, 3\}$. Thus, for any $\lambda \in \{\alpha, \beta, \gamma\}$, $\mathrm{ord}_p(\lambda)|p^{[L_p:\mathbb{Q}_p]} - 1$, and by (2.7), we have $h(p)|p^{[L_p:\mathbb{Q}_p]} - 1$. This implies that, for any prime $p \neq 2, 11$, $h(p) \not\equiv 0 \pmod p$. If $p = 2, 11$, then $h(p) \equiv 0 \pmod p$. Exactly, $h(2^t) = 2^{t+1}$ and $h(11^t) = 10 \cdot 11^t$ for any $t \in \mathbb{N}$.

Lemma 2.6. *For any prime $p \neq 2, 11$, we have $A_p \equiv 0 \pmod{p}$ if and only if $\mathrm{ord}_{p^2}(\lambda) \not\equiv 0 \pmod{p}$ for each $\lambda \in \{\alpha, \beta, \gamma\}$.*

Proof. From Lemma 2.1 it follows that $A_p \equiv 0 \pmod{p}$ if and only if $h(p) = h(p^2)$. As $p \neq 2, 11$, by Remark 2.5, we have $p \nmid h(p)$, which, together with (2.7), yields $h(p) = h(p^2)$ if and only if $\mathrm{lcm}(\mathrm{ord}_{p^2}(\alpha), \mathrm{ord}_{p^2}(\beta), \mathrm{ord}_{p^2}(\gamma)) \not\equiv 0 \pmod{p}$. □

Lemma 2.7. *Let $p \neq 2, 11$. Then $\mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta)) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\gamma)) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\beta), \mathrm{ord}_{p^t}(\gamma)) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta), \mathrm{ord}_{p^t}(\gamma))$ for any $t \in \mathbb{N}$.*

Proof. This follows from the Viète equation $\alpha\beta\gamma = 1$. □

Theorem 2.8. *Let $p \neq 2, 11$ and $A_p \not\equiv 0 \pmod{p}$. Then $\det A_p \equiv 0 \pmod{p}$ if and only if there is a unique $\lambda \in \{\alpha, \beta, \gamma\}$ for which $\mathrm{ord}_{p^2}(\lambda) \not\equiv 0 \pmod{p}$. Moreover, for this λ, we have $\lambda \in \mathbb{Z}_p$ where $\mathbb{Z}_p$ is the ring of p-adic integers.*

Proof. Over the field L_p, the Tribonacci matrix T is similar to the diagonal matrix D with α, β, γ on the diagonal. Thus, an invertible matrix H exists such that $T = HDH^{-1}$ and thus $T^h = HD^hH^{-1}$ where $h = h(p)$. On the other hand, $T^h = E + pA_p$ where $A_p \not\equiv 0 \pmod{p}$. If we combine these two expressions, we have $E + pA_p = HD^hH^{-1}$, which implies $pH^{-1}A_pH = D^h - E$. By the well-known properties of determinants, we easily obtain that

$$p^3 \cdot \det A_p = (\alpha^h - 1)(\beta^h - 1)(\gamma^h - 1). \tag{2.9}$$

Let $\det A_p \equiv 0 \pmod{p}$. From (2.7) and (2.9), it now follows that at least one of the differences $\alpha^h - 1, \beta^h - 1, \gamma^h - 1$ is divisible by p^2. Consequently, for at least one $\lambda \in \{\alpha, \beta, \gamma\}$, we have $\mathrm{ord}_{p^2}(\lambda) \not\equiv 0 \pmod{p}$. Since $A_p \not\equiv 0 \pmod{p}$, it follows from Lemmas 2.6 and 2.7 that this λ is unique. Without loss of generality, we can assume $\lambda = \alpha$. Suppose that $\alpha \notin \mathbb{Z}_p$. The Galois group $\mathrm{Gal}(L_p/\mathbb{Q}_p)$ is cyclic, generated by the Frobenius automorphism σ. Then $\alpha^\sigma \neq \alpha$ and so $\alpha^\sigma \in \{\beta, \gamma\}$, say $\alpha^\sigma = \beta$. Then $\mathrm{ord}_{p^2}(\beta) = \mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$, which is a contradiction as α is the unique root with this property.

Conversely, let α be the unique $\lambda \in \{\alpha, \beta, \gamma\}$ such that $\mathrm{ord}_{p^2}(\lambda) \not\equiv 0 \pmod{p}$. Consequently, we have $\mathrm{ord}_{p^2}(\alpha) = \mathrm{ord}_p(\alpha)$. Put $r = \mathrm{ord}_p(\alpha)$. Then we have $p^2 | \alpha^r - 1$ in O_p. From (2.7), it follows that $r | h$ and thus $p^2 | \alpha^h - 1$ in O_p. Further from (2.7), it follows that $p | \beta^h - 1$ and $p | \gamma^h - 1$. If we combine these facts, we obtain $p^4 | (\alpha^h - 1)(\beta^h - 1)(\gamma^h - 1)$. From (2.9), it now follows that $\det A_p \equiv 0 \pmod{p}$. □

Corollary 2.9. *Let $t(x)$ be irreducible over $\mathbb{Q}_p$. Then we have*

$$A_p \equiv 0 \pmod{p} \quad \textit{if and only if} \quad \det A_p \equiv 0 \pmod{p}. \tag{2.10}$$

Proof. If $t(x)$ is irreducible over $\mathbb{Q}_p$, then there is no root of $t(x)$ in $\mathbb{Z}_p$. □

Corollary 2.10. *Let $p \neq 2, 11$. Then $\det A_p \equiv 0 \pmod{p}$ if and only if there is at least one $\lambda \in \{\alpha, \beta, \gamma\}$ such that $\mathrm{ord}_{p^2}(\lambda) \not\equiv 0 \pmod{p}$.*

Proof. This follows from Theorem 2.8 and Lemma 2.6. □

Our results can be summarized in the following theorem.

Theorem 2.11. *Let $p \neq 2, 11$ and let k be the number of roots α, β, γ of $t(x)$ in O_p whose order modulo p^2 is divisible by p. Then the following cases may occur:*

Case $k = 0$: $h(p) = h(p^2)$, or equivalently $A_p \equiv 0 \pmod{p}$.

Case $k = 1$: This case is impossible.
Case $k = 2$: $h(p) \neq h(p^2)$ and $\det A_p \equiv 0 \pmod{p}$.
Case $k = 3$: $h(p) \neq h(p^2)$ and $\det A_p \not\equiv 0 \pmod{p}$.

Proof. Theorem 2.4 gives that $k = 0$ if and only if $h(p) = h(p^2)$. Lemma 2.1 states that $h(p) = h(p^2)$ if and only if $A_p \equiv 0 \pmod{p}$. Using Lemma 2.7, we see that the case $k = 1$ is impossible and Theorem 2.8 distinguishes the remaining two cases. □

A natural question arises whether there is a prime p satisfying $k = 2$. Since the solution of this question seems to be as difficult as the question whether $h(p) \neq h(p^2)$ for all primes p, we state it as

Problem 2.12. Decide whether there is a prime p for which $h(p) \neq h(p^2)$ and $\mathrm{ord}_p(\alpha) = \mathrm{ord}_{p^2}(\alpha)$ where $\alpha \in \mathbb{Z}$ is a solution of $x^3 - x^2 - x - 1 \equiv 0 \pmod{p^2}$. The prime p satisfying this conditions may be called Tribonacci-Wieferich prime of the second kind.

3. Criteria for testing Tribonacci-Wieferich primes

In this section we derive two interesting criteria that can be used, without computing the roots of $t(x)$ in O_p, to decide whether $h(p) = h(p^2)$ or not. Let $p \neq 2, 11$. Put $q = |O_p/(p)|$. By Remark 2.5, $q = p^t$ where $t = [L_p : \mathbb{Q}_p] \in \{1, 2, 3\}$. For proofs of our criteria, we shall need the following lemma.

Lemma 3.1. *Let $p \neq 2, 11$. Then, for a unit $u \in O_p$, we have*

$$\mathrm{ord}_{p^2}(u) \not\equiv 0 \pmod{p} \quad \text{if and only if} \quad u^{q-1} \equiv 1 \pmod{p^2}. \tag{3.1}$$

Proof. Put $s = \mathrm{ord}_{p^2}(u)$. Clearly, $[O_p/(p^2)]^\times$ has $q(q-1)$ elements and so $s | q(q-1)$. Let $p \nmid s$. As $q = p^t$, we have $s | q - 1$ and $u^{q-1} \equiv 1 \pmod{p^2}$ follows. On the other hand, let $u^{q-1} \equiv 1 \pmod{p^2}$. Then $s | q-1$. As $p \nmid q - 1$, we have $\mathrm{ord}_{p^2}(u) \not\equiv 0 \pmod{p}$. □

Now we are ready for the following theorem.

Theorem 3.2. *Let $p \neq 2, 11$, $u \in O_p$ such that $t(u) \equiv 0 \pmod{p}$. Let $t(x)$ be irreducible over $\mathbb{Q}_p$. Then the following statements are equivalent:*

(i) $h(p) = h(p^2)$,
(ii) $u^{3q} - u^{2q} - u^q - 1 \equiv 0 \pmod{p^2}$.

Proof. Let $u \in O_p$, $t(u) \equiv 0 \pmod{p}$. Then we have $u \equiv \alpha \pmod{p}$ or $u \equiv \beta \pmod{p}$ or $u \equiv \gamma \pmod{p}$. We can assume $u \equiv \alpha \pmod{p}$. Then $u^q \equiv \alpha^q \pmod{p^2}$. If $h(p) = h(p^2)$, then $u^q \equiv \alpha^q \equiv \alpha \pmod{p^2}$ and $u^{3q} - u^{2q} - u^q - 1 \equiv \alpha^3 - \alpha^2 - \alpha - 1 = 0 \pmod{p^2}$. On the other hand, assume $u^{3q} - u^{2q} - u^q - 1 \equiv 0 \pmod{p^2}$. Let $u^q = \alpha + pv$. Then $(\alpha + pv)^3 - (\alpha + pv)^2 - (\alpha + pv) - 1 \equiv pv(3\alpha^2 - 2\alpha - 1) \equiv pv \cdot t'(\alpha) \equiv 0 \pmod{p^2}$. Now $p \neq 2, 11$ implies $t'(\alpha) \not\equiv 0 \pmod{p}$ and so $v \equiv 0 \pmod{p}$. Consequently, $u^q \equiv \alpha \pmod{p^2}$ and $\alpha^{q-1} \equiv u^{q(q-1)} \equiv 1 \pmod{p^2}$. This, together with Lemma 3.1, yields $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 (\mathrm{mod}\ p)$ and, by Corollary 2.10, we have $\det A_p \equiv 0 \pmod{p}$. As $t(x)$ is irreducible over $\mathbb{Q}_p$, Corollary 2.9 yields $A_p \equiv 0 \pmod{p}$ and $h(p) = h(p^2)$ follows using Lemma 2.1. □

Theorem 3.3. *Let $p \neq 2, 11$, $u \in O_p$ such that $t(u) \equiv 0 \pmod{p}$. Suppose that $t(x)$ is irreducible over $\mathbb{Q}_p$. Then the following statements are equivalent:*

(i) $h(p) = h(p^2)$,

(ii) $t(u) + (u^q - u)t'(u) \equiv 0 \pmod{p^2}$,
(iii) $3u^{q+2} - 2u^{q+1} - u^q - 2u^3 + u^2 - 1 \equiv 0 \pmod{p^2}$,

where t' is the derivative of the Tribonacci characteristic polynomial t.

Proof. Let α, β, γ are the roots of $t(x)$ in O_p and let $u \in O_p$, $t(u) \equiv 0 \pmod{p}$. We can assume $u \equiv \alpha \pmod{p}$. Let $u = \alpha + pw$. Then (ii) is equivalent to

$$(\alpha^q - \alpha)(t'(\alpha) + pw \cdot t''(\alpha)) \equiv 0 \pmod{p^2}. \tag{3.2}$$

If $h(p) = h(p^2)$, then by Lemmas 2.1 and 2.6 we have $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ which, together with Lemma 3.1, yields $\alpha^q \equiv \alpha \pmod{p^2}$ and (3.2) follows. Conversely, assume (3.2). As $p \neq 2, 11$, we have $t'(\alpha) + pw \cdot t''(\alpha) = 3\alpha^2 - 2\alpha - 1 + 6\alpha pw - 2\alpha \equiv 3(\alpha + pw)^2 - 2(\alpha + pw) - 1 \equiv f'(u) \not\equiv 0 \pmod{p}$. Consequently, (3.2) yields $\alpha^q - \alpha \equiv 0 \pmod{p^2}$. Using Lemma 3.1 and Corollary 2.10, we have $\det A_p \equiv 0 \pmod{p}$ and the irreducibility of $t(x)$ yields $A_p \equiv 0 \pmod{p}$ by (2.10). This, together with Lemma 2.1, implies $h(p) = h(p^2)$ as required. Finally, by expansion of (ii) we obtain (iii) and the proof is finished. □

Remark 3.4. The result of Theorem 3.3, part (iii), is similar to that found by Li [4, p. 83] for a Fibonacci sequence.

Remark 3.5. Theorems 3.2 and 3.3 have been proved on the assumption that $t(x)$ is irreducible over $\mathbb{Q}_p$. Let us now discuss the case of this assumption not being fulfilled. Clearly, the proofs of the $(i) \Rightarrow (ii)$ implications of both theorems remain valid even if the assumption of irreducibility of $t(x)$ is omitted. When proving the reverse $(ii) \Rightarrow (i)$ implication, the following two cases may occur.

If α is the unique root with the property $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ then, by Lemma 2.6, we have $A_p \not\equiv 0 \pmod{p}$ and thus $h(p) \neq h(p^2)$. By Theorem 2.8, we have $\det A_p \equiv 0 \pmod{p}$. Consequently, p is a Tribonacci-Wieferich prime of the second kind. In the opposite case, Lemma 2.6 and Lemma 2.7 yield $A_p \equiv 0 \pmod{p}$, and $h(p) = h(p^2)$ follows.

4. Computer investigation of Tribonacci-Wieferich primes

In addition to the main result formulated in Theorem 4.3, our computer search for the Tribonacci-Wieferich primes brought an interesting discovery.

Let I denote the set of all primes for which $t(x)$ is irreducible over $\mathbb{Q}_p$ and $I(x)$ be the number of all $p \in I$, $p \leq x$. Further, let Q denote the set of all primes p for which $t(x)$ is factorized over $\mathbb{Q}_p$ into a product of a linear factor and a quadratic irreducible factor, and $Q(x)$ be the number of all $p \in Q$, $p \leq x$. Finally, let L denote the set of all primes p for which $t(x)$ is factorized over $\mathbb{Q}_p$ into linear factors and $L(x)$ be the number of all $p \in L$, $p \leq x$. Clearly, $I \cup Q \cup L$ is the set of all primes and I, Q, L are pairwise disjoint. Consequently, $I(x) + Q(x) + L(x) = \pi(x)$ where $\pi(x)$ is the number of all primes p not exceding x. Note that $2 \in I$ and $11 \in Q$. The result of our computer examination of the exact values $I(x), Q(x), L(x)$ is summarized in the following table.

x	$I(x)$	$Q(x)$	$L(x)$	$\pi(x)$
10^2	11	12	2	25
10^3	59	84	25	168
10^4	412	616	201	1229
10^5	3212	4805	1575	9592
10^6	26135	39305	13058	78498
10^7	221524	332459	110596	664579
10^8	1920148	2881402	959905	5761455
10^9	16949462	25425162	8472910	50847534

(4.1)

Table 1.

From Table 1, we can see that, approximately, we have

$$I(x) : Q(x) : L(x) \approx 2 : 3 : 1. \tag{4.2}$$

Recall now that a subset A of the set of all primes has a natural density $d(A)$ if

$$d(A) = \lim_{x\to\infty} \frac{|\{p \in A; p \le x\}|}{\pi(x)}. \tag{4.3}$$

Using the Frobenius density theorem [2], we can prove that $d(I) = 1/3$, $d(Q) = 1/2$, and $d(L) = 1/6$. Thus we can formulate

Theorem 4.1. *For $d(I), d(Q), d(L)$ we have $d(I) : d(Q) : d(L) = 2 : 3 : 1$.*

This means that our computer observation (4.2) is a consequence of Theorem 4.1.

Remark 4.2. An interesting question is whether for some primes, the chance that they are Tribonacci-Wieferich is greater than for the others. This is supported by the fact that the following assertion holds: If $q = p^{[L_p:\mathbb{Q}_p]}$, then in the multiplicative group $[O_p/(p^2)]^\times$ there exist exactly $q-1$ elements α satisfying $\alpha^{q-1} \equiv 1 \pmod{p^2}$. Consequently, the number of $\alpha \in [O_p/(p^2)]^\times$ satisfying $\alpha^{q-1} \equiv 1 \pmod{p^2}$ strongly depends on the form of factorization of $t(x)$ over $\mathbb{Q}_p$. Supposing that the images of the roots α, β, γ in $[O_p/(p^2)]^\times$ are randomly distributed (such as when rolling a die) the probability strongly depends on which of the sets I, Q, L the prime p belongs to. A similar reasoning for the case of a Fibonacci sequence would lead to an interesting conclusion that the probability of finding the first Fibonacci-Wieferich prime is much greater for primes ending with the digits 1 or 9.

Now we state the main theorem. By means of an extensive computer search we have obtained the following two results:

Theorem 4.3. (i) *There is no Tribonacci-Wieferich prime $p < 10^9$.* (ii) *There is no Tribonacci-Wieferich prime of the second kind $p < 10^9$.*

Remark 4.4. By analogy with Problem 2.12, we can consider a similar problem for a Tetranacci sequence $(M_n)_{n=0}^{\infty}$ defined by $M_{n+4} = M_{n+3} + M_{n+2} + M_{n+1} + M_n$ with $M_0 = M_1 = M_2 = 0$ and $M_3 = 1$. Now, let $h(m)$ denote a period of $(M_n \bmod m)_{n=0}^{\infty}$. Is there a prime p for which $h(p) \ne h(p^2)$ and $\mathrm{ord}_p(\alpha) = \mathrm{ord}_{p^2}(\alpha)$ where $\alpha \in \mathbb{Z}$ is a solution of $x^4 - x^3 - x^2 - x - 1 \equiv 0 \pmod{p^2}$? To this problem we find the following solution.

Theorem 4.5. *For $p < 10^9$, there are exactly three Tetranacci-Wieferich primes of the second kind: $p_1 = 17$, $p_2 = 191$, and $p_3 = 11351$.*

References

[1] R. Crandall, K. Dilcher, C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 443–449.

[2] F. G. Frobenius, *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe*, Sitzungsberichte Königl. Preußisch. Akad. Wissenschaft. Berlin, (1896), 689–703; Gesammelte Abhandlungen II, Springer Berlin (1968), 719–733.

[3] J. Knauer, J. Richstein, *The continuing search for Wieferich primes*, Math. Comp. **74** (2005), 1559–1563.

[4] Hua-Chieh Li, *Fibonacci primitive roots and Wall's question*, The Fibonacci Quarterly **37** (1999), 77–84.

[5] R. J. McIntosh, E. L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp. **76** (2007), 2087–2094.

[6] Zhi-Hong Sun, Zhi-Wei Sun, *Fibonacci Numbers and Fermat's Last Theorem*, Acta Arith. **60** (1992), 371–388.

[7] A. Vince, *Period of a Linear Recurrence*, Acta Arith. **39** (1981), 303–311.

[8] M. E. Waddill, *Some Properties of a Generalized Fibonacci Sequence Modulo m*, The Fibonacci Quarterly **16** (1978), 344–353.

[9] D. D. Wall, *Fibonacci Series Modulo m*, Amer. Math. Monthly **67** (1960), 525–532.

[10] A. Wieferich, *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math. **136** (1909), 293–302.

AMS Classification Numbers: 11B50, 11B39, 11A07

CHAPTER 7

A SEARCH FOR TRIBONACCI - WIEFERICH PRIMES★

Abstract. Such problems as the search for Wieferich primes or Wall-Sun-Sun primes are intensively studied and often discussed at present. This paper is devoted to a similar problem related to the Tribonacci numbers.

1. Introduction

Let T_n denote the n-th Tribonacci number defined by $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ with $T_0 = 0$, $T_1 = 0$, and $T_2 = 1$. Tribonacci numbers has been examined by many authors. First by A. Agronomof [1] in 1914 and subsequently by many others. See, for example, [2], [5], [7], [8], [9], [10]. It is well known that $(T_n \bmod m)_{n=0}^{\infty}$ is periodic for any modulus $m > 1$. The least positive integer h satisfying $[T_h, T_{h+1}, T_{h+2}] \equiv [T_0, T_1, T_2] \pmod{m}$ is called a period of $(T_n \bmod m)_{n=0}^{\infty}$ and denoted by $h(m)$.

Two problems remain open: 1. Is there a prime p satisfying $h(p) = h(p^2)$ (M. E. Waddill 1978, [10])? 2. Is there a prime p such that $h(p) \neq h(p^2)$ and $\mathrm{ord}_p(\alpha) = \mathrm{ord}_{p^2}(\alpha)$ where $\alpha \in \mathbb{Z}$ is a solution of $x^3 - x^2 - x - 1 \equiv 0 \pmod{p^2}$ (J. Klaška 2007, [5])? Here, $\mathrm{ord}_{p^t}(\alpha)$ denotes the order of α in the multiplicative group of the ring $\mathbb{Z}/p^t\mathbb{Z}$, $t \in \mathbb{N}$. See also [6, Problem 3.2]. In [6], the primes p satisfying $h(p) = h(p^2)$ are called Tribonacci - Wieferich primes and the primes for which $h(p^2) \neq h(p)$ and $\mathrm{ord}_p(\alpha) = \mathrm{ord}_{p^2}(\alpha)$ where $\alpha \in \mathbb{Z}$ is a solution of $x^3 - x^2 - x - 1 \equiv 0 \pmod{p^2}$ are called Tribonacci-Wieferich primes of the second kind. In [6] we proved that neither of this problems has a solution for $p < 10^9$. In the present paper we substantially extend these results focussing on the case of the Tribonacci characteristic polynomial $t(x) = x^3 - x^2 - x - 1$ being irreducible modulo p.

2. Tribonacci modulo p^2 - an irreducible case

Let $I = \{3, 5, 23, 31, \dots\}$ be the set of all primes p for which $t(x)$ is irreducible over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let K be the splitting field of $t(x)$ over $\mathbb{F}_p$, $p \in I$ and α, β, γ the roots of $t(x)$ in K. Clearly, $K = GF(p^3)$ and the multiplicative group of K has $p^3 - 1$ elements. Using the Frobenius authomorphism, we can easily prove that $\beta = \alpha^p$ and $\gamma = \alpha^{p^2}$. This implies that α, β, γ have the same order in the multiplicative group of K. It is well known, see e.g. [5], [6], [8], that for any prime $p \neq 2, 11$:

$$h(p) = \mathrm{lcm}(\mathrm{ord}_L(\alpha), \mathrm{ord}_L(\beta), \mathrm{ord}_L(\gamma)) \tag{2.1}$$

where L is the splitting field of $t(x)$ over $\mathbb{F}_p$ and $\mathrm{ord}_L(\alpha), \mathrm{ord}_L(\beta), \mathrm{ord}_L(\gamma)$ are the orders of α, β, γ in the multiplicative group of L. Consequently, for $p \in I$, we can state

★ Published in J. Klaška, *A search for Tribonacci-Wieferich primes*, Acta Math. Univ. Ostrav. **16** (2008), 15–20.

Lemma 2.1. *Let $p \in I$. Then $h(p) = \mathrm{ord}_K(\alpha)$ where α is any root of $t(x)$ in a splitting field K of $t(x)$ over $\mathbb{F}_p$.*

Lemma 2.2. *For any prime $p \in I$ we have $h(p)|p^2 + p + 1$.*

Proof. The Viète equation $\alpha\beta\gamma = 1$ together with $\beta = \alpha^p$ and $\gamma = \alpha^{p^2}$ yields $\alpha^{p^2+p+1} = 1$. This implies $\mathrm{ord}_K(\alpha)|p^2+p+1$ and the relation $h(p)|p^2+p+1$ follows from Lemma 2.1. □

Remark 2.3. In the relation $h(p)|p^2 + p + 1$ it is often, but not always, true that $h(p) = p^2+p+1$. For example, $h(3) = 3^2+3+1 = 13$ but $h(31) = (31^2+31+1)/3 = 331$.

In 1978, M. E. Waddill [10, Theorem 8] proved that for any prime p:

$$\text{If } \ h(p) \neq h(p^2), \text{ then } h(p^t) = p^{t-1}h(p) \text{ for any } t \in \mathbb{N}. \tag{2.2}$$

Consequently, we have either $h(p^2) = p \cdot h(p)$ or $h(p^2) = h(p)$. If we combine Waddill's result (2.2) with Lemma 2.2, we obtain

Lemma 2.4. *For any prime $p \in I$, $h(p) = h(p^2)$ if and only if $h(p^2)|p^2 + p + 1$.*

Now we show that to calculate the powers of α in the multiplicative group of K we need to calculate with Tribonacci numbers.

Lemma 2.5. *For any positive integer $n \geq 3$ we have the identity*

$$x^n = T_n x^2 + (T_{n-1} + T_{n-2})x + T_{n-1} + s_n(x)t(x) \quad \textit{where} \quad s_n(x) = \sum_{k=1}^{n} T_k x^{n-k}. \tag{2.3}$$

Proof. Using induction on n. □

Reducing the identity (2.3) by the double modulus $\mathrm{modd}(m, t(x))$ where $m > 1$ is an arbitrary positive integer, we obtain the congruence

$$x^n \equiv T_n x^2 + (T_{n-1} + T_{n-2})x + T_{n-1}(\mathrm{modd}\ m, t(x)). \tag{2.4}$$

From (2.4) now it follows that

$$x^n \equiv 1(\mathrm{modd}\ m, t(x)) \ \text{ if and only if } \ [T_n, T_{n+1}, T_{n+2}] \equiv [0, 0, 1](\mathrm{mod}\ m). \tag{2.5}$$

Particulary, if $m = p$, $p \in I$ and $x = \alpha$ where α is any root of $t(x)$ in K, (2.5) implies Lemma 2.1.

Example 2.6. Let $p = 3$. Then $p^2 + p + 1 = 13$ and by (2.4) we have $x^{13} \equiv 504x^2 + 423x + 274 \equiv 4 \not\equiv 1(\mathrm{modd}\ 3^2, t(x))$. From (2.5) now it follows that $h(3) \neq h(3^2)$ and thus $p = 3$ is not a Tribonacci - Wieferich prime. Moreover, from Lemma 2.2 and $h(3) \neq 1$, it follows that $h(3) = 13$ and by (2.2) we have $h(3^2) = 39$.

Let $q \in I$. By I_q denote the set of all primes $p \in I$ not exceeding q. Theoretically, we have two posibilites when searching for Tribonacci - Wieferich primes in I_q. First, we can calculate a finite sequence $(T_n)_{n=0}^{q^2+q+1}$ and, subsequently, for any particular primes $p \in I_q$, test whether $[T_{p^2+p+1}, T_{p^2+p+2}, T_{p^2+p+3}] \equiv [0, 0, 1]$ (mod p^2). Second, we compute the reduced sequences $(T_n \bmod p^2)_{n=0}^{p^2+p+1}$ for any $p \in I_q$.

Let us now show that the first possibility is virtually excluded as it uses an enormous amount of computer memory. It can be easily proved that the Tribonacci polynomial $t(x)$ has one real root

$$\tau = \frac{1}{3}\left(\sqrt[3]{19+3\sqrt{33}} + \sqrt[3]{19-3\sqrt{33}} + 1\right) \approx 1.839\,286\,755\,214\,161\,132\,\cdots \quad (2.6)$$

and two complex roots $\sigma, \overline{\sigma}$ ($\overline{\sigma}$ is the complex conjugate of σ) where

$$\sigma = \frac{1}{6}\left(2 - \sqrt[3]{19+3\sqrt{33}} - \sqrt[3]{19-3\sqrt{33}}\right) + \frac{\sqrt{3}i}{6}\left(\sqrt[3]{19+3\sqrt{33}} - \sqrt[3]{19-3\sqrt{33}}\right). \quad (2.7)$$

Put $\varepsilon = \tau^2/|\tau - \sigma|^2 \approx 0.618\,419\,922\,319\,392\,550\cdots$. In [7], W. R. Spickerman proved that for T_n we have

$$T_n = [\varepsilon \cdot \tau^n + 0.5]. \quad (2.8)$$

Here $[x]$ denotes the greatest integer not exceeding x. Clearly, if x is positive, then $[x]$ is simply the integer part of x. Note that, in [7], σ is incorrect. See [7, p. 119]. From (2.8) it follows that, for $\log T_n$, we have

$$\log T_n \approx n \cdot \log \tau \quad \text{where} \quad \log \tau = 0.264\,649\,443\,484\,250\,871\cdots. \quad (2.9)$$

Evidently, T_n has exactly k digits for $n > 1$ if and only if $k - 1 \le \log T_n < k$. This, together with (2.9) yields an estimate for the number of digits of T_n. The following example may provide a more precise idea of the greatness of Tribonacci numbers T_n.

Example 2.7. The Tribonacci number T_{100} has 26 digits, T_{1000} has 264 digits, and T_{10000} has 2646 digits. Consider now the greatest prime p from the interval $[2, 10^9]$ for which $t(x)$ is irreducible modulo p. This p is equal to 999999929. To test whether $h(p) = h(p^2)$ we need to find $[T_q, T_{q+1}, T_{q+2}]$ where $q = p^2+p+1 = 999999859000004971$. Since, by (2.9), T_q has more than $5 \cdot 10^{15}$ digits, we need about 10^6 GB of memory for T_q, assuming that one byte is needed for one digit.

In this paper, we use a method based on matrix algebra to search for Tribonacci - Wieferich primes on a given set I_q using a computer. It is well known (see e.g. [5], [9]) that Tribonacci numbers can be computed by powers of the Tribonacci matrix T where

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad T^{n+1} = \begin{bmatrix} T_n & T_{n-1} + T_n & T_{n+1} \\ T_{n+1} & T_n + T_{n+1} & T_{n+2} \\ T_{n+2} & T_{n+1} + T_{n+2} & T_{n+3} \end{bmatrix} \quad \text{for} \quad n \in \mathbb{N}. \quad (2.10)$$

Clearly, $h(m)$ is the period of $(T_n \bmod m)_{n=0}^{\infty}$ if and only if $h(m)$ is the smallest positive integer h for which $T^h \equiv E \pmod{m}$ where E is the 3×3 identity matrix. This, together with Lemma 2.4, yields

Lemma 2.8. *For any $p \in I$ we have $h(p) = h(p^2)$ if and only if $T^{p^2+p+1} \equiv E \pmod{p^2}$ where E is the 3×3 identity matrix.*

Now we briefly describe the algorithm used to prove the main theorem of this section.

Algorithm for testing $h(p) = h(p^2)$ for $p \in I$

First, we find a 2-adic expansion of $p^2 + p + 1 = c_0 + 2c_1 + 2^2c_2 + \cdots + 2^k c_k$. Second, we define the matrix $T \bmod p^2$ and, subsequently, we compute k matrices $T^{2^i} \bmod p^2$ for $i = 1, \ldots, k$. Third, we compute the matrix

$$T^{p^2+p+1} \bmod p^2 = \prod_{i=0}^{k} (T^{2^i} \bmod p^2)^{c_i}. \tag{2.11}$$

Finally, we test whether $T^{p^2+p+1} \bmod p^2$ is equal to the identity matrix E. This process is repeated for every prime $p \in I$.

Implementing this algorithm in Pari GP, we have obtained the following result:

Theorem 2.9. *For any prime $p \in I$, $p < 10^{11}$ we have $h(p) \neq h(p^2)$.*

Let us remark that, achieving this result takes about 1500 hours of CPU time on a 1.6 GHz processor computer.

3. Searching for Tribonacci - Wieferich primes $p \notin I$

In the case of $p \notin I$ we can use the criteria derived in [6] to search for Tribonacci - Wieferich primes. Moreover, when dealing with this case, Tribonacci - Wieferich primes of the second kind may also be found easily. Indeed, by [5], from $h(p) = h(p^2)$, we have $\mathrm{ord}_p(\xi) = \mathrm{ord}_{p^2}(\xi)$ for any solution $\xi \in \mathbb{Z}$ of $t(x) \equiv 0 \pmod{p^2}$. Next, according to [6], if $\alpha \in \mathbb{Z}$ is the unique root of $t(x)$ modulo p with the property

$$3\alpha^{p+2} - 2\alpha^{p+1} - \alpha^p - 2\alpha^3 + \alpha^2 - 1 \equiv 0 \pmod{p^2} \tag{3.1}$$

or, equivalently, with the property

$$\alpha^{3p} - \alpha^{2p} - \alpha^p - 1 \equiv 0 \pmod{p^2} \tag{3.2}$$

then p is the Tribonacci-Wieferich prime of the second kind. It should be stressed that the criteria (3.1) and (3.2) make it possible to find Tribonacci - Wieferich primes of the second kind and thus also Tribonacci - Wieferich primes p with $p \notin I$ without having to calculate with Tribonacci numbers. The following result has been obtained using (3.1) in Pari GP.

Theorem 3.1. *There is no prime $p \notin I$, $p < 10^{11}$ satisfying $\mathrm{ord}_p(\xi) = \mathrm{ord}_{p^2}(\xi)$ where $\xi \in \mathbb{Z}$ is a solution of $t(x) \equiv 0 \pmod{p^2}$. Consequently, there is no Tribonacci-Wieferich prime of the second kind less than 10^{11}.*

Note that, as compared with Theorem 2.9, only about 700 hours of CPU time are needed to obtain Theorem 3.1 on the same computer.

Corollary 3.2. *For any prime $p \notin I$, $p < 10^{11}$, we have $h(p) \neq h(p^2)$.*

If we combine Corollary 3.2 with Theorem 2.9, we obtain the main theorem of this paper:

Theorem 3.3. *There is no Tribonacci - Wieferich prime $p < 10^{11}$.*

Moreover, based on (2.2), we can now state

Corollary 3.4. *For any prime $p < 10^{11}$ and for any $t \in \mathbb{N}$, we have $h(p^t) = p^{t-1}h(p)$.*

Remark 3.5. Like in the problem of finding Fibonacci - Wieferich primes (see [3], [4]) also in the Tribonacci case a question may be raised whether the probability of some primes being Tribonacci - Wieferich is greather than that of others. Using a reasoning similar to that used in [4], we can conclude that further search of the set I for $p > 10^{11}$ will virtually not increase the probability of finding a Tribonacci - Wieferich prime. Consequently, the chances of finding Tribonacci - Wieferich primes on a computer seem to be greater for primes not in I, particulary, for those for which $t(x)$ can be factorized into linear terms over $\mathbb{F}_p$.

References

[1] A. Agronomof, *Une série récurrente*, Mathesis **4** (1914), 125–126.
[2] M. Feinberg, *Fibonacci - Tribonacci*, The Fibonacci Quarterly **1.3** (1963), 70, 71–74.
[3] J. Klaška, *Criteria for testing Wall's question*, Czechoslovak Math. Journal, **58.4** (2008), 1241–1246.
[4] J. Klaška, *Short remark on Fibonacci-Wieferich primes*, Acta Math. Univ. Ostrav. **15** (2007), 21–25.
[5] J. Klaška, *Tribonacci modulo p^t*, Math. Bohem. **133.3** (2008), 267–288.
[6] J. Klaška, *On Tribonacci-Wieferich primes*, The Fibonacci Quarterly **46/47** (2008/2009), 290–297.
[7] W. R. Spickerman, *Binet's Formula for the Tribonacci Sequence*, The Fibonacci Quarterly **20.2** (1982), 118–120.
[8] A. Vince, *Period of a Linear Recurrence*, Acta Arith. **39** (1981), 303–311.
[9] M. E. Waddill, L. Sacks, *Another Generalized Fibonacci Sequence*, The Fibonacci Quarterly **5.3** (1967), 209–222.
[10] M. E. Waddill, *Some Properties of a Generalized Fibonacci Sequence Modulo m*, The Fibonacci Quarterly **16.4** (1978), 344–353.

Keywords: Tribonacci numbers, Tribonacci - Wieferich primes

MSC 2000: 11B50, 11B39

CHAPTER 8

TRIBONACCI PARTITION FORMULAS MODULO m ★

Abstract. Each Tribonacci sequence starting with an arbitrary triple of integers is periodic modulo m for any modulus $m > 1$. For a given m, the mapping between the set S of all m^3 triples of initial values and the set of their corresponding periods define a partition of the set S. In this paper we shall investigate some basic questions related to these partitions from the point of view of enumerative combinatorics.

1. Preliminary results

Let $(T_n)_{n=0}^{\infty}$ be a Tribonacci sequence defined by $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ with the triple of initial values $[T_0, T_1, T_2] = [a, b, c]$ where a, b, c are integers. It is well known, see for example [9], that $(T_n \bmod m)_{n=0}^{\infty}$ is periodic for any modulus $m > 1$. Let us denote the period of $(T_n \bmod m)_{n=0}^{\infty}$ by $h(m)[a, b, c]$. That is, $h(m)[a, b, c]$ is the least positive integer k for which we have $[T_k, T_{k+1}, T_{k+2}] \equiv [T_0, T_1, T_2] \pmod{m}$. Particularly, if $[T_0, T_1, T_2] = [0, 0, 1]$, then the period $h(m)[0, 0, 1]$ will be denoted by $h(m)$. It is well known [9, p. 155] that, if $m = p_1^{t_1} \dots p_k^{t_k}$ is a prime factorization of m, then

$$h(m)[a, b, c] = \operatorname{lcm}(h(p_1^{t_1})[a, b, c], \dots, h(p_k^{t_k})[a, b, c]).$$

Consequently, $h(m) = \operatorname{lcm}(h(p_1^{t_1}), \dots, h(p_k^{t_k}))$. See also [8, p. 347]. Furthermore, for any prime p and for any positive integers $r \leq t$, we have:

$$\text{If} \quad h(p) = \cdots = h(p^r) \neq h(p^{r+1}) \quad \text{then} \quad h(p^t) = p^{t-r} h(p).$$

Particularly, if $r = 1$, then $h(p^t) = p^{t-1} h(p)$. See [8, pp. 349–351]. Up to the present, no instance of $h(p) = h(p^2)$ has been found and the question whether $h(p) = h(p^2)$ never appears is open. In [5], the primes p satisfying $h(p) = h(p^2)$ were called Tribonacci-Wieferich primes. Note that, for a composite modulus m, the equality $h(m) = h(m^2)$ can occur. For example, for $m = 208919$ we have $m = p_1 p_2$ where $p_1 = 59$, and $p_2 = 3541$. Now it is not difficult to verify that $h(m) = \operatorname{lcm}(h(p_1), h(p_2)) = \operatorname{lcm}(3541, 181720) = 643470520$, and $h(m^2) = \operatorname{lcm}(h(p_1^2), h(p_2^2)) = \operatorname{lcm}(59 \cdot 3541, 3541 \cdot 181720) = h(m)$.

Let L_p be the splitting field of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ over the field of p-adic numbers $\mathbb{Q}_p$ and let α, β, γ be the roots of $t(x)$ in L_p. Further, let O_p be the ring of integers of L_p. Clearly, $\alpha, \beta, \gamma \in O_p$. As the discriminant of $t(x)$ is equal to -44, the Galois extension $L_p/\mathbb{Q}_p$ does not ramify for $p \neq 2, 11$. For any unit $\xi \in O_p$ and for any $t \in \mathbb{N}$, we denote by $\operatorname{ord}_{p^t}(\xi)$ the least positive rational integer k

★ Published in J. Klaška, *Tribonacci partition formulas modulo m*, Acta Mathematica Sinica, English Series, **26.3** (2010), 465–476.

such that $\xi^k \equiv 1 \pmod{p^t}$. If $p \neq 2, 11$, then, by [5, Theorem 2.4], we have

$$h(p^t) = \operatorname{lcm}(\operatorname{ord}_{p^t}(\alpha), \operatorname{ord}_{p^t}(\beta), \operatorname{ord}_{p^t}(\gamma)). \tag{1.1}$$

From (1.1) it follows easily that $h(p) = h(p^r)$ implies $\operatorname{ord}_p(\xi) = \operatorname{ord}_{p^r}(\xi)$ for any $\xi \in \{\alpha, \beta, \gamma\}$. Consequently, if r is the largest positive integer satisfying $h(p) = h(p^r)$ and s is the largest positive integer satisfying $\operatorname{ord}_p(\xi) = \operatorname{ord}_{p^s}(\xi)$, then $r \leq s$. In [5] an interesting question was opened whether the case $r < s$ really occurs and the primes p satisfying $\operatorname{ord}_p(\xi) = \operatorname{ord}_{p^2}(\xi)$ and $h(p) \neq h(p^2)$ were called Tribonacci-Wieferich primes of the second kind. Computer search in [5] showed that, for $p \leq 10^9$, there is neither a Tribonacci-Wieferich nor a Tribonacci-Wieferich prime of the second kind. Moreover, if $r < s$, then there is exactly one root $\xi \in \{\alpha, \beta, \gamma\}$ satisfying $\operatorname{ord}_p(\xi) = \operatorname{ord}_{p^s}(\xi)$. In this case, $\xi \in \mathbb{Z}_p$ where $\mathbb{Z}_p$ is the ring of p-adic integers. It is also well known that the periods $h(p)$ highly depend on the form of factorization of $t(x)$ modulo p. For $p \neq 2, 11$, we have (see [7, Theorem 4]):

$$\text{If } \left(\frac{p}{11}\right) = 1, \text{ then } \begin{cases} h(p) | p^2 + p + 1 \text{ if } t(x) \text{ is irreducible mod } p, \\ h(p) | p - 1 \quad \text{otherwise.} \end{cases}$$

If $\left(\frac{p}{11}\right) = -1$, then $h(p) | p^2 - 1$. Here $\left(\frac{p}{11}\right)$ denotes the Legendre symbol.

The relations between the periods $h(p)[a, b, c]$ and $h(p^t)[a, b, c]$ are examined in detail in [3] and [4]. Let $p \neq 2, 11$ and $[a, b, c] \not\equiv [0, 0, 0] \pmod p$. If $t(x)$ is irreducible over $\mathbb{Q}_p$ and $h(p) = \cdots = h(p^r) \neq h(p^{r+1})$, then, by [3], we have

$$h(p^t)[a, b, c] = \begin{cases} h(p) & \text{for } t \leq r, \\ p^{t-r} h(p) & \text{for } t > r. \end{cases} \tag{1.2}$$

In the opposite case, there is at least one root ξ of $t(x)$ such that $\xi \in \mathbb{Z}_p$. Putting $\xi \bmod p^t = \xi_t$, we can, for any $t \in \mathbb{N}$, define $E(\xi_t) = \{[q, q\xi_t, q\xi_t^2]; q \in \mathbb{Z}/p^t\mathbb{Z}\}$. Let $\operatorname{ord}_p(\xi) = \cdots = \operatorname{ord}_{p^s}(\xi) \neq \operatorname{ord}_{p^{s+1}}(\xi)$. Put $h_0 = \operatorname{ord}_p(\xi)$. If $[a, b, c] \in E(\xi_t)$, we have

$$h(p^t)[a, b, c] = \begin{cases} h_0 & \text{for } t \leq s, \\ p^{t-s} h_0 & \text{for } t > s. \end{cases} \tag{1.3}$$

On the other hand, if $[a, b, c] \notin E(\xi_t)$ for no root ξ of $t(x)$ and r is the largest positive integer satisfying $h(p) = h(p^r)$, we have (1.2).

2. Concept of partition formulas

Let us consider a binary relation $\sim$ on the set $S = [\mathbb{Z}/m\mathbb{Z}]^3$ defined by

$$[a_1, b_1, c_1] \sim [a_2, b_2, c_2] \quad \text{if and only if} \quad h(m)[a_1, b_1, c_1] = h(m)[a_2, b_2, c_2]. \tag{2.1}$$

Clearly, $\sim$ is an equivalence on S and $S/\sim$ is a partition of S. Let $N(h, m)$ denote the number of elements in the class $\{[a, b, c] \in S; h(m)[a, b, c] = h\}$, and let H denote the set of all possible periods $h(m)[a, b, c]$. Since, for a given modulus m, there are m^3 different initial conditions, we have

$$m^3 = \sum_{h \in H} N(h, m). \tag{2.2}$$

Further, for $[a_1, b_1, c_1], [a_2, b_2, c_2] \in S$, we put $[a_1, b_1, c_1] \approx [a_2, b_2, c_2]$ if and only if, in the sequence $(T_n \bmod m)_{n=1}^{\infty}$ that starts with a triple $[a_1, b_1, c_1]$, there is an index i such that $[T_i, T_{i+1}, T_{i+2}] \equiv [a_2, b_2, c_2] \pmod m$. The relation $\approx$ is also an equivalence on S and the partition $S/\approx$ is a refinement of $S/\sim$. Let $n(h,m)$ denote the number of classes in a partition $S/\approx$ that result from a refinement of the class $\{[a,b,c] \in S; h(m)[a,b,c] = h\}$. That is, $n(h,m)$ establishes the number of distinct Tribonacci sequences modulo m whose period is equal to h. Since we have $N(h,m) = n(h,m) \cdot h$, from (2.2) it follows that

$$m^3 = \sum_{h \in H} n(h,m) \cdot h = c_1 \cdot h_1 + \cdots + c_r \cdot h_r, \tag{2.3}$$

where $H = \{h_1, \ldots, h_r\}$ and $c_i = n(h_i, m)$ for $i \in \{1, \ldots, r\}$. The relation (2.3) will be called a Tribonacci partition formula modulo m, and the left-hand side of (2.3) will be writen as $[m]^3$. If, in (2.3), $c_i = 1$ occurs for some $1 \le i \le r$, then we shall write $1 \cdot h_i$ or h_i for short. For example, if $m = 10$, then $H = \{1, 2, 4, 31, 62, 124\}$ and the Tribonacci partition formula modulo 10 has the form $[10]^3 = 2 \cdot 1 + 2 + 4 + 8 \cdot 31 + 4 \cdot 62 + 4 \cdot 124$.

In a way similar to that in (2.3), we can define a partition formula for any $\emptyset \ne R \subseteq S$. This formula will be denoted by $[m]^3_R$. The following example will be useful in the sequel. Let $R = \{[a,b,c] \in [\mathbb{Z}/p^t\mathbb{Z}]^3; [a,b,c] \equiv [0,0,0] (\text{mod } p)\}$. Then $[p^t]^3_R = [p^{t-1}]^3$ for any $t > 1$.

The combinatorial problem to establish the numbers $n(h,m)$ for sequences defined by a given linear recurrence of order k was originally formulated by M. Ward [10] in 1935. A solution for Fibonacci sequences has been found by A. Andreassian [1]. In the present paper we resolve this problem for the case of Tribonacci sequences.

3. Sum and product of the formulas

In this section, we find two important methods that use known formulas to construct some others. These processess, together with the results obtained in [3], [4], and [5], enable us to establish the forms of Tribonacci formulas for any modulus $m > 1$.

Let $\emptyset \ne S_1, S_2 \subseteq S = [\mathbb{Z}/m\mathbb{Z}]^3$, and $S_1 \cap S_2 = \emptyset$. Further, let $[m]^3_{S_1} = c_1 \cdot h_1 + \cdots + c_r \cdot h_r$ and $[m]^3_{S_2} = c'_1 \cdot h'_1 + \cdots + c'_s \cdot h'_s$. We define the sum of $[m]^3_{S_1}$, $[m]^3_{S_2}$ as follows

$$[m]^3_{S_1} + [m]^3_{S_2} = c_1 \cdot h_1 + \cdots + c_r \cdot h_r + c'_1 \cdot h'_1 + \cdots + c'_s \cdot h'_s. \tag{3.1}$$

Clearly, if there is $1 \le j \le s$ such that $h_i = h'_j$ for some $1 \le i \le r$, then j is unique. In this case, in (3.1), we shall write $c_i h_i + c'_j h'_j$ as $(c_i + c'_j) \cdot h_i$. From (3.1) we can now establish

Theorem 3.1 *Let $\emptyset \ne \{S_1, \cdots, S_k\}$ be an arbitrary system of nonempty and pairwise disjunct subsets of $S = [\mathbb{Z}/m\mathbb{Z}]^3$. Put $R = \cup_{i=1}^k S_i$. Then we have*

$$[m]^3_R = \sum_{i=1}^k [m]^3_{S_i}. \tag{3.2}$$

Particulary, if $\{S_1, \ldots, S_k\}$ is a partition of S, then $[m]^3 = \sum_{i=1}^k [m]^3_{S_i}$.

Let $m_1, m_2 > 1$ be arbitrary modules such that $(m_1, m_2) = 1$. Further assume that the formulas $[m_1]^3 = c_1 \cdot h_1 + \cdots + c_r \cdot h_r$, and $[m_2]^3 = c'_1 \cdot h'_1 + \cdots + c'_s \cdot h'_s$ are known. We define the product of $[m_1]^3$ and $[m_2]^3$ by

$$[m_1]^3 \cdot [m_2]^3 = \sum_{i=1}^r \sum_{j=1}^s c_i c'_j \gcd(h_i, h'_j) \cdot \text{lcm}(h_i, h'_j). \tag{3.3}$$

Thus, the product of the formulas can be computed as the obvious product of polynomials and the product of $c_i \cdot h_i$ and $c'_j \cdot h'_j$ will be interpreted as $c_i c'_j \gcd(h_i, h'_j) \cdot \mathrm{lcm}(h_i, h'_j)$. Finally, after this expansion, in (3.3), we group the terms with the same period.

Theorem 3.2 *Let $m = m_1 m_2$ and $(m_1, m_2) = 1$. Then we have $[m]^3 = [m_1]^3 \cdot [m_2]^3$.*

Proof Let $h_1 = h(m_1)[a_1, a_2, a_3]$, $h_2 = h(m_2)[b_1, b_2, b_3]$. By the Chinese Remainder Theorem, it follows that any two triples $[a_1, a_2, a_3] (\mathrm{mod}\ m_1)$, $[b_1, b_2, b_3] (\mathrm{mod}\ m_2)$ determine exactly one triple $[c_1, c_2, c_3] (\mathrm{mod}\ m_1 m_2)$ such that $[c_1, c_2, c_3] \equiv [a_1, a_2, a_3] (\mathrm{mod}\ m_1)$ and $[c_1, c_2, c_3] \equiv [b_1, b_2, b_3] (\mathrm{mod}\ m_2)$. Moreover, for $[c_1, c_2, c_3]$, we have $h(m_1 m_2)[c_1, c_2, c_3] = \mathrm{lcm}(h(m_1)[c_1, c_2, c_3], h(m_2)[c_1, c_2, c_3]) = \mathrm{lcm}(h(m_1)[a_1, a_2, a_3], h(m_2)[b_1, b_2, b_3]) = \mathrm{lcm}(h_1, h_2) = h$. Hence, the number of all triples which determine modulo $m = m_1 m_2$ a period $h = \mathrm{lcm}(h_1, h_2)$ is equal to $N(h_1, m_1) N(h_2, m_2)$. Consequently, we have

$$N(h, m) = \sum_{(h_1, h_2)} N(h_1, m_1) N(h_2, m_2) \quad \text{and} \quad n(h, m) = \frac{1}{h} \sum_{(h_1, h_2)} N(h_1, m_1) N(h_2, m_2),$$

where the sum extends over all pairs (h_1, h_2) satisfying $\mathrm{lcm}(h_1, h_2) = h$. Further, let $H_1 = \{h_1, \ldots, h_r\}$ be the set of all possible periods modulo m_1, and $H_2 = \{h'_1, \ldots, h'_s\}$ be the set of all possible periods modulo m_2. Then $H = \{\mathrm{lcm}(h_i, h'_j); h_i \in H_1, h'_j \in H_2\}$ is the set of all periods modulo $m = m_1 m_2$. Using (2.2), and (3.3), we have

$$\begin{aligned}
[m]^3 &= \sum_{h \in H} n(h, m) \cdot h \\
&= \sum_{h \in H} \sum_{(h_i, h'_j)} N(h_i, m_1) N(h'_j, m_2) \\
&= \sum_{h_i \in H_1} \sum_{h'_j \in H_2} n(h_i, m_1) n(h'_j, m_2) \gcd(h_i, h'_j) \cdot \mathrm{lcm}(h_i, h'_j) \\
&= \sum_{i=1}^{r} \sum_{j=1}^{s} c_i c'_j \gcd(h_i, h'_j) \cdot \mathrm{lcm}(h_i, h'_j) = [m_1]^3 \cdot [m_2]^3.
\end{aligned}$$

By induction, we can easily extend Theorem 3.2 to an arbitrary finite number of pairwise relatively prime factors m_i. Particulary, we have

Corollary 3.3 *Let $m = p_1^{t_1} \ldots p_k^{t_k}$ be a prime factorization of m and let, for any $1 \le i \le k$, the formulas $[p_i^{t_i}]^3 = c_1^{(i)} \cdot h_1^{(i)} + \cdots + c_{s_i}^{(i)} \cdot h_{s_i}^{(i)}$ be known. Then we have*

$$[m]^3 = [p_1^{t_1}]^3 \ldots [p_k^{t_k}]^3 = \sum_{i_1=1}^{s_1} \cdots \sum_{i_k=1}^{s_k} [c_{i_1}^{(1)} \ldots c_{i_k}^{(k)} \gcd(h_{i_1}^{(1)}, \ldots, h_{i_k}^{(k)})] \cdot \mathrm{lcm}(h_{i_1}^{(1)}, \ldots, h_{i_k}^{(k)}). \tag{3.4}$$

Moreover,

$$n(h, m) = \frac{1}{h} \sum_{(h_1, \ldots, h_k)} N(h_1, p_1^{t_1}) \cdots N(h_k, p_k^{t_k}), \tag{3.5}$$

where the sum extends over all k-tuples $(h_1, \ldots, h_k)$ with $\mathrm{lcm}(h_1, \ldots, h_k) = h$.

Corollary 3.3 has a practical meaning. If we know the partition formulas for the modulus of the form of powers of primes, then we can use them to construct the partition formulas for any composite modulus m. By means of (3.4), we reduced the investigation of Tribonacci partition formulas to those moduli that are powers of primes.

Example 3.4 Using Theorem 3.2, we find the Tribonacci partition formula $[12]^3$. We assume that the formulas $[2^2]^3$ and $[3]^3$ are known. Since $[2^2]^3 = 2\cdot 1 + 2 + 3\cdot 4 + 6\cdot 8$, and $[3]^3 = 1 + 2\cdot 13$, Theorem 3.2 yields

$$\begin{aligned}[12]^3 &= [2^2]^3 \cdot [3]^3 = (2\cdot 1 + 1\cdot 2 + 3\cdot 4 + 6\cdot 8)\cdot(1\cdot 1 + 2\cdot 13) = \\ &= 2\cdot 1 + 2 + 3\cdot 4 + 6\cdot 8 + 4\cdot 13 + 2\cdot 26 + 6\cdot 52 + 12\cdot 104.\end{aligned}$$

4. Tribonacci partition formulas for powers of primes

We start our investigation with $p = 2$. By [4], for periods $h(2^t)[a,b,c]$ we have

Lemma 4.1 *Let $t > 1$ and $[a,b,c] \not\equiv [0,0,0] \pmod 2$. Then we have*

(i) *If $[a,b,c] \equiv [1,1,1] \pmod 2$, then $h(2^t)[a,b,c] = 2^t$.*
(ii) *If $[a,b,c] \not\equiv [1,1,1] \pmod 2$, then $h(2^t)[a,b,c] = 2^{t+1}$.*

By direct computation, we can establish

$$\begin{aligned}[\,2\,]^3 &= 2\cdot 1 + 2 + 4,\\ [2^2]^3 &= 2\cdot 1 + 2 + 3\cdot 4 + 6\cdot 8,\\ [2^3]^3 &= 2\cdot 1 + 2 + 3\cdot 4 + 14\cdot 8 + 24\cdot 16.\end{aligned}$$

See also [6, p. 84]. Now we are ready to prove

Theorem 4.2 *For any $t \geq 3$, the Tribonacci partition formula $[2^t]^3$ has the form*

$$[2^t]^3 = 2\cdot 1 + 2 + 3\cdot 2^2 + (7\cdot 2)\cdot 2^3 + (7\cdot 2^3)\cdot 2^4 + \ldots + (7\cdot 2^{2t-5})\cdot 2^t + (3\cdot 2^{2t-3})\cdot 2^{t+1}. \tag{4.1}$$

Proof Put $S = [\mathbb{Z}/2^t\mathbb{Z}]^3$, $S_1 = \{[a,b,c] \in S; [a,b,c] \equiv [0,0,0] \pmod 2\}$, $S_2 = \{[a,b,c] \in S; [a,b,c] \equiv [1,1,1] \pmod 2\}$, and $S_3 = S - (S_1 \cup S_2)$. Clearly, $\{S_1, S_2, S_3\}$ is a partition of S. By elementary combinatorial formulas we derive $|S_1| = 2^{3(t-1)}$, $|S_2| = 2^{3(t-1)}$, and $|S_3| = 6\cdot 2^{3(t-1)}$. Let $t > 1$. From Lemma 4.1, it follows that $[2^t]^3_{S_2} = 2^{2t-3}\cdot 2^t$, and $[2^t]^3_{S_3} = (3\cdot 2^{2t-3})\cdot 2^{t+1}$. Since $[2^t]^3_{S_1} = [2^{t-1}]^3$, using Theorem 3.1, we have

$$[2^t]^3 = [2^{t-1}]^3 + 2^{2t-3}\cdot 2^t + (3\cdot 2^{2t-3})\cdot 2^{t+1}. \tag{4.2}$$

Let $t \geq 3$. In the first induction step, we verify that (4.1) is true for $t = 3$. Since $[2^2]^3 = 2\cdot 1 + 2 + 3\cdot 4 + 6\cdot 8$, from (4.2), it follows that $[2^3]^3 = [2^2]^3 + 8\cdot 8 + 24\cdot 16 = 2\cdot 1 + 2 + 3\cdot 4 + 14\cdot 8 + 24\cdot 16$, and (4.1) holds. Furthermore, we assume that (4.1) is true for a fixed $t \geq 3$ and prove this for $t+1$. Using (4.2), we have

$$\begin{aligned}[2^{t+1}]^3 &= 2\cdot 1 + 2 + 3\cdot 2^2 + \sum_{i=3}^{t}(7\cdot 2^{2i-5})\cdot 2^i + (3\cdot 2^{2t-3})\cdot 2^{t+1}\\ &\quad + 2^{2t-1}\cdot 2^{t+1} + (3\cdot 2^{2t-1})\cdot 2^{t+2}\\ &= 2\cdot 1 + 2 + 3\cdot 2^2 + \sum_{i=3}^{t+1}(7\cdot 2^{2i-5})\cdot 2^i + (3\cdot 2^{2t-1})\cdot 2^{t+2}.\end{aligned}$$

Now we shall deal with the case of the prime $p = 11$. Over the field $\mathbb{Q}_{11}$, $t(x)$ has only one root $\alpha = 9 + 2\cdot 11 + 1\cdot 11^2 + \cdots \in \mathbb{Z}_{11}$. Put $E(\alpha_t) = \{[q, q\alpha_t, q\alpha_t^2]; q \in \mathbb{Z}/11^t\mathbb{Z}\}$ where $\alpha_t = \alpha \bmod 11^t$. By [4], for periods $h(11^t)[a,b,c]$ we have:

Lemma 4.3 *Let* $t \geq 1$ *and* $[a,b,c] \not\equiv [0,0,0] \pmod{11}$. *Then we have*

(i) *If* $[a,b,c] \notin E(\alpha_t)$ *and* $c \equiv 3a+5b \pmod{11}$, *then* $h(11^t)[a,b,c] = 10 \cdot 11^{t-1}$.
(ii) *If* $[a,b,c] \notin E(\alpha_t)$ *and* $c \not\equiv 3a+5b \pmod{11}$, *then* $h(11^t)[a,b,c] = 10 \cdot 11^t$.
(iii) *If* $[a,b,c] \in E(\alpha_t)$, *then* $h(11^t)[a,b,c] = \mathrm{ord}_{11^t}(\alpha_t) = 5 \cdot 11^{t-1}$.

