ON THE SOLUTIONS OF CERTAIN CONGRUENCES

SAHAR SIAVASHI
Master of Science, The University of Tehran, 2012

A Thesis
Submitted to the School of Graduate Studies
of the University of Lethbridge
in Partial Fulfillment of the
Requirements for the Degree

MASTER OF SCIENCE

Department of Mathematics and Computer Science
University of Lethbridge
LETHBRIDGE, ALBERTA, CANADA

ON THE SOLUTIONS OF CERTAIN CONGRUENCES

SAHAR SIAVASHI

Date of Defense: March 29, 2017

Dr. Amir Akbary-Majdabadno Supervisor	Professor	Ph.D.
Dr. Hadi Kharaghani Committee Member	Professor	Ph.D.
Dr. Nathan Ng Committee Member	Associate Professor	Ph.D.
Dr. Behnam Seyed-Mahmoud Committee Member	Associate Professor	Ph.D.
Dr. Howard Cheng Chair, Thesis Examination Committee	Associate Professor	Ph.D.

Abstract

We study the solutions of certain congruences in different rings. The congruences include

$$a^{p-1} \equiv 1 \pmod{p^2},$$

for integer $a > 1$ and prime p with $p \nmid a$, and

$$a^{\varphi(m)} \equiv 1 \pmod{m^2},$$

for integer m with $(a,m) = 1$, where φ is Euler's totient function. The solutions of these congruences lead to Wieferich primes and Wieferich numbers. In another direction this thesis explores the extensions of these concepts to other number fields such as quadratic fields of class number one. We also study the solutions of the congruence

$$g^m - g^n \equiv 0 \pmod{f^m - f^n},$$

where m and n are two distinct natural numbers and f and g are two relatively prime polynomials with coefficients in the field of complex numbers.

Acknowledgments

First I would like to thank my supervisor, Prof. Amir Akbary, for his guidance and help throughout the research development and writing the thesis and for his academic support that helped me to grow as a scholar.

Secondly I would like to thank my committee members Prof. Hadi Kharaghani, Prof. Nathan Ng and Prof. Behnam Seyed Mahmoud for their valuable comments and support. I would also like to thank Prof. Howard Cheng for serving as the chair of my defence committee.

Also I would like to thank my office mates Arnab Bose and Forrest Francis for their comments and suggestions about writing the thesis and programming.

Notation

- Throughout this thesis, unless otherwise stated, p is a prime, a, m, and k are integers greater than 1, and x is a positive real number.

- We use the conventional asymptotic notations of analytic number theory. For two real functions f and g, we write $f(x) = \mathrm{O}(g(x))$ or $f(x) \ll g(x)$, if there exists a positive real constant C such that

$$|f(x)| \leq C|g(x)|,$$

for sufficiently large values of x. We write $f(x) = \mathrm{O}_\alpha(g(x))$ or $f(x) \ll_\alpha g(x)$ to denote the dependence of the constant C to the parameter α. We also write $f(x) = \mathrm{o}(g(x))$ if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

By $f(x) \sim g(x)$ as $x \to \infty$ we mean that

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

- By $W_a(x)$ we denote the set of Wieferich primes in base a up to x. More precisely,

$$W_a(x) = \{p \leq x \,;\, a^{p-1} \equiv 1 \pmod{p^2}\}.$$

In the same way we denote the set of non-Wieferich primes up to x, in base a, by $W_a^c(x)$. Also we denote by $W_{a,k}^c(x)$ the set of non-Wieferich primes up to x, in base a, in the arithmetic progressions $p \equiv 1 \pmod{k}$. Moreover, by W_a and W_a^c we mean, respectively, the set of Wieferich primes in base a and the set of non-Wieferich primes

in base a.

- We write $\mathrm{rad}(n)$ to denote the radical of an integer $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, that is defined as

$$\mathrm{rad}(n) = p_1 \cdots p_k.$$

- The quality of a positive integer n is denoted by $\lambda(n)$, that is defined as

$$\lambda(n) = \frac{\log n}{\log \mathrm{rad}(n)}.$$

- For an natural number n, the n-th cyclotomic polynomial, $\Phi_n(x)$, is defined as

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - e^{\frac{2k\pi i}{n}}).$$

- The order of a mod p, denoted $\mathrm{ord}_p(a)$, is the smallest positive integer k for which

$$a^k \equiv 1 \pmod{p}.$$

- By $\varphi(x)$ we denote the Euler-totient function.

- We denote the Euler quotient for two relatively prime integers a and m by $q(a,m)$, which is defined as

$$q(a,m) = \frac{a^{\varphi(m)} - 1}{m}.$$

  For prime m, the Euler quotient is called the Fermat quotient.