Moreover, we have

Lemma 4.4 *If* $[a,b,c] \in E(\alpha_t)$ *then* $c \equiv 3a+5b \pmod{11}$.

Proof Let $[a,b,c] \in E(\alpha_t)$. Then there is a q such that $[a,b,c] \equiv [q, q\alpha_t, q\alpha_t^2] \pmod{11}$. As $\alpha \equiv 9 \pmod{11}$, we have $c \equiv q\alpha_t^2 \equiv 4q \equiv 3q + 5q\alpha_t \equiv 3a+5b \pmod{11}$.

Next, by direct calculation, we can find that

$$[\,11\,]^3 = 1 + 2\cdot 5 + 11\cdot 10 + 11 \cdot 110,$$
$$[11^2]^3 = 1 + 2\cdot 5 + 11\cdot 10 + 2\cdot 55 + 1462\cdot 110 + 1331\cdot 1210,$$
$$[11^3]^3 = 1 + 2\cdot 5 + 11\cdot 10 + 2\cdot 55 + 1462\cdot 110 + 2\cdot 605 + 177022\cdot 1210 + 161051\cdot 13310.$$

Now we are ready to state

Theorem 4.5 *For any* $t \geq 2$ *the Tribonacci partition formula* $[11^t]^3$ *has the form*

$$[11^t]^3 = 1 + 11\cdot 10 + \sum_{i=0}^{t-1} 2\cdot(5\cdot 11^i) + \sum_{i=1}^{t-2}(133\cdot 11^{2i-1}-1)\cdot(10\cdot 11^i) + 11^{2t-1}\cdot(10\cdot 11^t).$$

Proof Let $t \geq 2$. Put $S = [\mathbb{Z}/11^t\mathbb{Z}]^3$, $S_1 = \{[a,b,c] \in S; [a,b,c] \equiv [0,0,0] \pmod{11}\}$, $S_2 = E(\alpha_t) - S_1$, $S_3 = \{[a,b,c] \in S; c \equiv 3a+5b \pmod{11}\} - (S_1 \cup S_2)$, $S_4 = S - (S_1 \cup S_2 \cup S_3)$. From Lemma 4.4 it follows that $\{S_1, S_2, S_3, S_4\}$ is a partition of S. After short calculation, we obtain $|S_1| = 11^{3(t-1)}$, $|S_2| = 10\cdot 11^{t-1}$, $|S_3| = 120\cdot 11^{3(t-1)} - 10\cdot 11^{t-1}$, and $|S_4| = 1210\cdot 11^{3(t-1)}$. Lemma 4.3 now implies that $[11^t]^3_{S_2} = 2\cdot(5\cdot 11^{t-1})$, $[11^t]^3_{S_3} = (12\cdot 11^{2(t-1)}-1)\cdot(10\cdot 11^{t-1})$, $[11^t]^3_{S_4} = 11^{2t-1}\cdot(10\cdot 11^t)$. This, together with $[11^t]^3_{S_1} = [11^{t-1}]^3$ and Theorem 3.1 yields

$$[11^t]^3 = [11^{t-1}]^3 + 2\cdot(5\cdot 11^{t-1}) + (12\cdot 11^{2t-2}-1)\cdot(10\cdot 11^{t-1}) + 11^{2t-1}\cdot(10\cdot 11^t). \quad (4.3)$$

Using (4.3), we can now easily finish the proof by induction.

For the proofs of the subsequent theorems, the following partition $\{S_0, S_1, \ldots, S_t\}$ of the set $S = [\mathbb{Z}/p^t\mathbb{Z}]^3$ will be useful:

$$S_0 = \{[a,b,c]; [a,b,c] \not\equiv [0,0,0] \pmod{p}\},$$
$$S_j = \{[a,b,c]; [a,b,c] \equiv [0,0,0] \pmod{p^j} \text{ and } [a,b,c] \not\equiv [0,0,0] \pmod{p^{j+1}}\},\ 1 \leq j \leq t-1,$$
$$S_t = \{[0,0,0]\}. \quad (4.4)$$

Evidently, $|S_j| = p^{3(t-j)} - p^{3(t-j-1)}$ for any $0 \leq j \leq t-1$ and $|S_t| = 1$.

In our investigation, we shall continue with a case of $t(x)$ being irreducible over $\mathbb{Q}_p$.

Theorem 4.6 *Let* $t(x)$ *have no root over the field* $\mathbb{Q}_p$, $p \neq 2$. *Let* r *be the largest positive integer such that* $h(p^r) = h(p)$. *Then, for any positive integers* $r < t$, *we have*

$$[p^t]^3 = 1 + \frac{p^{3r}-1}{h}\cdot h + \sum_{i=1}^{t-r} \frac{p^{3r+2i} - p^{3r+2i-3}}{h}\cdot p^i h \quad \text{where} \quad h = h(p). \quad (4.5)$$

Particulary, if $r = 1$, we have

$$[p^t]^3 = 1 + \sum_{i=0}^{t-1} \frac{p^{2i}(p^3-1)}{h} \cdot p^i h. \tag{4.6}$$

Proof Let $\{S_0, S_1, \dots S_t\}$ be the partition defined by (4.4). If $[a,b,c] \in S_j$ where $0 \le j \le t-r-1$, then by (1.2) we have $h(p^t)[a,b,c] = p^{t-r-j}h$. This implies that

$$[p^t]^3_{S_j} = \frac{p^{3(t-j)} - p^{3(t-j-1)}}{p^{t-r-j}h} \cdot p^{t-r-j}h = \frac{p^{2t+r-2j} - p^{2t+r-2j-3}}{h} \cdot p^{t-r-j}h.$$

Using (3.2) and putting $i = t-r-j$, we obtain

$$\sum_{j=0}^{t-r-1} [p^t]^3_{S_j} = \sum_{i=1}^{t-r} [p^t]^3_{S_i} = \sum_{i=1}^{t-r} \frac{p^{3r+2i} - p^{3r+2i-3}}{h} \cdot p^i h. \tag{4.7}$$

Further, for any $[a,b,c] \in S_j$ where $t-r \le j \le t-1$, we have $h(p^t)[a,b,c] = h$. Hence

$$\sum_{j=t-r}^{t-1} [p^t]^3_{S_j} = \frac{p^{3r}-1}{h} \cdot h. \tag{4.8}$$

Combining (4.7) and (4.8) with $[p^t]^3_{S_t} = 1 \cdot 1$ and using Theorem 3.1, we obtain (4.5). Finally, for $r = 1$, from (4.5) we come to (4.6) and the proof is complete.

Example 4.7 We establish the form of the Tribonacci partition formula modulo 3^t. Clearly, $t(x)$ is irreducible over $\mathbb{Q}_3$. Let L be a splitting field of $t(x)$ over $\mathbb{F}_3$ and let ε be any root of $t(x)$ in L. As $L = GF(p^3)$, the multiplicative group of L has 26 elements and thus $\mathrm{ord}_L(\varepsilon)|26$. To determine the exact value of $\mathrm{ord}_L(\varepsilon)$, we can use the fact that ε is the root of $t(x)$. The powers of ε that are greather then 2 can be reduced by the equality $\varepsilon^3 = \varepsilon^2 + \varepsilon + 1$ in L. Hence, we have $\varepsilon^4 = 2\varepsilon^2 + 2\varepsilon + 1,\ \dots,\ \varepsilon^{12} = \varepsilon^2 + 2\varepsilon + 2,\ \varepsilon^{13} = 1$. This implies that $h(3) = \mathrm{ord}_L(\alpha) = 13$. Since $h(3) \ne h(3^2) = 39$, we have $r = 1$ and (4.6) yields $[3^t]^3 = 1 + \sum_{i=0}^{t-1}(2 \cdot 3^{2i}) \cdot (13 \cdot 3^i)$. Particulary, for $t = 1,2,3$ we have: $[\,3\,]^3 = 1 + 2 \cdot 13$, $[3^2]^3 = 1 + 2 \cdot 13 + 18 \cdot 39$, and $[3^3]^3 = 1 + 2 \cdot 13 + 18 \cdot 39 + 162 \cdot 117$.

Next we focus on a case of $t(x)$ having exactly one root over $\mathbb{Q}_p$. We have:

Theorem 4.8 *Let $t(x)$ have exactly one root α in the field of p-adic numbers $\mathbb{Q}_p$, $p \ne 11$. Let r be the largest positive integer satisfying $h(p) = h(p^r)$, and s be the largest positive integer satisfying* $\mathrm{ord}_p(\alpha) = \mathrm{ord}_{p^s}(\alpha)$. *If $r < s < t$, then we have*

$$\begin{aligned}[p^t]^3 = 1 &+ \frac{p^s-1}{h_1} \cdot h_1 + \frac{p^{3r}-p^r}{h} \cdot h + \sum_{i=1}^{t-s} \frac{p^s - p^{s-1}}{h_1} \cdot p^i h_1 + \\ &+ \sum_{i=1}^{t-r} \frac{p^{3r+2i} - p^{3r+2i-3} - p^r + p^{r-1}}{h} \cdot p^i h,\end{aligned} \tag{4.9}$$

where $h_1 = \mathrm{ord}_p(\alpha)$ and $h = h(p)$. Particulary, for $r = s = 1$, we have

$$[p^t]^3 = 1 + \sum_{i=0}^{t-1} \frac{p-1}{h_1} \cdot p^i h_1 + \sum_{i=0}^{t-1} \frac{p^{2i+3} - p^{2i} - p + 1}{h} \cdot p^i h. \tag{4.10}$$

Proof Let us consider the partition $\{S_0, S_1, \cdots, S_t\}$ defined by (4.4). For $0 \le j \le t-1$ we have $|S_j \cap E(\alpha_t)| = p^{t-j} - p^{t-j-1}$ and $|S_j - E(\alpha_t)| = p^{3(t-j)} - p^{3(t-j-1)} - p^{t-j} + p^{t-j-1}$.

Let $0 \le j \le t-s-1$. If $[a,b,c] \in S_j - E(\alpha_t)$, then $h(p^t)[a,b,c] = p^{t-r-j}h$. On the other hand, if $[a,b,c] \in S_j \cap E(\alpha_t)$, then $h(p^t)[a,b,c] = p^{t-s-j}h_1$. This follows from (1.2), and (1.3). Put $B_1 = \cup_{j=0}^{t-s-1} S_j$. Using (3.2), and performing short calculation, we obtain

$$[p^t]^3_{B_1} = \sum_{j=0}^{t-s-1} \frac{p^s - p^{s-1}}{h_1} \cdot p^{t-s-j}h_1 + \sum_{j=0}^{t-s-1} \frac{p^{2t+r-2j} - p^{2t+r-2j-3} - p^r + p^{r-1}}{h} \cdot p^{t-r-j}h.$$

Further, put $B_2 = \cup_{j=t-s}^{t-r-1} S_j$. By analogy, we deduce that

$$[p^t]^3_{B_2} = \frac{p^s - p^r}{h_1} \cdot h_1 + \sum_{j=t-s}^{t-r-1} \frac{p^{2t+r-2j} - p^{2t+r-2j-3} - p^r + p^{r-1}}{h} \cdot p^{t-r-j}h.$$

Similary, if $B_3 = \cup_{j=t-r}^{t-1} S_j$, then $[p^t]^3_{B_3} = \frac{p^r - 1}{h_1} \cdot h_1 + \frac{p^{3r} - p^r}{h} \cdot h$. Since $[p^t]^3_{S_t} = 1 \cdot 1$, using Theorem 3.1 we get

$$[p^t]^3 = 1 + \frac{p^s - 1}{h_1} \cdot h_1 + \frac{p^{3r} - p^r}{h} \cdot h + \sum_{j=0}^{t-s-1} \frac{p^s - p^{s-1}}{h_1} \cdot p^{t-s-j}h_1 +$$
$$+ \sum_{j=0}^{t-r-1} \frac{p^{2t+r-2j} - p^{2t+r-2j-3} - p^r + p^{r-1}}{h} \cdot p^{t-r-j}h.$$

Putting $i = t-s-j$, and $i = t-r-j$ respectively, we obtain (4.9). Since (4.10) is a direct consequence of (4.9), the theorem is proved.

Example 4.9 We find the partition formula $[7^t]^3$. Since $t(x)$ has only one root $\alpha = 3 + 2\cdot 7 + 3 \cdot 7^2 + \cdots \in \mathbb{Q}_7$, we can establish $[7^t]^3$ by Theorem 4.8. In much the same way as in Example 4.7, we find that $48 = h(7) \ne h(7^2) = 336$. Hence $r = 1$. Further calculation yields $\mathrm{ord}_7(\alpha) = 6$ and $\mathrm{ord}_{7^2}(\alpha) = 42$. This implies $s = 1$. Consequently, the partition formula $[7^t]^3$ can be established by (4.10):

$$[7^t]^3 = 1 + \sum_{i=0}^{t-1} 1 \cdot (6 \cdot 7^i) + \sum_{i=0}^{t-1} \frac{57 \cdot 7^{2i} - 1}{8} \cdot (48 \cdot 7^i).$$

Particulary, for $t = 1, 2, 3$ we have $[\ 7\ ]^3 = 1 + 6 + 7 \cdot 48$, $[7^2]^3 = 1 + 6 + 42 + 7 \cdot 48 + 349 \cdot 336$, and $[7^3]^3 = 1 + 6 + 42 + 294 + 7 \cdot 48 + 349 \cdot 336 + 17107 \cdot 2352$.

The most interesting case is that of $t(x)$ having exactly three roots α, β, γ in $\mathbb{Q}_p$. In this case, the forms of the partition formulas highly depend on the relationships between the orders of α, β, γ in the multiplicative group of the ring $\mathbb{Z}/p^t\mathbb{Z}$. Put $h_1 = \mathrm{ord}_p(\alpha)$, $h_2 = \mathrm{ord}_p(\beta)$, $h_3 = \mathrm{ord}_p(\gamma)$, and $h = h(p)$. By [3, Lemma 5.3], we have

$$\mathrm{lcm}(h_1, h_2) = \mathrm{lcm}(h_1, h_3) = \mathrm{lcm}(h_2, h_3) = \mathrm{lcm}(h_1, h_2, h_3) = h.$$

Moreover, by [3], exactly one of the four following events occurs

$$\text{(i) } h_1 < h_2 < h_3 < h, \quad \text{(ii) } h_1 < h_2 < h_3 = h, \quad \text{(iii) } h_1 < h_2 = h_3 = h, \quad \text{(iv) } h_1 = h_2 = h_3 = h. \tag{4.11}$$

Note that (i) occurs for the first time for $p = 4481$, (ii) for $p = 311$, (iii) for $p = 47$, and (iv) for $p = 103$. See also [2, p. 66]. For (i) in (4.11), we have

Theorem 4.10 *Let $t(x)$ have three roots α, β, γ in $\mathbb{Q}_p$, and assume that the numbers $h_1 = \mathrm{ord}_p(\alpha), h_2 = \mathrm{ord}_p(\beta), h_3 = \mathrm{ord}_p(\gamma)$, and $h = h(p)$ are distinct. Let r be the largest positive integer satisfying $h(p) = h(p^r)$, and let $s > r$ be the largest positive integer satisfying $\mathrm{ord}_p(\xi) = \mathrm{ord}_{p^s}(\xi)$ for a unique $\xi \in \{\alpha, \beta, \gamma\}$. Say, $\xi = \alpha$. Then, for any $t > s$, we have*

$$\begin{aligned}[p^t]^3 = 1 &+ \frac{p^s - 1}{h_1} \cdot h_1 + \frac{p^r - 1}{h_2} \cdot h_2 + \frac{p^r - 1}{h_3} \cdot h_3 + \frac{p^{3r} - 3p^r + 2}{h} \cdot h \\ &+ \sum_{i=1}^{t-s} \frac{p^s - p^{s-1}}{h_1} \cdot p^i h_1 + \sum_{i=1}^{t-r} \frac{p^r - p^{r-1}}{h_2} \cdot p^i h_2 + \sum_{i=1}^{t-r} \frac{p^r - p^{r-1}}{h_3} \cdot p^i h_3 \\ &+ \sum_{i=1}^{t-r} \frac{p^{3r+2i} - p^{3r+2i-3} - 3p^r + 3p^{r-1}}{h} \cdot p^i h.\end{aligned} \tag{4.12}$$

Particulary, if $r = s = 1$, we have

$$\begin{aligned}[p^t]^3 = 1 &+ \sum_{i=0}^{t-1} \frac{p-1}{h_1} \cdot p^i h_1 + \sum_{i=0}^{t-1} \frac{p-1}{h_2} \cdot p^i h_2 + \sum_{i=0}^{t-1} \frac{p-1}{h_3} \cdot p^i h_3 \\ &+ \sum_{i=0}^{t-1} \frac{p^{2i+3} - p^{2i} - 3p + 3}{h} \cdot p^i h.\end{aligned} \tag{4.13}$$

Proof Proceeding in much the same way, as in the proofs of the preceding theorems, we decompose the set $S = [\mathbb{Z}/p^t\mathbb{Z}]^3$ of p^{3t} triples into $t+1$ mutually disjunct subsets $S_0, S_1, \ldots, S_t$ defined by (4.4). Let $0 \le j \le t-1$. Clearly, $|S_j \cap E(\xi_t)| = p^{t-j} - p^{t-j-1}$ for any $\xi_t \in \{\alpha_t, \beta_t, \gamma_t\}$ and

$$|S_j - (E(\alpha_t) \cup E(\beta_t) \cup E(\gamma_t))| = p^{3(t-j)} - p^{3(t-j-1)} - 3p^{t-j} + 3p^{t-j-1}.$$

Let

$$B_1 = \bigcup_{j=0}^{t-s-1} S_j, \; B_2 = \bigcup_{j=t-s}^{t-r-1} S_j \text{ and } B_3 = \bigcup_{j=t-r}^{t-1} S_j.$$

If $0 \le j \le t-s-1$, then, by (1.2) and (1.3), we have

$$h(p^t)[a,b,c] = \begin{cases} p^{t-r-j}h, & \text{if } [a,b,c] \in S_j - (E(\alpha_t) \cup E(\beta_t) \cup E(\gamma_t)), \\ p^{t-s-j}h_1, & \text{if } [\mathrm{a,b,c}] \in \mathrm{S_j} \cap \mathrm{E}(\alpha_\mathrm{t}), \\ p^{t-r-j}h_2, & \text{if } [\mathrm{a,b,c}] \in \mathrm{S_j} \cap \mathrm{E}(\beta_\mathrm{t}), \\ p^{t-r-j}h_3, & \text{if } [\mathrm{a,b,c}] \in \mathrm{S_j} \cap \mathrm{E}(\gamma_\mathrm{t}), \end{cases} \tag{4.14}$$

and

$$\begin{aligned}[p^t]^3_{B_1} = &\sum_{j=0}^{t-s-1} \frac{p^s - p^{s-1}}{h_1} \cdot p^{t-s-j} h_1 + \sum_{j=0}^{t-s-1} \frac{p^r - p^{r-1}}{h_2} \cdot p^{t-r-j} h_2 \\ &+ \sum_{j=0}^{t-s-1} \frac{p^r - p^{r-1}}{h_3} \cdot p^{t-r-j} h_3 \\ &+ \sum_{j=0}^{t-s-1} \frac{p^{2t+r-2j} - p^{2t+r-2j-3} - 3p^r + 3p^{r-1}}{h} \cdot p^{t-r-j} h.\end{aligned}$$

If $t-s \le j \le t-r-1$, then (4.14) is valid except for the case of $[a,b,c] \in S_j \cap E(\alpha_t)$. Since, by (1.3), for these triples we have $h(p^t)[a,b,c] = h_1$, from (3.2) now it follows that

$$[p^t]^3_{B_2} = \frac{p^s - p^r}{h_1} \cdot h_1 + \sum_{j=t-s}^{t-r-1} \frac{p^r - p^{r-1}}{h_2} \cdot p^{t-r-j} h_2 + \sum_{j=t-s}^{t-s-1} \frac{p^r - p^{r-1}}{h_3} \cdot p^{t-r-j} h_3 + \sum_{j=t-s}^{t-r-1} \frac{p^{2t+r-2j} - p^{2t+r-2j-3} - 3p^r + 3p^{r-1}}{h} \cdot p^{t-r-j} h.$$

Similarly, for B_3 we have

$$[p^t]^3_{B_3} = \frac{p^r - 1}{h_1} \cdot h_1 + \frac{p^r - 1}{h_2} \cdot h_2 + \frac{p^r - 1}{h_3} \cdot h_3 + \frac{p^{3r} - 3p^r + 2}{h} \cdot h.$$

This, together with Theorem 3.1, yields

$$\begin{aligned}
[p^t]^3 = 1 &+ \frac{p^s - 1}{h_1} \cdot h_1 + \frac{p^r - 1}{h_2} \cdot h_2 + \frac{p^r - 1}{h_3} \cdot h_3 + \frac{p^{3r} - 3p^r + 2}{h} \cdot h \\
&+ \sum_{j=0}^{t-s-1} \frac{p^s - p^{s-1}}{h_1} \cdot p^{t-s-j} h_1 + \sum_{j=0}^{t-r-1} \frac{p^r - p^{r-1}}{h_2} \cdot p^{t-r-j} h_2 \\
&+ \sum_{j=0}^{t-r-1} \frac{p^r - p^{r-1}}{h_3} \cdot p^{t-r-j} h_3 + \sum_{j=0}^{t-r-1} \frac{p^{2t+r-2j} - p^{2t+r-2j-3} - 3p^r + 3p^{r-1}}{h} \cdot p^{t-r-j} h.
\end{aligned} \tag{4.15}$$

Using a suitable change of indexing in (4.15), we obtain (4.12) and (4.13) then follows.

In a similar way, we can also prove the following theorem which resolves the remaing cases in (4.11):

Theorem 4.11 *If $h_1 < h_2 < h_3 = h$, then*

$$\begin{aligned}
[p^t]^3 = 1 &+ \frac{p^s - 1}{h_1} \cdot h_1 + \frac{p^r - 1}{h_2} \cdot h_2 + \frac{p^{3r} - 2p^r + 1}{h} \cdot h + \sum_{i=1}^{t-s} \frac{p^s - p^{s-1}}{h_1} \cdot p^i h_1 \\
&+ \sum_{i=1}^{t-r} \frac{p^r - p^{r-1}}{h_2} \cdot p^i h_2 + \sum_{i=1}^{t-r} \frac{p^{3r+2i} - p^{3r+2i-3} - 2p^r + 2p^{r-1}}{h} \cdot p^i h.
\end{aligned} \tag{4.16}$$

If $h_1 < h_2 = h_3 = h$, then

$$\begin{aligned}
[p^t]^3 = 1 &+ \frac{p^s - 1}{h_1} \cdot h_1 + \frac{p^{3r} - p^r}{h} \cdot h + \sum_{i=1}^{t-s} \frac{p^s - p^{s-1}}{h_1} \cdot p^i h_1 \\
&+ \sum_{i=1}^{t-r} \frac{p^{3r+2i} - p^{3r+2i-3} - p^r + p^{r-1}}{h} \cdot p^i h.
\end{aligned} \tag{4.17}$$

If $h_1 = h_2 = h_3 = h$, *then*

$$[p^t]^3 = 1 + \frac{p^{3r} + p^s - p^r - 1}{h} \cdot h + \sum_{i=1}^{t-s} \frac{p^{3r+2i} - p^{3r+2i-3} + p^s - p^r + p^{r-1} - p^{s-1}}{h} \cdot p^i h$$
$$+ \sum_{i=t-s+1}^{t-r} \frac{p^{3r+2i} - p^{3r+2i-3} - p^r + p^{r-1}}{h} \cdot p^i h. \tag{4.18}$$

Specifically, if $r = s = 1$, then the formulas (4.16), (4.17), and (4.18) have more simple forms (4.16′), (4.17′), and (4.18′):

$$[p^t]^3 = 1 + \sum_{i=0}^{t-1} \frac{p-1}{h_1} \cdot p^i h_1 + \sum_{i=0}^{t-1} \frac{p-1}{h_2} \cdot p^i h_2 + \sum_{i=0}^{t-1} \frac{p^{2i+3} - p^{2i} - 2p + 2}{h} \cdot p^i h. \tag{4.16′}$$

$$[p^t]^3 = 1 + \sum_{i=0}^{t-1} \frac{p-1}{h_1} \cdot p^i h_1 + \sum_{i=0}^{t-1} \frac{p^{2i+3} - p^{2i} - p + 1}{h} \cdot p^i h. \tag{4.17′}$$

$$[p^t]^3 = 1 + \sum_{i=0}^{t-1} \frac{p^{2i}(p^3 - 1)}{h} \cdot p^i h. \tag{4.18′}$$

Example 4.12 We find the partition formula $[4481^t]^3$. Over $\mathbb{Q}_{4481}$, $t(x)$ has three roots $\alpha = 2677 + 3998 \cdot 4481 + \cdots$, $\beta = 3625 + 1879 \cdot 4481 + \cdots$, and $\gamma = 2661 + 3083 \cdot 4481 + \cdots$. Using simple calculation we obtain $h_1 = 640, h_2 = 896, h_3 = 2240$, and $h = 4480$. Moreover, we have $r = s = 1$. From (4.13) now it follows that

$$[\ 4481^t\ ]^3 = 1 + \sum_{i=0}^{t-1} 7 \cdot (640 \cdot 4481^i) + \sum_{i=0}^{t-1} 5 \cdot (896 \cdot 4481^i) + \sum_{i=0}^{t-1} 2 \cdot (2240 \cdot 4481^i) +$$
$$+ \sum_{i=0}^{t-1} (20083843 \cdot 4481^{2i} - 3) \cdot (4480 \cdot 4481^i).$$

References

[1] Andreassian, A.: Fibonacci Sequences Modulo m, *Fibonacci Quarterly,* **12.1** (1974), 51–64.

[2] Aydin, H., Dikici, R., Smith G. C.: Wall and Vinson revisited, *Applications of Fibonacci Numbers,* **5** (1993), 61–68.

[3] Klaška, J.: Tribonacci Modulo p^t *Mathematica Bohemica,* **133.3** (2008), 267–288.

[4] Klaška, J.: Tribonacci Modulo 2^t and 11^t, *Mathematica Bohemica,* **133.4** (2008), 377–387.

[5] Klaška, J.: On Tribonacci - Wieferich primes, *The Fibonacci Quarterly,* **46/47** (2008/2009), 290–297.

[6] Selmer, E. S.: Linear recurrence relations over finite fields, Bergen 1966

[7] Vince, A.: Period of a Linear Recurrence, *Acta Arith.,* **39** (1981), 303–311.

[8] Waddill, M. E.: Some Properties of a Generalized Fibonacci Sequence Modulo m, *The Fibonacci Quarterly,* **16.4** (1978), 344–353.

[9] Ward, M.: The characteristic number of a sequence of integers satisfying a linear recursion relation, *Trans. Amer. Math. Soc.,* **33** (1931), 153–165.

[10] Ward, M.: An enumerative problem in the arithmetic of linear recurring series, *Trans. Amer. Math. Soc.,* **37** (1935), 435–440.

CHAPTER 9

FURTHER RESEARCH OF MODULAR PERIODICITY OF TRIBONACCI SEQUENCE ★

Abstract. This paper deals with certain properties of a Tribonacci polynomial over finite fields. It can be viewed as a continuation of our preceding research of modular periodicity of integer sequences defined by a Tribonacci recurrence.

1. Introduction

Our extensive research [1], [2], [3] of modular periodicity of a Tribonacci sequence $(T_n)_{n=0}^{\infty}$ defined by the recurrence

$$T_{n+3} = T_{n+2} + T_{n+1} + T_n \quad \text{with} \quad T_0 = a,\ T_1 = b,\ T_2 = c \tag{1.1}$$

where a, b, c are arbitrary integers will now be completed by some further results. Particulary, an alternative proof will be found of the well known fact that $p = 2$ and $p = 11$ are only ramified primes of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$. Further, using the Frobenius density theorem, we prove Theorem 4.1 in [3]. In [3] this theorem was presented without a proof. Finally, a period $h(p)$ will be established of $(T_n \bmod p)_{n=0}^{\infty}$ for primes $p \leq 5000$.

2. Tribonacci ramified primes

It is well known (see e.g. [4, p. 86]) that the discriminant $d(a, b, c)$ of a cubic equation

$$x^3 + ax^2 + bx + c = 0 \tag{2.1}$$

is equal to

$$d(a, b, c) = a^2b^2 + 18abc - 4a^3c - 4b^3 - 27c^2. \tag{2.2}$$

If we apply (2.2) to $t(x)$, we obtain $d = -44 = -2^2 \cdot 11$. See also [5, p. 310]. The primes p satisfying $p|d$ are often referred to as ramified primes. Consequently, for a Tribonacci polynomial $t(x)$, there are only two ramified primes, $p = 2$ and $p = 11$. When investigating the modular periodicity of $(T_n \bmod p)_{n=0}^{\infty}$, the primes that divide the discriminant of $t(x)$ represent exceptions which must be examined separately, see [2]. Clearly, these primes correspond one-to-one to the cases of $t(x)$ having multiple roots over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of residue classes modulo p. In the subsequent lemma, we will prove, without using a discriminant, that the primes $p = 2, 11$ are the only primes for which the Tribonacci polynomial $t(x)$ has multiple roots.

Theorem 2.1. *The congruence $x^3 - x^2 - x - 1 \equiv 0 \pmod{p}$ has a triple root if and only if $p = 2$ and a double root if and only if $p = 11$.*

★ Published in J. Klaška, *Further research of modular periodicity of Tribonacci sequence*, Univ. S. Boh. Dept. of Mathematics Report Series **16** (2008), 57–63.

Proof. Let us first assume that the congruence has a triple root α. Then we have $x^3 - x^2 - x - 1 \equiv (x-\alpha)^3 \pmod p$. By expanding the right-hand side and matching the coefficients at identical powers of x, we get $3\alpha \equiv 1$, $3\alpha^2 \equiv -1$, $\alpha^3 \equiv 1$. From the first two congruences, it follows $\alpha \equiv -1$, which, together with $\alpha^3 \equiv 1$, yields $2 \equiv 0 \,(\operatorname{mod} p)$. Hence, we have $p = 2$ and $\alpha = 1$.

Let us next assume that the congruence has a double root β. Then $x^3 - x^2 - x - 1 \equiv (x-\alpha)(x-\beta)^2 \,(\operatorname{mod} p)$, with $\alpha \not\equiv \beta \,(\operatorname{mod} p)$. By matching the coefficients, we now obtain the congruences $\alpha + 2\beta \equiv 1$, $\beta^2 + 2\alpha\beta \equiv -1$, $\alpha\beta^2 \equiv 1$. From the first one, we get $\alpha \equiv 1 - 2\beta$. Substituting into the second and third ones yields

$$3\beta^2 - 2\beta - 1 \equiv 0 \,(\operatorname{mod} p) \quad \text{and} \quad 2\beta^3 - \beta^2 + 1 \equiv 0 \,(\operatorname{mod} p). \tag{2.3}$$

Adding the congruences in (2.3) yields $2\beta(\beta^2 + \beta - 1) \equiv 0$. Since $p \neq 2$ and $\beta = 0$ is not a solution of (2.3) for any prime p, we have $2\beta \not\equiv 0$. Hence

$$\beta^2 + \beta - 1 \equiv 0 \,(\operatorname{mod} p). \tag{2.4}$$

By multiplying the first congruence in (2.3) by 2β and subtracting it from the second congruence in (2.3) multiplied by 3, we have

$$\beta^2 + 2\beta + 3 \equiv 0 \,(\operatorname{mod} p). \tag{2.5}$$

From (2.4) and (2.5), we obtain $\beta \equiv -4$ which, together with $\alpha \equiv 1 - 2\beta$, implies $\alpha \equiv 9$. Now, it follows from $\beta^2 + 2\alpha\beta \equiv -1$ that $55 \equiv 0$ (mod p) and, from $\alpha\beta^2 \equiv 1$, we get $143 \equiv 0$ (mod p). Combining this facts, we have $11 \equiv 0$ (mod p). It follows now that $p = 11$ and $\alpha = 9, \beta = 7$. The validity of the inverse implications is obvious in both cases. ☐

Note that, for a Fibonacci polynomial $f(x) = x^2 - x - 1$, there is only one ramified prime $p = 5$. See for example [7, p. 528]. The table below can give us a more exact idea of the ramified primes corresponding to the polynomials of the form $f_k(x) = x^k - \cdots - x - 1$. It contains prime factorizations of the discriminants d_k of these polynomials for $1 < k \leq 15$.

Looking at Table 1, we can see, for example, that, for a Tetranacci polynomial, there is only one ramified prime $p = 563$, (see also [6, p. 237]), for a Pentanacci polynomial there are two ramified primes $p = 2$ and $p = 599$, etc.

3. Tribonacci and Frobenius density theorem

Let $f(x)$ be a monic polynomial with integer coefficients of degree n. Recall that $f(x)$ is monic if the leading coefficient of $f(x)$ is 1. Assume that the discriminant d of $f(x)$ does not vanish. This implies that $f(x)$ has n distinct roots $\alpha_1, \ldots, \alpha_n$ in a suitable extension field K of the field $\mathbb{Q}$ of rational numbers. Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. The Galois group $G = \operatorname{Gal}(K/\mathbb{Q})$ of $f(x)$ is the group of field automorphisms of K. As each $g \in G$ permutes the roots $\alpha_1, \ldots, \alpha_n$ of $f(x)$, we may consider G as a subgroup of the group S_n of permutations of n symbols. If we write $g \in G$ as a product of disjoint cycles, then the lengths of these cycles define the cycle pattern of g, which is a partition of n. Recall that a partition of n is an ordered set $(n_1, \ldots, n_k)$ of positive integers $n_1 \geq \cdots \geq n_k$ with $n = n_1 + \cdots + n_k$. Let p be a prime such that $p \nmid d$. Then we can write $f(x)$ modulo p as a product $f_1(x) \cdots f_k(x)$ of distinct irreducible factors over $\mathbb{F}_p$. Let the degrees of $f_1(x), \ldots, f_k(x)$ be $n_1, \ldots, n_k$. Since $n_1 + \cdots + n_k = n$, the partition $(n_1, \ldots, n_k)$ forms the splitting type τ of $f(x)$ modulo p. This is also

Table 1

$$\begin{aligned}
d_2 &= 5\\
d_3 &= -2^2 \cdot 11\\
d_4 &= -563\\
d_5 &= 2^4 \cdot 599\\
d_6 &= 205\,937\\
d_7 &= -2^6 \cdot 84\,223\\
d_8 &= -1\,319 \cdot 126\,913\\
d_9 &= 2^8 \cdot 17 \cdot 487 \cdot 2\,851\\
d_{10} &= 7 \cdot 35\,616\,734\,267\\
d_{11} &= -2^{10} \cdot 19 \cdot 131 \cdot 4\,550\,179\\
d_{12} &= -10\,607 \cdot 211\,723 \cdot 267\,679\\
d_{13} &= 2^{12} \cdot 6\,317 \cdot 1\,328\,851\,967\\
d_{14} &= 112\,589 \cdot 219\,361 \cdot 87\,132\,013\\
d_{15} &= -2^{14} \cdot 241 \cdot 2\,347 \cdot 2\,879 \cdot 5\,484\,307
\end{aligned}$$

a partition of n. Let S denote the set of unramified primes of $f(x)$, i.e., the set of primes $p \nmid d$. Consider the set S_τ of unramified primes for which $f(x)$ factors with the splitting type τ. The natural density $d(S_\tau)$ of primes $p \in S_\tau$ is defined as follows

$$d(S_\tau) = \lim_{x\to\infty} \frac{|\{p \in S_\tau; p \le x\}|}{|\{p \in S; p \le x\}|}. \tag{3.1}$$

Now we can state

Frobenius density theorem (1886). *The set S_τ of all primes p for which $f(x)$ has the splitting type τ over $\mathbb{F}_p$ has a natural density $d(S_\tau) = |G_\tau|/|G|$ where $|G_\tau|$ is the number of all permutations $g \in G$ with cycle type τ.*

As there is only one permutation in S_n with the cycle pattern $(1, \dots, 1)$, we have

Consequence 3.1. The set of primes p for which $f(x)$ modulo p splits completely into linear factors has density $1/|G|$.

Now we are ready to apply the Frobenius density theorem to a case of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$. By Theorem 2.1, the only ramified primes are 2 and 11. The degree of $t(x)$ is 3 and, for the number 3, there are the following partitions: $3, 2+1, 1+1+1$. Thus, the splitting types of $t(x)$ are $\tau_1 = (3)$, $\tau_2 = (2,1)$, and $\tau_3 = (1,1,1)$. For the Galois group G of $t(x)$, we have $G = S_3$. Clearly, S_3 consists of 6 permutations which can be written as a product of disjoint cycles as follows $g_1 = (1)(2)(3)$, $g_2 = (1,2)(3)$, $g_3 = (1,3)(2)$, $g_4 = (2,3)(1)$, $g_5 = (1,2,3)$, and $g_6 = (1,3,2)$. This implies that $|G_{\tau_1}| = 2$, $|G_{\tau_2}| = 3$, $|G_{\tau_3}| = 1$. Now we recall the notation used in [3]. Let I denote the set of all primes for which $t(x)$ is irreducible over $\mathbb{F}_p$, Q denote the set of all primes p for which $t(x)$ is factorized over

$\mathbb{F}_p$ into the product of a linear factor and a quadratic irreducible factor and L denote the set of all unramified primes for which $t(x)$ splits completely into linear factors. Since $S_{\tau_1} = I$, $S_{\tau_2} = Q$, and $S_{\tau_3} = L$, using Frobenius density theorem, we have $d(I) = 1/3, d(Q) = 1/2, d(L) = 1/6$. Consequently, the natural densities of I, Q, L satisfy

$$d(I) : d(Q) : d(L) = 2 : 3 : 1 \tag{3.2}$$

and we have [3, Theorem 4.1]:

Theorem 3.2. *For $d(I), d(Q), d(L)$ it hold $d(I) : d(Q) : d(L) = 2 : 3 : 1$.*

4. Exact values of the primitive periods $h(p)$.

Let L be the splitting field of $t(x)$ over $\mathbb{F}_p$, $p \neq 2, 11$ and α, β, γ be the roots of $t(x)$ in L. Then we have

$$h(p) = \mathrm{lcm}(\mathrm{ord}_L(\alpha), \mathrm{ord}_L(\beta), \mathrm{ord}_L(\gamma)) \tag{4.1}$$

where the numbers $\mathrm{ord}_L(\alpha), \mathrm{ord}_L(\beta), \mathrm{ord}_L(\gamma)$ are the orders of α, β, γ in the multiplicative group of L and lcm is their least common multiple. See [5]. In the following table, we present the exact values of $h(p)$ for $p \leq 5000$. Note that, up to present, no table of the periods $h(p)$ has been published.

References

[1] J. Klaška, *Tribonacci modulo p^t*, Mathematica Bohemica **133.3** (2008), 267–288.
[2] J. Klaška, *Tribonacci modulo 2^t and 11^t*, Mathematica Bohemica **133.4** (2008), 377–387.
[3] J. Klaška, *On Tribonacci-Wieferich primes*, The Fibonacci Quarterly **46/47** (2008/2009), 290–297.
[4] Š. Schwarz, *Základy náuky o riešení rovníc*, Bratislava, (1968).
[5] A. Vince, *Period of a Linear Recurrence*, Acta Arith. **39** (1981), 303–311.
[6] M. E. Waddill, *Some Properties of the Tetranacci Sequence Modulo m*, The Fibonacci Quarterly **30.3** (1992), 232–238.
[7] D. D. Wall, *Fibonacci Series Modulo m*, Amer. Math. Monthly **67.6** (1960), 525–532.

Keywords: Tribonacci polynomial, ramified primes, asymptotic density, periods

MSC 2000: 11B50, 11B39

TABLE 2. Table of primitive periods $h(p)$ for $p \leq 5000$.

p	$h(p)$	p	$h(p)$	p	$h(p)$	p	$h(p)$	p	$h(p)$
2	4	269	268	617	616	1009	509040	1427	678776
3	13	271	73440	619	127927	1013	1027183	1429	1021020
5	31	277	12788	631	132931	1019	43265	1433	1432
7	48	281	13160	641	411523	1021	340	1439	719
11	110	283	13348	643	138031	1031	354320	1447	2093808
13	168	293	28616	647	419257	1033	1067088	1451	701800
17	96	307	31416	653	22477	1039	360187	1453	704221
19	360	311	310	659	72380	1049	1101451	1459	236520
23	553	313	32761	661	145861	1051	73640	1471	360640
29	140	317	100807	673	113232	1061	1126783	1481	365560
31	331	331	36631	677	11752	1063	70623	1483	733591
37	469	337	16224	683	682	1069	95230	1487	184264
41	560	347	40136	691	159391	1087	1086	1489	739537
43	308	349	17400	701	54600	1091	99190	1493	743016
47	46	353	124963	709	167797	1093	398581	1499	2248501
53	52	359	42960	719	517681	1097	200568	1511	2284633
59	3541	367	45019	727	176419	1103	1217713	1523	2321053
61	1860	373	139128	733	89548	1109	1108	1531	58599
67	1519	379	48007	739	22755	1117	40248	1543	1542
71	5113	383	147073	743	46004	1123	1122	1549	800317
73	5328	389	151711	751	188251	1129	1274640	1553	14356
79	3120	397	132	757	756	1151	5520	1559	405080
83	287	401	400	761	193040	1153	443521	1567	1566
89	8011	409	41820	769	591360	1163	450856	1571	1570
97	3169	419	418	773	386	1171	457471	1579	207770
101	680	421	420	787	309684	1181	590	1583	417648
103	51	431	61920	797	636007	1187	469656	1597	212534
107	1272	433	62641	809	218160	1193	1424443	1601	854400
109	990	439	6424	811	36540	1201	1442400	1607	2584057
113	12883	443	196693	821	28085	1213	490861	1609	1608
127	5376	449	202051	823	226051	1217	246848	1613	867256
131	5720	457	34808	827	227976	1223	166192	1619	145620
137	18907	461	35420	829	229357	1229	503480	1621	810
139	3864	463	71611	839	704761	1231	757680	1627	882376
149	7400	467	218557	853	181902	1237	618	1637	2681407
151	2850	479	76480	857	61204	1249	780000	1657	305072
157	8269	487	79219	859	246247	1259	1586341	1663	1382784
163	162	491	10045	863	862	1277	1632077	1667	926296
167	9296	499	166	877	769128	1279	545707	1669	2785560
173	2494	503	42168	881	777043	1283	274348	1693	409464
179	32221	509	259591	883	441	1289	12040	1697	1696
181	10981	521	271963	887	131128	1291	1290	1699	566
191	36673	523	273528	907	906	1297	210276	1709	2922391
193	4656	541	58536	911	910	1301	1693903	1721	2963563
197	3234	547	149604	919	46920	1303	566371	1723	494788
199	198	557	103416	929	928	1307	653	1733	500548
211	5565	563	52828	937	877968	1319	579920	1741	32611
223	16651	569	53960	941	147580	1321	582121	1747	1017919
227	17176	571	40755	947	897757	1327	34528	1753	584
229	17557	577	111169	953	302736	1361	308720	1759	3094080
233	9048	587	293	967	467544	1367	683	1777	150368
239	4760	593	3256	971	943813	1373	1886503	1783	1060291
241	29040	599	598	977	136501	1381	381432	1787	3195157
251	63253	601	24080	983	967273	1399	652400	1789	533420
257	256	607	184224	991	990	1409	1986691	1801	1081200
263	23056	613	46971	997	331336	1423	675451	1811	1093240

p	$h(p)$	p	$h(p)$	p	$h(p)$	p	$h(p)$	p	$h(p)$
1823	1107776	2269	1716877	2699	1041043	3169	3348577	3613	516
1831	1118131	2273	26909	2707	2443519	3181	421615	3617	13086307
1847	1137136	2281	1735081	2711	7352233	3187	10156968	3623	1811
1861	91140	2287	1743456	2713	7360368	3191	3190	3631	1210
1867	1742844	2293	1753381	2719	7392960	3203	142489	3637	6613884
1871	500359	2297	5278507	2729	2728	3209	1716280	3643	13271448
1873	1872	2309	161560	2731	910	3217	3450769	3659	2231380
1877	1174376	2311	1781011	2741	313045	3221	10378063	3671	4492080
1879	1177507	2333	5445223	2749	2519000	3229	1737740	3673	1226448
1889	237888	2339	227955	2753	1083109	3251	352300	3677	3676
1901	3615703	2341	1827541	2767	79753	3253	2645502	3691	13623480
1907	1906	2347	1836919	2777	2776	3257	3256	3697	4557169
1913	304964	2351	1842400	2789	1296420	3259	1086	3701	3700
1931	1242920	2357	5557807	2791	519312	3271	509653	3709	1719585
1933	1245496	2371	5621640	2797	1398	3299	725560	3719	13834681
1949	1266200	2377	1884169	2801	2615200	3301	3633301	3727	4631419
1951	1269451	2381	2380	2803	2802	3307	5468124	3733	3732
1973	3894703	2383	236612	2819	7949581	3313	5487984	3739	13980120
1979	1305480	2389	5707320	2833	1337648	3319	1573680	3761	4715040
1987	1974084	2393	954408	2837	2682856	3323	3322	3767	14194057
1993	3972048	2399	5757601	2843	2842	3329	3694080	3769	109272
1997	147704	2411	242205	2851	8128200	3331	3699631	3779	1586760
1999	666000	2417	973648	2857	8162448	3343	3725216	3793	3792
2003	2002	2423	5873353	2861	8188183	3347	11205757	3797	200239
2011	1348711	2437	742371	2879	460480	3359	11286241	3803	4820936
2017	1356769	2441	397232	2887	2779219	3361	5648160	3821	14603863
2027	4110757	2447	5990257	2897	1448	3371	11367013	3823	2435888
2029	1372957	2459	403112	2903	1404568	3373	541768	3833	14695723
2039	2038	2467	2029519	2909	8465191	3389	11488711	3847	14799408
2053	4214808	2473	2039401	2917	1418148	3391	1130	3851	14834053
2063	709328	2477	2045176	2927	1463	3407	1934608	3853	963
2069	2068	2503	3132504	2939	575848	3413	1664569	3863	4974256
2081	360880	2521	6355440	2953	984	3433	1716	3877	1938
2083	1446991	2531	6408493	2957	8746807	3449	3965200	3881	15066043
2087	120988	2539	1269	2963	8782333	3457	3984769	3889	630180
2089	290928	2543	2155616	2969	587664	3461	998210	3907	1908081
2099	4407901	2549	166600	2971	2943271	3463	1154	3911	2549320
2111	67520	2551	325380	2999	374750	3467	1001674	3917	2192401
2113	704	2557	167713	3001	3003001	3469	4012477	3919	3918
2129	302176	2579	1289	3011	755510	3491	12190573	3923	1709992
2131	4541160	2591	149184	3019	434161	3499	1749	3929	5145680
2137	1522969	2593	1680912	3023	9141553	3511	12327120	3931	5152231
2141	1527960	2609	1134480	3037	3075469	3517	1546161	3943	1314
2143	1531531	2617	402864	3041	3040	3527	148092	3947	15582757
2153	772568	2621	2620	3049	9296400	3529	4152457	3967	15737088
2161	1557361	2633	365017	3061	3124261	3533	2080348	3989	530404
2179	1583407	2647	1000944	3067	3136519	3539	2087420	4001	1334000
2203	1618471	2657	2353216	3079	9480240	3541	181720	4003	16024008
2207	1623616	2659	883785	3083	9507973	3547	4194919	4007	2003
2213	408114	2663	7094233	3089	9545011	3557	12655807	4013	1003
2221	1233210	2671	890	3109	9665880	3559	12666480	4019	16156381
2237	2236	2677	2389669	3119	3242720	3571	12752040	4021	8084220
2239	1002624	2683	7198488	3121	1391520	3581	356210	4027	1342
2243	838508	2687	7222657	3137	1640128	3583	6418944	4049	16398451
2251	844500	2689	2411137	3163	3334856	3593	4303216	4051	5471551
2267	5141557	2693	7254943	3167	3343296	3607	542102	4057	5487769

p	$h(p)$	p	$h(p)$	p	$h(p)$	p	$h(p)$	p	$h(p)$
4073	16593403	4253	6029336	4451	3301900	4643	21562093	4817	7734496
4079	4078	4259	1209272	4457	6621616	4649	7204400	4831	11669280
4091	697345	4261	6053461	4463	1106576	4651	7212151	4861	1389960
4093	4092	4271	18245713	4481	4480	4657	7230769	4871	2435
4099	4200450	4273	6087601	4483	2512161	4663	7247856	4877	23790007
4111	16900320	4283	18348373	4493	20191543	4673	4672	4889	23907211
4127	5677376	4289	6131840	4507	10156524	4679	21897721	4903	24039408
4129	5684257	4297	18464208	4513	6790561	4691	22010173	4909	8034397
4133	1423474	4327	6242419	4517	1700274	4703	7372736	4919	8065520
4139	4138	4337	4336	4519	6808627	4721	7429280	4931	4930
4153	1437284	4339	6277087	4523	6819176	4723	4722	4933	4932
4157	960036	4349	4348	4547	4546	4729	7454480	4937	2468
4159	5767147	4357	6329269	4549	6897800	4733	22406023	4943	4942
4177	726972	4363	19035768	4561	10401360	4751	3762000	4951	2475
4201	88242	4373	6374376	4567	3476248	4759	7549360	4957	24571848
4211	17736733	4391	3213480	4583	7001296	4783	7627291	4967	342654
4217	17787307	4397	805567	4591	2295	4787	7638456	4969	352728
4219	17799960	4409	4408	4597	7044136	4789	4788	4973	24735703
4229	17888671	4421	1303016	4603	7064071	4793	3828808	4987	4986
4231	8950680	4423	6522451	4621	4620	4799	23035201	4993	958848
4241	5995360	4441	19722480	4637	895907	4801	7684801	4999	4998
4243	18003048	4447	6593419	4639	4304064	4813	23164968		

CHAPTER 10

THE CUBIC CHARACTER OF THE TRIBONACCI ROOTS ⋆

Abstract. If τ is any root of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ in the Galois field $\mathbb{F}_p$ where p is a prime, $p \equiv 1 \pmod 3$, then

$$\tau^{\frac{p-1}{3}} \equiv 2^{\frac{2(p-1)}{3}} \pmod p.$$

More generally, if χ is a root of $t(x)$ in any field extension $\mathbb{G}$ of $\mathbb{F}_p$, then 2χ is a cubic residue of the field $\mathbb{G}$.

1. Introduction

The quadratic character of the root $\theta = (1 + \sqrt{5})/2$ of the Fibonacci polynomial $f(x) = x^2 - x - 1$ was examined by E. Lehmer in [2]. The way we understand Lehmer's Theorem 1 in [2, p. 137], which was written in a different form, is as follows. Let p be a prime in the form $p = a^2 + b^2$ where $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod 4$. Furthermore, suppose that θ is a root of f in the Galois field $\mathbb{F}_p$; then we have

$$\theta^{\frac{p-1}{2}} = \left(\frac{\theta}{p}\right) = \begin{cases} 1 & \text{if } \ p = 20m + 1, b \equiv 0 \pmod 5 \text{ or } p = 20m + 9, a \equiv 0 \pmod 5 \\ -1 & \text{if } \ p = 20m + 1, a \equiv 0 \pmod 5 \text{ or } p = 20m + 9, b \equiv 0 \pmod 5). \end{cases}$$

In this paper we let τ be an arbitrary root of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ in the Galois field $\mathbb{F}_p$ where p is a prime, $p \equiv 1 \pmod 3$. The purpose of our article is to prove the following identity for the cubic character of τ and 2 in $\mathbb{F}_p$:

$$\tau^{\frac{p-1}{3}} = \left(\frac{\tau}{p}\right)_3 = 2^{\frac{2(p-1)}{3}}.$$

Moreover, if χ is a root of $t(x)$ in any field extension $\mathbb{G}$ of $\mathbb{F}_p$, then we show that 2χ is a cubic residue of the field $\mathbb{G}$, i.e. there exists $\omega \in \mathbb{G}$ such that $2\chi = \omega^3$.

2. Preliminaries

Let $\mathbb{F}$ be a field in which there exists an element $\varepsilon \neq 1$ such that $\varepsilon^3 = 1$. Then $\operatorname{char} \mathbb{F} \neq 3$ and $\varepsilon^2 + \varepsilon + 1 = 0$. For $a, b, c \in \mathbb{F}$, put

$$\begin{aligned} w_1(x) &= x^3 + ax^2 + bx + c, \\ w_2(x) &= w_1(\varepsilon x) = x^3 + \varepsilon^2 ax^2 + \varepsilon bx + c, \\ w_3(x) &= w_1(\varepsilon^2 x) = x^3 + \varepsilon ax^2 + \varepsilon^2 bx + c. \end{aligned}$$

By direct calculation we get the following lemma.

⋆ Published in J. Klaška, L. Skula, *The cubic character of the Tribonacci roots*, The Fibonacci Quarterly **48.1** (2010), 21–28.

Lemma 2.1. $w_1(x)w_2(x)w_3(x) = x^9 + (a^3 - 3ab + 3c)x^6 + (b^3 - 3abc + 3c^2)x^3 + c^3.$

For $c \in \mathbb{F}$ put

$$\begin{aligned} A(c) &= -18c^2 + 3, \\ B(c) &= -9c^2 - 27c - 24, \\ C(c) &= 9c^2 - 27c + 28, \\ f(x, c) &= x^3 + A(c)x^2 + B(c)x + C(c) \in \mathbb{F}[x]. \end{aligned}$$

Clearly, $f(x, -1) = x^3 - 15x^2 - 6x + 64 = (x - 2)g(x)$, where $g(x) = x^2 - 13x - 32$.

Furthermore, we shall consider the following polynomials over the field $\mathbb{F}$:

$$t(x) = x^3 - x^2 - x - 1, \quad u(x) = t(x^3) = x^9 - x^6 - x^3 - 1.$$

The polynomial $t(x)$ is the well-known Tribonacci polynomial. Let $c \in \{-1, -\varepsilon, -\varepsilon^2\}$. Using the identities $c^3 = -1$, $c^4 = -c$, $c^6 = 1$ and $c^{-1} = -c^2$, we obtain the following lemma.

Lemma 2.2. *For any* $c \in \{-1, -\varepsilon, -\varepsilon^2\}$, $b \in \mathbb{F}$, $b \neq 0$, *we have*

$$\frac{(b^3 + 3c^2 + 1)^3}{27b^3c^3} - \frac{b^3 + 3c^2 + 1}{c} + 3c + 1 = -\frac{b^9 + A(c)b^6 + B(c)b^3 + C(c)}{27b^3} = -\frac{f(b^3, c)}{27b^3}.$$

Theorem 2.3. *Let* char $\mathbb{F} \neq 2, 7$. *Then we have* $u(x) = w_1(x)w_2(x)w_3(x)$ *if and only if*

$$c \in \{-1, -\varepsilon, -\varepsilon^2\}, \quad f(b^3, c) = 0, \quad b \neq 0 \quad \textit{and} \quad a = \frac{b^3 + 3c^2 + 1}{3bc}. \tag{2.1}$$

Proof. Using Lemma 2.1 we have $u(x) = w_1(x)w_2(x)w_3(x)$ if and only if

$$\begin{aligned} a^3 - 3ab + 3c &= -1, \\ b^3 - 3abc + 3c^2 &= -1, \\ c^3 &= -1. \end{aligned} \tag{2.2}$$

First, assume that the identities (2.2) are valid. Then $c \in \{-1, -\varepsilon, -\varepsilon^2\}$. If $b = 0$, then from the second identity in (2.2) we get $3c^2 = -1$ and thus $27 = -1$, which is a contradiction with char $\mathbb{F} \neq 2, 7$. Consequently, $b \neq 0$ and $a = (b^3 + 3c^2 + 1)/3bc$. Substituting into the first identity in (2.2), we have

$$\frac{(b^3 + 3c^2 + 1)^3}{27b^3c^3} - \frac{b^3 + 3c^2 + 1}{c} + 3c + 1 = 0.$$

Combining Lemma 2.2 with $c^3 = -1$, we obtain $f(b^3, c) = 0$ and (2.1) follows.

Conversely, let $c \in \{-1, -\varepsilon, -\varepsilon^2\}$, $f(b^3, c) = 0$, $b \neq 0$, and $a = (b^3 + 3c^2 + 1)/3bc$. Then $c^3 = -1$ and, from $a = (b^3 + 3c^2 + 1)/3bc$, we have $b^3 - 3abc + 3c^2 = -1$. Put $d = a^3 - 3ab + 3c$. Then by Lemma 2.2 we have

$$d = \frac{(b^3 + 3c^2 + 1)^3}{27b^3c^3} - \frac{b^3 + 3c^2 + 1}{c} + 3c = -\frac{f(b^3, c)}{27b^3} - 1 = -1$$

as required. □

Now we recall a well known Stickelberger parity theorem [3] for the case of a cubic polynomial [5, p. 189]. See also Dickson's history [1, pp. 249 – 251] or consult [4, p. 42].

Theorem 2.4. *Let N be the number of solutions of $x^3 + Ax^2 + Bx + C \equiv 0 \pmod{p}$ where $A, B, C \in \mathbb{Z}$ and let*

$$D = A^2B^2 - 4B^3 - 4A^3C - 27C^2 + 18ABC \tag{2.3}$$

be the discriminant of the cubic polynomial $x^3 + Ax^2 + Bx + C$. If p is a prime, $p > 3$ and $p \nmid D$, we have:

$$\begin{aligned} &N = 1 \text{ if and only if } (D/p) = -1, \\ &N = 0 \text{ or } N = 3 \text{ if and only if } (D/p) = 1. \end{aligned} \tag{2.4}$$

Particulary, for the Tribonacci polynomial $t(x)$, we obtain the following corollary.

Corollary 2.5. *Let N be the number of distinct roots of the Tribonacci polynomial $t(x)$ in the field $\mathbb{F}_p$ where p is an arbitrary prime, $p \neq 2, 11$. Then $t(x)$ does not have multiple roots in $\mathbb{F}_p$, and we have:*

$$\begin{aligned} &N = 1 \text{ if and only if } (p/11) = -1, \\ &N = 0 \text{ or } N = 3 \text{ if and only if } (p/11) = 1. \end{aligned} \tag{2.5}$$

Proof. By (2.3), $D = -44 = -2^2 \cdot 11$. For $p = 3$, we have $(3/11) = 1$ and $N = 0$. Calculating the Legendre - Jacobi symbol, we get $(-44/p) = (p/11)$ and (2.5) follows from (2.4). □

Lemma 2.6. *For $c \in \{-1, -\varepsilon, -\varepsilon^2\}$, let D_c be the discriminant of $f(x, c)$. Then $D_c = 866052 = 2^2 \cdot 3^9 \cdot 11$ and $(D_c/p) = (p/11)$.*

Proof. For $c = -1$ we have $A(-1) = -15$, $B(-1) = -6$, $C(-1) = 64$ and, from (2.3), it follows that $D_{-1} = 866052$. For $c \in \{-\varepsilon, -\varepsilon^2\}$ we use the identity $c^2 - c + 1 = 0$ to determine D_c. From the quadratic reciprocity law and from further properties of the Legendre - Jacobi symbol it follows that

$$\begin{aligned} \left(\frac{866052}{p}\right) &= \left(\frac{3}{p}\right)\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{5(p-1)}{2}}\left(\frac{p}{11}\right) \\ &= (-1)^{3(p-1)}\left(\frac{1}{3}\right)\left(\frac{p}{11}\right) = \left(\frac{p}{11}\right). \end{aligned}$$

□

From now on, we will assume that p is an arbitrary prime such that $p \equiv 1 \pmod{3}$ and $\mathbb{F}$ is an arbitrary finite field with characteristic p. Then there is an $n \in \mathbb{N}$ such that $\mathbb{F} = \mathbb{F}_{p^n}$. Let $\mathbb{F}^\times$ denote the multiplicative group of the field $\mathbb{F}$. This group is cyclic of order $p^n - 1$ and its generator will be denoted by g. For any $\xi \in \mathbb{F}^\times$, there is exactly one integer $\operatorname{ind} \xi$ such that $\xi = g^{\operatorname{ind} \xi}$ and $0 \le \operatorname{ind} \xi \le p^n - 2$. Clearly, for $\xi_1, \xi_2 \in \mathbb{F}^\times$, we have $\operatorname{ind} \xi_1\xi_2 \equiv \operatorname{ind} \xi_1 + \operatorname{ind} \xi_2 \pmod{p^n - 1}$. We can assume that $\varepsilon = g^{(p^n-1)/3}$. Then $\operatorname{ind} \varepsilon = (p^n - 1)/3$ and $\operatorname{ind} \varepsilon^2 = 2(p^n - 1)/3$. For $e \in \{0, 1, 2\}$ put

$$C_e = \{\xi \in \mathbb{F}^\times; \operatorname{ind} \xi \equiv e \pmod{3}\} = \{\xi \in \mathbb{F}^\times; \xi = g^{3k+e}, k \in \mathbb{Z}, 0 \le k < (p^n - 1)/3\}.$$

We will call the sets C_0, C_1, C_2 *the cubic classes of the field* $\mathbb{F}$. Clearly, $\{C_0, C_1, C_2\}$ is a partition of $\mathbb{F}^\times$. *For $\xi \in \mathbb{F}^\times$ we have $\xi \in C_0$ if and only if there exists $\omega \in \mathbb{F}^\times$ such that $\omega^3 = \xi$.* Let us call the elements $\xi's$ with this property *the cubic residues of the field* $\mathbb{F}$.

Lemma 2.7. *Let $\alpha, \beta, \gamma \in \mathbb{F}$ and $\alpha\beta\gamma \in C_0$. Then there exists $e \in \{0, 1, 2\}$ such that $\{\alpha, \beta, \gamma\} \subseteq C_e$ or α, β, γ belong to distinct cubic classes of the field $\mathbb{F}$.*

Proof. Suppose that there are $e_1, e_2 \in \{0, 1, 2\}$, $e_1 \neq e_2$ such that $\alpha, \beta \in C_{e_1}$, $\gamma \in C_{e_2}$. Then $\operatorname{ind} \alpha\beta\gamma \equiv \operatorname{ind} \alpha + \operatorname{ind} \beta + \operatorname{ind} \gamma \pmod{p^n - 1}$ and thus $\operatorname{ind} \alpha\beta\gamma \equiv 2e_1 + e_2 \pmod 3$. On the other hand, we have $\operatorname{ind} \alpha\beta\gamma \equiv 0 \pmod 3$, which implies $2e_1 + e_2 \equiv 0 \pmod 3$. Consequently, we have $e_1 = e_2$ and a contradiction follows. □

For the next theorem we need the following lemma which can be verified by direct computation.

Lemma 2.8. *The Tribonacci polynomial $t(x)$ has a unique root in $\mathbb{F}_7$ equal to 3. In the field $\mathbb{F}_{49}$, the polynomial $t(x)$ has three distinct roots $3, -1 + 5i, -1 - 5i$ where $i \in \mathbb{F}_{49}$, $i^2 = -1$. These roots belong to the same residue class of $\mathbb{F}_{49}$ and, for any $\chi \in \{3, -1 + 5i, -1 - 5i\}$, we have $(2\chi)^{(7^2-1)/3} = 1$. Consequently, if $t(x)$ has three distinct roots in an extension field $\mathbb{F}$ of $\mathbb{F}_7$, then $\mathbb{F}$ is an extension field of $\mathbb{F}_{49}$ and $3, -1 + 5i, -1 - 5i$ are roots of $t(x)$ in $\mathbb{F}$ belonging to the same cubic class of $\mathbb{F}$.*

Theorem 2.9. *Let $t(x)$ have three distinct roots $\alpha, \beta, \gamma \in \mathbb{F}$. Then*

(i) There is an $e_1 \in \{0, 1, 2\}$ such that $\{\alpha, \beta, \gamma\} \subseteq C_{e_1}$.

(ii) If $\operatorname{char} \mathbb{F} \neq 7$, then, for each $c \in \{-1, -\varepsilon, -\varepsilon^2\}$, the polynomial $f(x, c)$ has three distinct roots in $\mathbb{F}$ belonging to the same cubic class C_{e_2} of $\mathbb{F}$ where $e_2 \in \{0, 1, 2\}$ and $e_1 + e_2 \equiv 0 \pmod 3$. In particular, for any $\tau \in \{\alpha, \beta, \gamma\}$, the element 2τ is a cubic residue of the field $\mathbb{F}$.

Proof. (i) For $p = 7$ the first part of the theorem follows from Lemma 2.8. Let $p \neq 7$. Suppose that for some $e \in \{0, 1, 2\}$ the inclusion $\{\alpha, \beta, \gamma\} \subseteq C_e$ is not valid. From the Viète equation $\alpha\beta\gamma = 1$ it follows that $\alpha\beta\gamma \in C_0$ and, by Lemma 2.7, the roots α, β, γ belong to distinct cubic classes of $\mathbb{F}$. We can assume that $\alpha \in C_0, \beta \in C_1, \gamma \in C_2$. Then there is $\xi_1 \in \mathbb{F}$ such that $\alpha = \xi_1^3$ and thus $t(x) = (x - \xi_1^3)(x - \beta)(x - \gamma)$. This implies that $\xi_1^3\beta\gamma = 1$.

Since $\beta \in C_1$, the polynomial $x^3 - \beta$ is irreducible over $\mathbb{F}$. Let K be the splitting field of $x^3 - \beta$ over $\mathbb{F}$. Then there is $\xi_2 \in K$ such that $\beta = \xi_2^3$ and $x^3 - \beta = (x - \xi_2)(x - \varepsilon\xi_2)(x - \varepsilon^2\xi_2)$. Let $\xi_3 = 1/(\xi_1\xi_2)$. As $\xi_1^3\beta\gamma = 1$, we have $\xi_3^3 = 1/(\xi_1^3\xi_2^3) = 1/(\xi_1^3\beta) = \gamma$ and thus $x^3 - \gamma = (x - \xi_3)(x - \varepsilon\xi_3)(x - \varepsilon^2\xi_3)$. Let $w_1(x) = (x - \xi_1)(x - \xi_2)(x - \xi_3)$, $w_2(x) = w_1(\varepsilon x) = (x - \varepsilon^2\xi_1)(x - \varepsilon^2\xi_2)(x - \varepsilon^2\xi_3)$, $w_3(x) = w_1(\varepsilon^2 x) = (x - \varepsilon\xi_1)(x - \varepsilon\xi_2)(x - \varepsilon\xi_3)$. In K we have $t(x) = (x - \xi_1^3)(x - \xi_2^3)(x - \xi_3^3)$. Hence $u(x) = w_1(x)w_2(x)w_3(x)$. Let $a = -\xi_1 - \xi_2 - \xi_3$, $b = \xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3$. Then $w_1(x) = x^3 + ax^2 + bx - 1$, $w_2(x) = x^3 + \varepsilon^2 ax^2 + \varepsilon bx - 1$, $w_3(x) = x^3 + \varepsilon ax^2 + \varepsilon^2 bx - 1$. Using Theorem 2.3 we get $b \neq 0$ and $f(b^3, -1) = 0$. After a short calculation we obtain

$$b^3 = \xi_1^3\xi_2^3 + \xi_1^3\xi_3^3 + \xi_2^3\xi_3^3 + 3(\xi_1^3\xi_2^2\xi_3 + \xi_1^3\xi_2\xi_3^2 + \xi_1^2\xi_2^3\xi_3 + \xi_1\xi_2^3\xi_3^2 + \xi_1^2\xi_2\xi_3^3 + \xi_1\xi_2^2\xi_3^3) + 6\xi_1^2\xi_2^2\xi_3^2.$$

Let $u = \xi_1^3\xi_2^3 + \xi_1^3\xi_3^3 + \xi_2^3\xi_3^3 + 6\xi_1^2\xi_2^2\xi_3^2$, $v = \xi_1^3\xi_2^2\xi_3 + \xi_1^3\xi_2\xi_3^2 + \xi_1^2\xi_2^3\xi_3 + \xi_1\xi_2^3\xi_3^2 + \xi_1^2\xi_2\xi_3^3 + \xi_1\xi_2^2\xi_3^3$. Then $b^3 = u + 3v$ and, for u, we have $u = \alpha\beta + \alpha\gamma + \beta\gamma + 6 = 5$. Clearly, $\xi_3 = \xi_2^2/(\xi_1\beta)$ and $\xi_3^2 = \xi_2/(\xi_1^2\beta)$. This implies that

$$v = \frac{\xi_1^3\xi_2^4}{\xi_1\beta} + \frac{\xi_1^3\xi_2^2}{\xi_1^2\beta} + \frac{\xi_1^2\beta\xi_2^2}{\xi_1\beta} + \frac{\xi_1\beta\xi_2}{\xi_1^2\beta} + \xi_1^2\xi_2\gamma + \xi_1\xi_2^2\gamma = \xi_2^2(\frac{\xi_1}{\beta} + \xi_1 + \xi_1\gamma) + \xi_2(\xi_1^2 + \frac{1}{\xi_1} + \xi_1^2\gamma).$$

Let $r = \xi_1/\beta + \xi_1 + \xi_1\gamma$, $s = \xi_1^2 + 1/\xi_1 + \xi_1^2\gamma$. Then $r, s \in \mathbb{F}$ and $b^3 = 3r\xi_2^2 + 3s\xi_2 + 5$. Since, for $b^3 \neq 2$, we have $g(b^3) = 0$ and $[K : \mathbb{F}] = 3$, we obtain $b^3 \in \mathbb{F}$. Clearly, the elements $1, \xi_2, \xi_2^2 \in K$ are linear independent over $\mathbb{F}$ and thus we have $r = s = 5 - b^3 = 0$. Hence

$b^3 = 5$. Consequently, $5 \equiv 2 \pmod p$ or 5 is a root of $g(x)$ in $\mathbb{F}$. As $g(5) = -2^3 \cdot 3^2 = 0$, we have a contradiction with char $\mathbb{F} \neq 2, 3$. This proves part (i).

(ii) According to (i) there exists $e_1 \in \{0, 1, 2\}$ such that $\{\alpha, \beta, \gamma\} \subseteq C_{e_1}$. Therefore, there exist $\omega_1, \omega_2 \in \mathbb{F}$ with the property $\beta = \alpha\omega_1^3$, $\gamma = \alpha\omega_2^3$ and $1 \neq \omega_1^3 \neq \omega_2^3 \neq 1$. Let $c \in \{-1, -\varepsilon, -\varepsilon^2\}$. Since $1 = \alpha\beta\gamma = \alpha^3\omega_1^3\omega_2^3$, we can choose the element ω_1 such that $\alpha\omega_1\omega_2 = -c$. Let K be the splitting field of $x^3 - \alpha$ and let $\xi \in K$ such that $\xi^3 = \alpha$. Then $\xi^3\omega_1\omega_2 = -c$. Set $H_1 = \omega_1 + \omega_2 + \omega_1\omega_2$, $H_2 = \omega_1 + \varepsilon\omega_2 + \varepsilon^2\omega_1\omega_2$, $H_3 = \omega_1 + \varepsilon^2\omega_2 + \varepsilon\omega_1\omega_2$. Using $1 \neq \omega_1^3 \neq \omega_2^3 \neq 1$, we can prove $H_1^3 \neq H_2^3 \neq H_3^3 \neq H_1^3$. Furthermore, set

$$\begin{aligned} w_{11}(x) &= (x - \xi)(x - \xi\omega_1)(x - \xi\omega_2) = x^3 + a_1x^2 + b_1x + c, \\ w_{21}(x) &= (x - \varepsilon\xi)(x - \varepsilon^2\xi\omega_1)(x - \xi\omega_2) = x^3 + a_2x^2 + b_2x + c, \\ w_{31}(x) &= (x - \varepsilon^2\xi)(x - \varepsilon\xi\omega_1)(x - \xi\omega_2) = x^3 + a_3x^2 + b_3x + c, \end{aligned}$$

and, for $i \in \{1, 2, 3\}$, set $w_{i2}(x) = w_{i1}(\varepsilon x)$, $w_{i3}(x) = w_{i1}(\varepsilon^2 x)$. Then $b_i = \xi^2 H_i$, $i \in \{1, 2, 3\}$. Since $\varepsilon^j\xi$, $\varepsilon^j\xi\omega_1$, $\varepsilon^j\xi\omega_2$, $j \in \{0, 1, 2\}$ are distinct roots of $u(x)$, we have $u(x) = w_{i1}(x)w_{i2}(x)w_{i3}(x)$ for each $i \in \{1, 2, 3\}$. Theorem 2.3 then implies $f(b_i^3, c) = 0$, $b_i \neq 0$. Thus, b_i^3, $i \in \{1, 2, 3\}$ are distinct roots of $f(x, c)$. Since $b_i^3\alpha = \xi^6 H_i^3\alpha = (\alpha H_i)^3$, $i \in \{1, 2, 3\}$, there exists $e_2 \in \{0, 1, 2\}$ such that $b_i \in C_{e_2}$ for each $i \in \{1, 2, 3\}$ and $e_1 + e_2 \equiv 0 \pmod 3$. The theorem is proved. □

Remark 2.10. *The second part of the proof of Theorem 2.9 gives explicit formulas for the roots of the polynomial* $f(x, c)$, *namely* $\alpha^2 H_1^3$, $\alpha^2 H_2^3$, $\alpha^2 H_3^3$.

3. The cubic character of the Tribonacci roots

Let $t(x)$ be irreducible over $\mathbb{F}_p$ and $p \equiv 1 \pmod 3$. Let K be the splitting field of $t(x)$ over $\mathbb{F}_p$. Then $[K : \mathbb{F}_p] = 3$ and the multiplicative group $K^\times$ of the field K is of order $p^3 - 1 = (p-1)(p^2+p+1)$. We denote the generator of $K^\times$ by g. Let $\alpha, \beta, \gamma \in K$ satisfy $t(x) = (x - \alpha)(x - \beta)(x - \gamma)$. With respect to the automorphism $\xi \to \xi^p$ of the field K, we can assume that $\beta = \alpha^p$, $\gamma = \alpha^{p^2}$. Consequently, the roots α, β, γ are distinct. Let $\alpha = g^u$ where $u \in \mathbb{Z}$, $0 < u < p^3 - 1$. Then $1 = \alpha^{1+p+p^2} = g^{u(1+p+p^2)}$ and thus $u(1 + p + p^2) \equiv 0 \pmod{p^3 - 1}$. This implies $p - 1 | u$ and thus there is a $k \in \mathbb{Z}$, $1 \le k < p^2 + p + 1$ such that $u = k(p - 1)$. We get $\alpha = g^{k(p-1)}$ and ind $\alpha = k(p - 1)$ in K. Put

$$\xi_\alpha = g^{\frac{k(p-1)}{3}}, \ \xi_\beta = \xi_\alpha^p = g^{\frac{kp(p-1)}{3}}, \ \xi_\gamma = \xi_\beta^p = \xi_\alpha^{p^2} = g^{\frac{kp^2(p-1)}{3}}.$$

Then $\xi_\alpha, \xi_\beta, \xi_\gamma \in K^\times$, $\xi_\alpha^3 = \alpha$, $\xi_\beta^3 = \beta$, $\xi_\gamma^3 = \gamma$ and $(\xi_\alpha\xi_\beta\xi_\gamma)^3 = 1$. This implies that $\xi_\alpha\xi_\beta\xi_\gamma \in \{1, \varepsilon, \varepsilon^2\}$. Further, put $c(p) = -\xi_\alpha\xi_\beta\xi_\gamma = -\xi_\alpha^{1+p+p^2} \in \{-1, -\varepsilon, -\varepsilon^2\}$. It can be shown that $c(p)$ depends only on the prime p. By investigating the relation $C(c) = 0$ for $c \in \{-1, -\varepsilon, -\varepsilon^2\}$, we get the following lemma.

Lemma 3.1. *If* $f(0, c) = 0$ *for an element* $c \in \{-1, -\varepsilon, -\varepsilon^2\}$ *of* $\mathbb{F}$, *then* char $\mathbb{F} = 2$ *or* 7.

Theorem 3.2. *Let* $t(x)$ *be irreducible over* $\mathbb{F}_p$. *Then* $f(x, c(p))$ *has three distinct roots in* $\mathbb{F}_p$ *belonging to distinct cubic classes of the field* $\mathbb{F}_p$.

Proof. Let $w_1(x) = (x - \xi_\alpha)(x - \xi_\beta)(x - \xi_\gamma) = x^3 + ax^2 + bx + c$ where $a = -\xi_\alpha - \xi_\beta - \xi_\gamma$, $b = \xi_\alpha\xi_\beta + \xi_\alpha\xi_\gamma + \xi_\beta\xi_\gamma$, $c = c(p) = -\xi_\alpha\xi_\beta\xi_\gamma$. Since $a^p = a$, $b^p = b$, we have $a, b, c \in \mathbb{F}_p$ and $w_1(x), w_2(x), w_3(x) \in \mathbb{F}_p[x]$ where $w_2(x) = w_1(\varepsilon x)$ and $w_3(x) = w_1(\varepsilon^2 x)$. Furthermore, we have $w_2(x) = (x - \varepsilon^2\xi_\alpha)(x - \varepsilon^2\xi_\beta)(x - \varepsilon^2\xi_\gamma)$ and $w_3(x) = (x - \varepsilon\xi_\alpha)(x - \varepsilon\xi_\beta)(x - \varepsilon\xi_\gamma)$. Clearly, $\varepsilon^i\xi_\alpha$, $\varepsilon^i\xi_\beta$, $\varepsilon^i\xi_\gamma$, $i \in \{0, 1, 2\}$ are the distinct roots of

$u(x)$ and $u(x) = w_1(x)w_2(x)w_3(x)$. By Theorem 2.3 we have $b \neq 0$ and $f(b^3, c(p)) = 0$. From Theorem 2.4 and Lemma 2.6 it follows that there exist $\rho, \sigma \in \mathbb{F}_p$ such that $\rho \neq b^3 \neq \sigma \neq \rho$, $f(\rho, c(p)) = f(\sigma, c(p)) = 0$. Suppose that there is $b' \in \mathbb{F}_p$, $b'^3 = \rho$. Let $w_1'(x) = x^3 + a'x^2 + b'x + c$, $c = c(p)$, where $a' = (b'^3 + 3c^2 + 1)/3b'c$, $w_2'(x) = w_1'(\varepsilon x)$, $w_3'(x) = w_1'(\varepsilon^2 x)$. By Theorem 2.3 we have $u(x) = w_1'(x)w_2'(x)w_3'(x)$. Since $b^3 \neq \rho = b'^3$, we have $\{w_1(x), w_2(x), w_3(x)\} \cap \{w_1'(x), w_2'(x), w_3'(x)\} = \emptyset$. Consequently, there exists $\tau \in \mathbb{F}_p$ such that $u(\tau) = 0$. Hence τ^3 is a root of $t(x)$ which is a contradiction. Therefore exactly one root of $f(x, c(p))$ is a cubic residue of $\mathbb{F}_p$. Since $C(-1) = 4^3$, $C(-\varepsilon) = 18\varepsilon + 19 = (\varepsilon + 3)^3$ and $C(-\varepsilon^2) = 18\varepsilon^2 + 19 = (\varepsilon^2 + 3)^3$, we get, using Lemma 2.7, that the roots of $f(x, c(p))$ belong to distinct cubic classes of $\mathbb{F}_p$. □

Lemma 3.3. *Let $t(x)$ be irreducible over $\mathbb{F}_p$, $c_1, c_2 \in \{-1, -\varepsilon, -\varepsilon^2\}$ and $b_1, b_2 \in \mathbb{F}_p$. If $f(b_1^3, c_1) = f(b_2^3, c_2) = 0$, then $c_1 = c_2$.*

Proof. For $i \in \{1, 2\}$, let $w_{i1}(x) = x^3 + a_i x^2 + b_i x + c_i$ where $a_i = (b_i^3 + 3c_i^2 + 1)/3b_i c_i$. Further, put $w_{i2}(x) = w_{i1}(\varepsilon x)$, $w_{i3}(x) = w_{i1}(\varepsilon^2 x)$. Then, by Theorem 2.3, we have $u(x) = w_{i1}(x)w_{i2}(x)w_{i3}(x)$, $i \in \{1, 2\}$. If $c_1 \neq c_2$, then $\{w_{11}(x), w_{12}(x), w_{13}(x)\} \cap \{w_{21}(x), w_{22}(x), w_{23}(x)\} = \emptyset$, and thus there is $\tau \in \mathbb{F}_p$ such that $u(\tau) = 0$. Since τ^3 is a root of $t(x)$ in $\mathbb{F}_p$, a contradiction follows. □

Theorem 3.4. *Let $c \in \{-1, -\varepsilon, -\varepsilon^2\}$ and let $f(x, c)$ have three distinct roots in $\mathbb{F}_p$ belonging to distinct cubic classes of $\mathbb{F}_p$. Then $t(x)$ is irreducible over $\mathbb{F}_p$ and $c = c(p)$.*

Proof. Let ρ be the root of $f(x, c)$ in $\mathbb{F}_p$ such that $\rho \in C_0$. Then there is $b \in \mathbb{F}_p$ such that $b^3 = \rho$. Put $a = (b^3 + 3c^2 + 1)/3bc$, $w_1(x) = x^3 + ax^2 + bx + c$, $w_2(x) = w_1(\varepsilon x)$, $w_3(x) = w_1(\varepsilon^2 x)$. By Theorem 2.3 we have $u(x) = w_1(x)w_2(x)w_3(x)$.

Suppose that $t(x)$ is not irreducible over $\mathbb{F}_p$. Since $f(x, c)$ has three distinct roots in $\mathbb{F}_p$, then by Theorem 2.4 and Lemma 2.6, we have $(p/11) = 1$. By (2.5), there are distinct elements $\tau_1, \tau_2, \tau_3 \in \mathbb{F}_p$ such that $t(x) = (x - \tau_1)(x - \tau_2)(x - \tau_3)$ and thus $u(x) = (x^3 - \tau_1)(x^3 - \tau_2)(x^3 - \tau_3)$. For any $i \in \{1, 2, 3\}$, there is $k = k(i) \in \{1, 2, 3\}$ such that $1 \leq \deg(\gcd(x^3 - \tau_i, w_k(x))) \leq 2$. Thus there is $\xi_i \in \mathbb{F}_p$ which is the root of $x^3 - \tau_i$. Since $\varepsilon\xi_1$, $\varepsilon^2\xi_i$ are also the roots of $x^3 - \tau_i$, we have $x^3 - \tau_i = (x - \xi_i)(x - \varepsilon\xi_i)(x - \varepsilon^2\xi_i)$ for $i \in \{1, 2, 3\}$. This implies that $u(x)$ completely splits over $\mathbb{F}_p$ into the product of the linear terms $x - \varepsilon^i\xi_j$, $i \in \{0, 1, 2\}$, $j \in \{1, 2, 3\}$. We can assume

$$
\begin{aligned}
w_1(x) &= (x - \xi_1)(x - \xi_2)(x - \xi_3),\\
w_2(x) &= w_1(\varepsilon x) = (x - \varepsilon^2\xi_1)(x - \varepsilon^2\xi_2)(x - \varepsilon^2\xi_3),\\
w_3(x) &= w_1(\varepsilon^2 x) = (x - \varepsilon\xi_1)(x - \varepsilon\xi_2)(x - \varepsilon\xi_3).
\end{aligned}
$$

It follows that $b = \xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3$ and $c = -\xi_1\xi_2\xi_3$. Put

$$
\begin{aligned}
\overline{w}_1(x) &= (x - \varepsilon\xi_1)(x - \varepsilon^2\xi_2)(x - \xi_3),\\
\overline{w}_2(x) &= \overline{w}_1(\varepsilon x) = (x - \xi_1)(x - \varepsilon\xi_2)(x - \varepsilon^2\xi_3),\\
\overline{w}_3(x) &= \overline{w}_1(\varepsilon^2 x) = (x - \varepsilon^2\xi_1)(x - \xi_2)(x - \varepsilon\xi_3).
\end{aligned}
$$

Letting $\overline{a} = -\varepsilon\xi_1 - \varepsilon^2\xi_2 - \xi_3$ and $\overline{b} = \xi_1\xi_2 + \varepsilon\xi_1\xi_3 + \varepsilon^2\xi_2\xi_3$, we get $\overline{w}_1(x) = x^3 + \overline{a}x^2 + \overline{b}x + c$. Since $u(x) = \overline{w}_1(x)\overline{w}_2(x)\overline{w}_3(x)$, it follows from Theorem 2.3 that $f(\overline{b}^3, c) = 0$.

We prove that $b \notin \{\overline{b}, \varepsilon\overline{b}, \varepsilon^2\overline{b}\}$. Suppose that $b = \overline{b}$. Then $\xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3 = \xi_1\xi_2 + \varepsilon\xi_1\xi_3 + \varepsilon^2\xi_2\xi_3$ and thus $\xi_2\xi_3(\varepsilon^2 - 1) + \xi_1\xi_3(\varepsilon - 1) = 0$. Hence $\xi_2(\varepsilon + 1) = -\xi_1$. Since $(\varepsilon + 1)^3 = -1$ we have $\tau_2 = \xi_2^3 = \xi_1^3 = \tau_1$, which is a contradiction. Similarly we can prove that $b \neq \varepsilon\bar{b}$ and $b \neq \varepsilon^2\bar{b}$. Hence $b \notin \{\bar{b}, \varepsilon\bar{b}, \varepsilon^2\bar{b}\}$, and thus $b^3 \neq \bar{b}^3$. Consequently, the roots $b^3, \bar{b}^3$ of $f(x,c)$ belong to the same cubic class and a contradiction follows. Thus $t(x)$ is irreducible over $\mathbb{F}_p$. From Theorem 3.2 we get that $f(x, c(p))$ has a root b_1^3 where $b_1 \in \mathbb{F}_p$ and Lemma 3.3 implies $c = c(p)$. □

Theorem 3.5. *Let $t(x)$ have exactly one root τ in the field $\mathbb{F}_p$ and $p \neq 7$. Then, for any $c \in \{-1, -\varepsilon, -\varepsilon^2\}$, there exists the unique $\rho = \rho(c) \in \mathbb{F}_p$ such that $f(\rho, c) = 0$. Furthermore, $\rho\tau$ is a cubic residue of the field $\mathbb{F}_p$.*

Proof. According to Corollary 2.5 we have $(p/11) = -1$. Let $\mathbb{F} = \mathbb{F}_{p^2}$. Then $t(x)$ has three distinct roots $\tau, \alpha, \beta \in \mathbb{F}$ and $t(x) = (x-\tau)(x-\alpha)(x-\beta)$. Let $c \in \{-1, -\varepsilon, -\varepsilon^2\}$. Using Theorem 2.9, we get that τ, α, β belong to the same cubic class C_{e_1} of the field $\mathbb{F}$ and $f(x,c)$ has three distinct roots in $\mathbb{F}$ which belong to the same cubic class C_{e_2}, $e_2 \in \{0,1,2\}$ of $\mathbb{F}$ and $e_1 + e_2 \equiv 0 \pmod 3$.

Using Theorem 2.4 and Lemma 2.6, we get that there exists exactly one element $\rho = \rho(c) \in \mathbb{F}_p$ such that $f(\rho, c) = 0$. Since $\tau \in C_{e_1}$ and $\rho \in C_{e_2}$, there exists $\omega \in \mathbb{F} = \mathbb{F}_{p^2}$ such that $\rho\tau = \omega^3$. The element $\rho\tau$ belongs to $\mathbb{F}_p$ and $[\mathbb{F} : \mathbb{F}_p] = 2$, thus $\omega \in \mathbb{F}_p$ and the result follows. □

The case $p = 7$ will be investigated separately. The polynomial $t(x)$ has only one root $\tau = 3$ in the field $\mathbb{F}_7$. The set $\{-1, -\varepsilon, -\varepsilon^2\} = \{3, 5, 6\}$ and the polynomials $f(x,c)$, $c = 3, 5, 6$ have the following roots in $\mathbb{F}_7$:

c	$\rho = \rho(c)$	$\rho^{(p-1)/3} = \rho^2$	$(\rho\tau)^{(p-1)/3} = (\rho\tau)^2$
3	0	0	0
5	5	4	1
6	2	4	1

where $\rho = \rho(c)$ is the only root of $f(x,c)$ in $\mathbb{F}_7$. Therefore, we can state the following proposition.

Proposition 3.6. *Let $p = 7$. Then the Tribonacci polynomial $t(x)$ has a unique root $\tau = 3$ in $\mathbb{F}_7$ and, for $c \in \{-1, -\varepsilon, -\varepsilon^2\} - \{3\}$, there exists a unique $\rho = \rho(c) \in \mathbb{F}_7$ with $f(\rho, c) = 0$ and $\rho\tau$ is a cubic residue in $\mathbb{F}_7$.*

Combining Theorem 3.5 with Proposition 3.6, we obtain the following theorem.

Theorem 3.7. *Let $t(x)$ have a unique root τ in the field $\mathbb{F}_p$. Then 2τ belongs to the cubic class C_0 of $\mathbb{F}_p$ and therefore*

$$\tau^{\frac{p-1}{3}} \equiv 2^{\frac{2(p-1)}{3}} \pmod p.$$

Using Theorem 2.9 we get the following theorem.

Theorem 3.8. *Let $t(x)$ have three distinct roots $\alpha, \beta, \gamma \in \mathbb{F}_p$. Then there exists $e_1 \in \{0,1,2\}$ such that $\{\alpha, \beta, \gamma\} \subseteq C_{e_1}$ and any polynomial $f(x,c)$, $c \in \{-1, -\varepsilon, -\varepsilon^2\}$ has three distinct roots in $\mathbb{F}_p$ which belong to the same cubic class C_{e_2} of $\mathbb{F}_p$ where $e_2 \in \{0,1,2\}$ and $e_1 + e_2 \equiv 0 \pmod 3$. In particular, for any $\tau \in \{\alpha, \beta, \gamma\}$, the element 2τ belongs to the cubic class C_0 of $\mathbb{F}_p$ and thus*

$$\tau^{\frac{p-1}{3}} \equiv 2^{\frac{2(p-1)}{3}} \pmod p.$$

4. Conclusion

In conclusion, we prove a theorem on the relation between the roots of $t(x)$ and the number 2 in any extension of the field $\mathbb{F}_p$.

Theorem 4.1. *Let* $\mathbb{G}$ *be an arbitrary extension of the field* $\mathbb{F}_p$ *and* $\chi \in \mathbb{G}$ *be a root of* $t(x)$ *in* $\mathbb{G}$. *Then there exists* $\omega \in \mathbb{G}$ *such that* $2\chi = \omega^3$.

Proof. We will discuss three cases. (i) Let $t(x)$ be irreducible over $\mathbb{F}_p$. Then $t(x)$ has three distinct roots α, β, γ in the splitting field K over $\mathbb{F}_p$. Thus $K \subseteq \mathbb{G}$ and $\chi \in \{\alpha, \beta, \gamma\}$. Using Theorem 2.9, we see that 2χ is a cubic residue of the field K and the result follows.

(ii) Let $t(x)$ have the unique root τ in the field $\mathbb{F}_p$. By Theorem 3.7, the element 2τ is a cubic residue of the field $\mathbb{F}_p \subseteq \mathbb{G}$. Thus, for $\chi = \tau$, the theorem is valid. If $\chi \neq \tau$, then $\chi \in \mathbb{F}_{p^2}$. Since $\mathbb{F}_{p^2} \subseteq \mathbb{G}$, we get the result from Theorem 2.9 provided that $p \neq 7$. For $p = 7$, we get the assertion from Lemma 2.8.

(iii) Let $t(x)$ have three distinct roots in $\mathbb{F}_p$. According to Theorem 3.8, the element 2χ is a cubic residue of the field $\mathbb{F}_p$ and hence $2\chi = \omega^3$ for an element $\omega \in \mathbb{F}_p \subseteq \mathbb{G}$. The proof is complete. □

References

[1] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York, 1952.
[2] E. Lehmer, *On the quadratic character of the Fibonacci root*, The Fibonacci Quarterly, **4.2** (1966), 135 – 138.
[3] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress, (1897) 182 – 193.
[4] Z. – H. Sun, *Cubic and quartic congruences modulo a prime*, Journal of Number Theory, **102**, (2003), 41 – 89.
[5] G. Voronoï, *Sur une propriété du discriminant des fonctions entirès*, Verhand. III. Internat. Math. Kongress, (1905), 186 – 189.

AMS Classification Numbers: 11B39, 11A15
Tribonacci polynomial, cubic residue, cubic classes

CHAPTER 11

PERIODS OF THE TRIBONACCI SEQUENCE MODULO A PRIME P ≡ 1 (MOD 3) ⋆

Abstract. Let the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ be irreducible over the Galois field $\mathbb{F}_p$ where p is an arbitrary prime such that $p \equiv 1 \pmod 3$ and let τ be any root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$. We prove that $\tau^{(p^2+p+1)/3} = 1$. Using this identity we show that the period $h(p)$ of the sequence $(T_n \bmod p)_{n=0}^{\infty}$ where T_n is the nth Tribonacci number divides $(p^2 + p + 1)/3$. Similar results will also be obtained for $t(x)$ being reducible over $\mathbb{F}_p$. In this case we prove that the period $h(p)$ divides $(q - 1)/3$ where q is the number of elements of the splitting field of $t(x)$ over $\mathbb{F}_p$ if and only if 2 is a cubic residue of $\mathbb{F}_p$.

1. Introduction and preliminaries

The Tribonacci sequence $(T_n)_{n=0}^{\infty}$ is defined by the third order linear recurrence $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ with a triple of initial values $T_0 = 0$, $T_1 = 0$ and $T_2 = 1$. It is well-known, [9, Theorem 1] that $(T_n \bmod m)_{n=0}^{\infty}$ is simply periodic for any modulus $m > 1$. That is, the first three terms which are repeated in $(T_n \bmod m)_{n=0}^{\infty}$ are $0, 0, 1$. The least positive integer $h(m)$ satisfying $T_{h(m)} \equiv T_{h(m)+1} \equiv 0 \pmod m$ and $T_{h(m)+2} \equiv 1 \pmod m$ is called a period of $(T_n \bmod m)_{n=0}^{\infty}$. If $m = p$ is a prime, $h(p)$ depends in an essential way on the form of the factorization of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ over the Galois field $\mathbb{F}_p$. Let K denote the splitting field of $t(x)$ over $\mathbb{F}_p$ and let α, β, γ be the roots of $t(x)$ in K. Since the discriminant of $t(x)$ is equal to $-2^2 \cdot 11$, for $p \neq 2, 11$, the roots α, β, γ are distinct. For any $0 \neq \xi \in K$, let $\mathrm{ord}_K(\xi)$ denote the order of ξ in the multiplicative group $K^\times$ of K. By [10, Section 8], the problem of determining $h(p)$ is equivalent to the problem of determining the orders of α, β, γ in $K^\times$. See also [1], [2], [7]. Let $I = \{3, 5, 23, 31, \dots\}$ be the set of all primes p for which $t(x)$ is irreducible over $\mathbb{F}_p$, $Q = \{7, 13, 17, 19, \dots\}$ be the set of all primes for which $t(x)$ splits over $\mathbb{F}_p$ into the product of a linear factor and an irreducible quadratic factor and let $L = \{2, 11, 47, 53, \dots\}$ be the set of all primes for which $t(x)$ completely splits over $\mathbb{F}_p$ into linear factors. Then we can state the following theorem.

Theorem 1.1. *Let $p \neq 2, 11$ be a prime. Then*

(i) $h(p) = \mathrm{lcm}(\mathrm{ord}_K(\alpha), \mathrm{ord}_K(\beta), \mathrm{ord}_K(\gamma))$.
(ii) *If $p \in I$, then $h(p) = \mathrm{ord}_K(\tau)$ where τ is any root of $t(x)$ in K.*
(iii) *$p \in I$ or $p \in L$ if and only if the Legendere-Jacobi symbol $(p/11) = 1$.*
(iv) *$p \in I$ if and only if $T_p^2 \equiv -4/11 \pmod p$.*
(v) *$p \in L$ if and only if $T_p \equiv 0 \pmod p$.*

⋆ Published in J. Klaška, L. Skula, *Tribonacci sequence modulo a prime p ≡ 1(mod 3)*, The Fibonacci Quarterly **48.3** (2010), 228–235.

Statements (i) and (ii) are well-known. For example, see [1, p. 292], [7, p. 306] or consult [10, p. 161]. Statement (iii) is a consequence of more general results of L. Stickelberger [5] and G. Voronoï [8]. For details see [3]. Finally, statements (iv) and (v) are straightforward consequences of [6, Theorem 4.3].

The following theorem is due to A. Vince. See [7, Theorem 4].

Theorem 1.2. *Let $p \neq 2, 11$ be a prime. Then*

(i) *If $p \in L$, then $h(p) | p-1$.*
(ii) *If $p \in Q$, then $h(p) | p^2-1$.*
(iii) *If $p \in I$, then $h(p) | p^2+p+1$.*

In Theorem 4.1 of this paper, we strengthen Vince's result for $p \equiv 1 \pmod 3$ as follows:

(i) If $p \in L$, then $h(p) | \frac{p-1}{3}$ if and only if 2 is a cubic residue of the field $\mathbb{F}_p$.
(ii) If $p \in Q$, then $h(p) | \frac{p^2-1}{3}$ if and only if 2 is a cubic residue of the field $\mathbb{F}_p$.
(iii) If $p \in I$, then $h(p) | \frac{p^2+p+1}{3}$.

To prove this statement, we shall need the following result presented in [3].

Theorem 1.3. *Let p be an arbitrary prime such that $p \equiv 1 \pmod 3$ and let τ be any root of $t(x)$ in the field $\mathbb{F}_p$. Then*

$$\tau^{\frac{p-1}{3}} \equiv 2^{\frac{2(p-1)}{3}} \pmod p. \tag{1.1}$$

Moreover, if τ is any root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$, then 2τ is a cubic residue of K, i.e., there exists $\omega \in K$ such that $2\tau = \omega^3$.

2. A way to distinguish the cases $p \in L$ and $p \in I$ for primes $(p/11) = 1$, $p \equiv 1 \pmod 3$

Let $\mathbb{F}$ be a finite field with prime characteristic $p \equiv 1 \pmod 3$. Then $\mathbb{F} = \mathbb{F}_{p^n}$ for a positive integer n and there exists an $\varepsilon \in \mathbb{F}^\times$ with the property $\varepsilon^3 = 1$, $\varepsilon \neq 1$. Therefore, $\varepsilon^2 + \varepsilon + 1 = 0$. Let $\mathbb{F}^\times$ denote the multiplicative group of $\mathbb{F}$ with a generator g. For $e \in \{0, 1, 2\}$, put $C_e = \{\xi \in \mathbb{F}^\times; \xi = g^{3k+e}, k \in \mathbb{Z}, 0 \leq k < (p^n-1)/3\}$. The sets C_e are called the cubic classes of $\mathbb{F}$ and the elements of C_0 the cubic residues of $\mathbb{F}$. The following lemma can be found in [3, Lemma 2.7].

Lemma 2.1. *Let $\alpha, \beta, \gamma \in \mathbb{F}$. If $\alpha\beta\gamma$ is the cubic residue of $\mathbb{F}$, then either α, β, γ belong to distinct cubic classes of $\mathbb{F}$ or α, β, γ belong to the same cubic class of $\mathbb{F}$.*

Let $f(x) = x^3 + rx + s \in \mathbb{F}[x]$, $r, s \neq 0$. Assume that $f(x)$ is irreducible over $\mathbb{F}$ or $f(x)$ has three distinct roots in $\mathbb{F}$. Put $d = \frac{s^2}{4} + \frac{r^3}{27}$. Since char $\mathbb{F} \neq 2, 3$, the element d is well defined. Next, assume that there exists a $\lambda \in \mathbb{F}$ such that $\lambda^2 = d$. Let

$$A = -\frac{s}{2} + \lambda \quad \text{and} \quad B = -\frac{s}{2} - \lambda. \tag{2.1}$$

Then $AB = \frac{s^2}{4} - d = (-\frac{r}{3})^3$, which implies that

$$A \text{ is a cubic residue of } \mathbb{F} \text{ if and only if } B \text{ is a cubic residue of } \mathbb{F}. \tag{2.2}$$

The following lemma is essentially Cardano's formula for the field $\mathbb{F}$.

Lemma 2.2. *Let A, B be cubic residues of the field $\mathbb{F}$. Then there exist $\alpha, \beta \in \mathbb{F}$ such that $\alpha^3 = A$, $\beta^3 = B$, $\alpha\beta = -\frac{r}{3}$ and $\alpha + \beta$ is a root of $f(x)$ in $\mathbb{F}$.*

Proof. Since A, B are cubic residues of $\mathbb{F}$, there exist $\alpha, \gamma \in \mathbb{F}$ such that $\alpha^3 = A$, $\gamma^3 = B$. Then $(\alpha\gamma)^3 = AB = (-\frac{r}{3})^3$ and, consequently, there exists $e \in \{0, 1, 2\}$ such that $\alpha\gamma\varepsilon^e = -\frac{r}{3}$. Let $\beta = \gamma\varepsilon^e$. Then $\beta^3 = B$, $\alpha\beta = -\frac{r}{3}$ and $f(\alpha + \beta) = (\alpha + \beta)^3 + r(\alpha+\beta)+s = A+3\alpha\beta(\alpha+\beta)+B+r\alpha+r\beta+s = -s-r(\alpha+\beta)+r\alpha+r\beta+s = 0$. □

Lemma 2.3. *Let $f(x)$ have three distinct roots in $\mathbb{F}$. Then A, B are cubic residues of $\mathbb{F}$.*

Proof. Suppose that A and B are not cubic residues of $\mathbb{F}$ and let $\mathbb{G}$ be the splitting field of $x^3 - A$ over $\mathbb{F}$. Since A is a cubic residue of $\mathbb{G}$, B is a cubic residue of $\mathbb{G}$ by (2.2). Applying Lemma 2.2 to the field $\mathbb{G}$, we see that there exist $\alpha, \beta \in \mathbb{G}$ such that $\alpha^3 = A$, $\beta^3 = B$, $\alpha\beta = -\frac{r}{3}$ and $\alpha + \beta$ is a root of $f(x)$ in $\mathbb{G}$. As assumed, the roots of $f(x)$ belong to $\mathbb{F}$ and thus $\alpha + \beta \in \mathbb{F}$. Since $1, \alpha, \alpha^2$ is a basis of the extension $\mathbb{G}/\mathbb{F}$, there exist $a, b, c \in \mathbb{F}$ such that $\beta = a\alpha^2 + b\alpha + c$. Furthermore, $\alpha + \beta \in \mathbb{F}$ and $\alpha + \beta = a\alpha^2 + (b + 1)\alpha + c$, implies $a = 0$, $b = -1$ and thus $\beta = -\alpha + c$. Then $B = \beta^3 = -\alpha^3 + 3\alpha^2 c - 3\alpha c^2 + c^3 = -A + 3\alpha^2 c - 3\alpha c^2 + c^3$, which implies $A + B = 3\alpha^2 c - 3\alpha c^2 + c^3$. Next, $A + B \in \mathbb{F}$ implies $c = 0$. Hence, $-\frac{s}{2} - \lambda = B = -A = \frac{s}{2} - \lambda$, which yields $s = 0$, and a contradiction follows. □

Combining (2.2), Lemma 2.2 and Lemma 2.3 we get the following theorem.

Theorem 2.4. *The following statements are equivalent:*

(i) *The polynomial $f(x) = x^3 + rx + s \in \mathbb{F}[x]$ has three distinct roots in $\mathbb{F}$.*
(ii) *$A = -\frac{s}{2} + \lambda$ is a cubic residue of $\mathbb{F}$.*
(iii) *$B = -\frac{s}{2} - \lambda$ is a cubic residue of $\mathbb{F}$.*

Now we apply Theorem 2.4 to a Tribonacci polynomial $t(x)$ and field $\mathbb{F} = \mathbb{F}_p$ where p is an arbitrary prime such that $p \equiv 1 \pmod 3$ and $(p/11) = 1$.

The assumption $(p/11) = 1$ implies, by Theorem 1.1, part (iii), that $t(x)$ is irreducible over $\mathbb{F}_p$, or $t(x)$ has three distinct roots in $\mathbb{F}_p$. Using the substitution $x = y + \frac{1}{3}$, we can easily convert $t(x)$ to the form $\bar{t}(y) = y^3 - \frac{4}{3}y - \frac{38}{27}$. Hence, $r = -\frac{4}{3}$, $s = -\frac{38}{27}$, and $d = \frac{11}{27}$. Since $(19/11) = -1$, we have $r, s, d \neq 0$ in the field $\mathbb{F}_p$ where $p \equiv 1 \pmod 3$ and $(p/11) = 1$. After some calculation, we find that $(d/p) = (33/p) = 1$ and thus there exists $\lambda \in \mathbb{F}_p$ such that $\lambda^2 = d$. Put $\varkappa = 9\lambda$. Then $\varkappa^2 = 33$ and (2.1) yields $A = \frac{1}{27}(19 + 3\varkappa)$ and $B = \frac{1}{27}(19 - 3\varkappa)$.

From this and from Theorem 2.4, we get the following criterion, which can be used for $t(x)$ and for a prime $p \equiv 1 \pmod 3$, $(p/11) = 1$ to decide whether $p \in L$ or $p \in I$.

Theorem 2.5. *Let p be a prime, $p \equiv 1 \pmod 3$ and let $(p/11) = 1$. Then the following statements are equivalent:*

(i) *The Tribonacci polynomial $t(x)$ has three distinct roots in $\mathbb{F}_p$.*
(ii) *$19 + 3\varkappa$ is a cubic residue of $\mathbb{F}_p$.*
(iii) *$19 - 3\varkappa$ is a cubic residue of $\mathbb{F}_p$.*

The following proposition will be needed in the next section.

Proposition 2.6. *Let p be a prime, $p \equiv 1 \pmod 3$ and let $(p/11) = 1$. Furthermore, let $\rho = (13 + 3\varkappa)/2$ and $\sigma = (13 - 3\varkappa)/2$ where $\varkappa \in \mathbb{F}_p$ such that $\varkappa^2 = 33$. Then the following statements are equivalent:*

(i) *The elements $2, \rho, \sigma$ belong to the same cubic class of $\mathbb{F}_p$.*
(ii) *$26 + 6\varkappa$ is a cubic residue of $\mathbb{F}_p$.*

(iii) $26 - 6\varkappa$ *is a cubic residue of* $\mathbb{F}_p$.

Proof. The equivalence of (ii) and (iii) follows from the equality $(26 + 6\varkappa)(26 - 6\varkappa) = (-8)^3$. We prove that (i) implies (ii). Since 2 and ρ belong to the same cubic class of $\mathbb{F}_p$, there exists $\omega \in \mathbb{F}_p$ such that $\rho = 2\omega^3$. Hence $\omega^3 = \rho/2 = (13 + 3\varkappa)/4 = (26 + 6\varkappa)/8$, which proves that $26 + 6\varkappa$ is a cubic residue of $\mathbb{F}_p$. Conversely, assume (ii). Then $(26 + 6\varkappa)/8$ is a cubic residue of $\mathbb{F}_p$ and thus there exists $\omega \in \mathbb{F}_p$ such that $\omega^3 = (26 + 6\varkappa)/8$. Hence, we have $2\omega^3 = (13 + 3\varkappa)/2 = \rho$, which means that 2 and ρ belong to the same cubic class of $\mathbb{F}_p$. In a similar way, we can deduce that 2 and σ belong to the same cubic class of $\mathbb{F}_p$. Hence, (ii) implies (i). The proof is complete. □

3. The existence and properties of the roots of the polynomial $x^3 - \tau$ in the field extension $K/\mathbb{F}_p$ for a prime $p \in I$

Let $p \in I$. Recall that K is the splitting field of $t(x)$ over $\mathbb{F}_p$ and α, β, γ are the roots of $t(x)$ in K. Then $\{\alpha, \beta, \gamma\} = \{\tau, \tau^p, \tau^{p^2}\}$ for any $\tau \in \{\alpha, \beta, \gamma\}$. Together with the Viète equation $\alpha\beta\gamma = 1$, this yields $\tau^{p^2+p+1} = 1$. Now we can prove

Lemma 3.1. *Let* $p \in I$, $p \equiv 1 \pmod 3$ *and let* τ *be an arbitrary root of* $t(x)$ *in* K. *Then there exist exactly three distinct roots* ξ_1, ξ_2, ξ_3 *of* $x^3 - \tau$ *in* K.

Proof. Since K is a finite field, the multiplicative group $K^\times$ is cyclic. Let g be a generator of $K^\times$. Then $\tau = g^t$ for a positive integer t. Since $1 = \tau^{p^2+p+1} = g^{t(p^2+p+1)}$, we have $p - 1|t$. Hence $3|t$. Set $\xi_i = g^{t/3+(i-1)(p^3-1)/3}$ for $i \in \{1, 2, 3\}$. Then ξ_1, ξ_2, ξ_3 are three distinct roots of $x^3 - \tau$ in K. □

The proofs of the following lemmas are easy to see.

Lemma 3.2. *Let* $p \in I$, $p \equiv 1 \pmod 3$ *and let* τ *be an arbitrary root of* $t(x)$ *in* K. *Furthermore, let* ξ_1, ξ_2, ξ_3 *be the roots of* $x^3 - \tau$ *in* K. *Then:*

(i) $\{\xi_1, \xi_2, \xi_3\} = \{\xi, \varepsilon\xi, \varepsilon^2\xi\}$ *for any* $\xi \in \{\xi_1, \xi_2, \xi_3\}$.
(ii) $\xi_1\xi_2\xi_3 = \tau$.
(iii) $\xi_1 + \xi_2 + \xi_3 = \xi_1^2 + \xi_2^2 + \xi_3^2 = \xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3 = 0$.

Let $p \in I$, $p \equiv 1 \pmod 3$ and let τ be an arbitrary root of $t(x)$ in K. Further, let ξ be an arbitrary root of $x^3 - \tau$ in K. Put $c(p) = -\xi^{p^2+p+1}$. It is easy to see that $c(p)$ does not depend on the choice of ξ and τ. Since $\xi^3 = \tau$ and $\tau^{p^2+p+1} = 1$, we have $c(p)^3 = -1$. Hence $c(p) \in \{-1, -\varepsilon, -\varepsilon^2\}$. Furthermore, put $w(x) = (x - \xi)(x - \xi^p)(x - \xi^{p^2})$. Then $w(x) \in \mathbb{F}_p[x]$ and $w(x)$ is irreducible over $\mathbb{F}_p$. For further considerations we will need the following polynomials defined in [3, Section 2]. For $c = c(p)$, put $f(x, c) = x^3 + A(c)x^2 + B(c)x + C(c) \in \mathbb{F}_p[x]$ where $A(c) = -18c^2 + 3$, $B(c) = -9c^2 - 27c - 24$, and $C(c) = 9c^2 - 27c + 28$. In particular, for $c = -1$ we have $f(x, -1) = x^3 - 15x^2 - 6x + 64$.

Lemma 3.3. *For any prime* $p \in I$, $p \equiv 1 \pmod 3$, *the following is true:*
(i) $f(x, c(p))$ *has three distinct roots in* $\mathbb{F}_p$ *belonging to distinct cubic classes of* $\mathbb{F}_p$.
(ii) *Let* $c_1, c_2 \in \{-1, -\varepsilon, -\varepsilon^2\}$ *and* $b_1, b_2 \in \mathbb{F}_p$. *If* $f(b_1^3, c_1) = f(b_2^3, c_2) = 0$ *then* $c_1 = c_2$.

For a proof of (i) see [3, Theorem 3.2] and for a proof of (ii) consult [3, Lemma 3.3]. The validity of the following lemma is easy to verify.

Lemma 3.4. *Let* p *be a prime,* $p \equiv 1 \pmod 3$ *and let* $(p/11) = 1$. *Then the polynomial* $f(x, -1) = x^3 - 15x^2 - 6x + 64$ *completely splits into linear factors over the field* $\mathbb{F}_p$

and has three distinct roots $2, \rho = (13+3\varkappa)/2$, *and* $\sigma = (13-3\varkappa)/2$ *where* $\varkappa \in \mathbb{F}_p$ *such that* $\varkappa^2 = 33$.

Now we are ready for the following theorem.

Theorem 3.5. *Let* $p \in I$ *and* $p \equiv 1 \pmod 3$. *Then* $c(p) = -1$.

Proof. By Theorem 2.5, $19 - 3\varkappa$ is not a cubic residue of the field $\mathbb{F}_p$. Since $(19 - 3\varkappa)(26+6\varkappa) = (-1+\varkappa)^3$, the element $26+6\varkappa$ is not a cubic residue of $\mathbb{F}_p$ either. By Lemma 3.4, the polynomial $f(x,-1)$ has three distinct roots $2, \rho, \sigma$ in $\mathbb{F}_p$ and Lemma 2.1, together with Proposition 2.6, yields that $2, \rho, \sigma$ belong to distinct cubic classes of $\mathbb{F}_p$. Hence, there exists a $b_2 \in \mathbb{F}_p$ such that $b_2^3 \in \{2, \rho, \sigma\}$ and $f(b_2^3, -1) = 0$. By Lemma 3.3, part (i), there exists $b_1 \in \mathbb{F}_p$ such that $f(b_1^3, c(p)) = 0$ and from Lemma 3.3, part (ii) we get $c(p) = -1$. ☐

Theorem 3.6. *Let* $p \in I$, $p \equiv 1 \pmod 3$ *and let* τ *be an arbitrary root of* $t(x)$ *in the splitting field* K *of* $t(x)$ *over* $\mathbb{F}_p$. *Furthermore, let* ξ *be any root of* $x^3 - \tau$ *in* K. *Then* $\xi^{p^2+p+1} = 1$ *and*

$$\tau^{\frac{p^2+p+1}{3}} = 1. \tag{3.1}$$

Proof. From Theorem 3.5 and the definition of $c(p)$ we immediately get $\xi^{p^2+p+1} = 1$. Since $\xi^3 = \tau$, we have $\tau^{(p^2+p+1)/3} = \xi^{p^2+p+1} = 1$ as required. ☐

Corollary 3.7. *Let* $p \in I$ *and* $p \equiv 1 \pmod 3$. *Then* $u(x) := t(x^3) = x^9 - x^6 - x^3 - 1$ *factors over* $\mathbb{F}_p$ *into the product of three irreducible polynomials* $w(x)$, $w(\varepsilon x)$, $w(\varepsilon^2 x)$ *with constant terms equal to* -1.

Remark 3.8. (i) Let $p \in I$ and τ be an arbitrary root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$. It is easy to prove by induction that

$$\tau^k = T_k\tau^2 + (T_{k-1} + T_{k-2})\tau + T_{k-1}, \ k > 1. \tag{3.2}$$

From equality (3.2) it follows for $k > 1$ that

$$\tau^k = \varepsilon \text{ if and only if } T_k \equiv T_{k+1} \equiv 0 \pmod p \text{ and } T_{k+2} \equiv \varepsilon \pmod p. \tag{3.3}$$

(ii) Put $H =< g^{p-1} >$ where g is the generator of $K^\times$. Then H is a cyclic group of order p^2+p+1. Since $\tau^{p^2+p+1} = 1$, we have $\tau \in H$ and $G =< \tau >$ is a subgroup of H. Let $p \equiv 1 \pmod 3$. Then in H, there exist exactly three elements belonging to $\mathbb{F}_p$. These are $1, \varepsilon, \varepsilon^2$. Moreover, together with $9 \nmid p^2+p+1$, (3.1) yields $\varepsilon, \varepsilon^2 \notin G$.