- We denote the set of Wieferich numbers up to x, in base a, by $N_a(x)$, which is defined as

$$N_a(x) = \{m \le x \,;\, a^{\varphi(m)} \equiv 1 \pmod{m^2}\}.$$

In the same fashion, we define the set of non-Wieferich numbers up to x, in base a, and denote it by $N_a^c(x)$. Moreover, N_a and N_a^c are the set of Wieferich numbers in base a and the set of non-Wieferich numbers in base a.

- The largest power of p in an integer n is denoted by $\nu_p(n)$.

- A modified form of the Fermat quotient is denoted by $\overline{q}(a,p)$ and is

$$\overline{q}(a,p) = \begin{cases} q(a,p) & \text{if } p \neq 2 \text{ or } p = 2 \text{ and } a \equiv 1 \pmod 4, \\ \frac{a+1}{2} & \text{if } p = 2 \text{ and } a \equiv 3 \pmod 4. \end{cases}$$

- The set S_a is the set of primes generated by primes in W_a. It is defined inductively as follows. Let

$$S_a^{(0)} = \begin{cases} W_a \cup \{2\} & \text{if } \nu_2(\overline{q}(a,2)) \geq 1, \\ W_a & \text{otherwise.} \end{cases}$$

For $i \geq 1$, let

$$S_a^{(i)} = \{p \,;\, p | q-1 \text{ where } q \in S_a^{(i-1)}\}.$$

Then, we define $S_a = \cup_{i=0}^{\infty} S_a^{(i)}$.

- An algebraic number field is denoted by K and its ring of integers by $\mathfrak{O}_K$.

- The norm of an ideal $\mathfrak{a}$ is denoted by $N(\mathfrak{a})$ and is defined it as $|\mathfrak{O}_K/\mathfrak{a}|$.

- By $\langle \pi \rangle$ we mean the ideal generated by π.

- The generalized Euler totient function for an ideal $\mathfrak{a}$ is denoted by $\varphi(\mathfrak{a})$ and is defined as

$$\varphi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

where $\mathfrak{p}$ is a prime ideal divisor of $\mathfrak{a}$.

- We denote the set of K-Wieferich primes in base α with norm not exceeding x by $W_\alpha(K,x)$. It is defined as

$$W_\alpha(K,x) = \{\pi \in \mathfrak{O}_K \ ; \ N(\pi) \leq x \text{ and } \alpha^{N(\pi)-1} \equiv 1 \pmod{\pi^2}\}.$$

- By h_K we denote the class number of a number field K.

- We denote a quadratic field by $\mathbb{Q}(\sqrt{m})$, where m is a square-free integer.

- We write $\mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$ for the Galois group of the extension $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$.

- By $\mathbb{Q}(i)$ we denote the Gaussian rational field which is

$$\mathbb{Q}(i) = \{a+bi \ ; \ a,b \in \mathbb{Q}\}.$$

  We denote its ring of integers by $\mathbb{Z}[i]$ and it is called the Gaussian integers.

- We write $\mathbb{C}[x]$ to denote the ring of polynomials with the coefficients in $\mathbb{C}$.

- If

$$f(x) = \alpha \prod_i (x - \alpha_i),$$

  where $\alpha \in \mathbb{C}$ and α_i's are distinct numbers in $\mathbb{C}$, then we define the radical of f by

$$\mathrm{rad}(f) = \prod_i (x - \alpha_i).$$

- The degree of a polynomial in $\mathbb{C}[x]$ is denoted by $\deg(f)$.

- We write $f^{(i)}(x)$ to denote the i-th derivative of f at x.

Contents

Chapter 1

Introduction and statement of results

1.1 Wieferich primes and Wieferich numbers

The study of primes has fascinated humans from early times. The primes were extensively studied by ancient Greek mathematicians. The fundamental theorem of arithmetic that every integer greater than 1 can be written uniquely as the product of certain primes, is first stated in Euclid's Elements [8]. Some important classes of primes include, primes in arithmetic progressions, Mersenne primes, Wilson primes, and twin primes. A sequence of primes that is of our interest in this thesis is the so-called Wieferich primes. An odd prime p is called a *Wieferich prime* (in base 2), if $2^{p-1} \equiv 1 \pmod{p^2}$. These primes first were considered by Arthur Wieferich in 1909, while he was working on a proof of Fermat's last theorem. Fermat in 1637, in the margin of his copy of Diophantus's *Arithmetica*, stated that the equation $a^n + b^n = c^n$, for $n > 2$, has no integer solutions (a,b,c), with $abc \neq 0$. Despite claiming that he knew the proof, he did not provide it. This statement became famous as Fermat's last theorem. Sophie Germain was one of the mathematicians who had worked on Fermat's last theorem (see [7] for a historical account). She showed that Fermat's last theorem can be divided into two cases and she proved the first case for $p < 100$ (More precisely, the first case is the statement taht the equation $a^p + b^p = c^p$ has no nontrivial solution (a,b,c) where $p \nmid abc$). Fermat's last Theorem, also received the attention of Wieferich. In [26] he proved that if for a prime exponent p the first case of Fermat's last theorem is false then p must satisfy the congruence $2^{p-1} \equiv 1 \pmod{p^2}$. Such primes have became known as Wieferich primes.