Theorem 3.9. *Let* $p \in I$, $p \equiv 1 \pmod 3$ *and let* τ *be an arbitrary root of* $t(x)$ *in the splitting field* K *of* $t(x)$ *over* $\mathbb{F}_p$. *Furthermore, let* $\xi \in \{\xi_1, \xi_2, \xi_3\}$ *be any root of* $x^3 - \tau$ *in* K. *Then* $\mathrm{ord}_K(\xi) = \mathrm{ord}_K(\tau)$ *or* $\mathrm{ord}_K(\xi) = 3 \cdot \mathrm{ord}_K(\tau)$. *Moreover, exactly one of the roots* ξ_1, ξ_2, ξ_3 *is of an order equal to* $\mathrm{ord}_K(\tau)$ *and two roots are of orders equal to* $3 \cdot \mathrm{ord}_K(\tau)$.

Proof. For brevity, put $\mathrm{ord}_K(\tau) = h$ and $\mathrm{ord}_K(\xi) = k$. We have $\xi^3 = \tau$ and so $\xi^{3h} = \tau^h = 1$, which means that $k | 3h$. On the other hand, $\xi^k = 1$ implies $\xi^{3k} = 1$. Together with $\xi^3 = \tau$ this yields $\tau^k = 1$ and $h|k$ follows. Consequently, there exist positive integers c_1, c_2 such that $c_1 \cdot k = 3 \cdot h$ and $k = c_2 \cdot h$. Hence, we have $c_1c_2 = 3$, which yields $c_1 = 1, c_2 = 3$ or $c_1 = 3, c_2 = 1$. Consequently, $\mathrm{ord}_K(\xi) = \mathrm{ord}_K(\tau)$ or $\mathrm{ord}_K(\xi) = 3 \cdot \mathrm{ord}_K(\tau)$.

Since the orders of the elements ξ_1, ξ_2, ξ_3 can only take on two values h and $3h$, at least two of them have the same order. Denote this order by h_0. Without loss of generality, we can assume $\mathrm{ord}_K(\xi_1) = \mathrm{ord}_K(\xi_2) = h_0$. Put $\xi_1 = \xi$. Since $\{\xi_1, \xi_2, \xi_3\} = \{\xi, \varepsilon\xi, \varepsilon^2\xi\}$, either $\mathrm{ord}_K(\xi) = \mathrm{ord}_K(\varepsilon\xi) = h_0$ or $\mathrm{ord}_K(\xi) = \mathrm{ord}_K(\varepsilon^2\xi) = h_0$. Hence, it easily follows that $3|h_0$ and thus $h_0 = 3r$ for some positive integer r. Using Lemma 3.2, part (ii), we get $\tau^{3r} = (\xi_1\xi_2\xi_3)^{h_0} = \xi_3^{h_0} = \tau^r$. Hence, $\tau^{2r} = 1$. Since $2 \nmid h$, we have $h|r$. This, together with $h_0 \in \{h, 3h\}$, yields $h_0 = 3h$. Consequently, we have either

$$\mathrm{ord}_K(\xi_1) = \mathrm{ord}_K(\xi_2) = \mathrm{ord}_K(\xi_3) = 3 \cdot \mathrm{ord}_K(\tau) = 3h \tag{3.4}$$

or

$$\mathrm{ord}_K(\xi_1) = \mathrm{ord}_K(\xi_2) = 3 \cdot \mathrm{ord}_K(\tau) \text{ and } \mathrm{ord}_K(\xi_3) = \mathrm{ord}_K(\tau). \tag{3.5}$$

In both cases, there exist $u, v \in \{\varepsilon, \varepsilon^2\}$ such that $\xi_1^h = u$, and $\xi_2^h = v$. First, assume that $u \neq v$. Then $\xi_1^h\xi_2^h = \varepsilon^3 = 1$, which yields $\xi_3^h = (\xi_1\xi_2\xi_3)^h = \tau^h = 1$. Hence, we have $\mathrm{ord}_K(\xi_3)|h$ and (3.5) follows. Further, assume that $u = v$. Since we have put $\xi_1 = \xi$, we have either $\xi^h = \varepsilon^h\xi^h$ or $\xi^h = \varepsilon^{2h}\xi^h$. Hence $3|h$. Suppose (3.4). Then $\mathrm{ord}_K(\xi_3) = 3h$ and, thus, $9|\mathrm{ord}_K(\xi)$ for any $\xi \in \{\xi_1, \xi_2, \xi_3\}$. Since $9 \nmid p^2 + p + 1$, we have $\xi^{p^2+p+1} \neq 1$, which is a contradiction to Theorem 3.6. Hence, we have (3.5) and the theorem follows. □

Corollary 3.10. *Let* $p \in I$, $p \equiv 1 \pmod 3$ *and let* τ *be an arbitrary root of* $t(x)$ *in the splitting field* K *of* $t(x)$ *over* $\mathbb{F}_p$*. Then* $x^9 - \tau$ *has exactly* 9 *distinct roots in* K*.*

Proof. Since $\tau^{\frac{p^2+p+1}{3}} = 1$, the proof is a simple modification of the proof of Lemma 3.1. □

Example 3.11. Let $p = 37$. Then $p \equiv 1 \pmod 3$ and it can be verified that $p \in I$. Let K be the splitting field of $t(x)$ over $\mathbb{F}_{37}$ and let τ be any root of $t(x)$ in K. By Lemma 3.1, the polynomial $x^3 - \tau$ has three distinct roots ξ_1, ξ_2, ξ_3 in K. In the field $\mathbb{F}_{37}$ we have $\varepsilon = 10$, and Lemma 3.2, part (i), yields $\xi_2 = 10\xi_1$ and $\xi_3 = 15\xi_1$. Using the basis $1, \tau, \tau^2$ of the field extension $K/\mathbb{F}_p$, ξ_1, ξ_2, ξ_3 can be written in the form

$$\xi_1 = 2 + 16\tau + 24\tau^2,\ \xi_2 = 20 + 12\tau + 18\tau^2,\ \xi_3 = 15 + 9\tau + 32\tau^2.$$

By direct calculation we obtain $\mathrm{ord}_K(\tau) = 469$, $\mathrm{ord}_K(\xi_1) = \mathrm{ord}_K(\xi_2) = 1407$ and $\mathrm{ord}_K(\xi_3) = 469$. Consequently, by Theorem 1.1, part (ii), and Theorem 3.9, $h(37) = \mathrm{ord}_K(\tau) = \mathrm{ord}_K(\xi_3) = 469$. Furthermore, by Corollary 3.10, there exist 9 distinct roots of $x^9 - \tau$ in K:

$$\begin{array}{lllllllll}
\xi_{11} & = & 4 + 36\tau + 12\tau^2, & \xi_{12} & = & 3 + 27\tau + 9\tau^2, & \xi_{13} & = & 30 + 11\tau + 16\tau^2, \\
\xi_{21} & = & 21 + 4\tau + 26\tau^2, & \xi_{22} & = & 25 + 3\tau + \tau^2, & \xi_{23} & = & 28 + 30\tau + 10\tau^2, \\
\xi_{31} & = & 11 + 25\tau + 33\tau^2, & \xi_{32} & = & 27 + 21\tau + 7\tau^2, & \xi_{33} & = & 36 + 28\tau + 34\tau^2.
\end{array}$$

Moreover, for any $i, j \in \{1, 2, 3\}$, we have $\xi_{ij}^3 = \xi_i$. Put $w_1(x) = x^3 + 17x^2 + 31x - 1$, $w_2(x) = w_1(\varepsilon x) = x^3 + 22x^2 + 29x - 1$, and $w_3(x) = w_1(\varepsilon^2 x) = x^3 + 35x^2 + 14x - 1$. Then ξ_i, ξ_i^p, $\xi_i^{p^2}$, $i \in \{1, 2, 3\}$ are the roots of $w_i(x)$ and

$$x^9 - x^6 - x^3 - 1 \equiv w_1(x)w_2(x)w_3(x) \pmod{37}$$

as required by Corollary 3.7.

4. Periods of the Tribonacci sequence modulo a prime $p \equiv 1 \pmod 3$

Recall that, for a prime p, $h(p)$ denotes the period of $(T_n \bmod p)_{n=0}^{\infty}$. In this section we prove our main theorem extending Vince's result [7, Theorem 4].

Theorem 4.1. *Let p be an arbitrary prime, $p \equiv 1 \pmod 3$.*

(i) *If $p \in L$, then $h(p) | \frac{p-1}{3}$ if and only if 2 is a cubic residue of the field $\mathbb{F}_p$.*
(ii) *If $p \in Q$, then $h(p) | \frac{p^2-1}{3}$ if and only if 2 is a cubic residue of the field $\mathbb{F}_p$.*
(iii) *If $p \in I$, then $h(p) | \frac{p^2+p+1}{3}$.*

Proof. The congruence $p \equiv 1 \pmod 3$ implies $p \neq 2, 11$.

(i) Let $p \in L$ and let τ be any root of $t(x)$ in $\mathbb{F}_p$. If 2 is a cubic residue of $\mathbb{F}_p$, it follows from (1.1) that $\tau^{(p-1)/3} \equiv 1 \pmod p$. Hence, $\mathrm{ord}_{\mathbb{F}_p}(\tau) | \frac{p-1}{3}$ and Theorem 1.1, part (i), imply $h(p) | \frac{p-1}{3}$. On the other hand, if $h(p) | \frac{p-1}{3}$, then $\mathrm{ord}_{\mathbb{F}_p}(\tau) | \frac{p-1}{3}$ for any root τ of $t(x)$ in $\mathbb{F}_p$. Consequently, $\tau^{(p-1)/3} \equiv 1 \pmod p$ and (1.1) yields $2^{2(p-1)/3} \equiv 1 \pmod p$. This implies that either $2^{(p-1)/3} \equiv -1 \pmod p$ or 2 is a cubic residue of $\mathbb{F}_p$. Suppose that $2^{(p-1)/3} \equiv -1 \pmod p$. Then $1 \equiv 2^{p-1} \equiv (2^{(p-1)/3})^3 \equiv (-1)^3 \equiv -1$, which yields $2 \equiv 0 \pmod p$. Since $p \neq 2$, a contradiction follows.

(ii) Let $p \in Q$. Then the multiplicative group $K^{\times}$ of the splitting field K of $t(x)$ over $\mathbb{F}_p$ has $p^2 - 1$ elements. Let τ be any root of $t(x)$ in K. Then, by Theorem 1.3, there exists $\omega \in K$ such that $2\tau = \omega^3$. Let 2 be a cubic residue of $\mathbb{F}_p$. Then $2^{(p^2-1)/3} = 1$ in K and so $\tau^{(p^2-1)/3} = (2\tau)^{(p^2-1)/3} = \omega^{p^2-1} = 1$. This implies $\mathrm{ord}_K(\tau) | \frac{p^2-1}{3}$ and Theorem 1.1, part (i), yields $h(p) | \frac{p^2-1}{3}$. Conversely, assume that $h(p) | \frac{p^2-1}{3}$. Then $\mathrm{ord}_K(\tau) | \frac{p^2-1}{3}$ for any root τ of $t(x)$ in K and $\tau^{(p^2-1)/3} = 1$. From $2\tau = \omega^3$, we get $(2\tau)^{(p^2-1)/3} = \omega^{p^2-1} = 1$, which implies $2^{(p^2-1)/3} = 1$ in K. Clearly, $1 \equiv 2^{(p^2-1)/3} \equiv (2^{(p-1)/3})^{p+1} \equiv 2^{2(p-1)/3} \pmod p$. Using an argument similar to that in (i), we obtain $2^{(p-1)/3} \equiv 1 \pmod p$ and (ii) follows.

(iii) Let $p \in I$ and let τ be any root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$. Then, by (3.1), we have $\tau^{(p^2+p+1)/3} = 1$. This implies $\mathrm{ord}_K(\tau) | \frac{p^2+p+1}{3}$ and part (ii) of Theorem 1.1 yields $h(p) | \frac{p^2+p+1}{3}$ as required. □

Remark 4.2. If $p \equiv 1 \pmod 3$, then 2 is a cubic residue of the field $\mathbb{F}_p$ if and only if there are integers u and v such that $p = u^2 + 27v^2$. See [4, p. 119].

Let m be a positive integer, $m > 1$. In 1978, M. E. Waddill [9, Theorem 2] proved:

$$\text{If } \ T_k \equiv T_{k+1} \equiv 0 \pmod m, \ \text{ then } \ T_{k+2}^3 \equiv 1 \pmod m. \tag{4.1}$$

Moreover, if k is the least positive integer such that $T_k \equiv T_{k+1} \equiv 0 \pmod m$, then either $T_{k+2} \equiv 1 \pmod m$ or $T_{3k+2} \equiv 1 \pmod m$ and the period $h(m)$ of $(T_n \bmod m)_{n=0}^{\infty}$ is k or $3k$. See [9, Theorem 10]. If $m = p \in I$, we can say more.

Proposition 4.3. *Let k be the least positive integer such that $T_k \equiv T_{k+1} \equiv 0 \pmod p$. If $p \in I$, then $h(p) = k$.*

Proof. By (4.1), the congruences $T_k \equiv T_{k+1} \equiv 0 \pmod p$ imply $T_{k+2}^3 \equiv 1 \pmod p$. Suppose that $T_{k+2} \not\equiv 1 \pmod p$. First, it is evident that, for $p \equiv 2 \pmod 3$, we have $T_{k+2}^3 \equiv 1 \pmod p$ if and only if $T_{k+2} \equiv 1 \pmod p$. Hence, $p \equiv 1 \pmod 3$ or $p = 3$. Let $p \equiv 1 \pmod 3$. Then $T_{k+2} \not\equiv 1 \pmod p$ implies $T_{k+2} \equiv \varepsilon \pmod p$ and (3.3) yields $\tau^k = \varepsilon$. Since, by Remark 3.8, we have $\varepsilon \notin G =< \tau >$, a contradiction follows. Finally, for $p = 3$, the proof can be done by direct calculation. □

Let $(t_n)_{n=0}^{\infty} = (a, b, c, a+b+c, a+2b+2c, \dots)$ be a generalized Tribonacci sequence beginning with an arbitrary triple of integers $t_0 = a, t_1 = b, t_2 = c$. In 2008, J. Klaška [2] investigated the period $h(m)[a,b,c]$ of the sequence $(t_n \bmod m)_{n=0}^{\infty}$ where the modulus m is a power of a prime. In particular, if $m = p \in I$, then, by [2, pp. 271–274], we have $h(p)[a,b,c] = h(p)$ if and only if $[a,b,c] \not\equiv [0,0,0] \pmod p$. Together with part (iii) of Theorem 4.1 this yields the following proposition.

Proposition 4.4. *Let a, b, c be arbitrary integers and $(t_n)_{n=0}^{\infty}$ the generalized Tribonacci sequence beginning with $t_0 = a, t_1 = b, t_2 = c$. If p is a prime, $p \in I$, $p \equiv 1 \pmod 3$ then $h(p)[a,b,c] | \frac{p^2+p+1}{3}$.*

References

[1] W. Adams, D. Shanks, *Strong primality tests that are not sufficient*, Math. Comp. **39** (1982), 255–300.

[2] J. Klaška, *Tribonacci modulo p^t*, Math. Bohemica **133.3** (2008), 267–288.

[3] J. Klaška, L. Skula, *The cubic character of the Tribonacci roots*, The Fibonacci Quarterly **48.1** (2010), 21–28.

[4] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1992.

[5] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress (1897), 182–193.

[6] Z. – H. Sun, *Cubic and quartic congruences modulo a prime*, J. Number Theory **102** (2003), 41–89.

[7] A. Vince, *Period of a linear recurrence*, Acta Arith. **39** (1981), 303–311.

[8] G. Voronoï, *Sur une propriété du discriminant des fonctions entières*, Verhand. III. Internat. Math. Kongress (1905), 186–189.

[9] M. E. Waddill, *Some properties of a generalized Fibonacci sequence modulo m*, The Fibonacci Quarterly **16** (1978), 344–353.

[10] M. Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. **33** (1931), 153–165.

MSC 2010: 11B50, 11B39, 11A07

CHAPTER 12

A NOTE ON THE CUBIC CHARACTERS OF TRIBONACCI ROOTS ⋆

Abstract. In this paper we complete our preceding research concerning the cubic character of the roots of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ over the Galois field $\mathbb{F}_p$ where p is an arbitrary prime, $p \equiv 1 \pmod 3$.

1. Introduction

Let τ be any root of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ in the Galois field $\mathbb{F}_p$ where p is a prime, $p \equiv 1 \pmod 3$. In [1], we proved that

$$\tau^{\frac{p-1}{3}} = \left(\frac{\tau}{p}\right)_3 = 2^{\frac{2(p-1)}{3}}. \tag{1.1}$$

Next, in [2], we showed that, if $t(x)$ is irreducible over $\mathbb{F}_p$, $p \equiv 1 \pmod 3$ and τ is any root of $t(x)$ in the splitting field of $t(x)$ over $\mathbb{F}_p$, then

$$\tau^{\frac{p^2+p+1}{3}} = 1. \tag{1.2}$$

The number-theoretic results (1.1) and (1.2) were used in [2] to investigate the period $h(p)$ of the Tribonacci sequence $(T_n)_{n=0}^{\infty}$ reduced by a modulus p. Recall that $(T_n)_{n=0}^{\infty}$ is defined recursively by $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ with $T_0 = T_1 = 0$, $T_2 = 1$ and that the period $h(p)$ of $(T_n \bmod p)_{n=0}^{\infty}$ is the least positive integer satisfying $T_{h(p)} \equiv T_{h(p)+1} \equiv 0 \pmod p$, $T_{h(p)+2} \equiv 1 \pmod p$. Let I be the set of all primes p for which $t(x)$ is irreducible over $\mathbb{F}_p$, Q be the set of all primes for which $t(x)$ splits over $\mathbb{F}_p$ into the product of a linear factor and an irreducible quadratic factor, and let L be the set of all primes for which $t(x)$ completely splits over $\mathbb{F}_p$ into linear factors. Furthermore, let $D = -2^2 \cdot 11$ be the discriminant of $t(x)$. By [1, Corollary 2.5], $p \in Q$ if and only if $\left(\frac{p}{11}\right) = -1$. Moreover, if $p \neq 2, 11$, then $p \in I \cup L$ if and only if $\left(\frac{p}{11}\right) = 1$. In [2], we established, for $p \equiv 1 \pmod 3$, the following properties of $h(p)$:

$$\begin{aligned} &\textit{If } p \in L, \textit{ then } h(p) \mid \tfrac{p-1}{3} \textit{ if and only if } 2 \textit{ is a cubic residue of the field } \mathbb{F}_p.\\ &\textit{If } p \in Q, \textit{ then } h(p) \mid \tfrac{p^2-1}{3} \textit{ if and only if } 2 \textit{ is a cubic residue of the field } \mathbb{F}_p.\\ &\textit{If } p \in I, \textit{ then } h(p) \mid \tfrac{p^2+p+1}{3}. \end{aligned} \tag{1.3}$$

In the proofs of (1.1) – (1.3), which were presented in [1] and [2], a significant role is played by the cubic polynomials $f(x, c) = x^3 + A(c)x^2 + B(c)x + C(c) \in \mathbb{F}_p[x]$, $p \equiv 1 \pmod 3$ with

$$A(c) = -18c^2 + 3,\ B(c) = -9c^2 - 27c - 24,\ C(c) = 9c^2 - 27c + 28, \tag{1.4}$$

⋆ Published in J. Klaška, L. Skula, *A note on the cubic characters of Tribonacci roots*, The Fibonacci Quarterly **48.4** (2010), 324–326.

and $c \in \{-1, -\varepsilon, -\varepsilon^2\}$. Here, $\varepsilon \in \mathbb{F}_p$ denotes a primitive third root of unity so that $\varepsilon^2 + \varepsilon + 1 = 0$. Let D_c be the discriminant of $f(x, c)$. Then $D_c = 2^2 \cdot 3^9 \cdot 11$ for any $c \in \{-1, -\varepsilon, -\varepsilon^2\}$ and, by [1, Lemma 2.6], we have

$$\left(\frac{D_c}{p}\right) = \left(\frac{D}{p}\right) = \left(\frac{p}{11}\right). \tag{1.5}$$

Consequently, the Stickelberger parity theorem [1, Theorem 2.4] can be used to prove the following lemma:

Lemma 1.1. *Let p be an arbitrary prime, $p \equiv 1 \pmod 3$ such that $\left(\frac{p}{11}\right) = -1$. Then the Tribonacci polynomial $t(x)$ has exactly one root in the field $\mathbb{F}_p$ if and only if each of the polynomials $f(x, c)$, $c \in \{-1, -\varepsilon, -\varepsilon^2\}$ has exactly one root in $\mathbb{F}_p$.*

Since 2 is the root of $f(x, -1)$ in any Galois field $\mathbb{F}_p$, to find the further relations between the number of roots of $t(x)$ and $f(x, -1)$ is quite easy. The polynomial $f(x, -1)$ has three distinct roots in $\mathbb{F}_p$ if and only if $t(x)$ has no root or three distinct roots in $\mathbb{F}_p$. By means of the results derived in [1] and [2], these two cases may be distinguished as follows: The Tribonacci polynomial $t(x)$ has no root in $\mathbb{F}_p$ if and only if all three roots of $f(x, -1)$ belong to distinct cubic classes of $\mathbb{F}_p$. On the other hand, $t(x)$ has three distinct roots in $\mathbb{F}_p$ if and only if all three roots of $f(x, -1)$ belong to a single cubic class of $\mathbb{F}_p$.

In the present short note we complete what we know about the relations between the Tribonacci polynomial $t(x)$ and the polynomials $f(x, c)$, $c \in \{-\varepsilon, -\varepsilon^2\}$. In particular, we prove that, in any Galois field $\mathbb{F}_p$, where $p \equiv 1 \pmod 3$, these polynomials have the same number of roots.

2. The number of roots of the polynomials $t(x)$, $f(x, -\varepsilon)$, $f(x, -\varepsilon^2)$ over the Galois field $\mathbb{F}_p$ where $p \equiv 1 \pmod 3$

For proof of our main result, we shall need the following two statements:

(i) Let p be a prime, $p \equiv 1 \pmod 3$ and let $g(x) = x^3 + rx + s \in \mathbb{F}_p[x]$, $r, s \neq 0$. Assume that there exists $\lambda \in \mathbb{F}_p$ such that $\lambda^2 = d$ where $d = \frac{s^2}{4} + \frac{r^3}{27}$. Further assume that $g(x)$ is irreducible over $\mathbb{F}_p$ or $g(x)$ has three distinct roots in $\mathbb{F}_p$. Then $g(x)$ is irreducible over $\mathbb{F}_p$ if and only if $A = -\frac{s}{2} + \lambda$ is not a cubic residue of $\mathbb{F}_p$.

(ii) For an arbitrary prime p, $p \equiv 1 \pmod 3$, there exists $\varkappa \in \mathbb{F}_p$ such that $\varkappa^2 = 33$. If $p \equiv 1 \pmod 3$ and $\left(\frac{p}{11}\right) = 1$, then $t(x)$ is irreducible over $\mathbb{F}_p$ if and only if $19 - 3\varkappa$ is not a cubic residue of $\mathbb{F}_p$.

Part (i) is a direct consequence of [2, Theorem 2.4]. For (ii), see [2, Theorem 2.5].

Theorem 2.1. *Let p be an arbitrary prime, $p \equiv 1 \pmod 3$ such that $\left(\frac{p}{11}\right) = 1$. Then the Tribonacci polynomial $t(x)$ is irreducible over the field $\mathbb{F}_p$ if and only if $f(x, -\varepsilon)$, $f(x, -\varepsilon^2)$ are irreducible over $\mathbb{F}_p$.*

Proof. After substituting $x = y - \frac{A(-\varepsilon)}{3}$, the polynomial $f(x, -\varepsilon)$ becomes a cubic polynomial $g(y) = y^3 + ry + s \in \mathbb{F}_p[y]$ with

$$r = \frac{1}{3}(3B(-\varepsilon) - A(-\varepsilon)^2) \quad \text{and} \quad s = \frac{1}{27}(2A(-\varepsilon)^3 - 9A(-\varepsilon)B(-\varepsilon) + 27C(-\varepsilon)). \tag{2.1}$$

From (1.4), we obtain $A(-\varepsilon) = 18\varepsilon + 21$, $B(-\varepsilon) = 36\varepsilon - 15$, and $C(-\varepsilon) = 18\varepsilon + 19$. Substituting into (2.1) and using the identity $\varepsilon^2 + \varepsilon + 1 = 0$, r and s can be written in the form

$$r = -2 \cdot 3^3(2\varepsilon + 1), \quad s = 2 \cdot 3^3(6\varepsilon - 1). \tag{2.2}$$

We show that $r, s \neq 0$. Suppose $r = 0$. From (2.2) we have $2\varepsilon + 1 = 0$. This implies $9 = 0$, which yields a contradiction with $p \equiv 1 \pmod 3$. Next suppose $s = 0$. Then $6\varepsilon - 1 = 0$ and $215 = 5 \cdot 43 = 0$ follows. Since $5 \not\equiv 1 \pmod 3$ and $(\frac{43}{11}) = -1$, we have a contradiction.

By (ii), there exists $\varkappa \in \mathbb{F}_p$ such that $\varkappa^2 = 33$. Let $d = \frac{s^2}{4} + \frac{r^3}{27}$, $\mu = 2\varepsilon + 1$, $\nu = \frac{\varkappa}{\mu}$, $\lambda = 27\nu$, and $A = -\frac{s}{2} + \lambda$. Then $d = -3^6 \cdot 11$, $\lambda^2 = d$, and $A = (-3)^3(-4 + 3\mu - \nu)$.

It is evident that $f(x, -\varepsilon)$ and $g(y)$ have the same number of roots in $\mathbb{F}_p$. Hence, the assumption $\left(\frac{p}{11}\right) = 1$ implies that $g(y)$ is irreducible over $\mathbb{F}_p$ or has three distinct roots in $\mathbb{F}_p$. Moreover, according to (i),

$$g(y) \text{ is irreducible if and only if } -4 + 3\mu - \nu \text{ is not a cubic residue of } \mathbb{F}_p. \tag{2.3}$$

By direct calculation, we can verify that

$$(19 - 3\varkappa)(-4 + 3\mu - \nu) = (2 - \mu - \nu)^3. \tag{2.4}$$

By (ii), $t(x)$ is irreducible over $\mathbb{F}_p$ if and only if $19 - 3\varkappa$ is not a cubic residue of $\mathbb{F}_p$. From (2.4), it follows that $19 - 3\varkappa$ is not a cubic residue of $\mathbb{F}_p$ if and only if $-4 + 3\mu - \nu$ is not cubic residue of $\mathbb{F}_p$. Finally, using (2.3), we conclude that $g(y)$ and $f(x, -\varepsilon)$ are irreducible over $\mathbb{F}_p$. Since we can replace ε by ε^2, this is also true for $f(x, -\varepsilon^2)$. This completes the proof. □

Together with Lemma 1.1, Theorem 2.1 yields the desired result.

Theorem 2.2. *Let p be an arbitrary prime, $p \equiv 1 \pmod 3$. Then the polynomials $t(x)$, $f(x, -\varepsilon)$, $f(x, -\varepsilon^2)$ have the same number of roots over the field $\mathbb{F}_p$.*

References

[1] J. Klaška, L. Skula, *The cubic character of the Tribonacci roots*, The Fibonacci Quarterly **48.1** (2010), 21–28.

[2] J. Klaška, L. Skula, *Periods of the Tribonacci sequence modulo a prime $p \equiv 1 \pmod 3$*, The Fibonacci Quarterly **48.3** (2010), 228–235.

MSC 2010: 11B39, 11B50, 11D25

CHAPTER 13

MORDELL'S EQUATION AND THE TRIBONACCI FAMILY ⋆

Abstract. We define a Tribonacci family as the set T of all cubic polynomials $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ having the same discriminant as the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$. Using integral solutions of Mordell's equation $Y^2 = X^3 + 297$, we establish explicit forms of all polynomials in T. As the main result we prove that all polynomials in T have the same type of factorization over any Galois field $\mathbb{F}_p$ where p is a prime.

1. Introduction

Mordell's equation

$$Y^2 = X^3 + k,\ 0 \neq k \in \mathbb{Z}. \tag{1.1}$$

has had a long and interesting history. A synopsis of the first discoveries concerning (1.1) is given in Dickson [1, pp. 533–539]. See also [6, pp. 1–5]. In 1909, A. Thue [9] showed that (1.1) has only a finite number of solutions in integers X, Y. Various methods for finding the integral solutions of (1.1) are known [3, 6, 7]. Extensive lists of further references related to (1.1) can be found in [3] and [6].

In this paper we show an interesting application of integral solutions of (1.1) with $k = 297$ to the theory of factorizations of the cubic polynomials $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ with a discriminant $D_f = -44$ over a Galois field $\mathbb{F}_p$ where p is a prime. In particular, we prove that the set

$$T = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = -44\}$$

contains infinitely many polynomials, which can be partitioned into eight pairwise disjoint classes such that the polynomials of each class are given by a simple formula that depends on some integral solution of $Y^2 = X^3 + 297$. Since the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ belongs to T, we call T the Tribonacci family. As the main result we prove that, over any Galois field $\mathbb{F}_p$ where p is a prime, all polynomials in T have the same type of factorization and, consequently, the same number of roots in $\mathbb{F}_p$. We do this by combining the Stickelberger Parity Theorem [8] for the case of a cubic polynomial [10], a modification of the results presented in [5, pp. 229–230], and the relations between the cubic characters of certain elements of the field $\mathbb{F}_{p^2}$ corresponding to integral solutions of $Y^2 = X^3 + 297$. In general, we show that, for any $D \in \mathbb{Z}$, the set

$$C = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = D\}$$

⋆ Published in J. Klaška, L. Skula, *Mordell's equation and the Tribonacci family*, The Fibonacci Quarterly **49.4** (2011), 310–319.

can be obtained by means of integral solutions of Mordell's equation $Y^2 = X^3 - 432D$. This fact opens an interesting question, namely, for which $D \in \mathbb{Z}$ can our main result be generalized.

2. Connection between Mordel's equation $Y^2 = X^3 - 432D$ and cubic polynomials with discriminant D

Let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ and let $D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$ be the discriminant of $f(x)$. Let $g_f(x) = f(x - a/3)$. Then $D_{g_f} = D_f$ and $g_f(x) = x^3 + rx + s \in \mathbb{Q}[x]$ where

$$r = b - \frac{a^2}{3} \quad \text{and} \quad s = \frac{2a^3}{27} - \frac{ab}{3} + c. \tag{2.1}$$

Next, let

$$d_f = \frac{r^3}{27} + \frac{s^2}{4}. \tag{2.2}$$

Then $D_f = -108 d_f$ and $d_f = d_{g_f}$. If $f(x) \in \mathbb{Z}[x]$, then (2.1) implies

$$r, s \in \mathbb{Z} \iff 3|a. \tag{2.3}$$

On the other hand, for $f(x) \in \mathbb{Z}[x]$,

$$3 \nmid a \iff \text{there exists } u, v \in \mathbb{Z} : r = \frac{u}{3},\ s = \frac{v}{27},\ 3 \nmid uv. \tag{2.4}$$

Moreover, by (2.1), we obtain

$$u = 3b - a^2 \text{ and } v = 2a^3 - 9ab + 27c. \tag{2.5}$$

For $e \in \{0, 1, 2\}$, let $\mathbb{D}_e$ denote the set of all $d \in \mathbb{Q}$ for which there exists $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ such that $a \equiv e \pmod 3$ and $d_f = d$. Some basic properties of $\mathbb{D}_e$ will be established in the following lemma.

Lemma 2.1. *For $\mathbb{D}_0$, $\mathbb{D}_1$ and $\mathbb{D}_2$ we have*

$$\mathbb{D}_0 = \left\{ d \in \mathbb{Q};\ d = \frac{4u^3 + 27v^2}{108}, u, v \in \mathbb{Z} \right\} \tag{2.6}$$

and $\mathbb{D}_1 = \mathbb{D}_2 =$

$$\left\{ d \in \mathbb{Q}; d = \frac{4u^3 + v^2}{2916}, u, v \in \mathbb{Z}, u \equiv 2 \pmod 3, 3u + v + 1 \equiv 0 \pmod{27} \right\}. \tag{2.7}$$

Proof. (i) Let $d \in \mathbb{D}_0$. Then there exists $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ such that $3|a$ and $d_f = d$. By (2.3), $g_f(x) = x^3 + rx + s \in \mathbb{Z}[x]$. Put $u = r$, $v = s$. Then $u, v \in \mathbb{Z}$ and, by (2.2), $d = d_f = (4u^3 + 27v^2)/108$. Conversely, assume that $d = (4u^3 + 27v^2)/108$ where $u, v \in \mathbb{Z}$. For any $w \in \mathbb{Z}$, let

$$a = 3w,\ b = 3w^2 + u,\ c = w^3 + uw + v. \tag{2.8}$$

Then $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$, $3|a$ and, $g_f(x) = x^3 + rx + s \in \mathbb{Z}[x]$. Substituting (2.8) into (2.1), we obtain $r = u$ and $s = v$, which together with (2.2) yields $d = d_f = (4u^3 + 27v^2)/108$. This proves (2.6).

(ii) Let $e \in \{1, 2\}$. First show

$$\mathbb{D}_e = \left\{ d \in \mathbb{Q}; d = \frac{4u^3 + v^2}{2916}, u, v \in \mathbb{Z}, u \equiv 2 \pmod 3, e^3 + 3eu + v \equiv 0 \pmod{27} \right\}. \tag{2.9}$$

Let $d \in \mathbb{D}_e$. Then there exists $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ such that $a \equiv e \pmod 3$ and, $d_f = d$. By (2.4), $g_f(x) = x^3 + ux/3 + v/27 \in \mathbb{Q}[x]$ where $u, v \in \mathbb{Z}$ and $3 \nmid uv$. Hence, by (2.2), $d = d_f = (4u^3 + v^2)/2916$. Moreover, from (2.5) it follows that $u = 3b - a^2 \equiv -e^2 \equiv 2 \pmod 3$. Since $a = 3w + e$ for some $w \in \mathbb{Z}$, the first identity of (2.1) yields $b = (a^2 + u)/3 = 3w^2 + 2ew + (u + e^2)/3$. Hence, by (2.5), $v \equiv 2(3w + e)^3 - 9(3w + e)(3w^2 + 2ew + (u + e^2)/3) \equiv -3eu - e^3 \pmod{27}$, and $e^3 + 3eu + v \equiv 0 \pmod{27}$ follows. Conversely, assume that $d = (4u^3 + v^2)/2916$ where $u, v \in \mathbb{Z}$ such that $u \equiv 2 \pmod 3$ and $e^3 + 3eu + v \equiv 0 \pmod{27}$. For any $w \in \mathbb{Z}$, put $a = 3w + e$, $b = (a^2 + u)/3$, $c = (-2a^3 + 9ab + v)/27$. Since $u \equiv 2 \pmod 3$, we have $a^2 + u \equiv e^2 + 2 \equiv 0 \pmod 3$. Hence, $b \in \mathbb{Z}$. Next, after some calculation, we obtain $-2a^3+9ab+v \equiv -2(3w+e)^3+9(3w+e)(3w^2+2ew+(u+e^2)/3)-e^3-3eu \equiv 0 \pmod{27}$. Hence, $c \in \mathbb{Z}$. Let $f(x) = x^3+ax^2+bx+c$. Using (2.1), we get $g_f(x)=x^3+ux/3+v/27$ and (2.2) yields $d_f = (4u^3 + v^2)/(4 \cdot 27^2) = d$ as required. This proves (2.9).

It remains to prove $\mathbb{D}_1 = \mathbb{D}_2$. Let u be an integer, $u \equiv 2 \pmod 3$. Then $9u + 9 \equiv 0 \pmod{27}$, which implies

$$v + 3u + 1 \equiv 0 \pmod{27} \iff -v + 6u + 8 \equiv 0 \pmod{27} \tag{2.10}$$

for any $v \in \mathbb{Z}$. Clearly, if $d = d(u, v) = (4u^3 + v^2)/2916$, then $d(u, v) = d(u, -v)$. This, together with (2.9) and (2.10), yields (2.7). The proof is complete. □

Remark 2.2. Let $\mathbb{D} = \mathbb{D}_1 = \mathbb{D}_2$. Then $\mathbb{D}_0 \cap \mathbb{D}$, $\mathbb{D}_0 - \mathbb{D}$, and $\mathbb{D} - \mathbb{D}_0$ are nonempty sets. For example, $23/108 \in \mathbb{D}_0 \cap \mathbb{D}$, $-13/108 \in \mathbb{D}_0 - \mathbb{D}$, and $11/27 \in \mathbb{D} - \mathbb{D}_0$.

For any $d \in \mathbb{Q}$ let

$$C(d) = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; d_f = d\}.$$

Then, $C(d) = \{f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]; D_f = -108d\}$. Furthermore, $C(d) = \emptyset$ if and only if $d \in \mathbb{Q} - (\mathbb{D}_0 \cup \mathbb{D})$. For $d \in \mathbb{D}_0 \cup \mathbb{D}$, the following theorem can be stated.

Theorem 2.3. *Assume that* $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.

(i) *Let* $d \in \mathbb{D}_0$. *Then* $f(x) \in C(d)$ *if and only if there exists* $u, v, w \in \mathbb{Z}$ *such that*

$$a = 3w,\ b = 3w^2 + u,\ c = w^3 + uw + v \text{ and, } 4u^3 + 27v^2 = 108d. \tag{2.11}$$

(ii) *Let* $d \in \mathbb{D}_e$ *and* $e \in \{1, 2\}$. *Then* $f(x) \in C(d)$ *if and only if there exist* $u, v, w \in \mathbb{Z}$ *such that*

$$a=3w+e,\ b=3w^2+2ew+\frac{e^2+u}{3},\ c=w^3+ew^2+\frac{e^2+u}{3}w+\frac{e^3+3eu+v}{27} \tag{2.12}$$

and

$$4u^3 + v^2 = 2916d \text{ where } u \equiv 2 \pmod 3,\ e^3 + 3eu + v \equiv 0 \pmod{27}. \tag{2.13}$$

Moreover, in (i) *we have* $g_f(x) = x^3 + ux + v$ *and, in* (ii), $g_f(x) = x^3 + ux/3 + v/27$.

Proof. (i) Let $d \in \mathbb{D}_0$ and $f(x) \in C(d)$. Then there exist $w \in \mathbb{Z}$ such that $a = 3w$ and, by (2.3), $g_f(x) = x^3 + rx + s \in \mathbb{Z}[x]$. Let $u = r$ and $v = s$. By (2.2), $d = d_f = (4u^3+27v^2)/108$ and $4u^3+27v^2 = 108d$ follows. Since $a = 3w$, the first equation of (2.1) implies $b = 3w^2 + u$. Similarly, the second equation of (2.1) together with $a = 3w$ and $b = 3w^2+u$ yields $c = w^2+uw+v$. Hence (2.11) follows. Conversely, assume that a, b, c satisfy (2.11). Substituting $a = 3w$, $b = 3w^2 + u$ and $c = w^3 + uw + v$ into (2.1), after short calculation, we get, $r = u$ and $s = v$. Hence, by (2.2), $d_f = (4u^3 + 27v^2)/108 = d$ and $f(x) \in C(d)$ follows. This proves (i).

(ii) Let $d \in \mathbb{D}_e$, $e \in \{1,2\}$, and $f(x) \in C(d)$. Then there exists $w \in \mathbb{Z}$ such that $a = 3w+e$ and, by (2.4), $g_f(x) = x^3+ux/3+v/27 \in \mathbb{Q}[x]$ where $u,v \in \mathbb{Z}$ and, $3 \nmid uv$. By (2.2), $d = d_f = (4u^3+v^2)/2916$ and $4u^3+v^2 = 2916d$ follows. Substituting $a = 3w+e$ into the first equality of (2.1), we obtain, $b = 3w^2+2ew+(u+e^2)/3$. This together with the second equality of (2.1) yields $c = w^3+ew^2+(u+e^2)w/3+(3eu+v+e^3)/27$ and (2.13) follows. Conversely, assume that a,b,c satisfy (2.12) and (2.13). Substituting (2.12) into (2.1), we get $r = u/3$ and $s = v/27$. Hence, $g_f(x) = x^3+ux/3+v/27$ and, by (2.2), we conclude that $d_f = (4u^3+v^2)/2916 = d$. □

The following corollary states that both Diophantine equations $4u^3+27v^2 = 108d$ and $4u^3+v^2 = 2919d$ can be reduced to the same Mordell equation $Y^2 = X^3 - 432D$ with $D = -108d$. Consequently, the coefficients a,b,c from (2.12) and (2.13) can be given by the integral solutions of $Y^2 = X^3 - 432D$.

Corollary 2.4. (i) *Let $d \in \mathbb{D}_0$ and $D = -108d$. Then $f(x) = x^3+ax^2+bx+c \in C(d)$ if and only if there exist $w, X, Y \in \mathbb{Z}$ such that*

$$a = 3w,\ \ b = 3w^2 - \frac{X}{12},\ \ c = w^3 - \frac{X}{12}w + \frac{Y}{108} \tag{2.14}$$

and

$$Y^2 = X^3 - 432D \quad \textit{where} \quad 12|X, 108|Y.$$

(ii) *Let $d \in \mathbb{D}_e, e \in \{1,2\}$ and $D = -108d$. Then $f(x) = x^3+ax^2+bx+c \in C(d)$ if and only if there exist $w, X, Y \in \mathbb{Z}$ such that*

$$a=3w+e, b=3w^2+2ew+\frac{4e^2-X}{12}, c=w^3+ew^2+\frac{4e^2-X}{12}w+\frac{4e^3-3eX+Y}{108} \tag{2.15}$$

and

$$Y^2=X^3-432D \ \textit{where}\ 4|X, 4|Y, X\equiv 1 \ (\mathrm{mod}\ 3), 4e^3-3eX+Y\equiv 0\,(\mathrm{mod}\ 27).$$

Corollary 2.4 can be easily obtained from Theorem 2.3 by the substitutions $X = -12u$, $Y = 108v$ in case (i) and $X = -4u$, $Y = 4v$ in case (ii).

Remark 2.5. The coefficients a,b,c given by (2.11), (2.12), (2.14) and (2.15) can be written using derivatives as follows: if $c = c(w)$, then $b = c'(w)$ and $a = c''(w)/2$.

Remark 2.6. A straightforward application of Corollary 2.4 with $d = 11/27$ leads to Mordell's equation (1.1) with $k = 19008$. In the following section, we show that the set $C(11/27)$ can also be obtained by means of integral solutions of (1.1) with $k = 297$.

3. The Tribonacci family

Let $t(x) = x^3 - x^2 - x - 1$ be the Tribonacci polynomial. First, observe that

$$D_t = -44,\ d_t = \frac{11}{27} \ \text{ and } \ g_t(x) = x^3 - \frac{4}{3}x - \frac{38}{27}.$$

Since

$$t(x) \in T = \{f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]; D_f = -44\} = C(11/27),$$

the set T can be called the *Tribonacci family*. In this section, explicit forms of all polynomials in T will be given.

Lemma 3.1. *Assume that* $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.
(i) *We have* $11/27 \notin \mathbb{D}_0$.
(ii) $f(x) \in T$ *if and only if there exists* $e \in \{1, 2\}$ *and* $w, X, Y \in \mathbb{Z}$ *such that*

$$a=3w+e,\ b=3w^2+2ew+\frac{e^2-X}{3},\ c=w^3+ew^2+\frac{e^2-X}{3}w+\frac{e^3-3eX+2Y}{27} \tag{3.1}$$

and

$$Y^2 = X^3 + 297 \text{ where } X \equiv 1 \pmod 3 \text{ and } e^3 - 3eX + 2Y \equiv 0 \pmod{27}. \tag{3.2}$$

Moreover, $g_f(x) = x^3 + rx + s$ *where* $r = -X/3$, $s = 2Y/27$ *with* X, Y *satisfying* (3.2).

Proof. (i) Suppose $11/27 \in \mathbb{D}_0$. Then, by (2.12), there exist $u, v \in \mathbb{Z}$ such that $4u^3 + 27v^2 = 44$. Hence, $2|v$ and $u^3 + 27k^2 = 11$ for some $k \in \mathbb{Z}$. Since $u^3 \equiv 11 \pmod{27}$ has no solution, we get a contradiction. Consequently, $11/27 \notin \mathbb{D}_0$ and $3 \nmid a$. Part (ii) can be obtained easily from Theorem 2.3 by substituting $u = -X$, $v = 2Y$. □

Theorem 3.2. *Mordell's equation* $Y^2 = X^3+297$ *has exactly eighteen integral solutions* (X, Y)*:* $(-6, \pm 9)$, $(-2, \pm 17)$, $(3, \pm 18)$, $(4, \pm 19)$, $(12, \pm 45)$, $(34, \pm 199)$, $(48, \pm 333)$, $(1362, \pm 50265)$, *and* $(93844, \pm 28748141)$.

See Table 3 in [2, p. 96] or consult [6, p. 127].

Corollary 3.3. *There exist exactly eight integral solutions* (X, Y) *of* $Y^2 = X^3 + 297$ *satisfying* $X \equiv 1 \pmod 3$ *and* $e^3 - 3eX + 2Y \equiv 0 \pmod{27}$ *where* $e = 1$ *or* $e = 2$*:* $(-2, \pm 17)$, $(4, \pm 19)$, $(34, \pm 199)$, *and* $(93844, \pm 28748141)$.

Combining Lemma 3.1 and Corollary 3.3, we see that there exist exactly eight polynomials $g_j(x) = x^3 + r_j x + s_j \in \mathbb{Q}[x]$, $j \in \{1, \cdots, 8\}$ with $D_{g_j} = -44$:

$$\begin{array}{ll} g_1(x) = x^3+\frac{2}{3}x - \frac{34}{27}, & g_2(x) = x^3+\frac{2}{3}x + \frac{34}{27}, \\ g_3(x) = x^3-\frac{4}{3}x - \frac{38}{27}, & g_4(x) = x^3-\frac{4}{3}x + \frac{38}{27}, \\ g_5(x) = x^3-\frac{34}{3}x - \frac{398}{27}, & g_6(x) = x^3-\frac{34}{3}x + \frac{398}{27}, \\ g_7(x) = x^3-\frac{93844}{3}x - \frac{57496282}{27}, & g_8(x) = x^3-\frac{93844}{3}x + \frac{57496282}{27}. \end{array} \tag{3.3}$$

Next, letting $k = w$ in (3.1) and using Corollary 3.3, we find that $f(x) \in T$ if and only if $f(x) = t_j(x, k)$ for some $j \in \{1, \cdots, 8\}$ and $k \in \mathbb{Z}$ where

$$\begin{array}{l} t_1(x,k)=x^3+(3k+1)x^2+\ (3k^2+2k+1)x+k^3+k^2+k-1, \\ t_2(x,k)=x^3+(3k+2)x^2+\ (3k^2+4k+2)x+k^3+2k^2+2k+2, \\ t_3(x,k)=x^3+(3k+2)x^2+\ (3k^2+4k)x+k^3+2k^2-2, \\ t_4(x,k)=x^3+(3k+1)x^2+\ (3k^2+2k-1)x+k^3+k^2-k+1, \\ t_5(x,k)=x^3+(3k+2)x^2+\ (3k^2+4k-10)x+k^3+2k^2-10k-22, \\ t_6(x,k)=x^3+(3k+1)x^2+\ (3k^2+2k-11)x+k^3+k^2-11k+11, \\ t_7(x,k)=x^3+(3k+1)x^2+(3k^2+2k-31281)x+k^3+k^2-31281k-2139919, \\ t_8(x,k)=x^3+(3k+2)x^2+(3k^2+4k-31280)x+k^3+2k^2-31280k+2108638. \end{array} \tag{3.4}$$

Consequently, T can be written as $T = \bigcup_{j=1}^{8}\{t_j(x, k); k \in \mathbb{Z}\}$ where $\{t_j(x, k); k \in \mathbb{Z}\}$ are pairwise disjoint sets. Finally, by (3.4), $t(x) = t_3(x, -1)$.

4. The cubic character of the field $\mathbb{F}_{p^2}$

We start this section with a more general theorem.

Theorem 4.1. *Let $\mathbb{H}$ be a subfield of the field $\mathbb{G}$, $[\mathbb{G} : \mathbb{H}] = 2$, $\operatorname{char} \mathbb{H} \neq 2, 3$ and let $g(x) = x^3 + rx + s \in \mathbb{H}[x]$ with $r \neq 0$. Assume that $g(x)$ is irreducible over $\mathbb{H}$ or $g(x)$ has three distinct roots in $\mathbb{H}$. Further let $d_g = r^3/27 + s^2/4$ and $\varepsilon, \lambda \in \mathbb{G}$ be such that $\varepsilon^2 + \varepsilon + 1 = 0$ and $\lambda^2 = d_g$. Then the following statements are equivalent:*

(i) *$g(x)$ has three distinct roots in $\mathbb{H}$.*
(ii) *$g(x)$ has three distinct roots in $\mathbb{G}$.*
(iii) *$A = -s/2 - \lambda$ is a cubic residue of $\mathbb{G}$.*
(iv) *$B = -s/2 + \lambda$ is a cubic residue of $\mathbb{G}$.*

Proof. Clearly, (i) implies (ii). Assume (ii) and suppose that $g(x)$ is irreducible over $\mathbb{H}$. Then $\mathbb{G}$ is a splitting field of $g(x)$ over $\mathbb{H}$. Hence, $[\mathbb{G} : \mathbb{H}] = 3$ which is a contradiction. This proves that (i) and (ii) are equivalent. Next, a simple calculation yields $AB = (-r/3)^3$. Since $r \neq 0$, it follows that (iii) and (iv) are equivalent.

Let $\mathbb{K}$ be an arbitrary over-field of $\mathbb{G}$ such that A, B are cubic residues of $\mathbb{K}$. Then there exists $\alpha, \gamma \in \mathbb{K}$ satisfying $\alpha^3 = A$, $\gamma^3 = B$. Since $(\alpha\gamma)^3 = AB = (-r/3)^3$ there exist $i \in \{0, 1, 2\}$ such that $\alpha\gamma\varepsilon^i = -r/3$. Let $\beta = \gamma\varepsilon^i$. Then $\beta^3 = B$ and $\alpha\beta = -r/3$. Since $A + B = -s$, we have $g(\alpha + \beta) = A + B + (\alpha + \beta)(3\alpha\beta + r) + s = 0$.

Hence, it follows for $\mathbb{K} = \mathbb{G}$ that (iii) implies (ii). Finally, assume (ii) and suppose that A is not a cubic residue of $\mathbb{G}$. Let $\mathbb{S}$ be a splitting field of $x^3 - A$ over $\mathbb{G}$. Then A is a cubic reside of $\mathbb{S}$ and $AB = (-r/3)^3$ yields that B is a cubic reside of $\mathbb{S}$, too. By what was proved above, in the field $\mathbb{K} = \mathbb{S}$, there exist α, β such that $g(\alpha + \beta) = 0$. Since $g(x)$ has three distinct roots in $\mathbb{G}$, we have $\alpha + \beta \in \mathbb{G}$. Put $\eta = \alpha + \beta$. Then $-s = A+B = \alpha^3 + (\eta - \alpha)^3 = 3\alpha^2\eta - 3\alpha\eta^2 + \eta^3$. Since $1, \alpha, \alpha^2$ is a base of the extension $\mathbb{S}/\mathbb{G}$, we have $\eta = 0$ and $s = 0$. Let $\rho = -3\lambda/r$. Then $\rho \in \mathbb{G}$ and $\lambda^2 = d_g = r^3/27$ yields $\rho^3 = -27\lambda^3/r^3 = -\lambda = A$, a contradiction. Hence, (ii) implies (iii) as required. The proof is complete. □

Note that Theorem 4.1 generalizes the results obtained in [5, pp. 229–230]. The following statement which is an easy consequence of Theorem 4.1 will be used in proving the main result presented in Section 5.

Theorem 4.2. *Let p be a prime, $p > 3$ and let $g(x) = x^3 + rx + s \in \mathbb{F}_p[x]$ with $r \neq 0$. Assume that $g(x)$ is irreducible over $\mathbb{F}_p$ or $g(x)$ has three distinct roots in $\mathbb{F}_p$. Then the following statements are equivalent:*

(i) *$g(x)$ has three distinct roots in $\mathbb{F}_p$.*
(ii) *$g(x)$ has three distinct roots in $\mathbb{F}_{p^2}$.*
(iii) *$A = -s/2 - \lambda$ is a cubic residue of $\mathbb{F}_{p^2}$.*
(iv) *$B = -s/2 + \lambda$ is a cubic residue of $\mathbb{F}_{p^2}$.*

Remark 4.3. Theorems 4.1 and 4.2 also hold in the case of $r = 0$ if we let $A = B = s$.

Let $\mathbb{F}_{p^2}^\times$ denote the multiplicative group of the Galois field $\mathbb{F}_{p^2}$ where p is a prime, $p > 3$. Recall that the cubic character χ of $\mathbb{F}_{p^2}$ is a mapping $\chi : \mathbb{F}_{p^2}^\times \to \mathbb{F}_{p^2}^\times$ defined by $\chi(\xi) = \xi^{(p^2-1)/3}$ for any $\xi \in \mathbb{F}_{p^2}^\times$. Let $\varepsilon \in \mathbb{F}_{p^2}^\times$ be such that $\varepsilon^2 + \varepsilon + 1 = 0$. Then $\varepsilon^3 = 1$ and $\varepsilon \neq 1$. Clearly, if $\xi \in \mathbb{F}_{p^2}^\times$, then $\chi(\xi) = \varepsilon^i$ for some $i \in \{0, 1, 2\}$. Next, recall the following familiar properties of χ:

If $\xi_1, \xi_2 \in \mathbb{F}_{p^2}^{\times}$, *then* $\chi(\xi_1 \cdot \xi_2) = \chi(\xi_1) \cdot \chi(\xi_2)$.
If $\xi \in \mathbb{F}_{p^2}^{\times}$, *then* $\chi(\xi) = 1$ *if and only if* ξ *is a cube in the field* $\mathbb{F}_{p^2}$.
If $\xi \in \mathbb{F}_{p}^{\times}$ *and* $\chi(\xi) = 1$, *then* ξ *is a cube in the field* $\mathbb{F}_p$.

Let $\lambda \in \mathbb{F}_{p^2}$ be such that $\lambda^2 = d_t = 11/27 \in \mathbb{F}_p$ and $g_j(x) = x^3 + r_j x + s_j$, $j \in \{1, \cdots, 8\}$ be the cubic polynomials established in (3.3) considered as polynomials in $\mathbb{F}_p[x]$. For any $j \in \{1, \cdots, 8\}$, we define the elements $A(y_j), B(y_j) \in \mathbb{F}_{p^2}$ as follows:

$$A(y_j) = -\frac{y_j}{27} - \frac{1}{9}\varkappa,\ B(y_j) = -\frac{y_j}{27} + \frac{1}{9}\varkappa \text{ where } y_j = \frac{27}{2}s_j \text{ and } \varkappa = 9\lambda.$$

Let $\mathbb{Y} = \{y_j, j = 1, \cdots, 8\}$. Then $\mathbb{Y} = \{\pm 17, \pm 19, \pm 199, \pm 28748141\}$ and $A(y)$, $B(y)$ $\neq 0$ in $\mathbb{F}_{p^2}$ for any $y \in \mathbb{Y}$ and $p \neq 17, 29, 809$. Furthermore, it is easy to verify that

$$\chi(A(y)) = \chi(B(-y)) \text{ and } \chi(A(y)) \cdot \chi(A(-y)) = 1 \text{ for any } y \in \mathbb{Y}. \tag{4.1}$$

Let

$R = \{A(17), B(-17), A(-19), B(19), A(-199), B(199), A(28748141), B(-28748141)\}$,
$S = \{A(-17), B(17), A(19), B(-19), A(199), B(-199), A(-28748141), B(28748141)\}$.

The fundamental relations between the cubic characters of the elements of R and S will be stated in the following lemma.

Lemma 4.4. *Let* p *be an arbitrary prime,* $p \neq 2, 3, 17, 29, 809$. *Then*
(i) *All elements of* R *have the same cubic character in* $\mathbb{F}_{p^2}$.
(ii) *All elements of* S *have the same cubic character in* $\mathbb{F}_{p^2}$.
(iii) *If* $\rho \in R$ *and* $\sigma \in S$, *then* $\chi(\rho) \cdot \chi(\sigma) = 1$.

Proof. By direct calculation we can easily verify that

$$\begin{aligned} &(19 + 3\sqrt{33}) \cdot (17 + 3\sqrt{33}) = (5 + \sqrt{33})^3, \\ &(19 + 3\sqrt{33}) \cdot (199 - 3\sqrt{33}) = (13 + \sqrt{33})^3, \\ &(19 + 3\sqrt{33}) \cdot (28748141 + 3\sqrt{33}) = (692 + 56\sqrt{33})^3. \end{aligned} \tag{4.2}$$

Since the mapping $H : \mathbb{Z}[\sqrt{33}] \to \mathbb{F}_{p^2}$ defined by $H(\alpha + \beta\sqrt{33}) = \alpha + \beta\varkappa$ is a homomorphism of $\mathbb{Z}[\sqrt{33}]$ into $\mathbb{F}_{p^2}$, (4.2) yields that $\chi(19 + 3\varkappa) \cdot \chi(17 + 3\varkappa) = \chi(19 + 3\varkappa) \cdot \chi(199 - 3\varkappa) = \chi(19 + 3\varkappa) \cdot \chi(28748141 + 3\varkappa) = 1$. Multiplying by $\chi(19 - 3\varkappa)$ and using the second equality of (4.1) for $y = 19$ we get $\chi(B(-17)) = \chi(A(-199)) = \chi(B(-28748141)) = \chi(A(-19))$. This together with the first equality of (4.1) implies that all elements of R have the same cubic character. Since S can be written in the form $S = \{A(-y); A(y) \in R\} \cup \{B(-y); B(y) \in R\}$, the second equality of (4.1) implies that all elements of S have the same cubic character and that $\chi(\rho) \cdot \chi(\sigma) = 1$ for any $\rho \in R$ and $\sigma \in S$. ∎

5. The main theorem

There exist five types of factorization of the cubic polynomial $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ over the Galois field $\mathbb{F}_p$ with p a prime:

Type I: *$f(x)$ is irreducible over $\mathbb{F}_p$, i.e., $f(x)$ has no root in $\mathbb{F}_p$.*
Type II: *$f(x)$ splits over $\mathbb{F}_p$ into a linear factor and an irreducible quadratic factor.*
Type III: *$f(x)$ has three distinct roots in $\mathbb{F}_p$.*
Type IV: *$f(x)$ has a double root in $\mathbb{F}_p$.*
Type V: *$f(x)$ has a triple root in $\mathbb{F}_p$.*

Cases I–V can partially be distinguished using the quadratic character of D_f. Let (D_f/p) denote the Legendere–Jacobi symbol. By the Stickelberger Parity Theorem [8] for the case of a cubic polynomial [10, p. 189], we can distinguish case II from cases I and III as follows:

Let N be the number of distinct roots of $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ over the Galois field $\mathbb{F}_p$ with p a prime, $p > 3$ and $p \nmid D_f$. Then

$$\begin{gathered} N = 1 \text{ if and only if } (D_f/p) = -1, \\ N = 0 \text{ or } N = 3 \text{ if and only if } (D_f/p) = 1. \end{gathered} \tag{5.1}$$

For distinguishing the types I and III, we can use the cubic character and the field $\mathbb{F}_{p^2}$ by Theorem 4.2 as follows: Let $p > 3$ and $(D_f/p) = 1$. Set $r = b - a^2/3$, $s = 2a^3/27 - ab/3 + c$, $d = r^3/27 + s^2/4$ and let $\lambda \in \mathbb{F}_{p^2}$ with $\lambda^2 = d$. Further let $A = -s/2 - \lambda$, $B = -s/2 + \lambda$ if $a^2 \not\equiv 3b \pmod p$ and $A = B = s$ if $a^2 \equiv 3b \pmod p$. Then

$f(x)$ is of the type III *if and only if A and B are cubic residues of $\mathbb{F}_{p^2}$.*

Furthermore, for an arbitrary prime p, $f(x)$ has a multiple root in $\mathbb{F}_p$ if and only if $p|D_f$. Clearly, for $p > 2$, the condition $p|D_f$ is equivalent to $(D_f/p) = 0$. Moreover, if $p > 2$ and $p|D_f$, then using Viètes relations between the roots and coefficients of $f(x)$, it is easy to see that

$$f(x) \textit{ is of the type } \begin{cases} \text{IV } \textit{if and only if } p \nmid ab - 9c \textit{ or } p \nmid a, p|b, p|c, \\ \text{V } \textit{otherwise.} \end{cases}$$

Our next considerations will be restricted to polynomials $f(x)$ belonging to the Tribonacci family T. In this case, $D_f = -44$ and, for any prime $p \neq 2, 11$, we have $(D_f/p) = (-44/p) = (p/11)$. See also [4, p. 23]. To prove the main theorem, we will need the following proposition.

Proposition 5.1. *Let p be a prime, $p > 3$ and $(p/11) = 1$. Then all polynomials in T have the same type of factorization over $\mathbb{F}_p$.*

Proof. It is evident that, for any fixed $j \in \{1, \cdots, 8\}$, the polynomials $g_j(x)$ and $t_j(x, k)$, $k \in \mathbb{Z}$ defined by (3.3) and (3.4) have the same type of factorization over an arbitrary Galois field $\mathbb{F}_p$ with p a prime, $p > 3$. Hence, it follows that all polynomials in T have the same type of factorization over $\mathbb{F}_p$ if and only if the polynomials $g_j(x) = x^3 + r_j x + s_j \in \mathbb{F}_p[x]$, $j \in \{1, \cdots, 8\}$ have the same type of factorization over $\mathbb{F}_p$. Now we show that, if $p > 3$ and $(p/11) = 1$, then $r_j \neq 0$ in $\mathbb{F}_p$ for any $g_j(x)$. Suppose that $r_j = 0$ for some j. Then it follows from (3.4) that $p \in \{17, 29, 809\}$. Since $(p/11) = -1$ for any $p \in \{17, 29, 809\}$, a contradiction follows. Furthermore, if $p > 3$ and $(p/11) = 1$, then, by (5.1), any $g_j(x)$, $j \in \{1, \cdots, 8\}$ is of type I or type III. By Lemma 4.4, for any $\tau_1, \tau_2 \in R \cup S$, we have $\chi(\tau_1) = 1$ if and only if $\chi(\tau_2) = 1$. This together with Theorem 4.2 concludes the proof. □

Now we can to prove our main theorem.

Main Theorem 5.2. Let p be an arbitrary prime. Then all polynomials in T have the same type of factorization over the Galois field $\mathbb{F}_p$.

Proof. If $p > 3$ and $(p/11) = -1$, then the Stickelberger Parity Theorem says that each polynomial in T is of the type II over $\mathbb{F}_p$. If $p > 3$ and $(p/11) = 1$, then all polynomials in T have the same type of factorization over $\mathbb{F}_p$ by Proposition 5.1. Moreover, by the Stickelberger Parity Theorem, this type is either I or III.

Let $p = 2$. Substituting $k = 0, 1$ into (3.4), we obtain the following identities over $\mathbb{F}_2[x]$: $t_1(x,0) = t_2(x,1) = t_3(x,1) = t_4(x,0) = t_5(x,1) = t_6(x,0) = t_7(x,0) = t_8(x,1) = (x-1)^3$, and $t_1(x,1) = t_2(x,0) = t_3(x,0) = t_4(x,1) = t_5(x,0) = t_6(x,1) = t_7(x,1) = t_8(x,0) = x^3$. This proves that each polynomial in T if of type V over $\mathbb{F}_2$. Let $p=3$. Substituting $k=0,1,2$ into (3.4), we get the following identities over $\mathbb{F}_3[x]$:

$$\begin{aligned}
t_1(x,0) = t_4(x,1) = t_6(x,0) = t_7(x,2) &= x^3 + x^2 + x + 2, \\
t_1(x,1) = t_4(x,2) = t_6(x,1) = t_7(x,0) &= x^3 + x^2 + 2, \\
t_1(x,2) = t_4(x,0) = t_6(x,2) = t_7(x,1) &= x^3 + x^2 + 2x + 1, \\
t_2(x,0) = t_3(x,2) = t_5(x,0) = t_8(x,1) &= x^3 + 2x^2 + 2x + 2, \\
t_2(x,1) = t_3(x,0) = t_5(x,1) = t_8(x,2) &= x^3 + 2x^2 + 1, \\
t_2(x,2) = t_3(x,1) = t_5(x,2) = t_8(x,0) &= x^3 + 2x^2 + x + 1.
\end{aligned} \tag{5.2}$$

By direct calculation, it is easy to verify, that all polynomials in (5.2) are irreducible over $\mathbb{F}_3$. This means that each polynomial in T is of type I over $\mathbb{F}_3$.

Finally, let $p = 11$. Then the polynomials $g_j(x)$, $j \in \{1, \cdots, 8\}$ established in (3.3), have the following factorizations over $\mathbb{F}_{11}$:

$$\begin{aligned}
g_1(x) &= (x+10)^2(x+2), & g_2(x) &= (x+1)^2(x+9), \\
g_3(x) &= (x+8)^2(x+6), & g_4(x) &= (x+3)^2(x+5), \\
g_5(x) &= (x+4)^2(x+3), & g_6(x) &= (x+7)^2(x+8), \\
g_7(x) &= (x+9)^2(x+4), & g_8(x) &= (x+2)^2(x+7).
\end{aligned} \tag{5.3}$$

From (5.3) it follows that each polynomial in T is of type IV over $\mathbb{F}_{11}$. The proof is complete. □

6. Conclusion

The results presented in Theorem 2.3 and Corollary 2.4 make it possible to find the set of all cubic polynomials $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ with a given discriminant $0 \neq D \in \mathbb{Z}$ if all integral solutions of Mordell's equation $Y^2 = X^3 + k$, $k = 432D$ are known. Thanks to the computations made by Gebel, Pethö and Zimmer [3], all integral solutions of this equation are determined for any $0 \neq |k| \leq 10^5$ and thus, for any $0 \neq |D| \leq 231$. Consequently, the method used in proving the Main Theorem 5.2 can actually be applied to any particular $0 \neq |D| \leq 231$. These facts open a new and interesting question, namely, for which $D \in \mathbb{Z}$ can the Main Theorem 5.2 be generalized. However, to determine all such D's can be a difficult problem.

References

[1] L. E. Dickson, *History of the Theory of Numbers*, Vol. II, Chelsea, New York (1952).
[2] O. Hemer, *On the Diophantine Equation* $y^2 - k = x^3$, Doctoral Dissertation, Uppsala (1952).
[3] J. Gebel, A. Pethö, G. H. Zimmer, *On Mordell's equation*, Compositio Mathematica **110** (1998), 335–367.
[4] J. Klaška, L. Skula, *The cubic character of the Tribonacci roots*, The Fibonacci Quarterly **48.1** (2010), 21–28.
[5] J. Klaška, L. Skula, *Periods of the Tribonacci sequence modulo a prime* $p \equiv 1 \pmod 3$, The Fibonacci Quarterly **48.3** (2010), 228–235.
[6] J. London, M. Finkelstein, *On Mordell's Equation* $y^2 - k = x^3$, Bowling Green, Ohio Bowling Green State University (1973).
[7] L. J. Mordell, *The diophantine equation* $y^2 - k = x^3$, London Math. Soc. **13** (1913), 60–80.

[8] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress (1897), 182–193.

[9] A. Thue, *Über Annährungswerte algebraischer Zahlen*, Reine u. Angew. Math. **135** (1909), 284–305.

[10] G. Voronoï, *Sur une propriété du discriminant des fonctions entières*, Verhand. III. Internat. Math. Kongress (1905), 186–189.

MSC 2010: 11B39, 11D25

CHAPTER 14

LAW OF INERTIA FOR THE FACTORIZATION OF CUBIC POLYNOMIALS – THE REAL CASE ⋆

Abstract. Let $D \in \mathbb{Z}$ and $C_D := \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = D\}$ where D_f is the discriminant of $f(x)$. Assume that $D < 0$, D is square-free, $3 \nmid D$, and $3 \nmid h(-3D)$ where $h(-3D)$ is the class number of $\mathbb{Q}(\sqrt{-3D})$. We prove that all polynomials in C_D have the same type of factorization over any Galois field $\mathbb{F}_p$, p being a prime, $p > 3$.

1. Introduction

Let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ and let

$$D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc \tag{1.1}$$

be the discriminant of $f(x)$. Next, for any $D \in \mathbb{Z}$, put

$$C_D := \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = D\}. \tag{1.2}$$

In [8] we thoroughly examined the set C_{-44} containing the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$. As the main result we proved that all polynomials in C_{-44} have the same type of factorization and, consequently, the same number of roots over an arbitrary Galois field $\mathbb{F}_p$ with p a prime. This result suggested an interesting question, namely, for which $D \in \mathbb{Z}$ it can be generalized. Recall [8, p. 316] that there exist five distinct types of factorization of $f(x)$ over the Galois field $\mathbb{F}_p$ with p a prime. For these types, we shall use the standard notation found in M. Ward [17, p. 161]:

Case	Type of $f(x)$ over $\mathbb{F}_p$	Number of roots of $f(x)$ in $\mathbb{F}_p$
I	[3]	$f(x)$ has no root in $\mathbb{F}_p$
II	[2,1]	$f(x)$ has exactly one root in $\mathbb{F}_p$
III	[1,1,1]	$f(x)$ has three distinct roots in $\mathbb{F}_p$
IV	$[1^2, 1]$	$f(x)$ has a double root in $\mathbb{F}_p$
V	$[1^3]$	$f(x)$ has a triple root in $\mathbb{F}_p$

In case I, $f(x)$ is irreducible over $\mathbb{F}_p$, in case II, $f(x)$ splits over $\mathbb{F}_p$ into a linear factor and an irreducible quadratic factor and, in cases III, IV, and V, $f(x)$ completely splits over $\mathbb{F}_p$ into linear factors. Note that, in any case, the factorization is unique.

⋆ Published in J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the real case*, Utilitas Mathematica, **102** (2017), 39–50.

As the main result of this paper, we state a general theorem for a discriminant $D \in \mathbb{Z}$ satisfying the conditions

$$D < 0, \ D \text{ is square-free}, \ 3 \nmid D, \ 3 \nmid h(-3D) \tag{1.3}$$

where $h(-3D)$ is the class number of $\mathbb{Q}(\sqrt{-3D})$. Our main result is the following:

Main theorem 1.1. *Let $p > 3$ be a prime and let $f(x), g(x) \in \mathbb{Z}[x]$ be monic cubic polynomials with the same discriminant $D \in \mathbb{Z}$ satisfying* (1.3). *Then $f(x)$ and $g(x)$ have the same type of factorization over the field $\mathbb{F}_p$. Consequently, if $C_D \neq \emptyset$, then all polynomials in C_D have the same type of factorization over $\mathbb{F}_p$.*

Note that for an arbitrary $D \in \mathbb{Z}$, $D < 0$ the statement does not hold. Consider, for example, $D = -61 \cdot 191$, $f(x) = x^3 + 2x^2 - 14x - 41$, and $g(x) = x^3 - 9x^2 + 23x + 6$. Then $D_f = D_g = D$ and $h(-3D) = 6$. However, $f(x)$ is of type $[1, 1, 1]$ and $g(x)$ of type $[3]$ over $\mathbb{F}_{13}$. Next, consider $D = -2^2 \cdot 6011$, $f(x) = x^3 + x^2 - 11x - 37$, and $g(x) = x^3 - 3x^2 + 17x + 7$. Then $D_f = D_g = D$ and $h(-3D) = 1$. However, $f(x)$ is of type $[3]$ and $g(x)$ of type $[1, 1, 1]$ over $\mathbb{F}_7$.

If the factorization type of all polynomials in $C_D \neq \emptyset$ is the same, for any fixed prime p, we can call this property *the law of inertia for the factorization in C_D*. Of course, if $C_D = \emptyset$, the law of inertia in C_D holds trivially.

2. Preliminaries

Let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ and let $g_f(x) := f(x - a/3) = x^3 + rx + s \in \mathbb{Q}[x]$. First observe that $D_f = D_{g_f}$. Next, if $f(x) \in \mathbb{Z}[x]$, then, for any prime $p \neq 3$, $f(x)$ and $g_f(x)$ can be regarded as polynomials in $\mathbb{F}_p[x]$. In this case, $f(x)$ and $g_f(x)$ have the same type of factorization over $\mathbb{F}_p$.

For our next considerations, it will be important to give a condition for $C_D \neq \emptyset$. The following Theorem 2.1 follows from Theorem 2.3 in [8, p. 312].

Theorem 2.1. *Let $D \in \mathbb{Z}$. Then D is a discriminant of some monic cubic polynomial with integer coefficients if and only if there exist $u, v \in \mathbb{Z}$ satisfying*

$$4u^3 + 27v^2 = -D \tag{2.1}$$

or there exist $u, v \in \mathbb{Z}$ and a unique $e \in \{1, 2\}$ satisfying

$$4u^3 + v^2 = -27D, \ u \equiv 2 \pmod 3, \ e^3 + 3eu + v \equiv 0 \pmod{27}. \tag{2.2}$$

Moreover, if $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ and $D_f = D$, then we have:

(i) *If $a \equiv 0 \pmod 3$ then there exist $u, v \in \mathbb{Z}$ satisfying* (2.1) *and*

$$g_f(x) = x^3 + ux + v.$$

(ii) *If $a \equiv e \pmod 3$ where $e \in \{1, 2\}$, then there exist $u, v \in \mathbb{Z}$ satisfying* (2.2) *and*

$$g_f(x) = x^3 + \frac{u}{3}x + \frac{v}{27}.$$

For fixed $D \in \mathbb{Z}$, put $V_1 := \{[u, v] \in \mathbb{Z}^2 : \text{satisfying (2.1)}\}$ and $V_2 := \{[u, v] \in \mathbb{Z}^2 : \text{satisfying (2.2)}\}$. In the following Proposition 2.2 we show that condition (2.2) defining the set V_2 can be simplified significantly.

Proposition 2.2. *Let $D, u, v \in \mathbb{Z}$, $3 \nmid u$ and $4u^3 + v^2 = -27D$. Then, $u \equiv 2 \pmod 3$ and there exists a unique $e \in \{1, 2\}$ satisfying $e^3 + 3eu + v \equiv 0 \pmod{27}$. Consequently,*

$$V_2 = \{[u, v] \in \mathbb{Z}^2 : 4u^3 + v^2 = -27D \text{ and } 3 \nmid u\}.$$

Proof. Let $4u^3 + v^2 = -27D$ and $3 \nmid u$. Then $3 \nmid v$ and $u^3 + 1 \equiv 0 \pmod 3$. Hence, $u \equiv 2 \pmod 3$. Next, direct calculation yields that the congruence $4u^3 + v^2 \equiv 0 \pmod{27}$ has exactly eighteen solutions $[u, v]$ with $u \equiv 2 \pmod 3$:

$$[2, \pm 20], [5, \pm 11], [8, \pm 2], [11, \pm 20], [14, \pm 11],$$
$$[17, \pm 2], [20, \pm 20], [23, \pm 11], [26, \pm 2]. \tag{2.3}$$

Since any $[u, v]$ in (2.3) satisfies either $1+3u+v \equiv 0 \pmod{27}$ or $8+6u+v \equiv 0 \pmod{27}$, we are done. □

Now we can characterize the discriminants D for which $V_1 \cap V_2 \neq \emptyset$.

Proposition 2.3. *Let $0 \neq D \in \mathbb{Z}$. Then $V_1 \cap V_2 \neq \emptyset$ if and only if there exists $T \in \mathbb{Z}$ such that $3 \nmid T$ and $D = 7^2 T^6$. In this case,*

$$V_1 \cap V_2 = \{[-7T^2, 7T^3], [-7T^2, -7T^3]\}. \tag{2.4}$$

Proof. Let $[u, v] \in V_1 \cap V_2$. Then $4u^3 + 27v^2 = -D$, $4u^3 + v^2 = -27D$ and $3 \nmid u$. Hence, $4 \cdot 27u^3 + 27^2 v^2 = 4u^3 + v^2$, which yields $u^3 = -7v^2$, $7|u$, $7|v$. Since $D \neq 0$, there exist $U, V \in \mathbb{Z}$, $U < 0$, $V \neq 0$ such that $u = 7U$, $v = 7V$ and $U^3 = -V^2$ follows. If $U = -1$, then $V = \pm 1$ and $[u, v] = [-7, \pm 7]$. Hence, for $T = \pm 1$, we obtain (2.4). Let $U < -1$ and let p be a prime such that $p|U$. Then, $p|V$ and there exist $\alpha(p), \beta(p) \in \mathbb{N}$, $A, B \in \mathbb{Z}$, $A \leq -1$ such that $U = p^{\alpha(p)} A$, $V = p^{\beta(p)} B$, $p \nmid AB$. From $U^3 = -V^2$, it follows now that $3\alpha(p) = 2\beta(p)$. Hence, there exists $\gamma(p) \in \mathbb{N}$ such that $U = p^{2\gamma(p)} A$ and $V = p^{3\gamma(p)} B$. Putting $T = \prod_{p|U} p^{\gamma(p)}$, we obtain $U = -T^2$, $V = \pm T^3$ and $[u, v] = [-7T^2, \pm 7T^3]$. Since $3 \nmid u$, we have $3 \nmid T$ and $4u^3 + 27v^2 = -D$ yields $D = 7^2 T^6$.

Let $D = 7^2 T^6$ for some $T \in \mathbb{Z}$ satisfying $3 \nmid T$. Put $u = -7T^2$ and $v = 7T^3$. Then $4u^3 + 27v^2 = -D$ and $4u^3 + v^2 = -27D$. Since $3 \nmid T$, we have $3 \nmid u$ and Proposition 2.2 yields $[-7T^2, 7T^3], [-7T^2, -7T^3] \in V_1 \cap V_2 \neq \emptyset$. □

Remark 2.4. The finding of all integer solutions of $4u^3 + 27v^2 = -D$ and $4u^3 + v^2 = -27D$ can be reduced to the finding of all integer solutions of Mordell's equation $Y^2 = X^3 - 432D$. We can use a substitution $X = -12u$, $Y = 108v$ in the case of $4u^3 + 27v^2 = -D$ and a substitution $X = -4u$, $Y = 4v$ in the case of $4u^3 + v^2 = -D$. See [8, p. 313].

The following very old Theorem 2.5 is dating from 1894 and originating in the thesis of G. F. Voronoï [14]. Consult also [15, p. 329], [16, p. 189] and [4, p. 137]. On the other hand, Theorem 2.5 follows from a more general Stickelberger Parity Theorem [12] published in 1897.

Theorem 2.5. (G. F. Voronoï, 1894). *Let $f(x)$ be a monic cubic polynomial with integer coefficients having a discriminant D. Then, for any prime $p > 3$, $p \nmid D$, it holds:*

(i) *$f(x)$ is of type $[2, 1]$ over $\mathbb{F}_p$ if and only if $\left(\frac{D}{p}\right) = -1$.*

(ii) *$f(x)$ is either of type $[3]$ or type $[1, 1, 1]$ over $\mathbb{F}_p$ if and only if $\left(\frac{D}{p}\right) = 1$.*

To distinguish types [3] and [1, 1, 1], we can use the following theorem, which follows from Theorem 4.2 and Remark 4.3 in [8, p. 315]. Consult also Dickson [5, p. 2].

Theorem 2.6. *Let p be a prime, $p > 3$, and let $g(x) = x^3 + rx + s \in \mathbb{Z}[x]$. Assume that $g(x)$ is of type* [3] *or of type* [1, 1, 1] *over $\mathbb{F}_p$. Next, assume that $D = D_g$, $d = -3D$ and $\omega \in \mathbb{F}_{p^2}$ such that $\omega^2 = d$ in $\mathbb{F}_{p^2}$. Let*

$$A = \begin{cases} (\omega - 9s)/18 & \text{for } r \neq 0 \text{ in } \mathbb{F}_{p^2}, \\ s & \text{for } r = 0 \text{ in } \mathbb{F}_{p^2}. \end{cases} \tag{2.5}$$

Then, $g(x)$ is of type [1, 1, 1] *over $\mathbb{F}_p$ if and only if A is a cubic residue in $\mathbb{F}_{p^2}$.*

The next lemma is needed in the proof of Theorem 2.8, which yields a new possibility of distinguishing types $[1^2, 1]$ and $[1^3]$. Compare with [8, p. 317].

Lemma 2.7. *Let p be a prime, $X, Y \in \mathbb{Z}$ and $p \nmid XY$. If $X^3 \equiv Y^2 \pmod{p}$, there exists $Z \in \mathbb{Z}$ such that $p \nmid Z$, $X \equiv Z^2 \pmod{p}$ and $Y \equiv Z^3 \pmod{p}$.*

Proof. The lemma can be proved by the usual method using index modulo p. □

Theorem 2.8. *Let $D \in \mathbb{Z}$ be the discriminant of a monic cubic polynomial $f(x) \in \mathbb{Z}[x]$ and let*

$$g_f(x) = x^3 + ux + v \text{ where } u, v \in \mathbb{Z} \text{ and } 4u^3 + 27v^2 = -D \tag{2.6}$$

or

$$g_f(x) = x^3 + \frac{u}{3}x + \frac{v}{27} \text{ where } u, v \in \mathbb{Z}, 3 \nmid u \text{ and } 4u^3 + v^2 = -27D. \tag{2.7}$$

Let p be a prime, $p > 3$ and let $p|D$. Then we have:

(i) *$f(x)$ is of type $[1^2, 1]$ over $\mathbb{F}_p$ if and only if $p \nmid uv$.*
(ii) *$f(x)$ is of type $[1^3]$ over $\mathbb{F}_p$ if and only if $p|uv$.*

Consequently, if $p|D$ and $p^2 \nmid D$, the polynomial $f(x)$ is of type $[1^2, 1]$ over $\mathbb{F}_p$.

Proof. (i) Assume that $p \nmid uv$. Let $X, Y \in \mathbb{Z}$ such that $X = -u/3$, $Y = v/2$ in $\mathbb{F}_p$ in case (2.6), and $X = -u$, $Y = v/2$ in $\mathbb{F}_p$ in case (2.7). Then, in both cases, $X^3 \equiv Y^2 \pmod{p}$ and $p \nmid XY$. By Lemma 2.7, there exists $Z \in \mathbb{Z}$ satisfying $p \nmid Z$, $X \equiv Z^2 \pmod{p}$ and $Y \equiv Z^3 \pmod{p}$. Hence,

$$g_f(x) = \begin{cases} (x + 2Z)(x - Z)^2 & \text{in case (2.6)}, \\ (x + \frac{2}{3}Z)(x - \frac{1}{3}Z)^2 & \text{in case (2.7)}, \end{cases}$$

which means that $f(x)$ is of type $[1^2, 1]$ over $\mathbb{F}_p$.

(ii) Assume $p|uv$. Since $p|D$, we have $p|u$ and $p|v$ in both cases (2.6) and (2.7). Consequently, $g_f(x) = x^3$ in $\mathbb{F}_p[x]$ and $f(x)$ is of type $[1^3]$ over $\mathbb{F}_p$. □

3. The diophantine equations $4u^3 + 27v^2 = -D$ and $4u^3 + v^2 = -27D$

For convenience, let $D \in \mathbb{Z}$ be square-free and $3 \nmid D$ in the sequel. Next, we will assume $C_D \neq \emptyset$, that is, $V_1 \cup V_2 \neq \emptyset$. Put $d = -3D$ and $\theta = (1 + \sqrt{d})/2$. Since $C_D \neq \emptyset$, we have $D \equiv d \equiv 1 \pmod{4}$ and the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to the ring $R = \mathbb{Z}[\theta]$. Denote by $J(R)$ the multiplicative semigroup of nonzero ideals of R. For $\alpha \in R$ and $I \in J(R)$, denote by α' and I' the conjugates of α and I, respectively. Clearly, if $\alpha = a + b\theta \in R$, then $\alpha' = a + b - b\theta$. Finally, we will assume that the class number $h(d)$ of $\mathbb{Q}(\sqrt{d})$ satisfies $3 \nmid h(d)$.

For any $[u, v] \in V_1$, put $A_1(v) = 3(9v + 1)/2 - 3\theta$ and, for any $[u, v] \in V_2$, put $A_2(v) = (v + 3)/2 - 3\theta$. Observe that, if $[u, v] \in V_1 \cup V_2$, v is odd and $3 \nmid u$. Hence, $A_1(v), A_2(v) \in R$. Now we are ready for Theorem 3.1.

Theorem 3.1. *Let $i \in \{1, 2\}$. Then, for any $[u, v] \in V_i$, there exists a unit ε of the ring R and $\beta \in R$ such that $A_i(v) = \varepsilon\beta^3$.*

Proof. (i) Assume $[u, v] \in V_1$ and consider the identity $4u^3 + 27v^2 = -D$ in R. Then, $12u^3 + 81v^2 = d$ and $(9v - \sqrt{d})(9v + \sqrt{d}) = -12u^3$ follows. Hence,

$$\left(\frac{9v+1}{2} - \theta\right)\left(\frac{9v-1}{2} + \theta\right) = -3u^3. \tag{3.1}$$

Since $3|d$, there exists a prime ideal P of R such that $P = P'$ and $P^2 = (3)$. Next, the relations $3 \nmid u$ and $((9v + 1)/2 - \theta)' = (9v - 1)/2 + \theta$ together with (3.1) yield

$$P \underset{J(R)}{|} \left(\frac{9v+1}{2} - \theta\right), \quad P^2 \underset{J(R)}{\nmid} \left(\frac{9v+1}{2} - \theta\right),$$

$$P \underset{J(R)}{|} \left(\frac{9v-1}{2} + \theta\right), \quad P^2 \underset{J(R)}{\nmid} \left(\frac{9v-1}{2} + \theta\right).$$

Hence, there exists an ideal J of R such that

$$\left(\frac{9v+1}{2} - \theta\right) = PJ, \quad \left(\frac{9v-1}{2} + \theta\right) = PJ' \text{ and } P \underset{J(R)}{\nmid} J.$$

From (3.1), it now follows

$$JJ' = (u)^3. \tag{3.2}$$

We will prove that J and J' are relatively prime. Assume that Q is a prime ideal of R such that $Q|J$, $Q|J'$ and $Q \neq P$ in $J(R)$. Next, let q be a rational prime such that $Q|(q)$ in $J(R)$. Then, $q|u$ by (3.2). First, suppose that $q|d$. Then, $4u^3 + 27v^2 = -D$ yields $q|v$ and $q^2|D$, which is a contradiction. Next, suppose that $q \nmid d$. If $(q) = QQ'$ and $Q \neq Q'$, then $Q'|J$ and $(q)|J$ follows. If $(q) = Q$, then $(q)|J$. Hence, $(q)|((9v+1)/2-\theta)$ in $J(R)$ and, therefore, $q|(9v + 1)/2 - \theta$ in R, which is a contradiction.

Since J and J' are relatively prime, from (3.2) it follows that there exists an ideal I of R such that $J = I^3$. Hence, $((9v + 1)/2 - \theta) = PI^3$ and $(A_1(v)) = (PI)^3$ follow. Since $3 \nmid h(d)$, the ideal PI is principal. Consequently, there exist a unit $\varepsilon \in R$ and a $\beta \in R$ satisfying $A_1(v) = \varepsilon\beta^3$.

(ii) Assume $[u, v] \in V_2$ and consider the identity $4u^3 + v^2 = -27D$ with $3 \nmid u$ in R. Since $A_2(v)' = (v - 3)/2 + 3\theta$, from $4u^3 + v^2 = -27D$, we get

$$A_2(v)A_2(v)' = (-u)^3. \tag{3.3}$$

We will prove that the principal ideals $(A_2(v))$, $(A_2(v))'$ of R are relatively prime. Let P be a prime ideal of R such that $P|(A_2(v))$ and $P|(A_2(v))'$ in $J(R)$. Next, let p be a rational prime, satisfying $P|(p)$ in $J(R)$. Hence, we get $P|(v)$ and $P|(3\sqrt{d})$ in $J(R)$. Since $3 \nmid v$, we have $p|v$ and $p|d$. Hence, $p|u$ and thus $p^2|D$, which is a contradiction.

From (3.3) now, it follows that there exists an ideal I of R such that $(A_2(v)) = I^3$. Finally, from $3 \nmid h(d)$, we get that I is a principal ideal and, therefore, for $[u, v] \in V_2$, there exist a unit $\varepsilon \in R$ and a $\beta \in R$ such that $A_2(v) = \varepsilon\beta^3$. The theorem is proved. □

Now we focus on the case $D < 0$, that is, $d > 0$. Then, R is the ring of integers of the real quadratic field $\mathbb{Q}(\sqrt{d})$.

Theorem 3.2. *Let $d > 0$, $i \in \{1, 2\}$, $[u, v] \in V_i$ and let ε^* be the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Then, there exist $e(v) \in \{1, 2\}$ and $\alpha(v) \in R$ such that $A_i(v) = (\varepsilon^*)^{e(v)}\alpha(v)^3$. Moreover, $e(v)$ and $\alpha(v)$ are uniquely determined and $e(v) + e(-v) = 3$.*

Since the numbers $e(v)$ and $\alpha(v)$ also depend on u, they should actually be denoted, say, by $e(u, v)$ and $\alpha(u, v)$. However, for simplicity, we will keep the notation $e(v)$ and $\alpha(v)$.

Proof. (i) By Theorem 3.1, there exist a unit $\varepsilon \in R$ and $\beta \in R$ such that $A_i(v) = \varepsilon\beta^3$. Let n be a rational integer satisfying $\varepsilon = (\varepsilon^*)^n$ or $\varepsilon = -(\varepsilon^*)^n$. Let $n = 3m + e(v)$ where $m \in \mathbb{Z}$ and $e(v) \in \{0, 1, 2\}$. Put $\alpha(v) = \beta(\varepsilon^*)^m$ for $\varepsilon = (\varepsilon^*)^n$ and $\alpha(v) = -\beta(\varepsilon^*)^m$ for $\varepsilon = -(\varepsilon^*)^n$. Then, $(\varepsilon^*)^{e(v)}\alpha(v)^3 = \pm\varepsilon^{3m+e(v)}\beta^3 = \varepsilon\beta^3 = A_i(v)$.

(ii) We will prove that $e(v) \neq 0$. Suppose that $e(v) = 0$ and let $\alpha(v) = k + l\theta$, $k, l \in \mathbb{Z}$. Then, $A_i(v) = (k + l\theta)^3 = k^3 + 3kl^2(d-1)/4 + l^3(d-1)/4 + l(3k^2 + 3kl + l^2(d+3)/4)\theta$. Hence, $l(3k^2 + 3kl + 3l^2(-D+1)/4) = -3$ and $l = \pm 1$ follows. If $l = 1$, we get a quadratic equation $k^2 + k + (-D+5)/4 = 0$ with the discriminant $D - 4$. Since $D < 0$ and k is a root, we have a contradiction. Similarly, if $l = -1$, we get $k^2 - k - (D+3)/4 = 0$ with the discriminant $D + 4$ which is negative for $D \leq -5$. Since $D \equiv 1 \pmod 4$, we have $D = -3$, for $-4 \leq D \leq -1$, which is a contradiction with $3 \nmid D$. Hence, $e(v) \in \{1, 2\}$.

(iii) We will prove that $e(v)$ and $\alpha(v)$ are uniquely determined. Let $e, f \in \{1, 2\}$ and $\beta, \gamma \in R$ such that $A_i(v) = (\varepsilon^*)^e\beta^3 = (\varepsilon^*)^f\gamma^3$. Suppose $e \neq f$. Without loss of generality, we can assume, $e = 1$ and $f = 2$. Hence, $(\varepsilon^*\beta)^3 = \varepsilon^*(\varepsilon^*\gamma)^3$ and $(\beta/\gamma)^3 = \varepsilon^*$. Since R is integrally closed, we see that β/γ is a unit of R, and a contradiction follows. Hence, $e = f$ and $\beta^3 = \gamma^3$. Consequently, $(\beta/\gamma)^3 = 1$ and β/γ is a real unit of R, which yields $\beta/\gamma = 1$ and $\beta = \gamma$ follows.

(iv) From (3.1), we get $A_1(v)A_1(v)' = (-3u)^3$ and, by (3.3), $A_2(v)A_2(v)' = (-u)^3$. Since $A_i(v)' = -A_i(-v)$, there exists a $\beta \in R$ such that

$$\beta^3 = A_i(v)A_i(-v) = (\varepsilon^*)^{e(v)+e(-v)}(\alpha(v)\alpha(-v))^3$$

and $e(v) + e(-v) = 3$ follows. The proof is complete. □

4. The field F_{p^2}

Let $p > 3$ be a prime and let $\omega \in \mathbb{F}_{p^2}$ be such that $\omega^2 = d$ in $\mathbb{F}_{p^2}$. Recall that $d = -3D > 0$ and that ε^* denotes the fundamental unit of the ring $R = \mathbb{Z}[\theta]$. Let $\widetilde{\theta} = (1+\omega)/2$ and, for $\alpha = a + b\theta \in R$, put $H(\alpha) = a + b\widetilde{\theta} = a + b/2 + b\omega/2$. Then, H is a homomorphism of R into the field $\mathbb{F}_{p^2}$. Next, for $\alpha, \beta \in \mathbb{F}_{p^2}^\times$, put $\alpha \approx \beta$ if and only if there exists $\gamma \in \mathbb{F}_{p^2}^\times$ such that $\alpha = \beta\gamma^3$. Then, $\approx$ is a congruence relation on the group $\mathbb{F}_{p^2}^\times$ by its subgroup $(\mathbb{F}_{p^2}^\times)^3 = \{\xi^3 : \xi \in \mathbb{F}_{p^2}^\times\}$. As usual, $\mathbb{F}_{p^2}^\times$ denotes the multiplicative group of the field $\mathbb{F}_{p^2}$.

Proposition 4.1. *Let $i \in \{1,2\}$, $[u,v] \in V_i$ and let $p > 3$ be a prime such that $p \nmid u$. Then*

$$H(A_1(v)) = \frac{3}{2}(9v - \omega) \neq 0,\ H(A_2(v)) = \frac{1}{2}(v - 3\omega) \neq 0,\ H(\varepsilon^*) \neq 0 \ \ in\ \mathbb{F}_{p^2} \tag{4.1}$$

and,

$$H(A_i(v)) \approx H(\varepsilon^*)^{e(v)}. \tag{4.2}$$

Proof. The identities $H(A_1(v)) = 3(9v-\omega)/2$ and $H(A_2(v)) = (v-3\omega)/2$ immediately follow from the definitions of $A_1(v)$, $A_2(v)$, and H. Suppose $H(A_1(v)) = 0$. Then, $81v^2 \equiv d \pmod{p}$ and the identity $4u^3+27v^2 = -D$ yields $p|u$, which is a contradiction. Similarly, from $H(A_2(v)) = 0$, we obtain $v^2 \equiv 9d \pmod{p}$ and $4u^3 + v^2 = -27D$ yields $p|u$, which is a contradiction. Hence, $H(A_i(v)) \neq 0$ for $i \in \{1,2\}$. Finally, from $H(\varepsilon^*)H({\varepsilon^*}^{-1}) = 1$ we obtain $H(\varepsilon^*) \neq 0$, and from Theorem 3.2 we get $H(A_i(v)) \approx H(\varepsilon^*)^{e(v)}$. ☐

Proposition 4.2. *Let $i \in \{1,2\}$, $[u,v] \in V_i$ and let $p > 3$ be a prime such that $p|u$. Then $p \nmid Dv$ and $H(A_i(v))H(A_i(-v)) = 0$ where either $H(A_i(v)) \neq 0$ or $H(A_i(-v)) \neq 0$. Moreover, if $H(A_i(-v)) = 0$, then $H(A_i(v)) \neq 0$ and*

$$H(A_i(v)) = \begin{cases} 27v & \text{for } i = 1, \\ v & \text{for } i = 2. \end{cases}$$

Proof. Since $p|u$, the relation $p|Dv$ implies $p^2|D$, which is a contradiction. Let $i = 1$. Then, $H(A_1(v))H(A_1(-v)) = -9(9v-\omega)(9v+\omega)/4 = -9(81v^2-\omega^2)/4 = -9(81v^2 + 3D)/4 = -27(27v^2+D)/4 = 0$ in $\mathbb{F}_{p^2}$. If $H(A_1(-v)) = 0$, then $9v = -\omega$, which yields $H(A_1(v)) = 3(9v-\omega)/2 = 27v \neq 0$ in $\mathbb{F}_{p^2}$. The case $i = 2$ can be proved in a similar manner. ☐

Remark 4.3. In Proposition 4.2, it is not possible to determine when $H(A_i(v)) \neq 0$ and when $H(A_i(-v)) = 0$. This follows from the fact that the element $\omega \in \mathbb{F}_{p^2}$ is not uniquely determined. Therefore, if $p|u$, we put

$$\overline{v} = \begin{cases} v & \text{if } H(A_i(v)) \neq 0, \\ -v & \text{if } H(A_i(-v)) \neq 0. \end{cases} \tag{4.3}$$

Combining Theorem 3.2 with Proposition 4.2, we get the following proposition.

Proposition 4.4. *Let $i \in \{1,2\}$, $[u,v] \in V_i$ and let $p > 3$ be a prime such that $p|u$. Then $H(A_i(\overline{v})) \neq 0$, $H(\varepsilon^*) \neq 0$, $H(A_i(\overline{v})) \approx H(\varepsilon^*)^{e(\overline{v})}$ and $H(A_i(\overline{v})) \approx \overline{v}$.*

Extending the definition of $\overline{v}$ to the case of $p \nmid u$ by putting $\overline{v} = v$ or $\overline{v} = -v$, from Proposition 4.1 and Proposition 4.4, we get immediately:

Theorem 4.5. *Let $i \in \{1,2\}$, $[u,v] \in V_i$ and let $p > 3$ be a prime. Then $H(A_i(\overline{v}))$ is a cubic residue in $\mathbb{F}_{p^2}$ if and only if $H(\varepsilon^*)$ is a cubic residue in $\mathbb{F}_{p^2}$.*

Now we are ready to formulate the principal theorem of this section.

Theorem 4.6. *Let $f(x) \in \mathbb{Z}[x]$ be a monic cubic polynomial with a discriminant D satisfying* (1.3). *Let $p > 3$ be a prime such that $p \nmid D$ and let $(D/p) = 1$. Then $f(x)$ is of type* $[1,1,1]$ *over $\mathbb{F}_p$ if and only if $H(\varepsilon^*)$ is a cubic residue in $\mathbb{F}_{p^2}$.*

Proof. By Theorem 2.1, there exists $[u, v] \in V_1 \cup V_2$ such that

$$g_f(x) = \begin{cases} x^3 + ux + v, & \text{if } [u, v] \in V_1, \\ x^3 + \frac{u}{3}x + \frac{v}{27}, & \text{if } [u, v] \in V_2. \end{cases} \tag{4.4}$$

Denote $g_{u,v}(x) = g_f(x)$. Then we see that $g_{u,v}(x) = -g_{u,-v}(-x)$ and that $f(x)$, $g_{u,v}(x)$ and $g_{u,-v}(x)$ have the same type of factorization over $\mathbb{F}_p$. Consequently, we can set $v = \overline{v}$. Now, by Theorem 4.5, $H(A_i(v))$ is the cubic residue in $\mathbb{F}_{p^2}$ if and only if $H(\varepsilon^*)$ is the cubic residue in $\mathbb{F}_{p^2}$. Next, for any $[u, v] \in V_1 \cup V_2$, define $A \in \mathbb{F}_{p^2}$ as follows

$$A = \begin{cases} (\omega - 9v)/18, & \text{if } [u, v] \in V_1 \text{ and } p \nmid u, \\ v, & \text{if } [u, v] \in V_1 \text{ and } p | u, \\ (3\omega - v)/54, & \text{if } [u, v] \in V_2 \text{ and } p \nmid u, \\ v/27, & \text{if } [u, v] \in V_2 \text{ and } p | u. \end{cases} \tag{4.5}$$

By Proposition 4.1 and Proposition 4.2, for any $i \in \{1, 2\}$ and $[u, v] \in V_i$, we get

$$H(A_i(v)) = \begin{cases} -27A, & \text{for } p \nmid u, \\ 27A, & \text{for } p | u. \end{cases} \tag{4.6}$$

Hence, $A \approx H(A_i(v))$. From Theorem 4.5, it follows that A is the cubic residue in $\mathbb{F}_{p^2}$ if and only if $H(\varepsilon^*)$ is the cubic residue in $\mathbb{F}_{p^2}$. Finally, from Theorems 2.5 and 2.6, our claim follows. □

5. The main theorem

Main theorem 5.1. *Let $p > 3$ be a prime and let $f(x), g(x) \in \mathbb{Z}[x]$ be monic cubic polynomials with the same discriminant $D \in \mathbb{Z}$ satisfying*

$$D < 0, \ D \text{ is square-free}, \ 3 \nmid D, \ 3 \nmid h(-3D).$$

Then, $f(x)$ and $g(x)$ have the same type of factorization over the field $\mathbb{F}_p$. Consequently, if $C_D \neq \emptyset$, then all polynomials in C_D have the same type of factorization over $\mathbb{F}_p$.

Proof. Let p be a prime, $p > 3$. If $p|D$, then Theorem 2.8 states that $f(x)$ and $g(x)$ are of type $[1^2, 1]$ over $\mathbb{F}_p$ and that type $[1^3]$ will never occur. If $p \nmid D$ and $(D/p) = -1$, then, by part (i) of Theorem 2.5, $f(x)$ and $g(x)$ are of type $[2, 1]$ over $\mathbb{F}_p$. Finally, assume that $p \nmid D$ and $(D/p) = 1$. Then, by part (ii) of Theorem 2.5, $f(x)$, $g(x)$ are of type $[3]$ or type $[1, 1, 1]$ over $\mathbb{F}_p$ and Theorem 4.6 says that both polynomials $f(x)$ and $g(x)$ are of the same type. In particular, $f(x)$ and $g(x)$ are of type $[1, 1, 1]$ if and only if $H(\varepsilon^*)$ is a cubic residue in $\mathbb{F}_{p^2}$. The theorem is proved. □

As a direct consequence of Main theorem 5.1, the law of inertia for the factorization of cubic polynomials applies to the sets C_{-23} and C_{-31} for any prime $p > 3$. As a concrete example covering the possible factoring types in a C_D, any polynomial in C_{-23} (such as $p(x) = x^3 - x - 1$) has factoring type $[1^2, 1]$ over $\mathbb{F}_{23}$ ($p(x)$ factors as $(x + 20)(x + 13)^2$ over $\mathbb{F}_{23}$), factoring type $[1, 1, 1]$ over $\mathbb{F}_{59}$ ($p(x)$ factors as $(x + 17)(x + 46)(x + 55)$ over $\mathbb{F}_{59}$), factoring type $[2, 1]$ over $\mathbb{F}_5$ ($p(x)$ factors as $(x^2 + 2x + 3)(x + 3)$ over $\mathbb{F}_5$), and factoring type $[3]$ over $\mathbb{F}_{13}$ ($p(x)$ is irreducible over $\mathbb{F}_{13}$).

Moreover, it can be proved by analogy with [8, pp. 317–318] that, in C_{-23} and C_{-31}, the law of inertia holds for $p = 2$ and $p = 3$, too. Hence, Corollary 5.2 follows.

Corollary 5.2. *Let p be an arbitrary prime. Then*

(i) *All polynomials in C_{-23} have the same type of factorization over $\mathbb{F}_p$.*
(ii) *All polynomials in C_{-31} have the same type of factorization over $\mathbb{F}_p$.*

Recall that C_{-23} contains a well-known Perrin polynomial $p(x) = x^3 - x - 1$ and that C_{-31} contains another interesting polynomial $q(x) = x^3 - x^2 - 1$. These polynomials, together with the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$, are studied in the literature in various contexts. See, for example, [1], [6] and [11]. For recent papers, see [2], [7], [9] and [13]. Next, it is remarkable that the discriminants $D = -23, -31, -44$ play a significant role in the theory of binary cubic forms. See Delone [3] and Nagell [10].

6. Conclusion

To conclude, let us note that Main theorem 5.1 can be extended for any $D \in \mathbb{Z}$ satisfying

$$D > 0,\ D \text{ is square-free},\ 3 \nmid D,\ 3 \nmid h(-3D).$$

It is, however, clear that, to prove this, some results concerning the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ where $d = -3D < 0$ will be necessary. As the nature of imaginary quadratic fields differs considerably from that of the real ones, we will present a proof in a future paper.

References

[1] W. Adams, D. Shanks, *Strong primality tests that are not sufficient*, Math. of Computation **39**, no. 159, (1982), 255–300.
[2] G. Back, M. Caragiu, *The greatest prime factor and recurrent sequences*, The Fibonacci Quarterly **48.4** (2010), 358–362.
[3] B. N. Delone, *Über die Darstellung der Zahlen durch die binäre kubischen Formen von negativer Diskriminante*, Math. Zeitsch. **31** (1930), 1–26.
[4] B. N. Delone, *The St. Petersburg School of Number Theory*, History of mathematics, Vol. 26, AMS, 2005.
[5] L. E. Dickson, *Criteria for the irreducibility of functions in a finite field*, Bull. Amer. Math. Soc. **13** (1906), 1–8.
[6] J. Grantham, *There are infinitely many Perrin pseudoprimes*, J. Number Theory **130**, no. 5, (2010), 1117–1128.
[7] J. Klaška, *Tribonacci partition formulas modulo m*, Acta Math. Sin. **26.3** (2010), 465-476.
[8] J. Klaška, L. Skula, *Mordell's equation and the Tribonacci family*, The Fibonacci Quarterly **49.4** (2011), 310–319.
[9] D. Marques, *On the intersection of two distinct k-generalized Fibonacci sequences*, Mathematica Bohemica **137.4** (2012), 403–413.
[10] T. Nagell, *Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante*, Math. Zeitsch. **28** (1928), 10–29.
[11] J-P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (New Series), **40.4** (2003), 429–440.
[12] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress (1897), 182–193.
[13] J. Šiuris, *A Tribonacci-like sequence of composite numbers*, The Fibonacci Quarterly **49.4** (2011), 298–302.
[14] G. F. Voronoï, *On integral algebraic numbers depending on a root of an irreducible equation of the third degree*, Master's dissertation 1894, (Russian).
[15] G. F. Voronoï, *On the number of roots of a congruence of the third degree with respect to a prime modulus*, Notes of the Xth conference of scientific professions (1897), 329, (Russian).

[16] G. F. Voronoï, *Sur une propriété du discriminant des fonctions entières*, Verhand. III. Internat. Math. Kongress (1905), 186–189.

[17] M. Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. **33** (1931), 153–165.

MSC 2010: 11T06, 11D25, 12D05

CHAPTER 15

LAW OF INERTIA FOR THE FACTORIZATION OF CUBIC POLYNOMIALS – THE IMAGINARY CASE ★

Abstract. Let $D \in \mathbb{Z}$, $D > 0$ be square-free, $3 \nmid D$, and $3 \nmid h(-3D)$ where $h(-3D)$ is the class number of $\mathbb{Q}(\sqrt{-3D})$. We prove that all cubic polynomials $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ with a discriminant D have the same type of factorization over any Galois field $\mathbb{F}_p$ where p is a prime, $p > 3$. Moreover, we show that any polynomial $f(x)$ with such a discriminant D has a rational integer root. A complete discussion of the case $D = 0$ is also included.

1. Introduction

In our recent paper [4] we presented the following result: Let $D \in \mathbb{Z}$ be such that

$$D < 0, \ D \text{ is square-free}, \ 3 \nmid D, \ \text{and } 3 \nmid h(-3D) \tag{1.1}$$

where $h(-3D)$ is the class number of $\mathbb{Q}(\sqrt{-3D})$. Let

$$D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc \tag{1.2}$$

be the discriminant of $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$. Then all polynomials in

$$C_D = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = D\} \tag{1.3}$$

have the same type of factorization over any Galois field $\mathbb{F}_p$ where p is a prime, $p > 3$. In [4] we called this property *the law of inertia for factorization of cubic polynomials in* C_D.

In this paper we extend our previous research to show that the law of inertia for factorization of cubic polynomials also holds for any C_D with $D \in \mathbb{Z}$ satisfying the conditions

$$D > 0, \ D \text{ is square-free}, \ 3 \nmid D, \ \text{and } 3 \nmid h(-3D). \tag{1.4}$$

Moreover, we prove an interesting fact that any polynomial belonging to C_D, with D satisfying (1.4), has a rational integer root. Note that, for $D \in \mathbb{Z}$ satisfying (1.1), an analogous statement does not hold. Finally, combining our new result with [4], we obtain the following:

Main theorem 1.1. Let $0 \neq D \in \mathbb{Z}$ be square-free, $3 \nmid D$, and $3 \nmid h(-3D)$. Then all polynomials in C_D have the same type of factorization over any Galois field $\mathbb{F}_p$ where p is a prime, $p > 3$.

★ Published in J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the imaginary case*, Utilitas Mathematica, **103** (2017), 99–109.

This result can be considered as a partial answer to a question asked in [3, p. 310], namely, for which $D \in \mathbb{Z}$ the law of inertia for factorization of cubic polynomials holds.

2. Background results and notations

In this section we recall some facts presented in [3] and [4] important for our next considerations. First, for any $D \in \mathbb{Z}$, we define

$$V_1 := \{[u, v] \in \mathbb{Z}^2 : 4u^3 + 27v^2 = -D\} \tag{2.1}$$

and

$$V_2 := \{[u, v] \in \mathbb{Z}^2 : 4u^3 + v^2 = -27D \text{ and } 3 \nmid u\}. \tag{2.2}$$

Then V_1 and V_2 are finite sets for any $0 \neq D \in \mathbb{Z}$. Next, for any $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$, we put $g_f(x) = f(x - a/3)$. Then $D_{g_f} = D_f$ and, $g_f(x) = x^3 + rx + s \in \mathbb{Q}[x]$ where

$$r = b - \frac{a^2}{3} \quad \text{and} \quad s = \frac{2a^3}{27} - \frac{ab}{3} + c. \tag{2.3}$$

Using V_1 and V_2, we can establish all polynomials in C_D as follows:

Theorem 2.1. *Let $D \in \mathbb{Z}$ and let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.*
(i) *If $a \equiv 0 \pmod 3$, then $f(x) \in C_D$ if and only if there exist $[u, v] \in V_1$ and $w \in \mathbb{Z}$ such that*

$$a = 3w, \; b = 3w^2 + u, \; c = w^3 + uw + v. \tag{2.4}$$

(ii) *If $a \equiv e \pmod 3$ and $e \in \{1, 2\}$, then $f(x) \in C_D$ if and only if there exist $[u, v] \in V_2$, $w \in \mathbb{Z}$ such that $e^3 + 3eu + v \equiv 0 \pmod{27}$ and*

$$a = 3w + e, \qquad b = 3w^2 + 2ew + \frac{e^2 + u}{3},$$

$$c = w^3 + ew^2 + \frac{e^2 + u}{3}w + \frac{e^3 + 3eu + v}{27}. \tag{2.5}$$

Moreover, in (i) *we have $g_f(x) = x^3 + ux + v$ and, in* (ii)*, $g_f(x) = x^3 + (u/3)x + v/27$.*

For proof, see [3, Theorem 2.3] and [4, Proposition 2.2].

Let $D \in \mathbb{Z}$ be square-free, $3 \nmid D$ and $C_D \neq \emptyset$ in the sequel. Put $d = -3D$ and $\theta = (1 + \sqrt{d})/2$. Since $C_D \neq \emptyset$, it follows from (1.2) that $D \equiv d \equiv 1 \pmod 4$ and the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to the ring $\mathbb{Z}[\theta]$. Finally, we will assume that the class number $h(d)$ of the field $\mathbb{Q}(\sqrt{d})$ satisfies $3 \nmid h(d)$.

Now, for any $[u, v] \in V_1$, we put

$$A_1(v) := \frac{27v + 3}{2} - 3\theta \tag{2.6}$$

and, for any $[u, v] \in V_2$, we put

$$A_2(v) := \frac{v + 3}{2} - 3\theta. \tag{2.7}$$

Since $D \equiv 1 \pmod 4$, (2.1) and (2.2) implies that $2 \nmid v$ for any $[u, v] \in V_1 \cup V_2$, and thus, $A_1(v), A_2(v) \in \mathbb{Z}[\theta]$. In [4, Theorem 3.1] we established the following significant property of the numbers $A_1(v)$ and $A_2(v)$.

Theorem 2.2. *Let $i \in \{1,2\}$. Then, for any $[u,v] \in V_i$, there exists a unit ε of the ring $\mathbb{Z}[\theta]$ and $\beta \in \mathbb{Z}[\theta]$ such that $A_i(v) = \varepsilon\beta^3$.*

After this short recapitulation we are ready for new results.

3. Main results

We begin with two useful lemmas.

Lemma 3.1. *Let $D \in \mathbb{Z}$, $D > 1$ satisfy (1.4). If $i \in \{1,2\}$, $[u,v] \in V_i$, then there exist uniquely determined $k, l \in \mathbb{Z}$ such that $A_i(v) = (k + l\theta)^3$.*

Proof. Since $D > 0$, the quadratic field $\mathbb{Q}(\sqrt{d})$ is imaginary and the group of the units of the ring $\mathbb{Z}[\theta]$ has only two elements ± 1. Hence, by Theorem 2.2, there exist $k, l \in \mathbb{Z}$ such that $A_i(v) = (k + l\theta)^3$ for any $i \in \{1,2\}$. Since $\mathbb{Z}[\theta]$ is integrally closed, the numbers $k, l \in \mathbb{Z}$ are uniquely determined. □

Lemma 3.2. *Let $D \in \mathbb{Z}$ and $D > 5$. Then $D - 4$ and $D + 4$ cannot be both squares.*

Proof. Suppose that there exist positive integers r, s such that $D - 4 = r^2$ and $D + 4 = s^2$. Then $r < s$ and $s^2 - r^2 = 8$. Hence, $s - r = 1$, $s + r = 8$ or $s - r = 2$, $s + r = 4$. The first case is not possible for $r, s \in \mathbb{Z}$ and the second yields $[r, s] = [1, 3]$. Hence, $D = 5$ follows, which is a contradiction. □

The following Theorem 3.3 can be regarded as a key for proving of our main result.

Theorem 3.3. *Let $D \in \mathbb{Z}$ be such that $D > 5$, D is square-free, $3 \nmid D$, and $3 \nmid h(-3D)$. If $V_1 \cup V_2 \neq \emptyset$, then either $D - 4$ or $D + 4$ is a square and we have:*

(i) *If $V_1 \neq \emptyset$ and $D - 4$ is a square, then $D \equiv 1 \pmod 3$ and*

$$V_1 = \Big\{\Big[\frac{1-D}{3}, \pm\frac{\sqrt{D-4}\cdot(2D+1)}{27}\Big]\Big\}. \tag{3.1}$$

(ii) *If $V_1 \neq \emptyset$ and $D + 4$ is a square, then $D \equiv 2 \pmod 3$ and*

$$V_1 = \Big\{\Big[\frac{-1-D}{3}, \pm\frac{\sqrt{D+4}\cdot(2D-1)}{27}\Big]\Big\}. \tag{3.2}$$

(iii) *If $V_2 \neq \emptyset$ and $D - 4$ is a square, then $D \equiv 2 \pmod 3$ and*

$$V_2 = \{[1-D, \pm\sqrt{D-4}\cdot(2D+1)]\}. \tag{3.3}$$

(iv) *The case of $V_2 \neq \emptyset$ and $D + 4$ being a square never occurs.*

Consequently, if $V_1 \neq \emptyset$, then $V_2 = \emptyset$.

Proof. Since $\theta = (1 + \sqrt{d})/2$, we have $\theta^2 = (d-1)/4 + \theta$ and $\theta^3 = (d - 1 + (d+3)\theta)/4$. Hence, by Lemma 3.1, there exist uniquely determined $k, l \in \mathbb{Z}$ satisfying the equations

$$k^3 + 3kl^2\frac{d-1}{4} + l^3\frac{d-1}{4} = w_i(v) \tag{3.4}$$

and

$$l\left(3k^2 + 3kl + l^2\frac{d+3}{4}\right) = -3 \tag{3.5}$$

where $i \in \{1,2\}$ and

$$w_i(v) = \begin{cases} (27v+3)/2 & \text{for } i=1, \\ (v+3)/2 & \text{for } i=2. \end{cases}$$

Since $k, l \in \mathbb{Z}$, (3.5) yields $l \in \{\pm1, \pm3\}$. For $l = \pm3$, (3.5) then becomes $\pm(3k^2 \pm 9k + 9(d+3)/4) = -1$, which is a contradiction with $k \in \mathbb{Z}$. Therefore, $l = \pm1$. Using $d = -3D$, (3.5) results in

$$k^2 - k - \frac{D+3}{4} = 0 \quad \text{and} \quad k^2 + k + \frac{-D+5}{4} = 0 \tag{3.6}$$

with the roots

$$\varkappa_1 = \frac{1-\sqrt{D+4}}{2}, \quad \varkappa_2 = \frac{1+\sqrt{D+4}}{2}$$

and

$$\varkappa_3 = \frac{-1-\sqrt{D-4}}{2}, \ \varkappa_4 = \frac{-1+\sqrt{D-4}}{2} \tag{3.7}$$

for $l = -1$ and $l = 1$, respectively.