The notion of Wieferich prime can be generalized to other bases. More precisely, if $a^{p-1} \equiv 1 \pmod{p^2}$ for a prime p and an integer $a > 1$ with $(a, p) = 1$, then p is called a *Wieferich prime in base a*. The only Wieferich primes in base 2 below 4.97×10^{17} are 1903 and 3511. The sequence of Wieferich primes in base 2 is the sequence A001220 in Sloane's encyclopedia.[1]

It is conjectured that there are infinitely many Wieferich primes in any base. Here we describe a heuristic that gives us an estimate on the size of the set of Wieferich primes up to a given real number x. Let $a > 1$ be a fixed integer, p be a prime number, and $W_a(x)$ be the set of Wieferich primes up to x. By Fermat's little theorem the quotient $(a^{p-1} - 1)/p$ is an integer. This is called the *Fermat quotient*. Under the assumption that the Fermat quotients are uniformly distributed in residue classes, the probability that $(a^{p-1} - 1)/p$ is divisible by p is $1/p$. Thus,

$$|W_a(x)| \approx \sum_{p \leq x} \frac{1}{p} \sim \log\log x.$$

as $x \to \infty$. Thus, $W_a(x) \to \infty$ as $x \to \infty$.

The above argument also shows that the set of Wieferich primes forms a very thin subset of primes, since by the prime number theorem the number of primes below x is asymptotic to $x/\log x$. Hence, the Wieferich primes in a given base are extremely rare. The largest number of known Wieferich primes in a given base a ($2 \leq a \leq 30$) is in bases 5 and 25. There are 7 known Wieferich primes in these two bases. Although it is expected that almost all primes are non-Wieferich, currently it is not known unconditionally that there are infinitely many non-Wieferich primes. The best result in this direction employ some far-reaching number theoretical conjectures.

To explain the work has been done regarding the size of the set of non-Wieferich primes, first we need to explain the *abc*-conjecture. The *abc*-conjecture was proposed by Oesterlé [21] and Masser [15] in 1980's. The conjecture was inspired by a statement related to elliptic curves proposed by Szpiro. The *abc*-conjecture is one of the most powerful conjectures

[1] https://oeis.org/A001220

in number theory due to its important consequences. For instance, it implies Fermat's last theorem for sufficiently large powers. In order to state the conjecture we need to define the notion of the radical of an integer. For a positive integer $n = p_1^{a_1} \cdots p_k^{a_k}$, let the *radical of* n, denoted by $\mathrm{rad}(n)$, be defined as $\mathrm{rad}(n) = p_1 \cdots p_k$. There are several equivalent versions of the *abc*-conjecture. The following is the most common form.

Conjecture 1.1 (**Masser**). Let a, b, and c be such that $a+b=c$ and $(a,b,c)=1$. Then, for $\varepsilon > 0$, we have

$$\max\{|a|,|b|,|c|\} \ll_\varepsilon \mathrm{rad}(abc)^{1+\varepsilon}.$$

Let $W_a^c(x)$ denote the set of non-Wieferich primes in base a, up to x. In 1988, J. Silverman [23] proved the following theorem about the size of the set $W_a^c(x)$.

Theorem 1.2 (**Silverman**). *Under the assumption of the abc-conjecture, we have*

$$|W_a^c(x)| = |\{p\ ;\ p \le x \ \text{ and } \ a^{p-1} \not\equiv 1 \pmod{p^2}\}| \gg_a \log x,$$

as $x \to \infty$.

Following the general approach of the above theorem, H. Graves and M. Ram Murty considered the finer problem regarding the size of the set of non-Wieferich primes in an arithmetic progression. More precisely, let $W_{a,k}^c(x)$ be the set of non-Wieferich primes up to x, in base a, in the arithmetic progression $p \equiv 1 \pmod{k}$ for an integer $k > 1$. The following result is proved in [9].

Theorem 1.3 (**Graves-Murty**). *Let* $k, a > 1$ *be integers. Under the assumption of the abc-conjecture we have*

$$|W_{a,k}^c(x)| = |\{p \ \le x\ ;\ p \equiv 1 \pmod{k} \ \text{ and } \ a^{p-1} \not\equiv 1 \pmod{p^2}\}| \gg_{a,k} \frac{\log x}{\log\log x},$$

as $x \to \infty$

In Chapter 2 we give an improvement of the above theorem.

Theorem 1.4. *Under the assumptions of Theorem 1.3, we have*

$$|W_{a,k}^{c}(x)| \gg_{a,k} \log x,$$

as $x \to \infty$.

In [6], J. De Koninck and N. Doyon showed that one can obtain the result of Theorem 1.2 under an assumption weaker than the *abc*-conjecture. (The main result of [6] is written in base 2, however the method works for any base $a > 1$.) In order to describe their result we need to introduce a new concept. *The quality of an integer n*, denoted $\lambda(n)$, is defined as

$$\lambda(n) = \frac{\log n}{\log \mathrm{rad}(n)}.$$

In [6, Theorem 3] the following result stated.

Theorem 1.5 (**De Koninck-Doyon**). *Let* $0 < \varepsilon < 1$ *be a fixed number such the set*

$$\{n \in \mathbb{N} \,;\, \lambda(2^n - 1) < 2 - \varepsilon\}$$

has density 1. That is,

$$\lim_{x \to \infty} \frac{|\{n \leq x \,;\, \lambda(2^n - 1) < 2 - \varepsilon\}|}{x} = 1.$$

Then,

$$|W_2^c(x)| = |\{p \,;\, p \leq x \text{ and } 2^{p-1} \not\equiv 1 \pmod{p^2}\}| \gg \log x,$$

as $x \to \infty$.

Inspired by the above theorem we prove the result of Theorem 1.4 under an assumption different from the *abc*-conjecture. In order to describe our new assumption we need to

consider the cyclotomic polynomials. The polynomial

$$\Phi_n(x) = \prod_{\substack{1\leq k\leq n\\ \gcd(k,n)=1}} (x - e^{\frac{2k\pi i}{n}})$$

is called the *n-th cyclotomic polynomial*. It is known that $\Phi_n(x) \in \mathbb{Z}[x]$, the ring of polynomials with integer coefficients. Thus, $\Phi_n(a)$ is an integer for $a \in \mathbb{Z}$. We propose the following assumption.

Conjecture 1.6. Let $a \geq 1$ be an integer and $0 < \varepsilon < 1$. Then, there exists an integer $n_0 = n_0(a,\varepsilon)$, such that for $n \geq n_0$ we have

$$\lambda(|\Phi_n(a)|) < 2 - \varepsilon.$$

We have done extensive computations in SAGE to provide evidence for the above conjecture. We have gathered a summary of our experiments in Table A.1. More precisely, we computed $\lambda(|\Phi_n(a)|)$, for n up to 110, for $2 \leq a \leq 20$, and for $21 \leq a \leq 100$ we computed $\lambda(|\Phi_n(a)|)$ for n up to 60. In Table A.1 we have recorded all the cases for which $\lambda(|\Phi_n(a)|) \geq 2$. As it is evident from from Table A.1 in the majority of cases we did not have any outcome. Also for different a, the largest n that $\lambda(|\Phi_n(a)|)$ is equal or greater than 2 is 6. This indicates that for any $a > 1$, when n gets large $\lambda(|\Phi_n(a)|)$ stays smaller than 2.

In Chapter 2 in Proposition 2.13 we will show that under the *abc*-conjecture $\lambda(|\Phi_p(a)|) < 1 + \varepsilon$, for prime p. In other words, the *abc*-conjecture implies Conjecture 1.6, when n is prime.

We prove the following result in Chapter 2.

Theorem 1.7. *Under the assumption of Conjecture 1.6 we have*

$$|W^c_{a,k}(x)| \gg_a \log x.$$

More precisely, for any $\varepsilon > 0$*, we have*

$$|W_{a,k}^{c}(x)| \geq \frac{9\varphi(k)^2}{(\pi k)^4}\left(\frac{1-\varepsilon}{2-\varepsilon}\right)^2\left(1+\mathrm{O}_{a,k}\left(\frac{\log\log x}{\log x}\right)\right)\log_a x,$$

as $x \to \infty$*, where* $\varphi(k)$ *is the Euler totient function.*

One can define the concept of Wieferich numbers in a similar fashion as Wieferich primes. Let $m, a > 1$ be integers with $(a,m) = 1$. By the Euler theorem we have $a^{\varphi(m)} \equiv 1 \pmod{m}$. The integer