Since, by Lemma 3.2, only one of the numbers $D-4$ and $D+4$ can be a square, we can assume that either $D-4 = r^2$ or $D+4 = s^2$ for some positive integers r, s. Denote the left-hand side of (3.4) by $F(k,l)$. By direct calculation, we now obtain

$$2F(\varkappa_1, -1) = 2s^3 - 9s + 3 > 0, \ 2F(\varkappa_2, -1) = -(2s^3 - 9s - 3) < 0, \tag{3.8}$$

and

$$2F(\varkappa_3, 1) = 2r^3 + 9r + 3 > 0, \ 2F(\varkappa_4, 1) = -(2r^3 + 9r - 3) < 0. \tag{3.9}$$

We prove (3.1) and (3.2). Taking $i = 1$, we can write (3.4) as $2F(k,l) = 27v+3$. First assume that $D-4 = r^2$. Then $l = 1$ and, from (3.9), we get $3|r$ and $v = \pm r(2r^2+9)/27$ follows. Since $3|r$ and $r^2 = D-4$, we have $v = \pm\sqrt{D-4}(2D+1)/27 \in \mathbb{Z}$. Substituting v into $4u^3 + 27v^2 = -D$, we obtain $u = (1-D)/3$. Since $3|r$, we have $9|D-4$, which implies $D \equiv 1 \pmod 3$. Hence, $u \in \mathbb{Z}$. If $v = 0$, then $4u^3 + 27v^2 = -D$ implies $D \equiv 0 \pmod 4$, which is a contradiction. This proves (3.1).

Next assume that $D + 4 = s^2$. Then $l = -1$ and, from (3.8), we get $3|s$ and $v = \pm s(2s^2 - 9)/27$ follows. Since $3|s$ and $s^2 = D + 4$, we have $v = \pm\sqrt{D+4}(2D - 1)/27 \in \mathbb{Z}$. Substituting v into $4u^3 + 27v^2 = -D$, we obtain $u = (-1-D)/3$. Since $3|s$, we have $9|D+4$, which implies $D \equiv 2 \pmod 3$. Hence, $u \in \mathbb{Z}$. This proves (3.2).

Next, we prove (3.3). Taking $i = 2$, we can write (3.4) as $2F(k,l) = v + 3$ and, using (2.2), we obtain $3 \nmid v$. Assume $D - 4 = r^2$. Then $l = 1$ and, by (3.9), we get $3 \nmid 2F(\varkappa_3, 1)$ and $3 \nmid 2F(\varkappa_4, 1)$. Hence, $3 \nmid r$. Since $r^2 = D-4$, we have $D \not\equiv 1 \pmod 3$, which, together with $3 \nmid D$, yields $D \equiv 2 \pmod 3$. Let $v > -3$. Then, by (3.9), $2F(\varkappa_3, 1) = 2r^3 + 9r + 3 = v + 3 > 0$. Hence, $v = r(2r^2 + 9) = \sqrt{D-4}(2D+1)$ and, from $4u^3 + v^2 = -27D$, we obtain $u = 1 - D$. If $v < -3$, then (3.9) yields $2F(\varkappa_4, 1) = -(2r^3 + 9r - 3) = v + 3 < 0$ and $v = -r(2r^2 + 9) = -\sqrt{D-4}(2D+1)$ follows. Hence, using $4u^3 + v^2 = -27D$, we obtain $u = 1 - D$. To complete the proof of (3.3) note that for $v = -3$ we get a contradiction with $3 \nmid v$.

Finally, let $V_2 \neq \emptyset$ and $D + 4 = s^2$. Then $l = -1$ and, from (3.8), it follows that $3 \nmid 2F(\varkappa_1, -1)$ and $3 \nmid 2F(\varkappa_2, -1)$. Hence, we have $3 \nmid s$, which yields $s^2 \equiv 1 \pmod 3$. Since $s^2 = D + 4$, we get $3|D$, which is a contradiction. The proof is complete. □

Remark 3.4. We also established the least value of D for which any of the cases (3.1)–(3.3) in Theorem 3.3 occurs. We find $D = 13$ for (3.1), $D = 221$ for (3.2), and $D = 53$ for (3.3).

Let us now recall that there exist five distinct types of factorization of cubic polynomial $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ over a Galois field $\mathbb{F}_p$ with p a prime. For these types, we adopted in [4] the notation found in M. Ward [5, p. 161]. The polynomial $f(x)$ is of type [3] over $\mathbb{F}_p$ if $f(x)$ is irreducible over $\mathbb{F}_p$, $f(x)$ is of type $[2, 1]$ if $f(x)$ splits over $\mathbb{F}_p$ into a linear factor and an irreducible quadratic factor, and $f(x)$ is of type $[1, 1, 1]$ if $f(x)$ splits over $\mathbb{F}_p$ into three distinct linear factors. Furthermore, $f(x)$ is of type $[1^2, 1]$ if $f(x)$ has a double root in $\mathbb{F}_p$, and $f(x)$ is of type $[1^3]$ if $f(x)$ has a triple root in $\mathbb{F}_p$. For more details see [3, pp. 316–317] or consult [4].

Theorem 3.5. *Let $D \in \mathbb{Z}$, $D > 5$ be square-free, $3 \nmid D$, and $3 \nmid h(-3D)$. Then all polynomials in C_D have the same type of factorization over any Galois field $\mathbb{F}_p$, p being a prime, $p > 3$.*

Proof. Let $h(x), k(x) \in C_D$ and let $g_h(x) \neq g_k(x)$. Next assume that $i, j \in \{1, 2\}$, $i \neq j$ and $V_i \neq \emptyset$. Then, by Theorem 3.3, $V_i = \{[u, v], [u, -v]\}$ for some $u, v \in \mathbb{Z}$ and $V_j = \emptyset$. By Theorem 2.1, we can now assume that $g_h(x) = x^3 + rx + s$ and $g_k(x) = x^3 + rx - s$ where $[r, s] = [u, v]$ for $i = 1$ and $[r, s] = [u/3, v/27]$ for $i = 2$. Since $g_h(-x) = -g_k(x)$, we conclude that the polynomials $h(x)$ and $k(x)$ have the same type of factorization over $\mathbb{F}_p$ for any prime p, $p > 3$. □

Note that, for any $D \in \mathbb{Z}$, $D > 5$, the law of inertia for factorization in C_D does not hold. We have the following examples: If $f(x) = x^3 + 12x^2 - 28x + 15$, $g(x) = x^3 + 2x^2 - 4x - 7$, then $D_f = D_g = 229$ is a prime and $h(-3 \cdot 229) = 12$. A short calculation shows that $f(x)$ is of type $[1, 1, 1]$ and $g(x)$ is of type [3] over $\mathbb{F}_5$. As a further example, consider $f(x) = x^3 + 9x^2 - 22x + 12$ and $g(x) = x^3 + x^2 - 13x - 23$. Then $D_f = D_g = 2^2 \cdot 37$ and $h(-3 \cdot 2^2 \cdot 37) = 8$. Over $\mathbb{F}_7$, $f(x)$ is of type $[1, 1, 1]$ and $g(x)$ is of type [3].

Our next lemma will be needed to resolve the remaining cases $0 < D \leq 5$. In fact, by (1.4), it remains to examine only $D = 1$ and $D = 5$.

Lemma 3.6. (i) *Mordell's equation $Y^2 = X^3 - 432$ has exactly two integer solutions $[X, Y] = [12, \pm 36]$. Consequently, for $D = 1$, we have $V_1 \cup V_2 = \emptyset$ and there exists no cubic polynomial $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ with a discriminant $D_f = D = 1$.*

(ii) *Mordell's equation $Y^2 = X^3 - 2160$ has exactly six integer solutions $[X, Y] = [16, \pm 44], [24, \pm 108], [321, \pm 5751]$. Consequently, for $D = 5$, we have $V_1 = \{[-2, \pm 1]\}$ and $V_2 = \{[-4, \pm 11]\}$.*

Recall that, thanks to Gebel, Pethö and Zimmer [1], all integer solutions of Mordell's equation $Y^2 = X^3 + k$, $0 \neq k \in \mathbb{Z}$ are known for any $0 < |k| \leq 10^5$. For tables of solutions, see [2]. Hence, Lemma 3.6 follows. Further, note that, for $D = 5$, the sets V_1 and V_2 can also be obtained by (3.4) and (3.5). We leave the details of the computation to the reader.

For the next theorem, we adopt the following useful notation. For any $D \in \mathbb{Z}$, $D > 5$ satisfying (1.4) and $V_1 \cup V_2 \neq \emptyset$, we let C be a positive integer such that $D - 4 = C^2$ or $D + 4 = C^2$. Obviously, by Lemma 3.2 and Theorem 3.3, such C exists and is unique.

Theorem 3.7. *Let $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$, $g_f(x) = x^3+rx+s$ and let $D_f = D$ where D satisfies* (1.4)*. Then, $f(x)$ has a rational integer root ξ.*

In particular, if $D > 5$, then

$$\xi = \begin{cases} (C-a)/3 & \text{if } s > 0, \\ -(C+a)/3 & \text{if } s < 0 \end{cases} \tag{3.10}$$

and, if $D = 5$, then

$$\xi = \begin{cases} -(3+a)/3 & \text{if } a \equiv 0 \pmod 3 \text{ and } s = -1, \\ (3-a)/3 & \text{if } a \equiv 0 \pmod 3 \text{ and } s = 1, \\ (1-a)/3 & \text{if } a \equiv 1 \pmod 3, \\ -(1+a)/3 & \text{if } a \equiv 2 \pmod 3. \end{cases} \tag{3.11}$$

Proof. First assume $D > 5$. Put

$$\eta = \begin{cases} C/3 & \text{if } s > 0, \\ -C/3 & \text{if } s < 0. \end{cases} \tag{3.12}$$

Since $g_f(x) = f(x-a/3)$, we have $f(\xi) = 0$ if and only if $g_f(\eta) = 0$. This, together with Theorem 3.3, reduces the proof of (3.10) to six distinct cases corresponding to (3.1) – (3.3). In cases (3.1) and (3.2), we have $g_f(x) = x^3 + rx + s$ where $[r, s] = [u, v] \in V_1$ and, in case (3.3), we have $g_f(x) = x^3+rx+s$ where $[r, s] = [u/3, v/27]$ and $[u, v] \in V_2$. In all cases, the validity of $g_f(\eta) = 0$ can be verified readily by a direct calculation. The fact that $\xi \in \mathbb{Z}$ in the cases (3.1) and (3.2) is evident. In case (3.3), we have $s = (2a^3 - 9ab + 27)/27 = v/27$, which implies $v \equiv 2a^3 \pmod 3$. Assume $s > 0$. Then, by (3.3), $v = \sqrt{D-4}(2D + 1) = C(2C^2 + 9)$, which yields $v \equiv -C \pmod 3$. Combining the above, we get $2a^3 \equiv -C \pmod 3$ and $a \equiv C \pmod 3$ follows. Hence, $\xi = (C - a)/3 \in \mathbb{Z}$. The proof for $s < 0$ is similar.

If $D = 5$, then, by part (ii) of Lemma 3.6, we have $V_1 = \{[-2, \pm 1]\}$ and $V_2 = \{[-4, \pm 11]\}$. Hence, using Theorem 2.1, we find that $f(x) \in C_5$ if and only if $f(x) = f_j(x, w)$ for some $j \in \{1, 2, 3, 4\}$ and $w \in \mathbb{Z}$ where

$$\begin{aligned} f_1(x,w) &= x^3 + 3wx^2 + (3w^2-2)x + w^3 - 2w - 1, \\ f_2(x,w) &= x^3 + 3wx^2 + (3w^2-2)x + w^3 - 2w + 1, \\ f_3(x,w) &= x^3 + (3w+1)x^2 + (3w^2+2w-1)x + w^3 + w^2 - w, \\ f_4(x,w) &= x^3 + (3w+2)x^2 + (3w^2+4w)x + w^3 + 2w^2 - 1. \end{aligned} \tag{3.13}$$

A straightforward calculating argument yields that

$$f_1(-1-w, w) = 0, \ \ f_2(1-w, w) = 0,$$

$$f_3(-w, w) = 0, \quad f_4(-1-w, w) = 0 \tag{3.14}$$

for any $w \in \mathbb{Z}$. From (3.14), (3.11) follows immediately, as desired. □

We now proceed to prove the Main Theorem.

Main theorem 3.8. Let $D \in \mathbb{Z}$, $D \neq 0$ be square-free, $3 \nmid D$, and $3 \nmid h(-3D)$. Then all polynomials in C_D have the same type of factorization over any Galois field $\mathbb{F}_p$, p being a prime, $p > 3$.

Proof. Since, for $D < 0$, the claim is true by [4], we can assume that $D > 0$. For $D > 0$, the proof splits into three parts. First, it is evident that, for $D > 5$ and $p > 3$, the assertion holds by Theorem 3.5. Next, if $D = 5$ and $p > 5$, then Theorem 3.7 states that any polynomial $f(x) \in C_5$ has a rational integer root. This means that $f(x)$ is not of type [3] over $\mathbb{F}_p$. Since $p \nmid 5$, by Voronoï [4, Theorem 2.5], $f(x)$ is of type $[2, 1]$ if and only if $(5/p) = -1$ and $f(x)$ is of type $[1, 1, 1]$ if and only if $(5/p) = 1$. Finally, if $D = 5$ and $p = 5$, then from (3.13) it follows that $g_{f_1}(x) = (x+1)(x-3)^2$, $g_{f_2}(x) = (x-1)(x-2)^2$, $g_{f_3}(x) = (x-2)(x+1)^2$ and $g_{f_4}(x) = (x+2)(x-1)^2$ over $\mathbb{F}_5$. This implies that any polynomial $f(x) \in C_5$ is of type $[1^2, 1]$ over $\mathbb{F}_5$. The proof is complete. □

4. The case $D = 0$

In this section, we give a complete discussion of the case $D = 0$. Recall that the sets V_1 and V_2 defined by (2.1) and (2.2) are finite for any $0 \neq D \in \mathbb{Z}$. In the following lemma we show that, for $D = 0$, both sets

$$V_1 = \{[u, v] \in \mathbb{Z}^2 : 4u^3 + 27v^2 = 0\}$$

and

$$V_2 = \{[u, v] \in \mathbb{Z}^2 : 4u^3 + v^2 = 0 \text{ and } 3 \nmid u\}$$

are infinite. Above all, we find simple formulas determining all elements in V_1 and V_2.

Lemma 4.1. *We have:* (i) $V_1 = \{[-3\alpha^2, 2\alpha^3] : \alpha \in \mathbb{Z}\}$.
(ii) $V_2 = \{[-\alpha^2, 2\alpha^3] : \alpha \in \mathbb{Z} \text{ and } 3 \nmid \alpha\}$.

Proof. We prove (i). Let $[u, v] \in V_1$ and $uv \neq 0$. Then $3|u$, $2|v$ and, thus, there exist $U, V \in \mathbb{Z}$ satisfying $u = 3U$, $v = 2V$. Hence, $V^2 = -U^3$. Let p be any prime such that $p|U$ or, equivalently, $p|V$. Then, there exist $a, b \in \mathbb{N}$ satisfying $p^a|V$, $p^b|U$ and $p^{a+1} \nmid V$, $p^{b+1} \nmid U$. Therefore, $V = p^aV_1$, $U = p^bU_1$ for some $U_1, V_1 \in \mathbb{Z}$ where $p \nmid U_1$ and $p \nmid V_1$. From $V^2 = -U^3$, we now obtain $2a = 3b$, which means that there exist $a_1, b_1 \in \mathbb{N}$ such that $a = 3a_1$ and $b = 2b_1$. Since $2a = 3b$ implies $a_1 = b_1$, we can put $c(p) = a_1 = b_1$. Then, $V = p^{3c(p)}V_1$, $U = p^{2c(p)}U_1$ and $V_1^2 = -U_1^3$. Let A be the set of all primes p satisfying $p|U$. For $A \neq \emptyset$, put $\alpha = \Pi_{p\in A}p^{c(p)}$ in case $v < 0$ and $\alpha = -\Pi_{p\in A}p^{c(p)}$ in case $v > 0$. Next, for $A = \emptyset$, put $\alpha = 1$ for $v > 0$ and $\alpha = -1$ for $v < 0$. Then, $[U, V] = [-\alpha^2, \alpha^3]$, which yields $[u, v] = [-3\alpha^2, 2\alpha^3]$. On the other hand, it is evident that $\{[-3\alpha^2, 2\alpha^3] : \alpha \in \mathbb{Z}\} \subseteq V_1$.

In case $uv = 0$, we put $\alpha = 0$. This proves (i). The proof of (ii) can be done in a similar manner. □

Theorem 4.2. *Let p be a prime, $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ and let $D_f = 0$. Then we have:*

(i) *If $p \neq 3$, then $f(x)$ is of type $[1^2, 1]$ over $\mathbb{F}_p$ if and only if $p \nmid a^2 - 3b$.*
(ii) *If $p \neq 3$, then $f(x)$ is of type $[1^3]$ over $\mathbb{F}_p$ if and only if $p|a^2 - 3b$.*
(iii) *If $p = 3$ and $3|a$, then $f(x)$ is of type $[1^3]$ over $\mathbb{F}_3$.*
(iv) *If $p = 3$ and $3 \nmid a$, then $f(x)$ is of type $[1^2, 1]$ over $\mathbb{F}_3$.*

Proof. First assume $3|a$. Combining Theorem 2.1 with part (i) of Lemma 4.1, we get $g_f(x) = x^3 + ux + v$ where $[u, v] \in \{[-3\alpha^2, 2\alpha^3] : \alpha \in \mathbb{Z}\}$. Therefore, $g_f(x) = x^3 - 3\alpha^2x + 2\alpha^3 = (x-\alpha)^2(x+2\alpha)$ for some $\alpha \in \mathbb{Z}$. Hence, by (2.3), assertions (i), (ii), and (iii) follow.

Next, assume $3 \nmid a$. Then, Theorem 2.1 together with part (ii) of Lemma 4.1 yields that $g_f(x) = x^3 + (u/3)x + v/27$ where $[u, v] \in \{[-\alpha^2, 2\alpha^3] : \alpha \in \mathbb{Z}$ and $3 \nmid \alpha\}$. Therefore, $g_f(x) = x^3 - (\alpha^2/3)x + 2\alpha^3/27 = (x - \alpha/3)^2(x + 2\alpha/3)$ for some $\alpha \in \mathbb{Z}$. Hence, by (2.3), (i) and (ii) follow. Finally, (iv) can be verified by direct calculation using (2.5). □

As a direct consequence of Theorem 4.2, we get that, in C_0, the law of inertia for factorization of cubic polynomials does not hold. For illustration, we give an example. If $f(x) = x^3 + 3x^2 - 9x + 5$ and $g(x) = x^3 + x^2 - 16x + 20$, then $D_f = D_g = 0$. A simple calculation yields that, over $\mathbb{F}_7$, $f(x)$ is of type $[1^2, 1]$ and $g(x)$ is of type $[1^3]$.

5. Conclusion

The results presented in this paper and in [4] provide a partial answer to the question [3, p. 310], that is, for which sets C_D, $D \in \mathbb{Z}$, the law of inertia for factorization of cubic polynomials holds. Moreover, for $D < 0$, an interesting connection of the problem with the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{-3D})$ has been found. For $D > 0$, our investigation has brought a new result on the rational integer roots of monic cubic polynomials with integer coefficients. Finally, the relationship between the arithmetic property $3 \nmid h(-3D)$ and our guess is also remarkable.

It is evident that, in connection with the problems studied, further relevant questions can be stated. For example, we could ask under which conditions the law of inertia for factorization of cubic polynomials holds in a Galois field $\mathbb{F}_q$ where q is a power of a prime. Another possible generalization is finding out whether this law also holds for polynomials of an order greater than three.

References

[1] J. Gebel, A. Pethö, G. H. Zimmer, *On Mordell's equation*, Compositio Mathematica **110** (1998), 335–367.

[2] J. Gebel, *Integer points on Mordell curves*, The On-Line Encyclopedia of Integer Sequences, `http://oeis.org/`.

[3] J. Klaška, L. Skula, *Mordell's equation and the Tribonacci family*, The Fibonacci Quarterly **49.4** (2011), 310–319.

[4] J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the real case*, Utilitas Mathematica, **102** (2017), 39–50.

[5] M. Ward, *The characteristic number of a sequences of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. **33** (1931), 153–165.

MSC 2010: 11T06, 11D25, 12D05

CHAPTER 16

LAW OF INERTIA FOR THE FACTORIZATION OF CUBIC POLYNOMIALS – THE CASE OF DISCRIMINANTS DIVISIBLE BY THREE ★

Abstract. In this paper we extend our recent results concerning the validity of the law of inertia for the factorization of cubic polynomials over the Galois field $\mathbb{F}_p$, p being a prime. As the main result, the following theorem will be proved: Let $D \in \mathbb{Z}$ and let C_D be the set of all cubic polynomials $x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ with a discriminant equal to D. If D is square-free and $3 \nmid h(-3D)$ where $h(-3D)$ is the class number of $\mathbb{Q}(\sqrt{-3D})$, then all cubic polynomials in C_D have the same type of factorization over any Galois field $\mathbb{F}_p$ where p is a prime, $p > 3$.

1. Introduction

In [2] and [3], we proved the following theorem: Let $D \in \mathbb{Z}$ be such that

$$D \text{ is square-free, } 3 \nmid D \text{ and } 3 \nmid h(-3D) \tag{1.1}$$

where $h(-3D)$ is the class number of the quadratic field $\mathbb{Q}(\sqrt{-3D})$. Let

$$D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc \tag{1.2}$$

be the discriminant of $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ and let p be a prime, $p > 3$. Then, all polynomials in

$$C_D = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = D\} \tag{1.3}$$

have the same type of factorization over the Galois field $\mathbb{F}_p$.

Recall that there exist five distinct types of factorization of $f(x)$ over the field $\mathbb{F}_p$ where p is a prime. For these types, we adopted the notation found in M. Ward [7, p. 161]: A polynomial $f(x)$ is of type $[3]$ over $\mathbb{F}_p$ if $f(x)$ is irreducible over $\mathbb{F}_p$, $f(x)$ is of type $[2, 1]$ if $f(x)$ splits over $\mathbb{F}_p$ into a linear factor and an irreducible quadratic factor, and $f(x)$ is of type $[1, 1, 1]$ if $f(x)$ splits over $\mathbb{F}_p$ into three distinct linear factors. Furthermore, $f(x)$ is of type $[1^2, 1]$ if $f(x)$ has a double root in $\mathbb{F}_p$, and $f(x)$ is of type $[1^3]$ if $f(x)$ has a triple root in $\mathbb{F}_p$. If the factorization type of all polynomials in $C_D \neq \emptyset$ is the same, for any fixed prime p, we call this property *the law of inertia for the factorization in C_D*.

In [2] and [3], we also found examples of discriminants D proving that neither of the assumptions, D is square-free and $3 \nmid h(-3D)$, can be omitted. On the other

★ Published in J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the case of discriminants divisible by three*, Math. Slovaca **66.4** (2016), 1019–1027.

hand, extensive computer search found no example of a discriminant D satisfying the conditions

$$D \text{ is square-free, } 3|D \text{ and } 3 \nmid h(-3D) \tag{1.4}$$

such that the law of inertia for factorization in C_D does not hold.

The purpose of this paper is to extend our previous results presented in [2] and [3] and prove that all polynomials in C_D where D satisfies (1.4) have the same type of factorization over any Galois field $\mathbb{F}_p$ where p is a prime, $p > 3$. Consequently, this extension together with [2] and [3] yields the following Theorem 1.1.

Theorem 1.1. *Let $D \in \mathbb{Z}$ be square-free and $3 \nmid h(-3D)$. Then, all polynomials in C_D have the same type of factorization over any Galois field $\mathbb{F}_p$ where p is a prime, $p > 3$.*

2. Background results

In this section, we briefly recall some known facts which will be needed for our next considerations. First, in [2] we defined, for any $D \in \mathbb{Z}$, the sets

$$V_1 = \{[u, v] \in \mathbb{Z}^2 : 4u^3 + 27v^2 = -D\} \tag{2.1}$$

and

$$V_2 = \{[u, v] \in \mathbb{Z}^2 : 4u^3 + v^2 = -27D \text{ and } 3 \nmid u\}. \tag{2.2}$$

Next, for any $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$, we put $g_f(x) = f(x - a/3)$. Then, $D_{g_f} = D_f$ and $g_f(x) = x^3 + rx + s \in \mathbb{Q}[x]$ where

$$r = b - \frac{a^2}{3} \quad \text{and} \quad s = \frac{2a^3}{27} - \frac{ab}{3} + c. \tag{2.3}$$

Using V_1 and V_2, we can establish all polynomials in $C_D = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = D\}$ as follows:

Theorem 2.1. *Let $D \in \mathbb{Z}$ and let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.*
(i) *If $a \equiv 0 \pmod 3$, then $f(x) \in C_D$ if and only if there exists $[u, v] \in V_1$ and $w \in \mathbb{Z}$ such that*

$$a = 3w, \; b = 3w^2 + u, \; c = w^3 + uw + v. \tag{2.4}$$

(ii) *If $a \equiv e \pmod 3$ and $e \in \{1, 2\}$, then $f(x) \in C_D$ if and only if there exist $[u, v] \in V_2$, $w \in \mathbb{Z}$ such that $e^3 + 3eu + v \equiv 0 \pmod{27}$ and*

$$a = 3w + e, \; b = 3w^2 + 2ew + \frac{e^2 + u}{3},$$

$$c = w^3 + ew^2 + \frac{e^2 + u}{3} w + \frac{e^3 + 3eu + v}{27}. \tag{2.5}$$

Moreover, in (i) we have $g_f(x) = x^3 + ux + v$ and, in (ii), $g_f(x) = x^3 + (u/3)x + v/27$.

See [1, Theorem 2.3] and [2, Proposition 2.2].

Theorem 2.2. *Let $f(x)$ be a monic cubic polynomial with integer coefficients having a discriminant D. If $p > 3$ is a prime such that $p \nmid D$, then the statements* (i), (ii), *and* (iii) *hold:*

(i) *$f(x)$ is of type $[2,1]$ over $\mathbb{F}_p$ if and only if $(D/p) = -1$.*

(ii) *$f(x)$ is of type $[3]$ or type $[1,1,1]$ over $\mathbb{F}_p$ if and only if $(D/p) = 1$.*

(iii) *Let $g_f(x) = x^3 + rx + s$ and $g_f(x)$ be of type $[3]$ or type $[1,1,1]$ over $\mathbb{F}_p$. Next, assume that $d = -3D$ and $\Omega \in \mathbb{F}_{p^2}$ such that $\Omega^2 = d$ in $\mathbb{F}_{p^2}$. Let*

$$A = \begin{cases} (\Omega - 9s)/18 \text{ for } r \neq 0 \text{ in } \mathbb{F}_{p^2}, \\ s \text{ for } r = 0 \text{ in } \mathbb{F}_{p^2}. \end{cases}$$

Then, $g_f(x)$ is of type $[1,1,1]$ over $\mathbb{F}_p$ if and only if A is a cubic residue in $\mathbb{F}_{p^2}$.

Furthermore, for any prime $p > 3$, we have (iv)*:*

(iv) *If $p|D$ and $p^2 \nmid D$, then $f(x)$ is of type $[1^2,1]$ over $\mathbb{F}_p$.*

The statements (i) and (ii) are well-known and have their origin in the master's dissertation of G. F. Voronoï [6] from 1894. See also [7]. On the other hand, (i) and (ii) are also known as consequences of Stickelberger Parity Theorem [5] published in 1897. The statement (iii) is a simple modification of Theorem 2.6 presented in [2]. Finally, for (iv) see [2, Theorem 2.8].

3. Two lemmas

The considerations in this paper will be placed in the following framework: We assume that $D \in \mathbb{Z}$, D is square-free, and $3|D$. For $D \neq \pm 3$, we put $\delta = -D/3$ and $\theta = (1+\sqrt{\delta})/2$. If $C_D \neq \emptyset$, it follows from (1.2) that $D \equiv \delta \equiv 1 \pmod 4$ and the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{\delta})$ is equal to the ring $\mathbb{Z}[\theta]$. Next, we assume that the class number $h(\delta)$ of $\mathbb{Q}(\sqrt{\delta})$ satisfies $3 \nmid h(\delta)$. Finally, observe that $\mathbb{Q}(\sqrt{\delta}) = \mathbb{Q}(\sqrt{-3D})$ and, thus, $h(\delta) = h(-3D)$.

We begin with a simple lemma, which substantially simplifies the proof of Theorem 1.1 for the case of D satisfying (1.4).

Lemma 3.1. *Let $D \in \mathbb{Z}$ be square-free and $3|D$. Then, $V_1 = \emptyset$. Moreover, if $D = -3$, we have $V_2 = \{[2, \pm 7]\}$ and, if $D = 3$, we have $C_3 = \emptyset$.*

Proof. Since $3|D$, we have $D = 3d$ for some $d \in \mathbb{Z}$. Suppose that $[u, v] \in V_1$. Then, $4u^3 + 27v^2 = -3d$, which implies $3|u$. Hence, we have $27|D$, which is a contradiction.

Let $D = -3$. By London and Finkelstein [4, p. 128], the Mordell equation $Y^2 = X^3 + 1296$ has exactly eight integral solutions $[X, Y]$: $[-8, \pm 28]$, $[0, \pm 36]$, $[9, \pm 45]$ and $[72, \pm 612]$. Since the substitutions $X = -4u$ and $Y = 4v$ transform $Y^2 = X^3 + 1296$ to $4u^3 + v^2 = 81$, we find, after some calculation, $V_2 = \{[2, \pm 7]\}$.

Finally, if $D = 3$, then $D \not\equiv 1 \pmod 4$ and, $C_3 = \emptyset$ follows.

□

Combining Lemma 3.1 and part (i) of Theorem 2.1, we get Corollary 3.2.

Corollary 3.2. *Let $D \in \mathbb{Z}$ be square-free and $3|D$. Then, there is no cubic polynomial $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ such that $D_f = D$ and $3|a$.*

Now we focus on V_2. First, observe that, if $[u,v] \in V_2$, then v is odd and $3 \nmid v$. Next, for an arbitrary $[u,v] \in V_2$, we define $A(v)$ such that

$$A(v) = \frac{v+9}{2} - 9\theta. \tag{3.1}$$

Since v is odd, we have $A(v) \in \mathbb{Z}[\theta]$. Some basic properties of the numbers $A(v)$ will be given in the following Lemma 3.3.

Lemma 3.3. *Let $D \in \mathbb{Z}$ be square-free, $3|D$, $3 \nmid h(\delta)$ and $[u,v] \in V_2$. Then,* (i), (ii), *and* (iii) *hold:*
(i) *In the ring $\mathbb{Z}[\theta]$, we have $A(v)A(-v) = u^3$.*
(ii) *The principal ideals $(A(v))$ and $(A(-v))$ are coprime in the semigroup of the ideals of the ring $\mathbb{Z}[\theta]$.*
(iii) *There exist a unit ε of the ring $\mathbb{Z}[\theta]$ and $\beta \in \mathbb{Z}[\theta]$ such that $A(v) = \varepsilon\beta^3$.*

Proof. (i) Since $D = -3\delta$ and $\sqrt{\delta} = 2\theta - 1$, we can write $4u^3 + v^2 = -27D$ in the form $(v - 18\theta + 9)(v + 18\theta - 9) = -4u^3$. Hence, by (3.1), $A(v)A(-v) = u^3$ follows.

(ii) Suppose that P is a prime ideal of $Z[\theta]$ such that $P|(A(v))$, $P|(A(-v))$ and let p be a prime satisfying $P|(p)$. Then, $P|(A(v) - A(-v)) = (v)$, which implies $p|v$. Since v is odd and $3 \nmid v$, we have $p \neq 2, 3$. Next, $P|(A(v) + A(-v)) = (9(1 - 2\theta))$, which implies $P|(9)$ or $P|(1 - 2\theta)$. Since $p \neq 3$, we have $P|(1 - 2\theta)$. Hence, we obtain $p|\delta$, which means $p|D$. Since $p|v$, from $4u^3 + v^2 = -27D$, we obtain $p|u$, which yields $p^2|D$, a contradiction.

(iii) Consider the identity $4u^3 + v^2 = -27D$ with $3 \nmid u$ in $\mathbb{Z}[\theta]$. Then, it follows from (i) and (ii) that, in the semigroup of ideals of $\mathbb{Z}[\theta]$, there exists an ideal I of $\mathbb{Z}[\theta]$ such that $(A(v)) = I^3$. From $3 \nmid h(\delta)$, we obtain that I is a principal ideal and, therefore, for $[u,v] \in V_2$, there exist a unit $\varepsilon \in \mathbb{Z}[\theta]$ and $\beta \in \mathbb{Z}[\theta]$ such that $A(v) = \varepsilon\beta^3$. □

The numbers $A(v)$ have a key role in further proving. However, as we will see in the sequel, their specific properties highly depend on whether the field $\mathbb{Q}(\sqrt{\delta})$ is real or imaginary.

4. The case of real quadratic field

Throughout this section, we shall assume that $D \in \mathbb{Z}$ satisfies

$$D < -3,\ D \text{ is square-free},\ 3|D \text{ and } 3 \nmid h(\delta) \tag{4.1}$$

where $\delta = -D/3$ and $h(\delta)$ is the class number of the real quadratic field $\mathbb{Q}(\sqrt{\delta})$. Further, we shall assume that $V_2 \neq \emptyset$. Under these assumptions, we can say more about the numbers $A(v)$.

Theorem 4.1. *Let $D \in \mathbb{Z}$ satisfy* (4.1), *$[u,v] \in V_2$ and let ε^* be the fundamental unit of $\mathbb{Q}(\sqrt{\delta})$. Then, there exist $e(v) \in \{1, 2\}$ and $\alpha(v) \in \mathbb{Z}[\theta]$ such that*

$$A(v) = (\varepsilon^*)^{e(v)}\alpha(v)^3. \tag{4.2}$$

Moreover, $e(v)$ and $\alpha(v)$ are uniquely determined and $e(v) + e(-v) = 3$.

Note that $e(v)$ and $\alpha(v)$ in (4.2) also depend on u. However, for simplicity, we will keep the notation $e(v)$ and $\alpha(v)$.

Proof. By part (iii) of Lemma 3.3, there exist a unit $\varepsilon \in \mathbb{Z}[\theta]$ and $\beta \in \mathbb{Z}[\theta]$ such that $A(v) = \varepsilon\beta^3$. Since ε is a unit, we have $\varepsilon = (\varepsilon^*)^n$ or $\varepsilon = -(\varepsilon^*)^n$ for some $n \in \mathbb{Z}$. Let $n = 3m + e(v)$ where $m \in \mathbb{Z}$ and $e(v) \in \{0, 1, 2\}$. Put

$$\alpha(v) = \begin{cases} (\varepsilon^*)^m\beta & \text{for } \varepsilon = (\varepsilon^*)^n, \\ -(\varepsilon^*)^m\beta & \text{for } \varepsilon = -(\varepsilon^*)^n. \end{cases}$$

Then,

$$(\varepsilon^*)^{e(v)}\alpha(v)^3 = \pm\beta^3(\varepsilon^*)^{3m+e(v)} = \beta^3\varepsilon = A(v). \tag{4.3}$$

Suppose $e(v) = 0$. Then, by (4.3), $A(v) = \alpha(v)^3$ where $\alpha(v) = k + l\theta$ for some $k, l \in \mathbb{Z}$. Since $\theta^2 = (\delta - 1)/4 + \theta$ and $\theta^3 = (\delta - 1)/4 + (\delta + 3)\theta/4$, we have

$$A(v) = (k + l\theta)^3 = k^3 + 3kl^2\frac{\delta - 1}{4} + l^3\frac{\delta - 1}{4} + \left(3k^2l + 3kl^2 + l^3\frac{\delta + 3}{4}\right)\theta.$$

On the other hand, by definition (3.1), we have $A(v) = (v + 9)/2 - 9\theta$. Matching the coefficients, we now obtain

$$k^3 + 3kl^2\frac{\delta - 1}{4} + l^3\frac{\delta - 1}{4} = \frac{v + 9}{2} \tag{4.4}$$

and

$$l\left(3k^2 + 3kl + l^2\frac{\delta + 3}{4}\right) = -9. \tag{4.5}$$

Since $k, l \in \mathbb{Z}$, (4.5) yields $l \in \{\pm 1, \pm 3, \pm 9\}$. First assume $l = \pm 1$. Then, (4.5) leads to the relation $3|\delta$, which is a contradiction with D being square-free. Next, assume $l = \pm 9$. Then, reducing (4.5) modulo 27, we obtain $0 \equiv -9 \pmod{27}$. Hence, we see that there is no $k \in \mathbb{Z}$ satisfying (4.5). Finally, if $l = \pm 3$, then (4.5) leads to quadratic equation

$$k^2 \pm 3k + \frac{3\delta + 9 \pm 4}{4} = 0 \tag{4.6}$$

with the discriminant $\triangle_{\pm 3} = -3\delta \mp 4$. For $l = 3$, we have $\triangle_3 \equiv -1 \pmod 3$, which means that $\triangle_3$ is not a square and, therefore, $k^2 + 3k + (3\delta + 13)/4 = 0$ has no integer solution. If $l = -3$, then $\triangle_{-3} = -3\delta + 4$. Since $\delta > 0$, we get $\delta = 1$ and $D = -3$, which is a contradiction. Hence, $e(v) \in \{1, 2\}$.

Now we prove that $e(v)$ and $\alpha(v)$ are uniquely determined. Assume that $e_1, e_2 \in \{1, 2\}$ and $\beta_1, \beta_2 \in \mathbb{Z}[\theta]$ such that $A(v) = (\varepsilon^*)^{e_1}\beta_1^3 = (\varepsilon^*)^{e_2}\beta_2^3$. Suppose $e_1 \neq e_2$. Without loss of generality, we can assume $e_1 = 1$ and $e_2 = 2$. Hence, $(\varepsilon^*\beta_1)^3 = \varepsilon^*(\varepsilon^*\beta_2)^3$ and $(\beta_1/\beta_2)^3 = \varepsilon^*$. Since $\mathbb{Z}[\theta]$ is integrally closed, we see that β_1/β_2 is a unit of $\mathbb{Z}[\theta]$ and a contradiction follows. Hence, $e_1 = e_2$ and $\beta_1^3 = \beta_2^3$. Consequently, $(\beta_1/\beta_2)^3 = 1$ and β_1/β_2 is a real unit of $\mathbb{Z}[\theta]$, which yields $\beta_1/\beta_2 = 1$ and $\beta_1 = \beta_2$ follows.

Finally, combining part (i) of Lemma 3.3 with (4.2), we obtain $u^3 = A(v)A(-v) = (\varepsilon^*)^{e(v)+e(-v)}(\alpha(v)\alpha(-v))^3$. Hence, $e(v) + e(-v) \equiv 0 \pmod 3$, which yields $e(v) + e(-v) = 3$, as required. □

Let $p > 3$ be a prime and let $\omega \in \mathbb{F}_{p^2}$ be such that $\omega^2 = \delta$ in $\mathbb{F}_{p^2}$. Put $\widetilde{\theta} = (1+\omega)/2 \in \mathbb{F}_{p^2}$ and, for $\alpha = a + b\theta \in \mathbb{Z}[\theta]$, put $H(\alpha) = a + b\widetilde{\theta} = a + b/2 + b\omega/2$. Then, H is a homomorphism of $\mathbb{Z}[\theta]$ into the field $\mathbb{F}_{p^2}$. Next, for $\alpha, \beta \in \mathbb{F}_{p^2}^{\times}$, put $\alpha \approx \beta$ if and only if there exists $\gamma \in \mathbb{F}_{p^2}^{\times}$ such that $\alpha = \beta\gamma^3$. Then, $\approx$ is a congruence relation on the group $\mathbb{F}_{p^2}^{\times}$ by its subgroup $\{\xi^3 : \xi \in \mathbb{F}_{p^2}^{\times}\}$.

Lemma 4.2. *Let $D \in \mathbb{Z}$ satisfy* (4.1), $[u, v] \in V_2$ *and let $p > 3$ be a prime.*
(i) *If $p \nmid u$, then $H(A(v)) = (v - 9\omega)/2 \neq 0$, $H(\varepsilon^*) \neq 0$ in $\mathbb{F}_{p^2}$ and $H(A(v)) \approx H(\varepsilon^*)^{e(v)}$.*
(ii) *If $p|u$, then $p \nmid Dv$ and $H(A(v)) \cdot H(A(-v)) = 0$ where either $H(A(v)) \neq 0$ or $H(A(-v)) \neq 0$. Moreover, if $H(A(-v)) = 0$, then $H(A(v)) \neq 0$ and $H(A(v)) = v$.*

Proof. (i) The identity $H(A(v)) = (v - 9\omega)/2$ immediately follows from the definitions of $A(v)$ and H. Suppose $H(A(v)) = 0$. Then, $v = 9\omega$ in $\mathbb{F}_{p^2}$. Hence, $v^2 = 81\delta = -27D$, which is a contradiction with $p \nmid u$. Next, $H(\varepsilon^*) \cdot H(\varepsilon^{*^{-1}}) = 1$ implies $H(\varepsilon^*) \neq 0$. Finally, Theorem 4.1 yields $H(A(v)) = H(\varepsilon^*)^{e(v)} H(\alpha(v))^3 \approx H(\varepsilon^*)^{e(v)}$.

(ii) Suppose $p|Dv$. Since $p|u$, it follows from $4u^3 + v^2 = -27D$ that $p|v$. Hence, $p^2|D$, which is a contradiction. Next, we have $H(A(v)) \cdot H(A(-v)) = (v - 9\omega)(-v - 9\omega)/4 = -(v^2 + 27D)/4 = u^3 = 0$ in $\mathbb{F}_{p^2}$. If $H(A(-v)) = 0$, then $v = -9\omega$ and $H(A(v)) = (v - 9\omega)/2 = v$. Since $p \nmid v$, we have $H(A(v)) \neq 0$ in $\mathbb{F}_{p^2}$. □

Since the element $\omega \in \mathbb{F}_{p^2}$ is not uniquely determined, in part (ii) of Lemma 4.2, it is not possible to determine when $H(A(v)) \neq 0$ and when $H(A(-v)) = 0$. Therefore, if $p|u$, we put

$$\overline{v} = \begin{cases} v \text{ if } & H(A(v)) \neq 0, \\ -v \text{ if } & H(A(-v)) \neq 0. \end{cases}$$

Furthermore, if $p \nmid u$, we put $\overline{v} = v$ or $\overline{v} = -v$. Combining Theorem 4.1 with Lemma 4.2, we now get the following Corollary 4.3.

Corollary 4.3. *Let $D \in \mathbb{Z}$ satisfy* (4.1), $[u, v] \in V_2$ *and let $p > 3$ be a prime. Then $H(A(\overline{v}))$ is a cubic residue in $\mathbb{F}_{p^2}$ if and only if $H(\varepsilon^*)$ is a cubic residue in $\mathbb{F}_{p^2}$.*

Theorem 4.4. *Let $f(x) \in \mathbb{Z}[x]$ be a monic cubic polynomial with a discriminant D satisfying* (4.1). *Let $p > 3$ be a prime such that $p \nmid D$ and let $(D/p) = 1$. Then, $f(x)$ is of type $[1, 1, 1]$ over $\mathbb{F}_p$ if and only if $H(\varepsilon^*)$ is a cubic residue in $\mathbb{F}_{p^2}$. Consequently, the factorization type over $\mathbb{F}_p$ is the same for all polynomials in C_D.*

Proof. Combining Theorem 2.1 with Lemma 3.1, we obtain that there exists $[u, v] \in V_2$ such that $g_f(x) = x^3 + (u/3)x + v/27$. Observe that $f(x)$, $g_f(x)$, and $-g_f(-x) = x^3 + (u/3)x - v/27$ have the same type of factorization over $\mathbb{F}_p$. Therefore, we can set $v = \overline{v}$. Now, by Corollary 4.3, $H(A(v))$ is the cubic residue in $\mathbb{F}_{p^2}$ if and only if $H(\varepsilon^*)$ is the cubic residue in $\mathbb{F}_{p^2}$. Next, for any $[u, v] \in V_2$, define $A \in \mathbb{F}_{p^2}$ such that

$$A = \begin{cases} (9\omega - v)/54 & \text{if } \ p \nmid u, \\ v/27 & \text{if } \ p|u. \end{cases}$$

Applying Lemma 4.2, we now obtain

$$H(A(v)) = \begin{cases} -27A & \text{if } \ p \nmid u, \\ \ \ 27A & \text{if } \ p|u. \end{cases}$$

Hence, we have $A \approx H(A(v))$ and, thus, A is a cubic residue in $\mathbb{F}_{p^2}$ if and only if $H(\varepsilon^*)$ is a cubic residue in $\mathbb{F}_{p^2}$. Put $\Omega = 3\omega$. Then, $\Omega^2 = 9\delta = -3D$ and, from part (iii) of Theorem 2.2, our claim follows. □

Proposition 4.5. *Let $p > 3$ be a prime and let $f(x), g(x) \in C_{-3}$. Then, $f(x)$ and $g(x)$ have the same type of factorization over the field $\mathbb{F}_p$.*

Proof. By Lemma 3.1, we have $V_1 = \emptyset$ and $V_2 = \{[2, \pm 7]\}$. Therefore, without loss of generality, we can assume that

$$g_f(x) = x^3 + \frac{2}{3}x + \frac{7}{27} \quad \text{and} \quad g_g(x) = x^3 + \frac{2}{3}x - \frac{7}{27}.$$

Since, $g_f(x) = -g_g(-x)$, the polynomials $g_f(x)$ and $g_g(x)$ have the same type of factorization over $\mathbb{F}_p$. Hence, our claim follows. □

5. The case of imaginary quadratic field

In this section, we shall assume that $D \in \mathbb{Z}$ is such that

$$D > 3, \ D \text{ is square-free}, \ 3|D \text{ and } 3 \nmid h(\delta) \tag{5.1}$$

where $\delta = -D/3$ and $h(\delta)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{\delta})$.

Lemma 5.1. *Let $D \in \mathbb{Z}$ satisfy* (5.1) *and let $[u, v] \in V_2$. Then, there exist uniquely determined $k, l \in \mathbb{Z}$ such that $A(v) = (k + l\theta)^3$ in $\mathbb{Z}[\theta]$.*

Proof. First recall that $\delta \equiv 1 \pmod 4$ and $3 \nmid \delta$. Hence, $\delta \notin \{-1, -3\}$, which implies that the group of the units of $\mathbb{Z}[\theta]$ has only two elements ± 1. Using part (iii) of Lemma 3.3, we now obtain that there exist $k, l \in \mathbb{Z}$ such that $A(v) = (k + l\theta)^3$. Since $\delta \neq 3$, the elements $k, l \in \mathbb{Z}$ are uniquely determined. □

Theorem 5.2. *Let $D \in \mathbb{Z}$ satisfy* (5.1). Then, $V_2 \neq \emptyset$ if and only if there exists a positive integer $C \in \mathbb{Z}$ such that $D + 4 = C^2$. In this case,

$$V_2 = \{[-D - 1, \pm(2D - 1)\sqrt{D + 4}]\}. \tag{5.2}$$

Proof. If $[u, v] \in V_2$, then, by Lemma 5.1, there exist uniquely determined $k, l \in \mathbb{Z}$ such that $A(v) = (k + l\theta)^3$. In the same way as in the proof of Theorem 4.1, we find that k, l satisfy the equations (4.4) and (4.5):

$$k^3 + 3kl^2\frac{\delta - 1}{4} + l^3\frac{\delta - 1}{4} = \frac{v + 9}{2}$$

and

$$l\left(3k^2 + 3kl + l^2\frac{\delta + 3}{4}\right) = -9.$$

The last equation implies $l \in \{\pm 1, \pm 3, \pm 9\}$ and, by arguments similar to those in the proof of Theorem 4.1, we obtain that the cases $l \in \{\pm 1, 3, \pm 9\}$ lead to a contradiction. However, for $l = -3$, we get the quadratic equation

$$k^2 - 3k + \frac{3\delta + 5}{4} = 0 \tag{5.3}$$

with the discriminant $-3\delta + 4 = D + 4 > 0$. Since $k \in \mathbb{Z}$, we have $D + 4 = C^2$ for some positive integer C and the roots of (5.3) can be written in the form $k_1 = (3 + C)/2$ and $k_2 = (3 - C)/2$. Substituting $l = -3$, $k = k_1 = (3 + C)/2$, $\delta = -D/3$ and $C^2 = D + 4$ into (4.4), we find $v = \sqrt{D + 4}(1 - 2D)$. Similarly, for $l = -3$, $k = k_2 = (3 - C)/2$, $\delta = -D/3$ and $C^2 = D + 4$, we obtain $v = -\sqrt{D + 4}(1 - 2D)$. Finally, to determine u, we use the identity $4u^3 + v^2 = -27D$. Hence, $u = -D - 1$ follows.

Since the validity of the inverse implication can be verified easily by direct calculation, the proof is complete. □

Lemma 5.3. *Let* $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$, $g_f(x) = x^3 + rx + s$ *and let* $D_f = D$ *where* D *satisfies* (5.1). *Then,* $f(x)$ *has a rational integer root* ξ. *In particular,*

$$\xi = \begin{cases} (\sqrt{D+4} - a)/3 & \text{if } s > 0, \\ -(\sqrt{D+4} + a)/3 & \text{if } s < 0. \end{cases} \tag{5.4}$$

Proof. Put

$$\eta = \begin{cases} \sqrt{D+4}/3 & \text{if } s > 0, \\ -\sqrt{D+4}/3 & \text{if } s < 0. \end{cases}$$

Since $g_f(x) = f(x - a/3)$, we have $f(\xi) = 0$ if and only if $g_f(\eta) = 0$. The validity of $g_f(\eta) = 0$ can be verified readily by direct calculation. The fact $\xi \in \mathbb{Z}$ follows immediately from $\xi \in \mathbb{Q}$ and $f(x)$ being monic. □

Recall that, in [3, Theorem 3.7], we proved the same statement under the assumptions $D > 0$, D is square-free, $3 \nmid D$ and $3 \nmid h(-3D)$. Consequently, Lemma 5.3 together with [3] yields the following Theorem 5.4.

Theorem 5.4. *Let* $f(x) \in C_D$ *and let* D *satisfy* $D > 0$, D *be square-free, and* $3 \nmid h(-3D)$. *Then,* $f(x)$ *has a rational integer root.*

6. The main theorem

We proceed to prove our main theorem.

Theorem 6.1. *Let* $p > 3$ *be a prime and let* $f(x), g(x) \in \mathbb{Z}[x]$ *be monic cubic polynomials with the same discriminant* $D \in \mathbb{Z}$ *satisfying* (1.4): D *is square-free,* $3|D$ *and* $3 \nmid h(-3D)$. *Then,* $f(x)$ *and* $g(x)$ *have the same type of factorization over the field* $\mathbb{F}_p$.

Proof. First if $p|D$, then part (iv) of Theorem 2.2 states that $f(x)$ and $g(x)$ are of type $[1^2, 1]$ over $\mathbb{F}_p$ and that type $[1^3]$ will never occur. If $p \nmid D$ and $(D/p) = -1$, then, by part (i) of Theorem 2.2, $f(x)$ and $g(x)$ are of type $[2, 1]$ over $\mathbb{F}_p$. Next, if $p \nmid D$ and $(D/p) = 1$, then, by part (ii) of Theorem 2.2, $f(x)$ and $g(x)$ are of type $[3]$ or type $[1, 1, 1]$ over $\mathbb{F}_p$. If $D < 0$, then Theorem 4.4 and Proposition 4.5 says that both polynomials $f(x)$ and $g(x)$ are of the same type over $\mathbb{F}_p$. In particular, for $D \neq -3$, $f(x)$ and $g(x)$ are of type $[1, 1, 1]$ if and only if $H(\varepsilon^*)$ is a cubic residue in $\mathbb{F}_{p^2}$. If $D > 0$, then, by Lemma 3.1 and Theorem 5.2, $V_1 = \emptyset$ and $V_2 = \{[u, v], [u, -v]\}$ for some $u, v \in \mathbb{Z}$. Hence, $g_f(x) = \pm g_g(\pm x)$. Therefore, $f(x)$ and $g(x)$ have the same type of factorization over $\mathbb{F}_p$ for any prime $p > 3$. The proof is complete. □

Theorem 6.1 together with the results presented in [2] and [3] proves the validity of Theorem 1.1.

7. Conclusion

Theorem 1.1 constitutes a partial answer to a question raised in [1, p. 310], namely, for which $D \in \mathbb{Z}$, the law of inertia for the factorization of cubic polynomials holds. Moreover, as shown in [2] and [3], none of our assumptions, D is square-free and $3 \nmid h(-3D)$, can be omitted. Finally, note that each polynomial in C_D where $D > 0$ meets the above conditions has a rational integer root.

References

[1] J. Klaška, L. Skula, *Mordell's equation and the Tribonacci family*, The Fibonacci Quarterly **49.4** (2011), 310–319.

[2] J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the real case*, Utilitas Mathematica, **102** (2017), 39–50.

[3] J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the imaginary case*, Utilitas Mathematica, **103** (2017), 99–109.

[4] J. London, M. Finkelstein, *On Mordell's Equation* $y^2 - k = x^3$, Bowling Green, Ohio Bowling Green State University (1973).

[5] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress (1897), 182–193.

[6] G. Voronoï, *On integral algebraic numbers depending on a root of an irreducible equation of the third degree*, Master's dissertation, Russian (1894).

[7] G. Voronoï, *Sur une propriété du discriminant des fonctions entières*, Verhand. III. Internat. Math. Kongress (1905), 186–189.

[8] M. Ward, *The characteristic number of a sequences of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. **33** (1931), 153–165.

MSC 2010: 11T06, 11D25, 11D05

CHAPTER 17

LAW OF INERTIA FOR THE FACTORIZATION OF CUBIC POLYNOMIALS – THE CASE OF PRIMES 2 AND 3 ★

Abstract. Let $D \in \mathbb{Z}$ and let C_D be the set of all monic cubic polynomials $x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ with the discriminant equal to D. Along the line of our preceding papers, the following theorem has been proved: If D is square-free and $3 \nmid h(-3D)$ where $h(-3D)$ is the class number of $\mathbb{Q}(\sqrt{-3D})$, then all polynomials in C_D have the same type of factorization over the Galois field $\mathbb{F}_p$ where p is a prime, $p > 3$. In this paper, we prove the validity of the above implication also for primes 2 and 3.

1. Introduction

Let $D \in \mathbb{Z}$ and let $C_D = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = D\}$ where $D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$ is the discriminant of $f(x)$. In [1], we thoroughly examined the set C_{-44} and the following theorem was proved: *Let p be an arbitrary prime. Then, all polynomials in C_{-44} have the same type of factorization over the Galois field $\mathbb{F}_p$.* Furthermore, in [1, p. 318], we raised an interesting question for which $D \in \mathbb{Z}$ our result can be generalized. Recall that there exist five distinct types of factorization of $f(x)$ over $\mathbb{F}_p$:

(i) $f(x)$ is of type $[1^3]$ if $f(x) = (x - \alpha)^3$ in $\mathbb{F}_p$,
(ii) $f(x)$ is of type $[1^2, 1]$ if $f(x) = (x - \alpha)^2(x - \beta)$ where $\alpha, \beta \in \mathbb{F}_p$ and, $\alpha \neq \beta$,
(iii) $f(x)$ is of type $[1, 1, 1]$ if $f(x) = (x - \alpha)(x - \beta)(x - \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_p$ are distinct,
(iv) $f(x)$ is of type $[2, 1]$ if $f(x) = (x - \alpha)(x^2 + \beta x + \gamma)$ where $\alpha, \beta, \gamma \in \mathbb{F}_p$ and, $x^2 + \beta x + \gamma$ is irreducible over $\mathbb{F}_p$,
(v) $f(x)$ is of type $[3]$ if $f(x)$ is irreducible over $\mathbb{F}_p$, or equivalently, $f(x)$ has no root in $\mathbb{F}_p$.

For these types, we adopted the notation found in M. Ward [5, p. 161]. If the factorization type of all polynomials in C_D is the same, for any fixed prime p, we call this property *the law of inertia for the factorization of cubic polynomials in C_D*. See [2]. Along the line of papers [2,3,4], the following theorem has been proved:

Theorem 1.1. *Let $D \in \mathbb{Z}$ be square-free and let $3 \nmid h(-3D)$ where $h(-3D)$ is the class number of $\mathbb{Q}(\sqrt{-3D})$. Let p be an arbitrary prime greater than 3. Then, all polynomials in C_D have the same type of factorization over $\mathbb{F}_p$.*

★ Published in J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the case of primes 2 and 3*, Math. Slovaca **67.1** (2017), 71–82.

Clearly, for some $D \in \mathbb{Z}$, we have $C_D = \emptyset$. In this case, Theorem 1.1 holds trivially. On the other hand, Theorem 1.1 can be applied in many non-trivial cases. Consider, for example, C_{-31}, C_{-23} and, C_5. Finally, in [2] and [3], it was proved by counterexamples that none of our assumptions, D is square-free and $3 \nmid h(-3D)$, can be omitted.

The aim of this paper is to prove that Theorem 1.1 also holds for primes $p = 2$ and $p = 3$. Indeed, for $p = 2$ we show that the implication holds in a stronger form because the assumption $3 \nmid h(-3D)$ is not needed. Still, the proof of case $p = 2$ is not difficult. On the other hand, the proof for $p = 3$ requires more complex reasoning and much computation in the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{-3D})$. Some background results for the proof will also be needed.

2. The set C_D

In this section, we recall some known facts on the set C_D. For any $D \in \mathbb{Z}$, we define sets V_1 and V_2 such that

$$V_1 = \{[u, v] \in \mathbb{Z}^2 : 4u^3 + 27v^2 = -D\} \tag{2.1}$$

and

$$V_2 = \{[u, v] \in \mathbb{Z}^2 : 4u^3 + v^2 = -27D \text{ and } 3 \nmid u\}. \tag{2.2}$$

Next, for any $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$, we put $g_f(x) = f(x - a/3)$. Then, $D_{g_f} = D_f$ and $g_f(x) = x^3 + rx + s \in \mathbb{Q}[x]$ where

$$r = b - \frac{a^2}{3} \quad \text{and} \quad s = \frac{2a^3}{27} - \frac{ab}{3} + c. \tag{2.3}$$

Using V_1 and V_2, we can establish all polynomials in C_D as follows:

Theorem 2.1. *Let $D \in \mathbb{Z}$ and let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.*
(i) *If $a \equiv 0 \pmod 3$, then $f(x) \in C_D$ if and only if there exist $[u, v] \in V_1$ and $w \in \mathbb{Z}$ such that*

$$a = 3w, \; b = 3w^2 + u, \; c = w^3 + uw + v. \tag{2.4}$$

(ii) *If $a \equiv e \pmod 3$ and $e \in \{1, 2\}$, then $f(x) \in C_D$ if and only if there exist $[u, v] \in V_2$, $w \in \mathbb{Z}$ such that $e^3 + 3eu + v \equiv 0 \pmod{27}$, and*

$$a = 3w + e, \; b = 3w^2 + 2ew + \frac{e^2 + u}{3},$$

$$c = w^3 + ew^2 + \frac{e^2 + u}{3}w + \frac{e^3 + 3eu + v}{27}. \tag{2.5}$$

Moreover, in (i)*, we have $g_f(x) = x^3 + ux + v$ and, in* (ii)*, $g_f(x) = x^3 + (u/3)x + v/27$.*

For proof of Theorem 2.1, see [1, Theorem 2.3] and [2, Proposition 2.2].