$$q(a,m) = \frac{a^{\varphi(m)} - 1}{m} \tag{1.1}$$

is called the *Euler quotient* of m in base a. An integer $m > 1$ is called a *Wieferich number in base a* if $q(a,m) \equiv 0 \pmod{m}$. T. Agoh, K. Dilcher and L. Skula studied Wieferich numbers and developed a criterion that determines them (see [1, Theorem 5.5]). Using this criterion, they showed that Wieferich numbers are closely related to Wieferich primes. For example it can be shown that, if the set of Wieferich primes is finite, then the set of Wieferich numbers is also finite. In [1, Page 47], given the two known Wieferich primes in base 2, all the known Wieferich numbers are determined. There are a total of 104 known Wieferich numbers in base 2. By employing the criterion for Wieferich numbers, W. Banks, F. Luca and I. Shparlinski in [3, Theorem 9] found an upper bound for the number of Wieferich numbers in base 2, given that there are finitely many Wieferich primes. More precisely, let W_2 be the set of Wieferich primes in base 2 and N_2 be the set of Wieferich numbers in base 2. Then the following is Theorem 9 of [3].

Theorem 1.8 (**Banks-Luca-Shparlinski**)**.** *If* W_2 *is a finite set, then* N_2 *is also finite. Moreover, let*

$$M = \prod_{p \leq w_0}(p-1),$$

where w_0 is the largest Wieferich prime in base 2. Then we have

$$\max N_2 \leq 2^{w_0|W_2|}M,$$

where $\max N_2 := \max_{x\in N_2} x$.

Theorem 1.8 can be generalized to any base a. More precisely, let W_a and N_a be the set of Wieferich primes in base a and Wieferich numbers in base a respectively. Then N_a is a finite set if W_a is finite. Moreover, we have

$$\max N_a \leq a^{w_a|W_a|} \prod_{p\leq w_a} (p-1), \tag{1.2}$$

where w_a is the largest Wieferich prime in base a.

In Chapter 2, we find an exact expression for max N_a. To explain our result first we introduce some notations. For a prime p and positive integer n we denote the largest power of p in n by $\nu_p(n)$. Denoting the *Fermat quotient* (i.e. the Euler quotient for $m = p$ prime) by $q(a,p)$ for an integer $a > 1$ and a prime p, for our purpose, we introduce a modified version of it as follows.

$$\overline{q}(a,p) = \begin{cases} q(a,p) & \text{if } p \neq 2 \text{ or } p = 2 \text{ and } a \equiv 1 \pmod 4, \\ \frac{a+1}{2} & \text{if } p = 2 \text{ and } a \equiv 3 \pmod 4. \end{cases}$$

Lastly, we define the sequence $S_a^{(n)}$ by the following procedure. Let

$$S_a^{(0)} = \begin{cases} W_a \cup \{2\} & \text{if } \nu_2(\overline{q}(a,2)) \geq 1, \\ W_a & \text{otherwise.} \end{cases}$$

For $i \geq 1$, let

$$S_a^{(i)} = \{p;\ p|q-1, \text{ where } q \in S_a^{(i-1)}\}.$$

Let $S_a = \bigcup_{i=0}^{\infty} S_a^{(i)}$. We call S_a *the set of primes generated by the set of primes in* W_a. In Chapter 2 (Lemma 2.20) we prove that every prime divisor of a Wieferich number in base a, is in S_a. We use this fact to provide an exact expression for $\max N_a$.

Theorem 1.9. *If W_a is a finite set, then N_a is also finite. Moreover, we have*

$$\begin{aligned}\max N_a &= \prod_{\substack{p\in S_a\\ p\nmid a}} p^{\nu_p(M)+\nu_p(\overline{q}(a,p))}\\ &= \prod_{p\in S_a^{(0)}} p^{\nu_p(M)+\nu_p(\overline{q}(a,p))} \prod_{\substack{p\in S_a\setminus S_a^{(0)}\\ p\nmid a}} p^{\nu_p(M)},\end{aligned}$$

where $M = \prod_{\substack{p\in S_a\\ p\nmid a}}(p-1)$.

By employing the above theorem, we calculated the largest known Wieferich numbers in different bases, using the known Wieferich primes in each base. We collected our results in Table A.2. We wrote a program in MAPLE to produce the maximum element of the set N_a for any base a from 2 to 30. In some bases the known Wieferich primes are too large and thus we could not compute $\nu_p(a^{p-1}-1)$. Because of this we were not able to compute the largest known Wieferich numbers in these bases. Therefore, we did not include those bases in the table.

By a rough heuristic like the one for the number of Wieferich primes, we can find a possible bound on the size of the set of Wieferich numbers. More precisely, let

$$N_a(x) = \{m \le x \,;\, a^{\varphi(m)} \equiv 1 \pmod{m^2}\}.$$

Then, if we assume that the Euler quotients are uniformly distributed in residue classes mod an integer m, then the probability that an Euler quotient falls into the residue class zero mod

m is $1/m$. Hence,

$$|N_a(x)| \approx \sum_{m \leq x} \frac{1}{m} \sim \log x, \tag{1.3}$$

as $x \to \infty$. Thus, it is expected that $|N_a(x)| \to \infty$ as $x \to \infty$.

Based on the heuristic described before for the size of the set of Wieferich primes, we present a conditional result for the size of the set of Wieferich numbers in any base.

Theorem 1.10. *If*

$$c_a \log\log x \leq |W_a(x)| \leq d_a \log\log x,$$

then

$$|N_a(x)| \geq (\log x)^{c_a \log 2 + o(1)} - 1,$$

where c_a and d_a are positive constants.

The case $a = 2$ of the above result (without the upper bound assumption on $|W_2(x)|$) is Theorem 8 of [3]. W. Banks, F. Luca and I. Shparlinski in [3] also obtained an unconditional lower bound, for the set of non-Wieferich numbers in base 2, denoted by $N_2^c(x)$. We generalize Theorem 5 of [3] to any base $a > 1$. Our proof of the following theorem follows closely the base 2 proof, although our O-term in the lower bound is different from the one in Theorem 5 of [3].

Theorem 1.11. *We have*

$$|N_a^c(x)| \geq x \exp\left(-2(\log a)^{1/2}(\log\log x)^{1/2} + \mathrm{O}(\log\log\log x)\right).$$

1.2 Wieferich primes and Wieferich numbers in number fields

Before we define the concept of a Wieferich prime in a number field, we need to present some notations and definitions. For $\theta \in \mathbb{C}$, let $K = \mathbb{Q}(\theta)$ be a number field of degree n with the ring of integer $\mathfrak{O}_K$. We define the congruence modulo an ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ as follows. Let

$\alpha, \beta \in \mathfrak{O}_K$ be two arbitrary elements. We write $\alpha \equiv \beta \pmod{\mathfrak{O}_K}$ if and only if $\alpha - \beta \in \mathfrak{O}_K$. Moreover, the norm of an ideal $\mathfrak{a}$ is defined as

$$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|.$$

One can define the prime ideal as follows. Let $\mathfrak{a} \neq \mathfrak{O}_K$ and $\mathfrak{b}, \mathfrak{c}$ be three ideals in $\mathfrak{O}_K$. Then $\mathfrak{a}$ is a *prime ideal* if $\mathfrak{bc} \subseteq \mathfrak{a}$ implies $\mathfrak{b} \subseteq \mathfrak{a}$ or $\mathfrak{c} \subseteq \mathfrak{a}$. It can be shown [24, Theorem 5.5] that every non-zero ideal I can be written uniquely as a product of prime ideals.

We define the generalized Euler totient function for an ideal $\mathfrak{a}$ in a number field $\mathfrak{O}_K$ as

$$\varphi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

where $\mathfrak{p}$ is a prime divisor of $\mathfrak{a}$.

If $\gcd(\langle\alpha\rangle, \mathfrak{a}) = 1$ where $\langle\alpha\rangle$ is the ideal generated by α, it is known that

$$\alpha^{\varphi(\mathfrak{a})} \equiv 1 \pmod{\mathfrak{a}} \tag{1.4}$$

(see [19, Theorem 1.19] for a proof).

An element $\pi \in K$ is called *prime* if $\pi|\alpha\beta$ then $\pi|\alpha$ or $\pi|\beta$. It is straightforward to show that if π is a prime element then $\langle\pi\rangle$ is a prime ideal. For a prime element $\pi \in \mathfrak{O}_K$ such that $(\langle\pi\rangle, \langle\alpha\rangle) = 1$, by (1.4), we have

$$\alpha^{\varphi(\langle\pi\rangle)} = \alpha^{N(\langle\pi\rangle)-1} \equiv 1 \pmod{\langle\pi\rangle}.$$

We call $\pi \in \mathfrak{O}_K$ a *K- Wieferich prime in base* $\alpha \in \mathfrak{O}_K$ if $\pi \nmid \alpha$ and

$$\alpha^{N(\langle\pi\rangle)-1} \equiv 1 \pmod{\langle\pi^2\rangle}. \tag{1.5}$$

Observe that if π is a K-Wieferich prime in a base α, then $\varepsilon\pi$, for a unit $\varepsilon \in \mathfrak{O}_K$, is also a Wieferich prime in base α. Thus, from now on we consider Wieferich primes up to units. Note that (1.5) holds if and only if

$$\pi^2 | \alpha^{N(\langle\pi\rangle)-1} - 1.$$

For simplicity from now on we denote $N(\langle\pi\rangle)$ by $N(\pi)$ and we write (1.5) as