Finally, recall that V_1 and V_2 can be obtained by using the set of all integral solutions to Mordell's equation $y^2 = x^3 + k$ with $k = -432D$. Consult [1, p. 313].

3. Basic statements

Now we give some statements concerning the factorization of monic cubic polynomials over the fields $\mathbb{F}_2$ and $\mathbb{F}_3$. First, it is evident that, over $\mathbb{F}_2$, there exist exactly eight monic cubic polynomials. Therefore, it is easy to get their list and, using it, establish the relationships between the factorization type of a polynomial over $\mathbb{F}_2$ and the parity of its discriminant as follows:

Lemma 3.1. *Let $D \in \mathbb{Z}$ be the discriminant of $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.*
(i) *$f(x)$ is of type $[1^3]$ or type $[1^2, 1]$ over $\mathbb{F}_2$ if and only if $D \equiv 0 \pmod 2$.*
(ii) *If $D \equiv 0 \pmod 2$, then $f(x)$ is of type $[1^3]$ if and only if $a \equiv b \equiv c \pmod 2$.*
(iii) *$f(x)$ is of type $[3]$ or type $[2, 1]$ over $\mathbb{F}_2$ if and only if $D \equiv 1 \pmod 2$.*
(iv) *If $D \equiv 1 \pmod 2$, then $f(x)$ is of type $[2, 1]$ if and only if $a \equiv b \not\equiv c \pmod 2$.*
(v) *If $D \equiv 0 \pmod 2$, then $D \equiv 0 \pmod 4$.*

Theorem 3.2. *Let $D \in \mathbb{Z}$ be square-free and let $f(x), g(x) \in C_D$. Then, D is odd and the polynomials $f(x)$ and $g(x)$ have the same type of factorization over $\mathbb{F}_2$.*

Proof. First, from part (v) of Lemma 3.1, it follows that D is odd and, by part (iii) of Lemma 3.1, any polynomial in $f(x) \in C_D$ is of type $[2, 1]$ or type $[3]$ over $\mathbb{F}_2$. Assume that $f(x)$ is of type $[2, 1]$ over $\mathbb{F}_2$. Then, by part (iv) of Lemma 3.1, there exist $r, s, t \in \mathbb{Z}$ such that $f(x) = f_1(x)$ or $f(x) = f_2(x)$ where

$$f_1(x) = x^3 + 2rx^2 + 2sx + 2t + 1, \;\; f_2(x) = x^3 + (2r + 1)x^2 + (2s + 1)x + 2t.$$

Reducing D_{f_1} and D_{f_2} by modulus 8, we get $D_{f_1} \equiv 5+4(r(r+1)+s(s+1)+t(t+1)) \equiv 5 \pmod 8$ and $D_{f_2} \equiv 5 + 4t(t + 1) \equiv 5 \pmod 8$. Hence, $D_f \equiv 5 \pmod 8$.

Suppose now that $g(x)$ is of type $[3]$ over $\mathbb{F}_2$. Then, there exist $u, v, w \in \mathbb{Z}$ such that $g(x) = g_1(x)$ or $g(x) = g_2(x)$ where

$$g_1(x) = x^3 + 2ux^2 + (2v + 1)x + 2w + 1, \;\; g_2(x) = x^3 + (2u + 1)x^2 + 2vx + 2w + 1.$$

Reducing D_{g_1} and D_{g_2} by modulus 8, we get $D_{g_1} \equiv 1+4(u(u+1)+w(w+1)) \equiv 1 \pmod 8$ and $D_{g_2} \equiv 1 + 4(v(v + 1) + w(w + 1)) \equiv 1 \pmod 8$. Hence, $D_g \equiv 1 \pmod 8$ and a contradiction follows. ∎

In the following Lemma 3.3, we establish the basic relationships between the factorization type of a cubic polynomial over $\mathbb{F}_3$ and the arithmetic properties of its discriminant. The proofs of all parts (i)-(viii) of Lemma 3.3 are easy and can be left to the reader.

Lemma 3.3. *Let $D \in \mathbb{Z}$ be the discriminant of $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.*
(i) *$f(x)$ is of type $[1^3]$ or type $[1^2, 1]$ over $\mathbb{F}_3$ if and only if $D \equiv 0 \pmod 3$.*
(ii) *If $D \equiv 0 \pmod 3$, then $f(x)$ is of type $[1^3]$ if and only if $a \equiv b \equiv 0 \pmod 3$.*
(iii) *If $f(x)$ is of type $[1^3]$ over $\mathbb{F}_3$, then $27|D$.*
(iv) *$f(x)$ is of type $[3]$ or type $[1, 1, 1]$ over $\mathbb{F}_3$ if and only if $D \equiv 1 \pmod 3$.*
(v) *If $D \equiv 1 \pmod 3$, then $f(x)$ is of type $[1, 1, 1]$ if and only if $c \equiv 0 \pmod 3$.*
(vi) *If $D \equiv 1 \pmod 3$ and $3 \nmid a$, then $f(x)$ is of type $[3]$ over $\mathbb{F}_3$.*
(vii) *$f(x)$ is of type $[2, 1]$ over $\mathbb{F}_3$ if and only if $D \equiv 2 \pmod 3$.*
(viii) *Let D be square-free, $D \not\equiv 1 \pmod 3$, and let $f(x), g(x) \in C_D$. Then, $f(x), g(x)$ have the same type of factorization over $\mathbb{F}_3$.*

We close this section with an example proving that, for $D \equiv 1 \pmod 3$, an analogy to part (viii) of Lemma 3.3 does not hold.

Example 3.4. (i) Let $f(x) = x^3 + 2x^2 - 14x + 13$ and $g(x) = x^3 - 18x^2 + 32x - 15$. Then, $D_f = D_g = 229 \equiv 1 \pmod 3$, $f(x)$ is of type [3], and $g(x)$ is of type [1, 1, 1] over $\mathbb{F}_3$. (ii) Let $f(x) = x^3 - 3x^2 + 17x - 10$ and $g(x) = x^3 - 9x^2 + 23x + 6$. Then, $D_f = D_g = -61 \cdot 191 \equiv 1 \pmod 3$, $f(x)$ is of type [3], and $g(x)$ is of type [1, 1, 1] over $\mathbb{F}_3$.

Now we will examine in detail the case of $D \equiv 1 \pmod 3$.

4. The ring $\mathbb{Z}[\theta]$

In this section, we prove some auxiliary results necessary to solve the case of $D \equiv 1 \pmod 3$ where $D < 0$. Let $D \in \mathbb{Z}$ such that

$$D < 0,\ D \equiv 1 \pmod 4 \text{ and } D \equiv \delta \pmod{27} \text{ where } \delta \in \{4, 13, 22\}. \tag{4.1}$$

Then, $D \equiv 1 \pmod 3$ and $D \equiv 4 \pmod 9$. Put $d = -3D$ and $\theta = (1 + \sqrt{d})/2$.

Consider now the ring of integers $Z[\theta] = \{x + y\theta : x, y \in \mathbb{Z}\}$ of the real quadratic field $\mathbb{Q}(\sqrt{d})$. First, observe that

$$\theta^2 = \frac{d-1}{4} + \theta \equiv 17 + \theta \pmod{27}. \tag{4.2}$$

Next, as usual, the norm of the element $\xi = x + y\theta \in \mathbb{Z}[\theta]$ is defined by

$$N(\xi) = \xi\xi' = x^2 + xy - \frac{d-1}{4}y^2.$$

Hence, $N(\xi) \equiv x^2 + xy + 10y^2 \pmod{27}$. Finally, for any $\alpha = a + b\theta$, $\beta = c + d\theta \in \mathbb{Z}[\theta]$ and $m \in \mathbb{Z}$, $m \geq 2$, put $\alpha \equiv \beta \pmod m$ if and only if $[a, b] \equiv [c, d] \pmod m$. In this case, we will say that α, β are congruent modulo m.

In the following Lemma 4.1, using the norm, we establish, the set of all units of $\mathbb{Z}[\theta]$ not-congruent modulo 27.

Lemma 4.1. *Let* $\varepsilon = a + b\theta \in \mathbb{Z}[\theta]$. *Then,* $N(\varepsilon) \equiv a^2 + ab + 10b^2 \equiv -1 \pmod{27}$ *has no solution and,* $N(\varepsilon) \equiv a^2 + ab + 10b^2 \equiv 1 \pmod{27}$ *has exactly* 54 *not-congruent solutions* $[a, b] \pmod{27}$*, shown by the below* Table 1*:*

a	1	2	3	4	5	6	7	8	9
b	0	21	2	11	15	7	14	1	19
b	8	22	22	21	25	14	15	9	26
a	10	11	12	13	14	15	16	17	18
b	9	3	4	3	7	16	23	10	1
b	17	4	11	20	24	23	24	18	8
a	19	20	21	22	23	24	25	26	0
b	18	12	13	2	6	5	5	0	10
b	26	13	20	12	16	25	6	19	17

Table 1

Proof. The solution of both congruences $N(\varepsilon) \equiv \pm 1 \pmod{27}$ can be obtained by direct calculation, possibly using a computer algebra system. ☐

Now, for any $K = x + y\theta \in \mathbb{Z}[\theta]$, let us define $\rho_D(x, y), \sigma_D(x, y) \in \mathbb{Z}$ such that

$$\rho_D(x,y) = x^3 - 3xy^2\frac{1+3D}{4} - y^3\frac{1+3D}{4} \tag{4.3}$$

and,

$$\sigma_D(x,y) = 3y\left(x^2 + xy + y^2\frac{1-D}{4}\right). \tag{4.4}$$

Then, $K^3 = \rho_D(x, y) + \sigma_D(x, y)\theta$ and the following relation holds:

Lemma 4.2. (i) $3|\rho_D(x, y)$ *if and only if* $x \equiv y \pmod 3$. (ii) *If* $3|\rho_D(x, y)$, *then*

$$\frac{\rho_D(x,y)}{3} \equiv \frac{x^3-y^3}{3} + y^3\frac{1-D}{4} + 17xy^2 \pmod{27}. \tag{4.5}$$

(iii) *If* $3 \nmid xy$, *then* $9|\sigma_D(x, y)$ *if and only if* $x \not\equiv y \pmod 3$.

Proof. From (4.3), $\rho_D(x, y) \equiv x - y \pmod 3$ follows immediately, which proves (i). Next, (4.3) can be written in the form

$$\rho_D(x,y) = x^3 - y^3 + 3y^3\frac{1-D}{4} - 3xy^2\frac{1+3D}{4}. \tag{4.6}$$

Hence, (4.5) follows. Finally, (4.4) together with $D \equiv 4 \pmod 9$ yields $\sigma_D(x, y) \equiv 3xy(x+y) \pmod 9$. Since $3 \nmid xy$, we have $x+y \equiv 0 \pmod 3$ if and only if $x \not\equiv y \pmod 3$. This proves (iii). □

Lemma 4.3. *Let* $K = x + y\theta \in \mathbb{Z}[\theta]$, $3 \nmid xy$ *and let* $K^3 = \rho_D(x, y) + \sigma_D(x, y)\theta$.
(i) *If* $x \equiv y \equiv 1 \pmod 3$, *then*

$$\left[\frac{\rho_D(x,y)}{3}, \frac{\sigma_D(x,y)}{3}\right] \pmod{27} \in \{[5, 17], [14, 26], [23, 8]\}. \tag{4.7}$$

(ii) *If* $x \equiv y \equiv 2 \pmod 3$, *then*

$$\left[\frac{\rho_D(x,y)}{3}, \frac{\sigma_D(x,y)}{3}\right] \pmod{27} \in \{[13, 1], [22, 10], [4, 19]\}. \tag{4.8}$$

Proof. The relationships between the numbers $\rho_D(x, y)/3 \pmod{27}$ and $\sigma_D(x, y)/3 (\mathrm{mod}\ 27)$ can be established by direct calculation. First observe that, for any $e \in \{1, 2\}$, $i, j \in \{1, 2, 3\}$ and $k, l \in \mathbb{Z}$, the following implication holds: If $[k, l] \equiv [i, j] \pmod 3$, then $\rho_D(e + 3k, e + 3l)/3 \equiv \rho_D(e + 3i, e + 3j)/3 \pmod{27}$ and $\sigma_D(e + 3k, e + 3l)/3 \equiv \sigma_D(e + 3i, e + 3j)/3] \pmod{27}$.

We prove (i). For $i, j \in \{1, 2, 3\}$, put $r_{ij} = \rho_D(1 + 3i, 1 + 3j)/3$ and $s_{ij} = \sigma_D(1 + 3i, 1 + 3j)/3$. Now, using (4.5) and (4.4), we obtain the congruences for $R = (r_{ij})$ and $S = (s_{ij})$ as follows:

If $D \equiv 4 \pmod{27}$, then

$$R \equiv \begin{bmatrix} 14 & 5 & 14 \\ 5 & 5 & 23 \\ 14 & 23 & 23 \end{bmatrix} \pmod{27} \quad \text{and} \quad S \equiv \begin{bmatrix} 26 & 17 & 26 \\ 17 & 17 & 8 \\ 26 & 8 & 8 \end{bmatrix} \pmod{27}. \tag{4.9}$$

If $D \equiv 13 \pmod{27}$, then

$$R \equiv \begin{bmatrix} 5 & 23 & 5 \\ 23 & 23 & 14 \\ 5 & 14 & 14 \end{bmatrix} \pmod{27} \quad \text{and} \quad S \equiv \begin{bmatrix} 17 & 8 & 17 \\ 8 & 8 & 26 \\ 17 & 26 & 26 \end{bmatrix} \pmod{27}. \tag{4.10}$$

If $D \equiv 22 \pmod{27}$, then

$$R \equiv \begin{bmatrix} 23 & 14 & 23 \\ 14 & 14 & 5 \\ 23 & 5 & 5 \end{bmatrix} \pmod{27} \quad \text{and} \quad S \equiv \begin{bmatrix} 8 & 26 & 8 \\ 26 & 26 & 17 \\ 8 & 17 & 17 \end{bmatrix} \pmod{27}. \tag{4.11}$$

Statement (i) now immediately follows from (4.9) – (4.11). The proof of part (ii) of Lemma 3.3 is much the same. □

For any odd $v \in \mathbb{Z}$, let us now define $A_1(v) \in \mathbb{Z}[\theta]$ such that

$$A_1(v) = 3\left(\frac{9v+1}{2} - \theta\right). \tag{4.12}$$

Lemma 4.4. *Let $v \in \mathbb{Z}$, $v \equiv 3 \pmod 6$, $K \in \mathbb{Z}[\theta]$ and let $\varepsilon = a + b\theta$ be a unit of the ring $\mathbb{Z}[\theta]$. If $\varepsilon A_1(v) = K^3$, then*

$$[a, b] \pmod{27} \in \{[1,0], [8,9], [10,9], [17,18], [19,18], [26,0]\}. \tag{4.13}$$

Proof. Since $v \equiv 3 \pmod 6$, there exists a $w \in \mathbb{Z}$ such that $v = 6w + 3$ and, by (4.12), $A_1(v) = 3(27w + 14 - \theta)$. Put $A(a,b) = 14a - 17b$ and $B(a,b) = 13b - a$. Then,

$$\frac{\varepsilon A_1(v)}{3} = (a + b\theta)(27w + 14 - \theta) \equiv A(a,b) + B(a,b)\theta \pmod{27}. \tag{4.14}$$

To establish $A(a,b) \pmod{27}$ and, $B(a,b) \pmod{27}$, we use Table 1. Hence, Table 2 follows:

a	b	A(a,b)	B(a,b)	a	b	A(a,b)	B(a,b)	a	b	A(a,b)	B(a,b)
1	0	14	26	10	9	14	26	19	18	14	26
1	8	13	22	10	17	13	22	19	26	13	22
2	21	22	1	11	3	22	1	20	12	22	1
2	22	5	14	11	4	5	14	20	13	5	14
3	2	8	23	12	4	19	13	21	13	19	13
3	22	19	13	12	11	8	23	21	20	8	23
4	11	4	4	13	3	23	26	22	2	4	4
4	21	23	26	13	20	4	4	22	12	23	26
5	15	4	1	14	7	23	23	23	6	4	1
5	25	23	23	14	24	4	1	23	16	23	23
6	7	19	4	15	16	19	4	24	5	8	14
6	14	8	14	15	23	8	14	24	25	19	4
7	14	22	13	16	23	22	13	25	5	22	13
7	15	5	26	16	24	5	26	25	6	5	26
8	1	14	5	17	10	14	5	26	0	13	1
8	9	13	1	17	18	13	1	26	19	14	5
9	19	19	22	18	1	19	22	0	10	19	22
9	26	8	5	18	8	8	5	0	17	8	5

Table 2

Let $K = x + y\theta \in \mathbb{Z}[\theta]$ be such that $\varepsilon A_1(v) = K^3$. Then, $K^3 = \rho_D(x,y) + \sigma_D(x,y)\theta$ where $\rho_D(x,y)$ and $\sigma_D(x,y)$ satisfy (4.3) and (4.4). Since $3 | A_1(v)$, we have $3 | \rho_D(x,y)$,

$3|\sigma_D(x,y)$ and (4.14) yields

$$\left[\frac{\rho_D(x,y)}{3}, \frac{\sigma_D(x,y)}{3}\right] \equiv [A(a,b), B(a,b)] \pmod{27}. \tag{4.15}$$

From Table 2, we see that $3 \nmid A(a,b)$ and $3 \nmid B(a,b)$, which, together with (4.15), yields $9 \nmid \rho_D(x,y)$ and $9 \nmid \sigma_D(x,y)$. Next, reducing (4.4) by modulus 27, we obtain

$$\sigma_D(x,y) \equiv 3y(x^2 + xy + 6y^2) \pmod{27}. \tag{4.16}$$

Since $9 \nmid \sigma_D(x,y)$, $3 \nmid xy$ follows from (4.16) and, by part (iii) of Lemma 4.2, we have $x \equiv y \pmod 3$. Applying Lemma 4.3, we now get

$$\left[\frac{\rho_D(x,y)}{3}, \frac{\sigma_D(x,y)}{3}\right] \pmod{27} \in \{[5,17],[14,26],[23,8],[13,1],[22,10],[4,19]\}.$$

Matching these values with $[A(a,b), B(a,b)] \pmod{27}$ in Table 2, the result follows. □

Theorem 4.5. *Let $v, V \in \mathbb{Z}$ be such that $v \equiv 3 \pmod 6$ and $V \equiv 1 \pmod 6$. Then, for any unit $\varepsilon = a + b\theta \in \mathbb{Z}[\theta]$, the following statements hold:*

(i) *$\varepsilon A_1(v)$ and $\varepsilon A_1(V)$ are not cubes in $\mathbb{Z}[\theta]$.*
(ii) *$\varepsilon A_1(v)$ and $\varepsilon^2 A_1(V)$ are not cubes in $\mathbb{Z}[\theta]$.*

Proof. Since $V \equiv 1 \pmod 6$, there exists a $w \in \mathbb{Z}$ such that $V = 6w+1$ and, by (4.12), $A_1(V) = 3(27w + 5 - \theta)$. Put $C(a,b) = 5a - 17b$ and $D(a,b) = 4b - a$. Then,

$$\frac{\varepsilon A_1(V)}{3} = (a + b\theta)(27w + 5 - \theta) \equiv C(a,b) + D(a,b)\theta \pmod{27}. \tag{4.17}$$

First, suppose that $K, L \in \mathbb{Z}[\theta]$ are such that $\varepsilon A_1(v) = K^3$ and $\varepsilon A_1(V) = L^3$. Since $\varepsilon A_1(v) = K^3$, Lemma 4.4 yields $[a,b] \pmod{27} \in \{[1,0],[8,9],[10,9],[17,18],[19,18],[26,0]\}$. Hence,

$$[C(a,b), D(a,b)] \pmod{27} \in \{[5,26],[22,1]\}. \tag{4.18}$$

On the other hand, if $L = x + y\theta$, then $L^3 = \rho_D(x,y) + \sigma_D(x,y)\theta = \varepsilon A_1(V)$. Since $3|A_1(V)$, we have $3|\rho_D(x,y)$, $3|\sigma_D(x,y)$ and (4.17) yields

$$\left[\frac{\rho_D(x,y)}{3}, \frac{\rho_D(x,y)}{3}\right] \equiv [C(a,b), D(a,b)] \pmod{27}. \tag{4.19}$$

Combining (4.18) and (4.19), we now get $9 \nmid \sigma_D(x,y)$. Hence, by (4.4), $3 \nmid xy$ and, by part (iii) of Lemma 4.2, we obtain $x \equiv y \pmod 3$. Finally, by Lemma 4.3,

$$\left[\frac{\rho_D(x,y)}{3}, \frac{\sigma_D(x,y)}{3}\right] \pmod{27} \in \{[5,17],[14,26],[23,8],[13,1],[22,10],[4,19]\}, \tag{4.20}$$

which is a contradiction with (4.18). This proves (i).

Next, suppose that $K, L \in \mathbb{Z}[\theta]$ is such that $\varepsilon A_1(v) = K^3$ and $\varepsilon^2 A_1(V) = L^3$. Since $\varepsilon A_1(v) = K^3$, we have (4.13). Put $\varepsilon^2 = \alpha + \beta\theta$. Using (4.2), we obtain $\varepsilon^2 \equiv a^2 + 17b^2 + (2ab + b^2)\theta \pmod{27}$ and (4.13) yields $[\alpha, \beta] \pmod{27} \in \{[1,0],[10,9],[19,18]\}$. Hence,

$$\frac{\varepsilon^2 A_1(V)}{3} = (\alpha + \beta\theta)(27w + 5 - \theta) \equiv C(\alpha,\beta) + D(\alpha,\beta)\theta \equiv 5 + 26\theta \pmod{27}. \tag{4.21}$$

On the other hand, if $L = x + y\theta$, then, as in the proof of part (i), we get (4.20), which is a contradiction with (4.21). The proof is complete. □

For any odd $V \in \mathbb{Z}$, let us define $A_2(V) \in \mathbb{Z}[\theta]$ such that

$$A_2(V) = \frac{V+3}{2} - 3\theta. \tag{4.22}$$

Theorem 4.6. *Let $v, V \in \mathbb{Z}$, $v \equiv 3 \pmod 6$, $V \equiv \pm 1 \pmod 6$ and let $\varepsilon = a + b\theta$ be a unit of $\mathbb{Z}[\theta]$. If $\varepsilon A_1(v)$ is a cube in $\mathbb{Z}[\theta]$, then $\varepsilon A_2(V)$ and $\varepsilon^2 A_2(V)$ are not cubes in $\mathbb{Z}[\theta]$.*

Proof. Let $\varepsilon A_1(v)$ be a cube in $\mathbb{Z}[\theta]$. Then, by (4.13), $3 \nmid a$ and $9|b$. Therefore, there exists $c \in \mathbb{Z}$ such that $b = 9c$. Put $w = (V+3)/2$. Then,

$$\varepsilon A_2(V) = (a + 9c\theta)(w - 3\theta) \equiv aw + 3(3cw - a)\theta \pmod{27}.$$

Suppose that $\varepsilon A_2(V) = K^3$ for some $K = x + y\theta \in \mathbb{Z}[\theta]$. Then, $K^3 = \rho_D(x,y) + \sigma_D(x,y)\theta \equiv aw + 3(-a + 3cw)\theta \pmod{27}$. Since $3 \nmid a$, we have $9 \nmid \sigma_D(x,y)$. Hence, by (4.4), $3 \nmid xy$. Next, combining part (i) and part (iii) of Lemma 4.2, we get $3|\rho_D(x,y)$, which means that $3|aw$. Hence, it follows $3|V$, which is a contradiction.

Next, suppose that $\varepsilon^2 A_2(V) = L^3$ for some $L = x + y\theta \in \mathbb{Z}[\theta]$. Then,

$$\varepsilon^2 A_2(V) = (a + 9c\theta)^2(w - 3\theta) \equiv a^2 w + 3a(6cw - a)\theta \pmod{27}$$

and $L^3 = \rho_D(x,y) + \sigma_D(x,y)\theta$. Hence, $\sigma_D(x,y) \equiv a(6cw - a) \pmod 9$. Since $3 \nmid a$, we have $9 \nmid \sigma_D(x,y)$ and (4.4) yields $3 \nmid xy$. Using Lemma 4.2, we now obtain $3|\rho_D(x,y)$, which means that $3|a^2 w$. Hence, $3|V$, which is a contradiction. □

Now we are ready to solve the case of $D \equiv 1 \pmod 3$ where $D < 0$.

5. Case of negative discriminant $D \equiv 1 \pmod 3$

First, for any $D \in \mathbb{Z}$, put $\mathbb{A} = \{f(x) = x^3 + ax^2 + bx + c \in C_D : 3|a\}$ and $\mathbb{B} = \{f(x) = x^3 + ax^2 + bx + c \in C_D : 3 \nmid a\}$. If $f(x) \in \mathbb{A}$, then, by part (i) of Theorem 2.1, there exist uniquely determined $u, v \in \mathbb{Z}$ such that $[u, v] \in V_1$ and $g_f(x) = f(x - a/3) = x^3 + ux + v$. Moreover, by (2.3), $v = (2a^3 - 9ab + 27c)/27$. Let $k \in \{0, 1, 2\}$ and, let $\mathbb{A}_k = \{f(x) \in \mathbb{A} : v \equiv k \pmod 3\}$. Then, $\mathbb{A}_0$, $\mathbb{A}_1$, $\mathbb{A}_2$, $\mathbb{B}$ are pairwise disjunct and, $\mathbb{A}_0 \cup \mathbb{A}_1 \cup \mathbb{A}_2 \cup \mathbb{B} = C_D$. Next, observe that, for any $D \in \mathbb{Z}$, the following implication holds: if D is square-free and $C_D \neq \emptyset$, then $D \equiv 1 \pmod 4$.

Further in this section, we will assume that $D \in \mathbb{Z}$ is such that

$$D < 0,\ D \equiv 1 \pmod 3,\ D \equiv 1 \pmod 4,\ D \text{ is square-free and, } 3 \nmid h(-3D) \tag{5.1}$$

where $h(-3D)$ is the class number of the real quadratic field $\mathbb{Q}(\sqrt{-3D})$.

Let $f(x) = x^3 + ax^2 + bx + c \in C_D$ where $D \in \mathbb{Z}$ satisfies (5.1). Then, $V_1 \cup V_2 \neq \emptyset$. If $V_1 = \emptyset$, then $\mathbb{A} = \emptyset$ and $C_D = \mathbb{B}$. Since $D \equiv 1 \pmod 3$, by part (vi) of Lemma 3.3, any $f(x) \in C_D = \mathbb{B}$ is of type [3] over $\mathbb{F}_3$. On the other hand, if $V_1 \neq \emptyset$, then there exist $u, v \in \mathbb{Z}$ such that $4u^3 + 27v^2 = -D$. Hence, $D \equiv -4u^3 \pmod{27}$, which, together with $D \equiv 1 \pmod 3$, yields $D \equiv \delta \pmod{27}$ where $\delta \in \{4, 13, 22\}$. Consequently, if $V_1 \neq \emptyset$, the results of Section 4 can be used. Finally, recall that, in (4.12) and (4.22), we defined, for any odd $v, V \in \mathbb{Z}$, the numbers $A_1(v), A_2(V) \in \mathbb{Z}[\theta]$ such that

$$A_1(v) = 3\left(\frac{9v+1}{2} - \theta\right) \text{ and } A_2(V) = \frac{V+3}{2} - 3\theta.$$

These numbers were studied extensively in [2,3,4]. Particularly in [2, Theorem 3.2], the following result was proved:

Theorem 5.1. *Let $D \in \mathbb{Z}$ be such that*

$$D < 0,\ 3 \nmid D,\ D \equiv 1 \pmod 4),\ D \text{ is square-free and, } 3 \nmid h(-3D)$$

where $h(-3D)$ is the class number of the real quadratic field $\mathbb{Q}(\sqrt{-3D})$. Let $i \in \{1, 2\}$, $[u, v] \in V_i$ and let ε^* be the fundamental unit of $\mathbb{Q}(\sqrt{-3D})$. Then, there exist $e(v) \in \{1, 2\}$ and $\alpha(v) \in \mathbb{Z}[\theta]$ such that

$$A_i(v) = (\varepsilon^*)^{e(v)}\alpha(v)^3. \tag{5.2}$$

Moreover, $e(v)$ and $\alpha(v)$ are uniquely determined and $e(v) + e(-v) = 3$.

Note that $e(v)$ and $\alpha(v)$ also depend on u and should actually be denoted, say, by $e(u, v)$ and $\alpha(u, v)$. However, for simplicity, we will keep the notation $e(v)$ and $\alpha(v)$.

The key to the main result of this section is the following lemma.

Lemma 5.2. *Let $D \in \mathbb{Z}$ satisfy* (5.1). *If $\mathbb{A}_0 \neq \emptyset$, then $\mathbb{A}_1 \cup \mathbb{A}_2 \cup \mathbb{B} = \emptyset$.*

Proof. The proof consists of two steps. First, we show that

$$\text{if } \ \mathbb{A}_2 \neq \emptyset, \ \text{ then } \ \mathbb{A}_1 \neq \emptyset. \tag{5.3}$$

Let $f(x) \in \mathbb{A}_2$. Then, $g_f(x) = x^3 + ux + v$ for some $[u, v] \in V_1$ where $v \equiv 2 \pmod 3$. Put $h(x) = -g_f(-x) = x^3 + ux - v$. Then, $-v \equiv 1 \pmod 3$ and $h(x) \in \mathbb{A}_1$.

Next, we show that,

$$\text{if } \ \mathbb{A}_0 \neq \emptyset, \ \text{ then } \ \mathbb{A}_1 \cup \mathbb{B} = \emptyset. \tag{5.4}$$

Let $f(x) \in \mathbb{A}_0$. Then, $g_f(x) = x^3 + ux + v$ for some $[u, v] \in V_1$ where $v \equiv 0 \pmod 3$. Since D is square-free, $v \equiv 1 \pmod 2$ follows from $4u^3 + 27v^2 = -D$. Therefore, $v \equiv 3 \pmod 6$. Next, by Theorem 5.1, there exist $a \in \{1, 2\}$ and $\alpha(v) \in \mathbb{Z}[\theta]$ such that $A_1(v) = (\varepsilon^*)^a\alpha(v)^3$. Put $\varepsilon = (\varepsilon^*)^{3-a}$ and $K = \varepsilon^*\alpha(v)$. Then, ε is a unit of the ring $\mathbb{Z}[\theta]$, $K \in \mathbb{Z}[\theta]$, and $K^3 = (\varepsilon^*)^{3-a}(\varepsilon^*)^a\alpha(v)^3 = \varepsilon A_1(v)$.

Suppose now that there exists an $h(x) \in \mathbb{A}_1 \cup \mathbb{B}$. Since, $\mathbb{A}_1 \cap \mathbb{B} = \emptyset$, we have either $h(x) \in \mathbb{A}_1$ or $h(x) \in \mathbb{B}$. If $h(x) \in \mathbb{A}_1$, then there exist $[U, V] \in V_1$ such that $g_h(x) = x^3 + Ux + V$ where $V \equiv 1 \pmod 3$. Since D is square-free, $V \equiv 1 \pmod 2$ follows from $4U^3 + 27V^2 = -D$. Hence, $V \equiv 1 \pmod 6$. On the other hand, if $h(x) \in \mathbb{B}$, then there exist $[U, V] \in V_2$ such that $g_h(x) = x^3 + (U/3)x + V/27$ where $U \not\equiv 0 \pmod 3$. Since D is square-free, $V \equiv 1 \pmod 2$ and $V \not\equiv 0 \pmod 3$ follows from $4U^3 + V^2 = -27D$. Hence, $V \equiv \pm 1 \pmod 6$. Next, let us put

$$i = \begin{cases} 1 \text{ if } h(x) \in \mathbb{A}_1, \\ 2 \text{ if } h(x) \in \mathbb{B}. \end{cases}$$

Then, by Theorem 5.1, there exist $b \in \{1, 2\}$ and $\alpha(V) \in \mathbb{Z}[\theta]$ such that $A_i(V) = (\varepsilon^*)^b\alpha(V)^3$. If $a = b$, put $L_1 = \varepsilon^*\alpha(V)$. Then, $L_1 \in \mathbb{Z}[\theta]$ and we have $L_1^3 = (\varepsilon^*)^{3-a}(\varepsilon^*)^a\alpha(V)^3 = \varepsilon A_i(V)$. Next, if $a \neq b$, put $L_2 = (\varepsilon^*)^{2+c}\alpha(V)$ where

$$c = \begin{cases} 0 \text{ if } [a, b] = [1, 2], \\ -1 \text{ if } [a, b] = [2, 1]. \end{cases}$$

Then, $b = 2a + 3c$, $L_2 \in \mathbb{Z}[\theta]$ and $L_2^3 = (\varepsilon^*)^{6+3c}\alpha(V)^3 = (\varepsilon^*)^{6-2a+2a+3c}\alpha(V)^3 = (\varepsilon^*)^{6-2a}(\varepsilon^*)^b\alpha(V)^3 = \varepsilon^2 A_i(V)$. Combining the identities $\varepsilon A_i(V) = L_1^3$ and $\varepsilon^2 A_i(V) =$

L_2^3 with $\varepsilon A_1(v) = K^3$ yields a contradiction. In particular, for $i = 1$, we get a contradiction with Theorem 4.5 and, for $i = 2$, we get a contradiction with Theorem 4.6. This proves (5.4).

Finally, combining (5.3) and (5.4) we get the desired result. □

We are now ready to state and prove the main theorem of this section.

Theorem 5.3. *Let $D \in \mathbb{Z}$ satisfy* (5.1) *and let $C_D \neq \emptyset$. Then, all polynomials in C_D have the same type of factorization over $\mathbb{F}_3$.*

Proof. First, from Lemma 5.2, it follows that either $C_D = \mathbb{A}_0$ or $C_D = \mathbb{A}_1 \cup \mathbb{A}_2 \cup \mathbb{B}$. Next, part (iv) of Lemma 3.3 says that any $f(x) = x^3 + ax^2 + bx + c \in C_D$ is of type [3] or type [1, 1, 1] over $\mathbb{F}_3$. We prove that $f(x)$ is of type [1, 1, 1] over $\mathbb{F}_3$ if and only if $f(x) \in \mathbb{A}_0$.

Let $f(x) \in \mathbb{A}_0$. Then, $3|a$ and, by part (i) of Theorem 2.1, $b = 3w^2+u$, $c = w^3+uw+v$ for some $w \in \mathbb{Z}$ and $[u, v] \in V_1$. Since $4u^3 + 27v^2 = -D$, we have $u \equiv -D \pmod 3$, which, together with $D \equiv 1 \pmod 3$, yields $u \equiv 2 \pmod 3$. Hence, $b \equiv 2 \pmod 3$ and $c \equiv v \pmod 3$. Since $f(x) \in \mathbb{A}_0$, we have $v \equiv 0 \pmod 3$ and $c \equiv 0 \pmod 3$ follows. Hence, $f(x) \equiv x^3 + 2x \equiv x(x + 1)(x + 2) \pmod 3$, which yields that $f(x)$ is of type [1, 1, 1] over $\mathbb{F}_3$.

On the other hand, assume that $f(x)$ is of type [1, 1, 1] over $\mathbb{F}_3$. Then, $f(x) \equiv x(x + 1)(x + 2) \equiv x^3 + 2x \pmod 3$. Therefore, $a \equiv 0 \pmod 3$, $b \equiv 2 \pmod 3$ and $c \equiv 0 \pmod 3$. Since $a \equiv 0 \pmod 3$, we have, by part (i) of Theorem 2.1, $b = 3w^2 + u$ and, $c = w^3 + uw + v$. Therefore, $u \equiv 2 \pmod 3$ and $c \equiv v \pmod 3$ follows. Since, $c \equiv 0 \pmod 3$, we have $v \equiv 0 \pmod 3$, which implies $f(x) \in \mathbb{A}_0$. □

We conclude this section by examples which prove that if D satisfies (5.1), both cases $C_D = \mathbb{A}_0 \neq \emptyset$ and $C_D = \mathbb{A}_1 \cup \mathbb{A}_2 \cup \mathbb{B} \neq \emptyset$ can occur.

Example 5.4. (i) Let $f(x) = x^3 - 3x^2 + 5x - 2$ and $g(x) = x^3 + 5x^2 + 7x + 4$. Then, $f(x), g(x) \in C_{-59}$ and $D = -59$ satisfies (5.1). Next, $f(x) \in \mathbb{A}_1$, $g(x) \in \mathbb{B}$ and $f(x)$, $g(x)$ are of type [3] over $\mathbb{F}_3$. (ii) Let $f(x) = x^3 - x + 3$. Then, $f(x) \in C_{-239}$, $D = -239$ satisfies (5.1), $f(x) \in \mathbb{A}_0$ and $f(x)$ is of type [1, 1, 1] over $\mathbb{F}_3$.

6. Case of positive discriminant $D \equiv 1 \pmod 3$

Throughout this section, we will assume that $D \in \mathbb{Z}$ is such that

$$D > 0,\ D \equiv 1 \pmod 3,\ D \text{ is square-free, and } 3 \nmid h(-3D) \tag{6.1}$$

where $h(-3D)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3D})$.

Theorem 6.1. *Let $D \in \mathbb{Z}$ satisfy* (6.1) *and let $C_D \neq \emptyset$. Then,* (i) *and,* (ii) *hold.*

(i) *The set V_1 has two elements and $V_2 = \emptyset$.*
(ii) *If $f(x) \in C_D$, then $f(x)$ has a rational integer root.*

For proof of (i), see [3, Theorem 3.3] and [3, part (i) of Lemma 3.6]. For proof of (ii), consult [3, Theorem 3.7].

Theorem 6.2. *Let $D \in \mathbb{Z}$ satisfy* (6.1) *and let $C_D \neq \emptyset$. Then, all polynomials in C_D have the same type of factorization over $\mathbb{F}_3$. Moreover, this type is* [1, 1, 1].

Proof. Assume that $f(x), g(x) \in C_D$ where D satisfies (6.1). Then, by Theorem 6.1, $V_1 = \{[u, v], [u, -v]\}$ and, $V_2 = \emptyset$. By part (i) of Theorem 2.1, we can now assume that $g_f(x) = x^3 + ux + v$ and, $g_g(x) = x^3 + ux - v$. Since $g_f(x) = -g_g(-x)$, $f(x)$ and $g(x)$ have the same type of factorization over $\mathbb{F}_3$. Moreover, part (iv) of Lemma 3.3 says that $f(x)$ is of type [3] or of type $[1, 1, 1]$ over $\mathbb{F}_3$ and, from part (ii) of Theorem 6.1, it follows that $f(x)$ is of type $[1, 1, 1]$ over $\mathbb{F}_3$. □

From Theorem 6.2 we immediately obtain the following corollary.

Corollary 6.3. *If $D \in \mathbb{Z}$ satisfies (6.1) and $C_D \neq \emptyset$, then $\mathbb{A}_0 \neq \emptyset$ and $\mathbb{A}_1 \cup \mathbb{A}_2 \cup \mathbb{B} = \emptyset$.*

Finally, we present an example showing that the case $C_D = \mathbb{A}_0 \neq \emptyset$ can occur.

Example 6.4. Let $f(x) = x^3 - 4x + 3$. Then, $f(x) \in C_{13}$ and $D = 13$ satisfies (6.1).

7. Conclusion

In this paper, we extended our preceding results presented in [2,3,4] to primes 2 and 3. Our main result is the following:

Theorem 7.1. *Let $D \in \mathbb{Z}$ be square-free and let $3 \nmid h(-3D)$ where $h(-3D)$ is the class number of $\mathbb{Q}(\sqrt{-3D})$. Let p be an arbitrary prime. Then, all polynomials in C_D have the same type of factorization over $\mathbb{F}_p$.*

References

[1] KLAŠKA, J.—SKULA, L.: *Mordell's equation and the Tribonacci family*, The Fibonacci Quarterly **49.4** (2011), 310–319.

[2] KLAŠKA, J.—SKULA, L.: *Law of inertia for the factorization of cubic polynomials – the real case*, Utilitas Mathematica, **102** (2017), 39–50.

[3] KLAŠKA, J.—SKULA, L.: *Law of inertia for the factorization of cubic polynomials – the imaginary case*, Utilitas Mathematica, **103** (2017), 99–109.

[4] KLAŠKA, J.—SKULA, L.: *Law of inertia for the factorization of cubic polynomials – the case of discriminants divisible by three*, Math. Slovaca **66.4** (2016), 1019–1027.

[5] WARD, M.: *The characteristic number of a sequences of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. **33** (1931), 153–165.

CHAPTER 18

APPLICATIONS OF FIBONACCI NUMBERS AND THE GOLDEN RATIO IN PHYSICS, CHEMISTRY, BIOLOGY AND ECONOMY ⋆

Abstract. The purpose of this paper, which was inspired by Hebrew mathematician Dov Jarden, is to give an extensive list of references to applications of Fibonacci numbers and the golden ratio in physics, chemistry, biology and economy. We focus, above all, on those published from 1963 to 2011. Our list can be interesting not only for students of applied mathematics but also for their teachers.

1. Introduction

The numbers F_n defined by $F_{n+2} = F_{n+1} + F_n$ with $F_0 = 0$, $F_1 = 1$ for all $n = 0, 1, 2 \cdots$ are known as the Fibonacci numbers. These numbers were named by nineteenth-century French mathematician François-Edouard-Anatole Lucas (1842–1891) after Italian mathematician Leonardo Pisano Bigollo (c. 1170–1250) also known as Leonardo of Pisa, Leonardo Bonacci, Leonardo Fibonacci or just Fibonacci.

The golden ratio (also known as golden mean, golden proportion or golden section) is an irrational number defined as $\Phi := (1 + \sqrt{5})/2 = 1.618 \cdots$. This number and $\varphi := -1/\Phi = (1 - \sqrt{5})/2 = 0.618 \cdots$ are the solutions of the quadratic equation $x^2 - x - 1 = 0$. It is well known that Fibonacci numbers F_n can be computed using Φ and φ as follows:

$$F_n = \frac{\Phi^n - \varphi^n}{\Phi - \varphi} = \frac{\Phi^n - (-\Phi^{-n})}{\sqrt{5}}, \text{ for all } n = 0, 1, 2, \cdots .$$

This explicit formula for F_n is called Binet's formula, after the French mathematician Jacques-Phillipe-Marie Binet (1786–1856), who discovered it in 1843. In fact, it was first discovered in 1718 by Abraham De Moivre (1667–1754) using generating functions, and also arrived at independently in 1844 by Gabriel Lamé (1795–1870).

A comprehensive survey of discoveries concerning the number–theoretic properties of Fibonacci numbers through 1202–1919 can be found in *History of the Theory of Numbers* [24] written by Leonard Eugene Dicson (1874–1954). Tens of books and monographs as well as thousands of scholary papers have been published on Fibonacci numbers and the golden ratio. Note that the first known book devoted to the golden ratio is *De Divina Proportione* by Luca Pacioli (1445–1519). Published in 1509, this book was illustrated by Leonardo da Vinci.

⋆ Published in J. Klaška, *Applications of Fibonacci numbers and the golden ratio in physics, chemistry, biology and economy*, 7th Conference on Mathematics and Physics on Technical Universities, Brno (2011), 243–254.

As a good introduction into the study of Fibonacci numbers, the book [30] by Nicolai Nicolaevich Vorobiev can be recommended together with the books by Thomas Koshy [153], Steven Vajda [123] and Richard A. Dunlap [145]. For advanced study, see the journal *The Fibonacci Quarterly* founded in 1963 by Alfred Brousseau (1907–1988) and Verner Emil Hoggatt (1921 – 1980). Further important facts on Fibonacci numbers can be found in the proceedings of international conferences *Applications of Fibonacci numbers* 1–14:

1984	Greece, Patras,	1998	US, NY, Rochester,
1986	US, CA, San Jose,	2000	Luxembourg,
1988	Italy, Pisa,	2002	US, AZ, Flagstaff,
1990	US, NC, Winston-Salem,	2004	Germany, Braunschweig,
1992	Scotland, St. Andrews,	2006	US, CA, San Francisco,
1994	US, WA, Pullman,	2008	Greece, Patras,
1996	Austria, Graz,	2010	Mexico, Morelia.

Fibonacci numbers appear in almost every branch of mathematics: in number theory obviously, but also in differential equations, probability, statistics, numerical analysis, and linear algebra. Recall, for example, that Fibonacci numbers played an important role in solving the tenth Hilbert problem (Matijasevich 1970 [61]) and that they are closely related to the Fermat Last Theorem (Sun–Sun 1992 [133]). In the first place, however, Fibonacci numbers and the golden ratio have many important and unexpected applications in physics, chemistry, biology economy, architecture, music, aesthetics and other fields.

In physics, for example, they are used in the network analysis of electric transmission lines, help study the atomic structures of some materials and investigate the light reflection paths in optics. In chemistry, they can be found in the theory of aromatic hydrocarbons and in questions related to the periodic table of elements. In biology, they are used to derive formulas for form growth, and in economy, they are part of Elliott's wave principle. Recently, interesting applications have appeared of Fibonacci numbers in the research of the human genome and cancer.

This paper should provide the reader with a list of references to papers on applications of Fibonacci numbers. It consists of three parts in chronological order. First we recall some oldest works from the period 1611–1938. In the second part, we mention the most important works from the period 1939–1962. Finally, we give a complete list of all references to papers published in *The Fibonacci Quarterly* (1963–2010) and presented at the international conferences *Applications of Fibonacci Numbers* (1984–2010). What follows can be taken for an introduction to the study of the applications of Fibonacci numbers.

2. Part I. Applications of Fibonacci Numbers

(Chronological Bibliography by D. Jarden 1611-1938)

In 1947, Dov Jarden [29] published in Riveon Lematematika (mathematical Journal in Hebrew with English summaries) *Bibliography of the Fibonacci sequence*. In [29, p. 45], you can also find the following selection of references related to applications of Fibonacci numbers in natural sciences in the period 1611–1938:

1611

1. J. Kepler, *Sterna seu de nive sexangula,* Opera, Frisch **7** (1611), 722–723.

1830

2. A. Braun, *Vergleichende Untersuchung über die Ordnung der Schuppen an den Tannenzapfen als Einleitung zur Untersuchung der Blätterstellung überhaupt,* Nova Acta Acad. Caes. Leopoldina **15** (1830), 199–401.

1835

3. K. F. Schimper, *Beschreibung des Symphytum Zeyheri etc.,* Geiger's Magazin für Pharmacie **29** (1835).
4. A. Braun, *Dr. K. Schimpers Vorträge über die Möglichkeit eines wissenschaftlichen Verständnisses der Blattstellung etc.,* Flora **18** (1835).

1837

5. L. Bravais et A., *Essai sur la disposition des feuilles curvisériées,* Ann. des. Sc. Nat. **(2)7** (1837), 42–110.

1838

6. L. Bravais et A., *Mémorie sur la disposition géométrique des feuilles et des inflorescenses,* Paris, (1838).

1850

7. B. Peirce, *Mathematical investigation of the fractions which occur in Phyllotaxis,* Amer. Assoc. Adv. Sc. Proc. **2** (1850), 444–447.

1851

8. A. Braun, *Betrachtungen über die Erscheinung der Verjüngung in der Natur, insbesondere in der Lebens-und Bildungsgeschichte der Pflanzen* (1851), 125.

1852

9. F. Unger, *Botanische Briefe,* Wien (1852).

1856

10. C. Wright, *On the phyllotaxis,* Astron. Il. **5** (1856), 22–24.

1863

11. R. L. Ellis, *On the theory of vegetable spirals, The mathematical and other writings,* Cambridge (1863), 358–372.

1865

12. C. de Candolle, *Théorie de l'angle unique en phyllotaxie,* Archives des Sc. Phys. et Nat. **23** (1865).

1871

13. A. Dickson, *On some abnormal cases of pinus pinaster,* Trans. Roy. Soc. Edinburgh **26** (1871), 505–520.
14. C. Wright, *The uses and origin of the arrangements of leaves in plants,* Mem. Amer. Acad. **9**, part 2, Cambridge, Mass. (1871), p. 384.

1872

15. P. G. Tait, *On phyllotaxis,* Proc. Roy. Soc. Edinburgh **7** (1872), 391–394.

1873

16. H. Airy, *On leaf arrangement,* Proc. Roy. Soc. London **21** (1873), 176–179.

1879

17. S. Günther, *Das mathematische Grundgesetz im Bau des Pflanzenkörpers,* Kosmos **(2)4**, (1879) 270–284.

1883

18. F. Ludwig, *Einige wichtige Abschnitte aus der mathematischen Botanik,* Zeitschrift für Math. u. Naturwiss. Unterricht **14** (1883), p. 161-.

1889

19. F. Ludwig, *Über Zahlen und Masse im Pflanzenreich,* Wiss. Rundsch. d. Münch. Neuest. Nachrichten **84** (1889).

1896

20. F. Ludwig, *Weiteres über Fibonaccicurven,* Botanisches Centralbl. **68** (1896), 1–8.

1904

21. A. H. Church, *On the relation of phyllotaxis to mechanical laws* (1904).

1907

22. G. van Iterson, *Mathematische und mikroskopisch – anatomische Studien über Blattstellungen,* Jena (1907).

1917

23. D'A. W. Thompson, *On growth and form,* Cambridge (1917), p. 643.

1919

24. L. E. Dickson, *History of the Theory of Numbers,* Vol. I, Carnegie Institute of Washington, (1919), 393–411.

1928

25. E. Žyliňski, *O liczbach Fibonacciego w statystyce biologicznej,* Kosmos **53** (1928), 511–516.

1932

26. J. Hambidge, *Practical applications of dynamic symmetry,* New Haven (1932), 27–29.

1936

27. R. E. Moritz, *On the beauty of geometrical forms,* Scripta Math. **4** (1936), 28–31.

1938

28. H. Geppert, S. Kotler, *Erbmathematik,* Kap. 3, Par. 15, Leipzig (1938), p. 236.

3. Part II. Applications of Fibonacci Numbers

(Chronological Bibliography 1939–1962)

The second part of our paper contains selected works on the applications of Fibonacci numbers published from 1939 to the foundation of *The Fibonacci Association* in 1963.

1947

29. D. Jarden, *Bibliography of the Fibonacci sequence,* Riveon Lematematika **2** (1947-8), 36–45.

1951

30. N. N. Vorobiev, *Chisla Fibonacci,* Gosudarstv. Izdat. Tehn.-Teor. Lit., Moscow-Leningrad, (1951), (1th edition), *Fibonacci numbers,* Birkhäuser, (2002).

1952

31. A. Turing, *The chemical basis of morphogenesis,* Philosophical Transactions of the Royal Society of London, Series B, Biological Sciences, vol. **237**, no. 641 (1952), 37–72.

1953

32. H. S. M. Coxeter, *The golden section, phyllotaxis, and Wythoff's game,* Scripta Mathematica, **19** (1953), 48–49.

1959

33. A. M. Morgan-Voyce, *Ladder-network analysis using Fibonacci numbers,* Proc. IRE. Trans. on Circuit Theory, Vol. CT- **6**, Sept. (1959), 321–322.
34. J. M. Fair, *Applications of the Fibonacci sequence,* (1959).

1960

35. F. E. Binet, R. T. Leslie, *The coefficients of inbreeding in case of repeated full-sib-matings,* J. of Genetics, June (1960), 127–130.

1961

36. H. S. M. Coxeter, *Introduction to Geometry,* John Wiley and Sons, (1961), pp. 169–172, A complete chapter on phyllotaxis and Fibonacci numbers appears in easily digestible treatment.

4. Part III. Applications of Fibonacci Numbers

(Chronological Bibliography by J. Klaška 1963–2011)

In this section we give a complete list of references to papers on applications of Fibonacci numbers published in *The Fibonacci Quarterly* from 1963 to 2010 and to those presented at the international conferences *Applications of Fibonacci Numbers* from 1984 to 2010. Other interesting references to papers from various scientific journals are also included.

1963

37. S. L. Basin, *The Appearance of Fibonacci Numbers and the Q-Matrix in Electrical Network Theory,* Mathematics Magazine, **36.2** (1963), 84–97.
38. S. L. Basin, *The Fibonacci sequence as it appears in nature,* The Fibonacci Quarterly, **1.1** (1963), 53–56.
39. A. F. Horadam, *Further appearance of the Fibonacci sequence,* The Fibonacci Quarterly, **1.4** (1963), 41–42, 46.
40. M. de Sales, *Phyllotaxis,* The Fibonacci Quarterly, **1.4** (1963), 57–60, 71.
41. J. Wlodarski, *The "Golden ratio" and the Fibonacci numbers in the world of atoms,* The Fibonacci Quarterly, **1.4** (1963), 61–63.
42. L. Moser, *Some reflections, Problem B-6,* The Fibonacci Quarterly, **1.4** (1963), 75–76.

1964

43. H. Norden, *Proportions in music,* The Fibonacci Quarterly, **2.3** (1964), 219–222.
44. R. Brian, *The problem of the little old lady trying to cross the busy street or Fibonacci gained and Fibonacci relost,* The Fibonacci Quarterly, **2.4** (1964), 310–313.
45. B. L. Swensen, *Application of Fibonacci numbers to solutions of system of linear equations,* The Fibonacci Quarterly, **2.4** (1964), 314–316.
46. A. J. Faulconbridge, *Fibonacci summation economics part I,* The Fibonacci Quarterly, **2.4** (1964), 320–322.

1965

47. E. J. Karchmar, *Phyllotaxis,* The Fibonacci Quarterly, **3.1** (1965), 64–66.
48. J. Arkin, *Ladder network analysis using polynomials,* The Fibonacci Quarterly, **3.2** (1965), 139–142.
49. J. Wlodarski, *The Fibonacci numbers and the "magic" numbers,* The Fibonacci Quarterly, **3.3** (1965), 208.
50. A. J. Faulconbridge, *Fibonacci summation economics part II,* The Fibonacci Quarterly, **3.4** (1965), 309–314.

1966

51. M. N. S. Swamy, *Properties of the polynomials defined by Morgan-Voyce,* The Fibonacci Quarterly, **4.1** (1966), 73–81.

1967

52. J. Wlodarski, *Achieving the "golden ratio" by grouping the "elementary" particles,* The Fibonacci Quarterly, **5.2** (1967), 193–194.

1968

53. A. Brousseau, *On the trail of the california pine,* The Fibonacci Quarterly, **6.1** (1968), 69–76.
54. C. R. S. Beard, *The Fibonacci drawing board design of the great pyramid of Gizeh,* The Fibonacci Quarterly, **6.1** (1968), 85–87.
55. J. Wlodarski, *More about the "Golden ratio" in the world of atoms,* The Fibonacci Quarterly, **6.4** (1968), 244, 249.
56. D. A. Preziosi, *Harmonic design in Minoan architecture,* The Fibonacci Quarterly, **6.6** (1968), 370–384, 317.

1969

57. E. A. Parberry, *A recursion relation for populations of diatoms,* The Fibonacci Quarterly, **7.5** (1969), 449–456, 463.
58. H. E. Huntley, *Fibonacci and the atom,* The Fibonacci Quarterly, **7.5** (1969), 523–524.
59. A. Brousseau, *Fibonacci statistics in conifers,* The Fibonacci Quarterly, **7.5** (1969), 525–532.
60. V. E. Hoggatt, *Fibonacci and Lucas Numbers,* section **13**: Fibonacci Numbers in Nature (1969), 79–82.

1970

61. Y. V. Matijasevich, *Enumerable sets are Diophantine,* Doklady Akademii Nauk, vol. **191** (1970), pp. 279–282. English translation: Soviet Math. Doklady vol. **11** (1970): pp. 354–358.
62. R. E. M. Moore, *Mosaic units: patterns in ancient mosiacs,* The Fibonacci Quarterly, **8.3** (1970), 281–310, 334.
63. B. A. Read, *Fibonacci series in the solar system,* The Fibonacci Quarterly, **8.4** (1970), 428–438, 448.
64. P. B. Onderdonk, Pineapples and Fibonacci numbers, The Fibonacci Quarterly, **8.5** (1970), 507–508.

1971

65. J. Wlodarski, *The possible end of the periodic table of elements and the "golden ratio",* The Fibonacci Quarterly, **9.1** (1971), 82, 92.
66. J. P. Munzenrider, *A new anthesis,* The Fibonacci Quarterly, **9.2** (1971), 163–176.
67. J. Wlodarski, *The golden ratio in an electrical network,* The Fibonacci Quarterly, **9.2** (1971), 188, 194.
68. T. A. Davis, *Why Fibonacci sequence for palm leaf spirals?,* The Fibonacci Quarterly, **9.3** (1971), 237–244.
69. T. A. Davis, T. K. Bose, *Fibonacci system in aroids,* The Fibonacci Quarterly, **9.3** (1971), 253–263.
70. D. Mangeron, M. N. Oguztorelli, V. E. Poterasu, *On the generation of Fibonacci numbers and the "polyvibrating" extension of these numbers,* The Fibonacci Quarterly, **9.3** (1971), 324–328, 323.
71. E. L. Lowman, *An example of Fibonacci numbers used to generate rhythmic values in modern music,* The Fibonacci Quarterly, **9.4** (1971), 423–426, 436.
72. E. L. Lowman, *Some striking proportions in the music of Bela Bartók,* The Fibonacci Quarterly, **9.5** (1971), 527–528, 536–537.

1972

73. Ch. Witzgall, *Fibonacci search with arbitrary first evaluation,* The Fibonacci Quarterly, **10.2** (1972), 113–134.
74. L. E. Blumenson, *A characterization ot the Fibonacci numbers suggested by a problem arising in cancer research,* The Fibonacci Quarterly, **10.3** (1972), 262–264, 292.
75. R. A. Deininger, *Fibonacci numbers and water pollution control,* The Fibonacci Quarterly, **10.3** (1972), 299–300, 302.
76. H. Norden, *Proportions and the composer,* The Fibonacci Quarterly, **10.3** (1972), 319–323.
77. R. H. Shudde, *A golden section search problem,* The Fibonacci Quarterly, **10.4** (1972), 422.
78. I. McCausland, *A simple optimal control sequence in terms Fibonacci numbers,* The Fibonacci Quarterly, **10.6** (1972), 561–564, 608.
79. W. E. Sharp, *Fibonacci drainage patterns,* The Fibonacci Quarterly, **10.6** (1972), 643–650, 655.