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi^2}.$$

Let

$$W_\alpha(K,x) = \{\pi \in \mathfrak{O}_K \ ; \ N(\pi) \leq x \text{ and } \alpha^{N(\pi)-1} \equiv 1 \pmod{\pi^2}\},$$

be the set of K-Wieferich primes in base α with norm not exceeding x. A heuristic argument similar to the one described for the case $K = \mathbb{Q}$ implies that

$$|W_\alpha(K,x)| \approx \sum_{N(\pi)\leq x} \frac{1}{N(\pi)},$$

as $x \to \infty$. If $\mathfrak{O}_K$ is a principal ideal domain, then

$$\sum_{N(\pi)\leq x} \frac{1}{N(\pi)} \sim \log\log x,$$

as $x \to \infty$. (See [22] for the asymptotic relation) Thus, in this case it is expected that

$$|W_\alpha(K,x)| \approx \log\log x,$$

as $x \to \infty$.

Example 1.12. For $K = \mathbb{Q}(i)$, the only K-Wieferich primes in base $1+i$ of norm not exceeding 4000 are $33-2i$ and $33+2i$. Also the only K-Wieferich primes in base $1+2i$ of

norm not exceeding 4000 are $1-4i, -15-4i$, and $-19-10i$. In Table A.2 we present K-Wieferich primes in $\mathbb{Q}(i)$ for some different bases. Our search for K-Wieferich primes include the following steps. Using MAPLE we first find all the primes with norms not exceeding 4000. Then for a fixed base we check whether or not these primes are K-Wieferich primes in that base. We order these bases based on their norm in $\mathbb{Q}(i)$. We considered all the norms up to 30. Note that based on Fermat's theorem on sums of two squares, some integers can not be written as the sum of two squares. Thus, for some specific integers a we can not find any element in $\mathbb{Q}(i)$ that have norm equal to a. If we could not find a K-Wieferich prime in the above specified ranges we denoted it by * in Table A.2. Also note that since $(-1)^{N(\pi)-1} \equiv 1 \pmod{\pi^2}$ for any π with $N(\pi) \neq 2$, if π is a K-Wieferich prime in base $\alpha \in \mathbb{Q}(i)$ then it is a K-Wieferich prime in base $-\alpha$ too. Thus, in Table A.2 for any base α we did not write the base $-\alpha$.

One may ask whether the known results for $W_a^c(x)$ can be generalized to the case of $W_\alpha^c(K,x)$. Since the best known results for $K=\mathbb{Q}$ is conditional to the *abc*-conjecture, we expect that the analogue result are conditional too. For generalizations of the *abc*-conjecture to the number fields see [10, Page 285].

Let $\sigma_1 = id, \sigma_2, \cdots, \sigma_n$ be the n monomorphisms from the degree n number field K to $\mathbb{Q}$. For $\alpha \in \mathfrak{O}_K$, we call $\sigma_i(\alpha)$ a conjugate of α. We know that $N(\alpha) = |\sigma_1(\alpha)\cdots\sigma_n(\alpha)|$ (see [24, Page 54]). Also note that for a unit ε we have $N(\varepsilon) = 1$.

The following result is proved in [12, Theorem 2].

Theorem 1.13 (**Kotyada-Muthukrishnan**). *Suppose that* $|\sigma_1(\varepsilon)| > 1$ *and* $|\sigma_j(\varepsilon)| < 1$ *for all* $j \neq 1$, *where* ε *is a fixed unit of* $\mathfrak{O}_K$. *Under the assumption of the abc-conjecture for* K, *there are infinitely many non-*K*-Wieferich primes in base* ε.

For a description of the *abc*-conjecture for K see [10, Section 3]. Note that by [17, Lemma 8.1.5(b)] in any degree n number field, there exists a unit ε such that $|\sigma_1(\varepsilon)| > 1$ and $|\sigma_j(\varepsilon)| < 1$ for all $1 < j \leq n$. Moreover, if $K = \mathbb{Q}(\sqrt{m})$ real quadratic field and $\varepsilon \in \mathfrak{O}_K$

is a unit such that $|\sigma_1(\varepsilon)| > 1$, then $|\sigma_2(\varepsilon)| < 1$. In order to show this let $\varepsilon = a + b\sqrt{m}$, with $|\sigma_1(\varepsilon)| > 1$. Note that

$$N(\sigma_1(\varepsilon)) = |\sigma_1(\varepsilon)\sigma_2(\varepsilon)| = |a^2 - mb^2| = 1.$$

Thus, if $|\sigma_1(\varepsilon)| > 1$, then $|\sigma_2(\varepsilon)| < 1$. So we have the following corollary of the above theorem, which is [12, Theorem 1].