80. B. Davis, *Fibonacci numbers in physics,* The Fibonacci Quarterly, **10.6** (1972), 659–660, 662.

1973

81. H. Hosoya, *Topological index and Fibonacci numbers with relation to chemistry,* The Fibonacci Quarterly, **11.3** (1973), 255–266.
82. B. Junge, V. E. Hoggatt, *Polynomials arising from reflections across multiple plates,* The Fibonacci Quarterly, **11.3** (1973), 285–291.
83. L. Moser, M. Wyman, *Multiple reflections,* The Fibonacci Quarterly, **11.3** (1973), 302–306.
84. D. C. Fielder, *A discussion of subscript sets with some Fibonacci counting help,* The Fibonacci Quarterly, **11.4** (1973), 420–428.
85. M. F. Lynch, *A Fibonacci-related series in an aspect of information retrieval,* The Fibonacci Quarterly, **11.5** (1973), 495–500.

1974

86. V. E. Hoggatt, M. Bicknell, *A primer for the Fibonacci numbers: part xiv, The Morgan–Voyce polynomials,* The Fibonacci Quarterly, **12.2** (1974), 147–156.

1975

87. A. Recski, *On the generalization of the Fibonacci numbers,* The Fibonacci Quarterly, **13.4** (1975), 315–317.

1976

88. L. G. Zukerman, *Fibonacci ratio in electric wave filters,* The Fibonacci Quarterly, **14.1** (1976), 25–26.
89. T. G. Lewis, B. J. Smith, M. Z. Smith, *Fibonacci sequences and memory management,* The Fibonacci Quarterly, **14.1** (1976), 37–41.
90. P. P. Majumder, A. Chakravarti, *Variation in the number of ray - and disc -florets in four species of compositae,* The Fibonacci Quarterly, **14.2** (1976), 97–100.
91. H. Norden, *Per Nørgård's "canon",* The Fibonacci Quarterly, **14.2** (1976), 126–128.
92. W. E. Greig, *Bode's rule and folded sequences,* The Fibonacci Quarterly, **14.2** (1976), 129–134.
93. D. A. Klarner,*A model for population growth,* The Fibonacci Quarterly, **14.3** (1976), 277–281.
94. K. Fischer, *The Fibonacci sequence encountered in nerve physiology,* The Fibonacci Quarterly, **14.4** (1976), 377–379.
95. H. Hedian, *The Golden section and the artist,* The Fibonacci Quarterly, **14.5** (1976), 406–418, 426.

1977

96. W. E. Greig, *The reciprocal period law,* The Fibonacci Quarterly, **15.1** (1977), 17–21.
97. A. A. Morton, *The Fibonacci series and the periodic table of elements,* The Fibonacci Quarterly, **15.2** (1977), 173–175.

98. A. Brousseau, *Fibonacci numbers in diatoms?,* The Fibonacci Quarterly, **15.4** (1977), 370.

99. G. J. Mitchison, *Phyllotaxis and the Fibonacci series,* Science, New Series, 196.4287 (1977), 270–275.

1978

100. F. A. Zenz, *The fluid mechanics of bubbling beds,* The Fibonacci Quarterly, **16.2** (1978), 171–183.

101. J. de Vita, *Fibonacci, insects, and flowers,* The Fibonacci Quarterly, **16.4** (1978), 315–317.

102. H. R. P. Ferguson, *The Fibonacci pseudogroup, characteristic polynomials and eigenvalues of tridiagonal matrices, periodic linear recurrence systems and application to quantum mechanics,* The Fibonacci Quarterly, **16.5** (1978), 435–447.

103. P. Larson, *The Golden section in the earliest notated western music,* The Fibonacci Quarterly, **16.6** (1978), 513–515.

104. W. E. Greig, *Folded sequences and bode's problem,* The Fibonacci Quarterly, **16.6** (1978), 530–539.

1979

105. W. I. McLaughlin, *Note on a Tetranacci alternative to bode's law,* The Fibonacci Quarterly, **17.2** (1979), 116–118.

106. V. E. Hoggatt, M. Bicknell–Johnson, *Reflections across two and three glas plates,* The Fibonacci Quarterly, **17.2** (1979), 118–142.

107. J. P. Gallinar, *Fibonacci ratio in a thermodynamical case,* The Fibonacci Quarterly, **17.3** (1979), 239–241.

108. T. A. Davis, R. Altevogt, *Golden mean of the human body,* The Fibonacci Quarterly, **17.4** (1979), 340–344, 384.

1980

109. R. J. Kinney, *Fibonacci sequence can serve physicians and biologists,* 18th Anniversary Volume of the Fibonacci Association, (1980), 210–212.

1981

110. M. J. Magazine, *The number of states in a class of serial queueing systems,* The Fibonacci Quarterly, **19.1** (1981), 43–45.

1982

111. L. C. Botten, *On the use of Fibonacci recurrence relations in the design of long wavelength filters and interferometers,* The Fibonacci Quarterly, **20.1** (1982), 1–6.

112. D. H. Fowler, *A generalization of the Golden section,* The Fibonacci Quarterly, **20.2** (1982), 146–158.

113. W. P. Risk, *Thevenin equivalents of ladder networks,* The Fibonacci Quarterly, **20.3** (1982), 245–248.

114. R. M. Ricketts, *The biologic significance of the divide proportion and Fibonacci series,* American Journal of Orthodontics, **81.5** (1982), 351–370.

1983

115. J. Šána, *Lucas triangle,* The Fibonacci Quarterly, **21.3** (1983), 192–195.

1984

116. O. W. Lombardi, M. A. Lombardi, *The Golden mean in the solar system,* The Fibonacci Quarterly, **22.1** (1984), 70–75.

117. G. R. Arce, *Fibonacci and related sequences indigital filtering,* The Fibonacci Quarterly, **22.3** (1984), 208–217.

1986

118. J. – P. Gallinar, *The Fibonacci ratio in a thermodynamical problem: a combinatorial approach,* The Fibonacci Quarterly, **24.3** (1986), 247–250.

119. I. Bruce, *Sequences generated by multiple reflections,* The Fibonacci Quarterly, **24.3** (1986), 268–272.

120. P. G. Anderson, *Fibonaccene,* Fibonacci Numbers and Their Applications, Reidel, Dordrecht, (1986), 1–8.

121. J. Lahr, *Fibonacci and Lucas numbers and the Morgan–Voyce polynomials in ladder networks and in electric line theory,* Fibonacci Numbers and Their Applications, Reidel, Dordrecht, (1986), 141–161.

1989

122. J. A. Brooks, *A general recurrence relation for reflections in multiple glass plates,* The Fibonacci Quarterly, **27.3** (1989), 267–271.

123. S. Vajda, *Fibonacci and Lucas Numbers, and the Golden Section,* Horwood, Chichester (1989).

1990

124. I. Gutman, S. J. Cyvin, *A result on* 1*-factors related to Fibonacci numbers,* The Fibonacci Quarterly, **28.1** (1990), 81–84.

125. M. Nodine, *Note on the resistance through a static carry look–ahead gate,* The Fibonacci Quarterly, **28.2** (1990), 102–106.

126. J. T. Butler, *On the number of propagation paths in multiplayer media,* The Fibonacci Quarterly, **28.4** (1990), 334–338.

127. P. Filipponi, E. Montolivo, *Representation of natural numbers as sums of Fibonacci numbers: an application to modern cryptography,* Applications of Fibonacci Numbers, Vol. **3**, Kluwer Academic Publishers, Dordrecht (1990), 89–99.

128. J. Lahr, *Recurrence relations in sinusoids and their applications to spectral analysis and to the resolution of algebraic equations,* Applications of Fibonacci Numbers, Vol. **3**, Kluwer Academic Publishers, Dordrecht (1990), 223–228.

129. R. A. Dunlap, *Periodicity and aperiodicity in mathematics and crystallography,* Sci. Progress Oxford **74** (1990) 311–346.

1991

130. R. Tǒsić, O. Bodroža, *An algebraic expression for the number of Kekulé structures of benzenoid chains,* The Fibonacci Quarterly, **29.1** (1991), 7–12.

1992

131. G. Ferri, M. Faccio, A. D'Amico, *Fibonacci numbers and ladder network impedance,* The Fibonacci Quarterly, **30.1** (1992), 62–67.

132. W. Lang, *A combinatorial problem in the Fibonacci number system and two-variable generalizations of Chebyshev's polynomials,* The Fibonacci Quarterly, **30.3** (1992), 199–210.

133. Z.-H. Sun, Z.-W. Sun, *Fibonacci numbers and Fermat's Last Theorem,* Acta Arith., **60** (1992), 371–388.

134. G. Markowsky, *Misconceptions about the Golden Ratio,* The College Math. J, **23.1** (1992), 2–19.

1993

135. C. Bender, *Fibonacci transmission lines,* The Fibonacci Quarterly, **31.3** (1993), 227–238.

136. N. Imada, *A sequence arising from reflections in multiple glas plates,* Applications of Fibonacci Numbers, Vol. **5**, Kluwer Academic Publishers, Dordrecht (1993), 379–386.

137. S. Sato, *Fibonacci sequence and its generalizations hidden in algorithms for generating Morse codes,* Applications of Fibonacci Numbers, Vol. **5**, Kluwer Academic Publishers, Dordrecht (1993), 481–486.

138. A. G. Shannon, R. L. Ollerton, D. R. Owens, *A Cholesky decomposition in matching insulin profiles,* Applications of Fibonacci Numbers, Vol. **5**, Kluwer Academic Publishers, Dordrecht (1993), 497–506.

1994

139. Z. W. Trzaska, *Modified numerical triangle and the Fibonacci sequence,* The Fibonacci Quarterly, **32.2** (1994), 124–129.

140. W. T. Hung, A. G. Shannon, B. S. Thornton, *The use of a second-order recurrence relation in the diagnosis of breast cancer,* The Fibonacci Quarterly, **32.3** (1994), 253–259.

1996

141. Z. W. Trzaska, *On Fibonacci hyperbolic trigonometry and modified numerical triangles,* The Fibonacci Quarterly, **34.2** (1996), 129–138.

142. F. Dubeau, A. G. Shannon, *A Fibonacci model of infectious disease,* The Fibonacci Quarterly, **34.3** (1996), 257–270.

1997

143. O. Bodroa–Pantić, I. Gutman, S. J. Cyvin, *Fibonacci numbers and algebraic structure count of some non-benzenoid conjugated polymers,* The Fibonacci Quarterly, **35.1** (1997), 75–83.

144. G. Ferri, *The appearance of Fibonacci and Lucas numbers in the simulation of electrical power lines supplied by two sides,* The Fibonacci Quarterly, **35.2** (1997), 149–155.

145. R. A. Dunlap, *The Golden Ratio and Fibonacci numbers,* World Scientific, Singapore (1997).

146. I. Adler, D. Barabe, R. V. Jean, *A history of the study of Phyllotaxis,* Annals of Botany, **80** (1997), 231–244.

1998

147. A. J. Reuben, A. G. Shannon, *Ellipses, cardioids, and Penrose tiles,* The Fibonacci Quarterly, **36.1** (1998), 45–54.
148. A. Stakhov, *The Golden section and modern harmony mathematics,* Applications of Fibonacci Numbers, Vol. **7**, Kluwer Academic Publishers, Dordrecht (1998), 393–399.

1999

149. M. N. S. Swamy, *Network properties of a pair of generalized polynomials,* The Fibonacci Quarterly, **37.4** (1999), 350–360.
150. J. A. Biles, *Composing with sequences: ... but is it art?,* Applications of Fibonacci Numbers, Vol. **8**, Kluwer Academic Publishers, Dordrecht (1999), 61–73.

2000

151. M. N. S. Swamy, *Generalizations of modified Morgan–Voyce polynomials,* The Fibonacci Quarterly, **38.1** (2000), 8–16.
152. J. Abrahams, *Nonexhaustive generalized Fibonacci trees in unequal costs coding problems,* The Fibonacci Quarterly, **38.2** (2000), 127–135.

2001

153. T. Koshy, *Fibonacci and Lucas Numbers with Applications,* Wiley, New York, (2001).

2002

154. W. Hasenpusch, *Mathematical bionics: Fibonacci series of numbers in nature,* CLB Chemie in Labour and Biotechnik, **53.7** (2002), 260–263.

2003

155. A. E. Park, J. J. Fernandez, K. Schmedders, M. S. Cohen, *Fibonacci sequence: Relationship to the human hand,* Journal of Hand Surgery, **28.1** (2003), 157–160.
156. J. C. A. Boeyens, *Number patterns innature,* Crystal Engineering, **6** (2003), 167–185.

2006

157. M. I. Al-Suwaiyel, D. Alani, A. Al-Swailem, *An investigation of Fibonacci-like sequences in biology and mathematics,* Int. J. of Nonlinear Sciences and Numerical Simulation, **7.2** (2006), 133–136.
158. T. J. Cooke, *Do Fibonacci numbers reveal the involvement of geometrical imperatives or biological interactions in phyllotaxis?,* Botanical Journal of the Linnean Society, **150** (2006), 3–24.

2007

159. O. Bodroža–Pantić, A. Ilić–Kovačević, *Algebraic structure count of angular hexagonal – square chains,* The Fibonacci Quarterly, **45.1** (2007), 3–9.

2008

160. M. E. B. Yamagishi, A. I. Shimabukuro, *Nucleotide frequences in human genome and Fibonacci numbers,* Bulletin of Mathematical Biology, **70** (2008), 643–653.

2010

161. J. C. A. Boeyens, *A molecular – structure hypothesis,* International Journal of Molecular Sciences, **11** (2010), 4267–4284.

2011

162. P. D. Shipman, Z. Sun, M. Pennybacker, A. C. Nowell, *How universal are Fibonacci patterns?,* Eur. Phys. J. D, **62** (2011), 5–17.
163. L. Debnath, *A short history of the Fibonacci and golden numbers with their applications,* International Journal of Mathematical Education in Science and Technology, **42.3** (2011), 337–367.

5. Conclusion

The author believes that the references presented in the paper will inspire further research of the applications of Fibonacci numbers.

CHAPTER 19

APPLICATIONS OF SEQUENCES OVER FINITE FIELDS★

Abstract. This paper mainly aims to inform the reader on engineering applications of sequences over finite fields. It may also provide students and teachers of applied mathematics with a creative inspiration.

1. Introduction

For the last 15 years I have been concerned with questions and problems concerning Fibonacci numbers and their cubic generalization called Tribonacci numbers. See, for example, [2,3] and, [4,5,6,7]. It is well known, that Fibonacci numbers have many practical applications outside mathematics such as in physics, chemistry, biology, and economy. In my recent paper [8] (published in 2011), I pointed out the immense extent of such applications giving an extensive list of relevant references. It has in fact helped two mathematical engineering students at the BUT Faculty of Mechanical Engineering in writing their final projects, [14] and [22]. In this paper, which can be seen as a free continuation of [8], I will briefly deal with applications of sequences over finite fields.

2. Sequences over finite fields

We begin with a short example. Let us consider the Fibonacci sequence

$$(F_n)_{n=0}^{\infty} = (0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \dots)$$

defined by $F_{n+2} = F_{n+1} + F_n$ with $F_0 = 0$, $F_1 = 1$. Applying the recurrence formula $F_{n+2} = F_{n+1} + F_n$ only to the last digits of the Fibonacci numbers (using modulo 10 arithmetic), we may be surprised to find that, after sixty terms, the sequence starts repeating itself:

0	1	1	2	3	5	8	3	1	4	5	9	4	3	7	0	7	7	4	1
5	6	1	7	8	5	3	8	1	9	0	9	9	8	7	5	2	7	9	6
5	1	6	7	3	0	3	3	6	9	5	4	9	3	2	5	7	2	9	1
0	1	1	.	.	.														

Table 1.

We may also notice further regularities. Applying to $(F_n)_{n=0}^{\infty}$ modulo 2 arithmetic, we obtain a period of length 3, while modulo 5 arithmetic will yield a length 20 period. This follows immediately from Table 1. Investigation of further cases leads to the discovery

★ Published in J. Klaška, *Applications of sequences over finite fields*, Mathematics Information Technologies and Applied Sciences, MITAV 2014, Brno (2014) p. 26.

of the following general theorem: Let $m \in \mathbb{Z}$ and let $m \geq 2$. Then $(F_n \bmod m)_{n=0}^{\infty}$ is periodic. This remarkable property is called the modular periodicity of $(F_n)_{n=0}^{\infty}$. Let $k(m)$ denote the length of the period of $(F_n \bmod m)_{n=0}^{\infty}$ and let $m = p_1^{t_1} \cdots p_k^{t_k}$ be the prime factorization of m. Then $k(m) = \mathrm{lcm}(k(p_1^{t_k}), \ldots, k(p_k^{t_k}))$. Furthermore, if $k(p^2) \neq k(p)$, then $k(p^t) = p^{t-1}k(p)$ for any positive integer t. These and many similar results are well-known. For more information, consult the first issues of the journal *The Fibonacci Quarterly.*

However, the modular periodicity of the Fibonacci sequence is only one from many examples of a more general theory of linear recurrence relations over finite fields. For this theory, see E. S. Selmer [15] and, for theory of finite fields in general, see [9,11,13]. Recall that, finite fields are also called Galois fields, after the French mathematician Evariste Galois (1811–1832). The tragic life story of this mathematical genius can be found in a book by M. Livio [10, pp. 112–157].

The basic theorem of the finite fields theory says that the number of elements in any finite field equals p^n where p is a prime, and n is a positive integer. Moreover, any two finite fields with the same number of elements are isomorphic. A finite field with p^n elements is usually denoted by $\mathbb{F}_{p^n}$ or by $\mathrm{GF}(p^n)$. If $n = 1$, then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. However, for any $n > 1$, $\mathbb{Z}/p^n\mathbb{Z}$ is not a field. If $n > 1$, then we can write $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(f(x))$ where $f(x)$ is any monic irreducible polynomial of degree n in $\mathbb{F}_p[x]$ and $(f(x))$ denotes the ideal generated by $f(x)$. Sequences defined over $\mathbb{F}_{p^n}$ are called the Galois sequences and they are closely related to linear recursions modulo p. See [15]. In the following sections we will show some remarkable and important examples of Galois sequences applications to real-world problems.

3. Einstein's Theory of General Relativity and Global Warming

One of the important experiments corroborating the veracity of Einstein's general-relativity theory is one called the Shapiro time delay. Being one of the four classic solar system experiments testing the general relativity, it is based on the idea that radar signals passing a massive object will travel along a trajectory longer that the one taken with no massive object in the vicinity. Thus, by the relativity theory, a radar signal will travel for a longer time with this time lag being measurable. The radar signal used in the Shapiro experiment was structured as a Galois sequence with a period length of $2^6 - 1 = 63$. For details of the experiment see [19] and [20]. Note that the Shapiro experiment has been repeated many times with different modifications.

Further remarkable application of Galois sequences is the measurement of ocean temperatures to monitor global warming [12]. Galois sequences were used to measure sound transmission delays between Heard Island in the Indian Ocean and Greenland, a distance exceeding 10000 km. In this case, the time delay of the sound is a function of the average ocean temperature.

4. Error correcting codes and further applications

Another important field of Galois sequences application is algebraic error correcting codes such as simplex and Hamming codes, see [21]. Error-correcting codes are used in CD players, high speed modems, and mobile phones. Early space probes such as Mariner used a type of error-correcting code called a block code while more recent space probes use convolution codes.

For illustration, we now give a short example of a simplex code. Let us consider $\mathbb{F}_{p^m}$ with $p = 2$ and $m = 3$. Then $p(x) = x^3 + x + 1$ is a primitive polynomial over $\mathbb{F}_8$ and the corresponding linear recurrence is given by $P_{n+3} = P_{n+1} + P_n$. Let $P_1 = 1, P_2 = 1$ and $P_3 = 1$. Reducing this sequence by the modulus 2, we obtain the sequence $1, 1, 1, 0, 0, 1, 0, 1, 1, 1, \cdots$ with a period length of $2^3 - 1 = 7$. In the context of coding theory, this is the simplex code of length 7. The initial conditions $(1, 1, 1)$ represent the information bits, while the rest of the period $(0, 0, 1, 0)$ is used for the check bits. The geometric representation of the code words is a simplex, in our example, in three dimensions. Note that the general binary simplex code has a length of $2^m - 1$, with m information bits and $2^m - 1 - m$ check bits. In a Hamming code, the roles of information and check bits are reversed.

Error-correcting codes are part of the coding theory, which has recently seen major advances in view of the growing importance data encryption and transfers on the Internet.

Galois sequences have also been used in many other fields. In neuropsychology, for example, [1] to measure brain–stem responses, in atmospheric physics [23], and in concert-hall acoustic [18]. Many other interesting applications of Galois sequences can be found in [16] and [17].

5. Conclusion

The above application examples of sequences over finite fields may serve as creative inspirations for mathematical engineering students writing their final projects on this subject.

References

[1] U. Eysholdt, C. E. Schreiner, *Maximum Length Sequences – A Fast Method for Measuring Brain–Stem–Evoked Responses*, Audiology **21** (1982), 242–250.

[2] J. Klaška, *Criteria for testing Wall's question*, Czechoslovak Math. J. **58.4** (2008), 1241-1246.

[3] J. Klaška, *Short remark on Fibonacci–Wieferich primes*, Acta Math. Univ. Ostrav. **15** (2007), 21–25.

[4] J. Klaška, *Tribonacci modulo p^t*, Math. Bohemica **133.3** (2008), 267–288.

[5] J. Klaška, *Tribonacci modulo 2^t and 11^t*, Math. Bohemica **133.4** (2008), 377–387.

[6] J. Klaška, *On Tribonacci–Wieferich primes*, The Fibonacci Quarterly **46/47** (2008/2009), 290–297.

[7] J. Klaška, *Tribonacci partition formulas modulo m*, Acta Math. Sinica **26.3** (2010), 465–476.

[8] J. Klaška, *Applications of Fibonacci numbers and the golden ratio in physics, chemistry, biology and economy*, 7 th Conference on Mathematics and Physics on Technical Universities, Brno, (2011), 243–254.

[9] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, (1994).

[10] M. Livio, *The Equation That Couldn't Be Solved: How Mathematical Genius Discovered the Language of Symmetry*, Simon & Schuster Paperbcks, (2005).

[11] G. L. Mullen, C. Mummert, *Finite Fields and Applications*, American Mathematical Society, SML Volume **41**, (2007).

[12] W. Munk, *Acoustic monitoring of ocean gyres*, J. Fluid Mech. **173** (1986), 43–53.

[13] S. Roman, *Field Theory*, Graduate Text in Mathematics **158**, Springer (2006).

[14] M. Rusyniak, *Application of Fibonacci Numbers in Economy – Elliott Wave Principle*, Institute of mathematics, Faculty of mechanical engineering, Brno University of Technology, (2013).

[15] E. S. Selmer, *Linear Recurrence Relations over Finite Fields*, Department of Mathematics University of Bergen, Norway, (1966).

[16] M. R. Schroeder, *Number Theory in Science and Communication*, Springer, Berlin, (1997).

[17] M. R. Schroeder, *Sequences from Number Theory for Physics, Signal Processing, and Art*, Acoustical Physics, **49.1** (2003), 97–108.

[18] M. R. Schroeder, *Fractals, Chaos, Power Laws*, Dover Publications Inc., New York, (1992).

[19] I. I. Shapiro, *Fourth test of general relativity*, Physical Review Letters **13** (1964), 789–791.

[20] I. I. Shapiro, G. H. Pettengill, M. E. Ash, M. L. Stone, W. B. Smith, R. P. Ingalls, R. A. Brockelman, *Fourth test of general relativity: preliminary results*, Physical Review Letters **20** (1968), 1265–1269.

[21] F. J. MacWilliams, N. J. F. Sloane, *The Theory of Error–Correcting Codes*, North-Holland, Amsterdam, (1977).

[22] V. Váňa, *Fibonacci Numbers with Applications*, Institute of mathematics, Faculty of mechanical engineering, Brno University of Technology, (2011).

[23] D. K. Wilson, D. W. Thomson, *Acoustic Tomographic Monitoring of the Atmospheric Surface Layer*, Atmos. Oceanic Technol. **11** (1994), 751–769.

CHAPTER 20

REAL - WORLD APPLICATIONS OF NUMBER THEORY★

Abstract. The present paper is concerned with practical applications of the number theory and is intended for all readers interested in applied mathematics. Using examples we show how human creativity can change the results of the pure mathematics into a practical usable form. Some historical notes are also included.

Dedicated to the eminent Czechoslovak mathematician Ladislav Skula

1. Introduction

German mathematician Johann Carl Friedrich Gauss (30 April 1777 - 23 February 1855), regarded as one of the greatest mathematicians of all time, claimed: "*Mathematics is the queen of the sciences and number theory is the queen of mathematics.*" However, for many years number theory had only few practical applications. It is well known that the great English number theorist Godfrey Harold Hardy (7 February 1877 - 1 December 1947) believed that number theory had no practical applications. See his essay *"A Mathematician's Apology"* [16]. Over the 20th and 21st centuries, this situation has changed significantly. Contrary to Hardy's opinion, many practical and interesting applications of number theory have been discovered. The present paper brings some remarkable examples of number theory applications in the real world. The paper can be regarded as a loose continuation of the author's preceding work [19] and [20].

2. Diophantine equations

Diophantine analysis is a branch of the theory of numbers studying polynomial equations in two or more unknowns which are to be solved in integers. The equations themselves are called Diophantine. Note, that the name Diophantine refers to the Greek mathematician Diophantus of Alexandria who lived in the third century B.C. Finding solutions of polynomial equations in integers is one of the oldest mathematical problems. Traditionally, the following basic questions are solved:

(i) Find whether a given Diophantine equation has at least one integer solution.
(ii) Decide whether the number of integer solutions is finite or infinite.
(iii) Establish all integer solutions of a given Diophantine equation.

It is also natural to ask whether there is an algorithm that will find the solutions to any given Diophantine equation. This question is known as Hilbert's tenth problem. In 1970, Russian mathematician Yuri Vladimirovich Matiyasevich [24] showed that such a general algorithm does not exist. However, for many specific Diophantine equations,

★ Published in J. Klaška, *Real-world applications of number theory*, South Bohemia Mathematical Letters **25.1** (2017), 39–47.

the general algorithm is well known. As an example, the theory of linear Diophantine equations can be given.

Let n be a positive integer, $n \geq 2$. Then, the equation

$$a_1x_1 + \cdots + a_nx_n = m \tag{2.1}$$

is said to be a linear Diophantine equation if all unknowns $x_1, \ldots, x_n$ and all coefficients $a_1, \ldots, a_n, m$ are integers. It is well known that an integer solution of (2.1) exists if and only if the greatest common divisor of $a_1, \ldots, a_n$ divides m. For general methods for solving (2.1), see for example [5], [25], and [27, pp. 27–31].

In the following sections we give three interesting examples of using Diophantine equations in the natural sciences.

3. Balancing of chemical equations

As the first example we show some application of a linear Diophantine equation to problems in chemistry. In particular, we will deal with the balancing of chemical equations. See [6]. Consider a chemical equation written in the form

$$x_1A_{a_1}B_{b_1}C_{c_1}\cdots + x_2A_{a_2}B_{b_2}C_{c_2}\cdots + \cdots \to x'_1A_{a'_1}B_{b'_1}C_{c'_1}\cdots + x'_2A_{a'_2}B_{b'_2}C_{c'_2}\cdots + \cdots$$

where $A, B, C, \cdots$ are the elements occurring in the reaction, $a_1, b_1, c_1, \cdots, a'_1, b'_1, c'_1, \cdots$ are positive integers or 0, and $x_1, x_2, \cdots, x'_1, x'_2, \cdots$ are the unknown coefficients of the reactants and products. Then, we have

$$\begin{array}{rcl} x_1a_1 + x_2a_2 + \cdots &=& x'_1a'_1 + x_2a'_2 + \cdots \\ x_1b_1 + x_2b_2 + \cdots &=& x'_1b'_1 + x_2b'_2 + \cdots \\ x_1c_1 + x_2c_2 + \cdots &=& x'_1c'_1 + x_2c'_2 + \cdots \\ & \cdots & \end{array} \tag{3.1}$$

Clearly, each equation of (3.1) expresses the law of conservation of the number of atoms for any particular element $A, B, C, \cdots$. Finding all integer solutions $[x_1, x_2, \cdots, x'_1, x'_2, \cdots]$ of (3.1) is a nice elementary problem of Diophantine analysis.

We show a concrete example. Let us consider the chemical equation

$$x_1\mathrm{KMnO_4} + x_2\mathrm{H_2SO_4} + x_3\mathrm{H_2O_2} \to x'_1\mathrm{K_2SO_4} + x'_2\mathrm{MnSO_4} + x'_3\mathrm{H_2O} + x'_4\mathrm{O_2}. \tag{3.2}$$

From (3.2) we immediately obtain

$$\begin{array}{rcll} 4x_1 + 4x_2 + 2x_3 &=& 4x'_1 + 4x'_2 + x'_3 + 2x'_4 & \text{for O} \\ x_1 &=& x'_2 & \text{for Mn} \\ x_1 &=& 2x'_1 & \text{for K} \\ x_2 &=& x'_1 + x'_2 & \text{for S} \\ 2x_2 + 2x_3 &=& 2x'_3 & \text{for H} \end{array} \tag{3.3}$$

This system is easily reduced to

$$5x_1 + 2x_3 - 4x'_4 = 0. \tag{3.4}$$

Clearly, (3.4) is a linear Diophantine equation in three variables with a solution $[x_1, x_3, x'_4] = [2, 1, 3]$. Hence, $[x_1, x_2, x_3, x'_1, x'_2, x'_3, x'_4] = [2, 3, 1, 1, 2, 4, 3]$. Consequently,

$$2\mathrm{KMnO_4} + 3\mathrm{H_2SO_4} + \mathrm{H_2O_2} \to \mathrm{K_2SO_4} + 2\mathrm{MnSO_4} + 4\mathrm{H_2O} + 3\mathrm{O_2}. \tag{3.5}$$

It is evident that (3.5) is not the only solution of our balancing problem. In fact, after a short calculation, we see that the set S of all positive integer solutions of (3.3) is infinite and can be written in the form

$$S = \{[2u, 3u, v, u, 2u, 3u + v, (5u + v)/2] : u, v, (5u + v)/2 \in \mathbb{N}\}. \tag{3.6}$$

Observe now that the solution (3.5) can be obtained from (3.6) by putting $u = v = 1$. Hence, (3.5) is the smallest possible solution of the balancing problem (3.2). Finally, we see that $(5u + v)/2 \in \mathbb{N}$ if and only if $u \equiv v \pmod 2$. Hence, it readily follows that S can be written in the form $S = S_1 \cup S_2$ where

$$S_1 = \{[4r - 2, 6r - 3, 2s - 1, 2r - 1, 4r - 2, 6r + 2s - 4, 5r + s - 3] : r, s \in \mathbb{N}\}$$

and,

$$S_2 = \{[4r, 6r, 2s, 2r, 4r, 6r + 2s, 5r + 2] : r, s \in \mathbb{N}\}.$$

For further examples of balancing equations see R. Crocker [6, p. 732].

4. Determination of the molecular formula

In this section we show how linear Diophantine equations can be used to determine the molecular formula [6]. Assume that a substance with a molecular weight of m contains elements $A, B, C, \cdots$ with atomic weights $a, b, c, \cdots$ and that $x, y, z, \cdots$ represent the numbers of atoms of $A, B, C, \cdots$ in a molecule. Then, we have

$$ax + by + cz + \cdots = m. \tag{4.1}$$

Let $\alpha, \beta, \gamma, \cdots$ denote the integers nearest the values $a, b, c, \cdots$ and μ denote the integer nearest m. Then, (4.1) can be replaced by the linear Diophantine equation

$$\alpha x + \beta y + \gamma z + \cdots = \mu. \tag{4.2}$$

If we require that the values $x, y, z, \cdots$ in (4.2) should be reasonably small, we can solve (4.2) under a condition

$$-\frac{1}{2} < (a - \alpha)x + (b - \beta)y + (c - \gamma)z + \cdots < \frac{1}{2}. \tag{4.3}$$

If more solutions of (4.2) are obtained, the true values may be found by substituting into (4.1) and finding which of them satisfies (4.1) with minimum deviation from m.

The following problem will be now solved: *The molecular weight of a substance containing only hydrogen and sulfur is* 66.146*. What is the molecular formula?*

Let a denote the atomic weight of hydrogen and b the atomic weight of sulfur. Using the periodic table of elements, we find that $a = 1.008$ and $b = 32.065$. Hence, we have $1.008x + 32.065y = 66.146$. Next, we see that $\alpha = 1$, $\beta = 32$, $\mu = 66$ and that $x \leq 34$, $y \leq 2$. Subject to these conditions, it is easy to obtain that the Diophantine equation $x + 32y = 66$ has only two positive integer solutions $[x, y] = [34, 1]$ and $[x, y] = [2, 2]$. Since a molecule of this size is not likely to contain 34 hydrogen atoms and 1 sulfur atom, this possibility may be eliminated. Therefore, $[x, y] = [2, 2]$ and, the resulting molecular formula is H_2S_2. However, in solving this problem, we can proceed in a more efficient way. The equation $1.008x + 32.065y = 66.146$ can be converted to the Diophantine equation $1008x + 32065y = 66146$, which has infinitely many integer solutions $[x, y] = [2 + 32065 \cdot k, 2 - 1008 \cdot k]$, $k \in \mathbb{Z}$. Since $x, y \in \mathbb{N}$ and $x \leq 34$, $y \leq 2$, the solution $[x, y] = [2, 2]$ immediately follows.

5. Structure of viruses

In this section we focus on an interesting problem in virology. Recall, that virus particles consist of protein subunits ordered geometrically according to strict symmetry rules. These rules highly depend on the chemical properties of the protein. For example, it is well known that spherical viruses prefer the icosahedral symmetry and that the total number N of nearly identical subunits that may be regularly ordered on the closed icosahedral surface is given by Goldberg's formula [8]

$$N = 10(a^2 + ab + b^2) + 2 = 10T + 2, \text{ where } a, b \in \mathbb{N} \cup \{0\}. \tag{5.1}$$

Using (2.11) we readily find, that

$$N \in \{12, 32, 42, 72, 92, 122, 132, \cdots\}.$$

On the other hand, it is known that an icosahedron has 30 axes of twofold symmetry, 20 axes of threefold symmetry and 12 axes of fivefold symmetry. Therefore, all subunits on the surface of an icosahedral virus may be divided into 30 identical groups each having a twofold symmetry, 20 groups with threefold symmetries and 12 groups with fivefold symmetries. These groups are often called disymmetrons, trisymmetrons and pentasymmetrons, respectively. Assume now that any disymmetron contains d_u subunits, any trisymmetron contains t_v subunits and any pentasymmetron contains p_w subunits. Then, by [22], we have

$$N = 30d_u + 20t_v + 12p_w = 10T + 2, \tag{5.2}$$

where

$$d_u = u - 1, \ t_v = \frac{(v-1)v}{2}, \ p_w = \frac{5(w-1)w}{2} + 1 \quad \text{and,} \quad u, v, w \in \mathbb{N}. \tag{5.3}$$

For each value of N defined by (5.1), the number $f(N)$ of all the solutions of (5.2) corresponds to the number of theoretically possible ways of making a virus with N subunits, but with different combinations of symmetrons. For example, if $N = 42$, then (5.2) has the unique solution $42 = 30 \cdot 1 + 20 \cdot 0 + 12 \cdot 1$, if $N = 72$, then (5.2) has exactly three solutions: $72 = 30\cdot 2+20\cdot 0+12\cdot 1 = 30\cdot 0+20\cdot 3+12\cdot 1 = 30\cdot 0+20\cdot 0+12\cdot 6$.

Putting $x = 2v - 1$, $y = 2w - 1$, $z = u - 1$ and using (5.3) equation (5.2) can be transformed, after some calculations, to the equivalent form

$$x^2 + 3y^2 + 12z = 4T. \tag{5.4}$$

In this way, the problem of describing the structure of viruses by means of geometric symmetries is reduced to the following Diophantine problem:

Find all odd positive integers x, y and all non-negative integers z, satisfying $x^2 + 3y^2 + 12z = 4(a^2 + ab + b^2)$ for any given values $a, b \in \mathbb{N} \cup \{0\}$.

There is no simple solution to this problem. In [22], W. Ljunggren proved that the total number $f(N)$ of solutions of (5.4) is equal to

$$f(N) = \frac{\pi\sqrt{3}}{180} N + k\sqrt{N}, \tag{5.5}$$

where the number k is bounded and independent of N. Furthermore, from (5.5) it can be easily deduced that $f(N)$ increases linearly with N. Surprising is that this increase is bi-modal. Geometrically, this means that, if $[x, y, z]$ is any solution of (5.4), then

$[x, y]$ lies in the neighbourhood of exactly one of two lines $y = 0.03x$ and $y = 0.015x$. A detailed analysis of this fact can be found in [22, pp. 54–56].

In [10] A. Grytczuk presented an effective method for determining all solutions of (5.4) in odd positive integers x, y and non-negative integers z. Moreover, in [11] A. Grytczuk and K. Grytczuk proved that (5.4) can be reduced to the form

$$x^2 + 3y^2 = 4(R^2 + 3S^2), \quad (R, S) = 1 \tag{5.6}$$

and that all solutions of (5.6) in odd positive integers x, y are given by the formulas

$$x = |R - 3S|, y = R + S \quad \text{or} \quad x = |R + 3S|, y = |R - S|. \tag{5.7}$$

Consequently, (5.7) gives the full solution of our Diophantine problem.

Note that, in fact, the solution (5.7) has been established earlier by G. Xeroudakes. Consult [30, p. 102]. Finally, a mathematical description of some viruses, using the above theory, can be found in [12] and [13]. In particular, parvovirus $T = 1, N = 12$, poliovirus $T = 3, N = 32$, togavirus $T = 4, N = 42$, reovirus $T = 13, N = 132$, herpesvirus $T = 16, N = 162$, and adenovirus $T = 25, N = 252$ are studied in detail and their geometrical models are presented.

6. Partitio numerorum and quantum physics

A partition of a natural number n is any non-increasing sequence of natural numbers whose sum is n. The number of partitions of n is denoted by $p(n)$. For example, if $n = 5$ then, $5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$. Hence, $p(5) = 7$. The problem of establishing the number $p(n)$ has a very long history and it is known under the name of *partitio numerorum*. Since 1674, when the problem was first mentioned by Gottfried Wilhelm Leibniz (1 July 1646 - 14 November 1716), many results concerning $p(n)$ have been discovered. For the basic theory of $p(n)$, see the books [2] and [17, pp. 361–392]. Some recent results on $p(n)$ can be found in the author's paper [18].

For small values of n, it can be found readily that

$$\{p(n)\}_{n=1}^{\infty} = \{1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, \cdots\}.$$

About 1916, Percy Alexander MacMahon (26 September 1854 - 25 December 1929) established the values of $p(n)$ for all n up to 200 [15, pp. 114-115]. For example, he found that

$$p(100) = 190569292 \quad \text{and} \quad p(200) = 3972999029388.$$

In 1934, H. Gupta [14] extended MacMahon's table up to $n = 300$ and later, in 1937, up to 600. For further historical notes, see [17, p. 391]. Nowadays, using a computer, we can establish that

$$p(1000) = 24061467864032622473692149727991 \approx 2.40615 \cdot 10^{31}$$

and

$$p(10000) \approx 3.61673 \cdot 10^{106}.$$

As we see, the growth of $p(n)$ is very rapid. It is, therefore, natural to ask about the size of $p(n)$. The answer to this question is given by the asymptotic formula

$$p(n) \sim \frac{1}{4n\sqrt{3}} \cdot \exp\left(\pi\sqrt{\frac{2n}{3}}\right) \quad \text{for} \quad n \to \infty, \tag{6.1}$$

which shows that the growth of $p(n)$ is subexponential. The formula (6.1) was discovered in 1917 by G. H. Hardy and the brilliant Indian mathematician Srinivasa Ramanujan (22 December 1887 - 26 April 1920). For a proof of (6.1) see [15]. It is remarkable that the formula (6.1) is extremely accurate and has found important applications in physics. Two interesting connections between the problem *partitio numerorum* and physics will now be mentioned.

First recall that the Hardy-Ramanujan formula has been used, with great success, in quantum physics. The connection between the theory of partitions and quantum physics was first discovered by Niels Henrik David Bohr (7 October 1885 - 18 November 1962) and talented physicist Fritz Kalckar (13 February 1910 - 6 January 1938) in their famous paper [4]. In [4], using Ramanujan - Hardy formula (6.1), Bohr and Kalckar achieved a crucial breakthrough in quantum physics: they described the decomposition of heavy atomic nuclei. Later Bohr pointed out the connection between the decomposition of Uranium 235 with the theory of partitions of natural numbers and the main idea of the nuclear bomb was clearly indicated. In this sense, the ideological creator of the nuclear bomb was Niels Bohr [23, p. 249].

The second very important application of Hardy-Ramanujan formula can be found in the problems of statistical mechanics. The significant role of (6.1) in this branch has been discussed by many authors. See, for example, the papers of C. Van Lier and G. E. Uhlenbeck [29], F. C. Auluck and D. S. Kothari [1], N. H. V. Temperly [28] and, L. Debnath [7]. Now we will give some details to one of these problems. In quantum theory, a boson is a particle that satisfies Bose-Einstein statistics. Examples of bosons are particles such as photons, gluons, W and Z bosons and the recently discovered Higgs boson. For basic definitions see [9, pp. 74-78].

Let us now consider a quantum system of N identical bosons. It is well known that such system can be viewed as a collection of one-dimensional harmonic oscillators. The energy levels of a quantum harmonic oscillator are determined by the equation $E_k = (k + 1/2)\hbar\omega$ where k is non-negative integer, $h = 2\pi\hbar$ is the Planck constant and ω is the angular frequency. For $k = 0$, we obtain the so-called ground state energy and, for $k = 1, 2, \cdots$, we get the excited states. Hence, in the ground state of the system, all bosons occupy the lowest level with $k = 0$. When an excitation energy is given to the system, there are many ways in which this energy can be distributed among N bosons. The fundamental problem is now to determine this number. In fact, this problem is the same as that of finding the number $p(n)$. This follows from the fact that the indistinguishability of boson particles is equivalent to the property that the order of summands is not significant in partitions.

Let us denote by $w(N, n)$ the number of all possible ways of distributing among N bosons the exciting energy $E = n\hbar\omega$. If $N \geq n$, then $w(N, n) = p(n)$ and, for $1 < N < n$, we have $w(N, n) = p_N(n)$ where $p_N(n)$ is the number of partitions of n into exactly N or less than N parts. Consequently, the asymptotic form of $w(N, n)$ for $N \geq n$ is precisely the Hardy-Ramanujan formula (6.1).

Now we explain, using a short example, the basic idea of the correspondence between the number $p(n)$ and the number $w(N, n)$ of states of quantum system of N bosonic harmonic oscillators. Assume that $N = 6$ and $n = 4$. Then, we have $4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$, which yields $p(4) = 5$. Consider now all possible realizations of the state with energy $E = 4\hbar\omega$ in the system of six harmonic oscillators. Clearly, there are exactly five ways (W1 − W5) to achieve the energy $E = 4\hbar\omega$: (W1) to put one boson into excited state with $k = 4$, (W2) to put one boson to the state with $k = 3$ and one boson into the state $k = 1$, (W3) to put two bosons to the state with $k = 2$, (W4) to put one boson to the state with $k = 2$ and two bosons to the state with $k = 1$, (W5) to put four bosons into the state $k = 1$. All remaining non-excited bosons in (W1-W5) remain in the ground state $k = 0$.

In the below figure, the correspondence between $p(4)$ and $w(6, 4)$ considered will be represented graphically.

$$\begin{array}{rccccc}
 & 4 & 3+1 & 2+2 & 2+1+1 & 1+1+1+1 \\
k=4 & \bullet & & & & \\
k=3 & & \bullet & & & \\
k=2 & & & \bullet\bullet & \bullet & \\
k=1 & & \bullet & & \bullet\bullet & \bullet\bullet\bullet\bullet \\
k=0 & \bullet\bullet\bullet\bullet\bullet & \bullet\bullet\bullet\bullet & \bullet\bullet\bullet\bullet & \bullet\bullet\bullet & \bullet\bullet \\
 & & & & & \\
 & W_1 & W_2 & W_3 & W_4 & W_5
\end{array} \qquad (6.2)$$

Figure 1.

Readers interested in the relationship between statistical mechanics and the problem of *partitio numerorum* will find large lists of references in [7], [23], and [26].

7. Concluding remarks

Finally, some further significant applications of the number theory will be shortly mentioned. Above all, it is well known that the theory of Fibonacci numbers has many applications in physics, chemistry, biology, economy, and architecture. Listing 163 chronological references to papers published from 1611 to 2011, paper [19] can serve as an introduction to this field. Further fields of number theory with important applications include the theory of sequences over finite fields [20]. This theory found an application in the testing of Einstein's general relativity or in testing the global warming of oceans. Furthermore, using methods of elementary number theory, practical problems have been solved concerning to the splicing of telephone cables [21]. Many further interesting applications can be found in the book *Number Theory and the Periodicity of Matter* [3]. Lastly, new attractive applications of the number theory include cryptography, coding theory, and random number generation. With the rise of computers, these fields develop very rapidly with their importance continuously increasing.

ACKNOWLEDGEMENT

The author would like to thank the anonymous referee for carefully reading the manuscript, and for the helpful comments and suggestions.

References

[1] F. C. Auluck, D. S. Kothari, *Statistical mechanics and the partitions of numbers*, Proc. Camb. Phil. Soc. **42** (1946), 272–277.
[2] G. E. Andrews, *The Theory of Partitions*, Cambridge University Press (1998).
[3] J. C. A. Boeyens, D. C. Levendis, *Number Theory and the Periodicity of Matter*, Springer (2008).

[4] N. Bohr, F. Kalckar *On the transmutation of atomic nuclei by impact of material particles. I. General theoretical remarks*, Kgl. Danske Vid. Selskab. Math. Phys. Medd. **14.10** (1937), 1–40.

[5] J. Bond, *Calculating the general solution of a linear Diophantine equation*, American Math. Monthly **74.8** (1967), 955–957.

[6] R. Crocker, *Application of Diophantine equations to problems in chemistry*, Journal of Chemical Education **45.11** (1968), 731–733.

[7] L. Debnath, *Srinivasa Ramanujan (1887 – 1920) and the theory of partitions of numbers and statistical mechanics. A centennial tribute*, Internat. J. Math. and Mat. Sci. **10.4** (1987), 625–640.

[8] M. Goldberg, *A class of multi-symmetric polyhedral*, Tohoku Math. Journal Soc. **43** (1937), 104–108.

[9] D. Greenberger, K. Hentschel, F. Weinert, *Compendium of Quantum Physics*, Springer, (2009).

[10] A. Grytczuk, *Ljunggren's Diophantine problem connected with virus structure*, Annales Mathemticae et Informaticae **33** (2006), 69–75.

[11] A. Grytczuk, K. Grytczuk, *Application of Ljunggren's Diophantine equation to the description of the viruses structure*, International J. of Applied Math. and Applications **2.1** (2010), 35–42.

[12] A. Grytczuk, *On some connections between virology and mathematics*, Vesnik VDU **74.2** (2013), 14–17.

[13] A. Grytczuk, K. Grytczuk, *On some application of the mathematical technics to virology*, Asian Journal of Mathematics and Applications (2013), Article ID ama 0025, 8 pages.

[14] H. Gupta, *A table of partitions*, Proc. London Math. Soc. **39** (1935), 47–53.

[15] G. H. Hardy, S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. (2) **17** (1918), 75–115.

[16] G. H. Hardy, *A Mathematician's Apology*, Cambridge University Press (1940).

[17] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, sixth edition (2008).

[18] J. Klaška, *Partitions, compositions and divisibility*, Ann. Univ. Mariae Curie - Sklodovska, Sect. A **49** (1995), 117–125.

[19] J. Klaška, *Applications of Fibonacci numbers and the golden ratio in physics, chemistry, biology and economy*, 7th Conference on Mathematics and Physics on Technical Universities, Brno (2011), 243–254.

[20] J. Klaška, *Applications of sequences over finite fields*, Mathematics Information Technologies and Applied Sciences, MITAV 2014, Brno (2014) p. 26.

[21] H. P. Lawther Jr., *An application of number theory to the splicing of telephone cables*, Bell System Technical Journal **14.2** (1935), 273–284.

[22] W. Ljunggren, *Diophantine analysis applied to virus structure*, Math. Scand. **34** (1974), 51–57.

[23] V. P. Maslov, *Topological phase transitions in the theory of partitions of integers*, Russian J. Math. Physics **24.2** (2017), 249–260.

[24] Y. V. Matiyasevich, *Hilbert's 10th Problem*, Cambridge, MIT Press (1993).

[25] S. Morito, H. M. Salkin, *Finding the general solution of a linear Diophantine equation*, The Fibonacci Quarterly **17.4** (1979), 361–368.

[26] A. Rovenchak, *Statistical mechanics approach in the counting of integer partitions*, arXiv:1603.01049v1 (2016), 17 pages.

[27] W. Sierpinski, *Elementary Theory of Numbers*, Warszawa (1964).

[28] H. N. V. Temperley, *Statistical mechanics and the partition of numbers. I. The transition of liquid helium*, Proc. R. Soc. London, Series A **199** (1949), 361–375.

[29] C. Van Lier, G. E. Uhlenbeck, *On the statistical calculation of the density of the energy levels of the nuclei*, Physica **4** (1937), 531–542.

[30] G. Xeroudakes, *A Diophantine equation in virus structure*, Math. Scand. **37** (1975), 102–104.

Keywords: number theory, applications, Diophantine equations, partitions, history.

MSC 2010: 00A69, 11D45, 05A17, 01Axx.

APPENDIX: LIST OF AUTHOR'S WORKS

References

[1] J. Klaška, *Partitions, compositions and divisibility*, Ann. Univ. Mariae Curie - Skłodowska, Sect. A **49** (1995), 117–125.
ISSN 0365-1029, MR1400071 (97d:11152), Zbl 0853.05011

[2] J. Klaška, *Partitions and partially ordered sets*, Acta Math. Inform. Univ. Ostrav. **3** (1995), 45–54.
ISSN 1211-4774, MR1474065 (98k:06006), Zbl 0849.06006

[3] J. Klaška, *Transitivity and partial order*, Mathematica Bohemica **122.1** (1997), 75–82.
ISSN 0862-7959, MR1446401 (98c:05006), Zbl 0889.05008

[4] J. Klaška, *History of the number of finite posets*, Acta Univ. M. Belii, Ser. Math. **5** (1997), 73–84.
ISSN 1338-712X, MR1618881 (99k:06001), Zbl 0906.06001

[5] J. Klaška, *The Birkhoff's combinatorial problem of the number of orderings and their history*, Mathematics throughout the ages I (Czech), Prometheus, Hist. Math. **11** (1998), 99–112.
ISBN 80-7196-107-8, MR1907328 (2003g:01033), Zbl 1072.01513

[6] J. Klaška, *Historical milestones in the study of special types of orderings*, Mathematics throughout the ages II (Czech), Prometheus, Hist. Math. **16** (2001), 138–153.
ISBN 80-7196-107-8, MR1890219, Zbl 1274.06001

[7] J. Klaška, *Contribution to the limit and continuity of functions of several variables*, 5. konference o matematice a fyzice na vysokých školách technických s mezinárodní účast, Univerzita obrany (2007), 164–170.
ISBN 978-80-7231-274-0

[8] J. Klaška, *Short remark on Fibonacci-Wieferich primes*, Acta Math. Univ. Ostrav. **15** (2007), 21–25.
ISBN 80-7368-436-5, MR2418779 (2009f:110118), Zbl 1203.11021

[9] J. Klaška, *Criteria for testing Wall's question*, Czechoslovak Math. Journal, **58.4** (2008), 1241–1246.
ISSN 0011-4642, MR2471180 (2010d: 11024), Zbl 1174.11020, IF 0.210

[10] J. Klaška, *Tribonacci modulo p^t*, Math. Bohem. **133.3** (2008), 267–288.
ISSN 0862-7959, MR2494781 (2010a: 11027), Zbl 1174.11021

[11] J. Klaška, *Tribonacci modulo 2^t and 11^t*, Math. Bohem. **133.4** (2008), 377–387.
ISSN 0862-7959, MR2472486 (2009j: 11031), Zbl 1174.11022

[12] J. Klaška, *On Tribonacci-Wieferich primes*, The Fibonacci Quarterly **46/47** (2008/2009), 290–297.
ISSN 0015-0517, MR2589607, Zbl 1214.11026

[13] J. Klaška, *A search for Tribonacci-Wieferich primes*, Acta Math. Univ. Ostrav **16** (2008), 15–20.
ISBN 978-80-7368-454-9, MR2498633 (2010b: 11022), Zbl 1203.11020, IF 0.140

[14] J. Klaška, *Further research of modular periodicity of Tribonacci sequence*, Univ. S. Boh. Dept. of Mathematics Report Series **16.1** (2008), 57–63.
ISSN 1214-4681

[15] J. Klaška, *On the applications of ordered sets*, South Bohemia Mathematical Letters **17.1** (2009), 11–25.
ISBN 978-80-7394-206-9

[16] J. Klaška, *Tribonacci partition formulas modulo m*, Acta Mathematica Sinica, English Series, **26.3** (2010), 465–476.
ISSN 1439-8516, MR2591606 (2011a: 11026), Zbl 1238.11016, IF 0.579

[17] J. Klaška, L. Skula, *The cubic character of the Tribonacci roots*, The Fibonacci Quarterly **48.1** (2010), 21–28.
ISSN 0015-0517, MR2663415, Zbl 1219.11030

[18] J. Klaška, L. Skula, *Periods of the Tribonacci sequence modulo a prime $p \equiv 1 (\mathrm{mod}\ 3)$*, The Fibonacci Quarterly **48.3** (2010), 228–235.
ISSN 0015-0517, MR2722219, Zbl 1217.11020

[19] J. Klaška, L. Skula, *A note on the cubic characters of Tribonacci roots*, The Fibonacci Quarterly **48.4** (2010), 324–326.
ISSN 0015-0517, MR2766780, Zbl 1220.11020

[20] J. Klaška, *Applications of Fibonacci numbers and the golden ratio in physics, chemistry, biology and economy*, 7th Conference on Mathematics and Physics on Technical Universities, Brno (2011), 243–254.
ISBN 978-80-7231-815-5

[21] J. Klaška, L. Skula, *Mordell's equation and the Tribonacci family*, The Fibonacci Quarterly **49.4** (2011), 310–319.
ISSN 0015-0517, MR 2852003, Zbl 1261.11034

[22] J. Klaška, *Applications of sequences over finite fields*, Mathematics Information Technologies and Applied Sciences, MITAV 2014, Brno (2014), p. 26.
ISBN 978-80-7231-961-9

[23] J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the real case*, Utilitas Mathematica, **102** (2017), 39–50.
ISSN 0315-3681, MR 3585552, Zbl 06739952, IF 0.273

[24] J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the imaginary case*, Utilitas Mathematica, **103** (2017), 99–109.
ISSN 0315-3681, MR 3675319, Zbl 06769200, IF 0.273

[25] J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the case of discriminants divisible by three*, Math. Slovaca **66.4** (2016), 1019–1027.
ISSN 0139-9918, MR3567913, Zbl 06662112, IF 0.366

[26] J. Klaška, L. Skula, *Law of inertia for the factorization of cubic polynomials – the case of primes* 2 *and* 3, Math. Slovaca **67.1** (2017), 71–82.
ISSN 0139-9918, MR 3630154, Zbl 06714938, IF 0.366

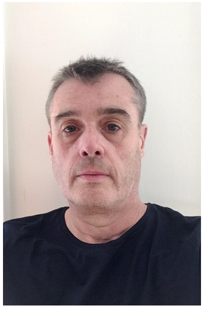
[27] J. Klaška, *Real-world applications of number theory*, to appear in South Bohemia Mathematical Letters **25.1** (2017), 39–47.
ISSN 2336-2081

[28] J. Klaška, *Donald Dines Wall's conjecture*, The Fibonacci Quarterly **56.1** (2018), 43–51.
ISSN 0015-0517

[29] J. Klaška, L. Skula, *On the factorizations of cubic polynomials with the same discriminant modulo a prime*, to appear in Math. Slovaca **68** (2018).
ISSN 0139-9918, IF 0.366

CURRICULUM VITAE

RNDr. Jiří Klaška, Dr.



Personal data

Date and place of birth: March 11^{th}, 1964, Brno
Citizenship: Czech republic
Nationality: Czech
Marital status: unmarried
Domicile: Martinkova 10, 602 00 Brno
E-mail: `klaska@fme.vutbr.cz`

Education and academic qualification

1970 – 1979: Elementary school Merhautova, Brno
1979 – 1983: Secondary school at tř. kpt. Jaroše, Brno
1983 – 1984: BUT Faculty of Mechanical Engineering, study branch: Mechanical Engineering
1984 – 1989: Faculty of Science, Jan Evangelista Purkyně University in Brno, study branch: Mathematical Analysis, degree of RNDr.
1990 – 1991: Study stay at Faculty of Science Masaryk University in Brno
1992 – 1993: Internal doctoral study at Faculty of Science Masaryk University in Brno
1994 – 1996: External doctoral study at the Faculty of Science Masaryk University in Brno, study branch:
Algebra and Number Theory
1996 – 1997: External doctoral study at the Institute of Mathematics BUT Faculty of Mechanical Engineering, academic degree of Dr.

Career overview

1993 – until now: senior lecturer at the Institute of mathematics FME BUT

Pedagogic activities

Teaching at Faculty of Science Masaryk University in Brno:
- seminars: Introduction into Set Theory, Discrete Mathematics, Combinatorics and Graph Theory, Linear Algebra, Mathematical Analysis in $\mathbb{R}$

Teaching at BUT Faculty of Mechanical Engineering:
- seminars: Mathematics I, II, III-B, Numerical Methods I, Combinatorial Analysis
- lectures: Mathematics I, II, II-B, III, Combinatorial Analysis

Author of 2 university textbooks

Scientific activities

- enumerative combinatorics, finite partially ordered sets,
- modular periodicity of integer sequences, Fibonacci numbers with applications,
- cubic polynomials over finite fields

Author or coauthor of 29 scientific papers

Non-University activities

Member of The Fibonacci Association, 2009 – until now