Corollary 1.14 (**Kotyada-Muthukrishna**). *Let $K = \mathbb{Q}(\sqrt{m})$. Let $\varepsilon \in \mathfrak{O}_K$ be a unit such that $|\varepsilon| > 1$. Then under the assumption of the abc-conjecture for K, there are infinitely many non-K-Wieferich primes in base ε.*

To explain our work in Chapter 2 regarding K-Wieferich primes, first we present the definition of the class group and the class number of a number field. To this aim, we present some notions. An $\mathfrak{O}_K$-submodule $\mathfrak{a}$ of K is called a *fractional ideal* of $\mathfrak{O}_K$, if there exists $0 \neq c \in \mathfrak{O}_K$ such that $\mathfrak{a} = c^{-1}\mathfrak{b}$ for some ideal $\mathfrak{b}$ of $\mathfrak{O}_K$. It is known that the non-zero fractional ideals of $\mathfrak{O}_K$ form an abelian group under multiplication (see [24, Theorem 5.4]). We denote this group by $\mathcal{F}_K$. A fractional ideal $\mathfrak{a}$ is called *principal* if $\mathfrak{a} = c^{-1}\mathfrak{b}$ for some principal ideal $\mathfrak{b}$ of $\mathfrak{O}_K$. Denoting the set of principal fractional ideals by $\mathcal{P}_K$, we have that $\mathcal{P}_K$ is a subgroup of $\mathcal{F}_K$. The quotient group $\mathcal{F}_K/\mathcal{P}_K$ is called the class group of K. It can be shown that this group is finite (see [24, Theorem 9.7]). The cardinality of the class group of K is called the class number of K and is denoted by h_K.

In Chapter 2 we prove an unconditional result on the relation between Wieferich primes in an integer base a an K-Wieferich primes in base a when K is a real quadratic field of class number 1. By [24, Theorem 9.1] a number field has class number one if and only if it is a principal ideal domain.

It is known that in a degree n algebraic number field K any ideal in $\mathfrak{O}_K$ generated by a rational prime can be written uniquely as the product of at most n prime ideals of $\mathfrak{O}_K$ (see [19, Theorem 4.5]). Thus if K is a quadratic field, then for any prime integer p we have one

of the following three possibilities.

(i) We have $p\mathfrak{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1 \neq \mathfrak{p}_2$ are prime ideals of $\mathfrak{O}_K$. In this case we say that p is a *split prime.* Let $\mathfrak{p}_1 = \langle \pi_1 \rangle$. Then π_1 is called a prime of $\mathfrak{O}_K$ *above the split prime* p. One can show that $N(\pi_1) = p$. Moreover, if $p\mathfrak{O}_K = \langle \pi_1 \rangle \langle \pi_2 \rangle$ and $\sigma_2 : K \to K$ is the nontrivial monomorphisms, then $\sigma_2(\pi_1) = \varepsilon\pi_2$ for a unit $\varepsilon \in \mathfrak{O}_K$.

(ii) We have $p\mathfrak{O}_K$ is a prime ideal of $\mathfrak{O}_K$. In this case we say that p is *an inert prime.* Let $p\mathfrak{O}_K = \langle \pi \rangle$. Then π is called a prime of $\mathfrak{O}_K$ *above the inert prime* p. In this case we have $N(\pi) = p^2$.

(iii) We have $p\mathfrak{O}_K = \mathfrak{p}^2$, where $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_K$. In this case we say that p is a *ramified prime.* Let $\mathfrak{p} = \langle \pi \rangle$. Then π is called a prime of $\mathfrak{O}_K$ *above the ramified prime* p. In this case we have $N(\pi) = p$.

Having established our terminology we can state our theorem on the relation between $\mathbb{Q}$-Wieferich primes and $\mathbb{Q}(\sqrt{m})$-Wieferich primes in an integer based a.

Theorem 1.15. *Let $K = \mathbb{Q}(\sqrt{m})$ with $h_K = 1$. Then the following assertions hold.*

(i) *Any prime of $\mathfrak{O}_K$ above a Wieferich prime p in an integer base a is a K-Wieferich prime in base a.*

(ii) *If π is a K-Wieferich prime in an integer base a above a split prime p, then p is a Wieferich prime in base a.*

We observe that by employing the result of Theorem 1.4 and the above theorem we can show for $K = \mathbb{Q}(i)$, that under the assumption of the *abc*-conjecture there are infinitely many non-K-Wieferich primes in an integer base a. More precisely, we prove the following.

Corollary 1.16. *Let $K = \mathbb{Q}(i)$, and $a > 1$ be an integer. Assuming the abc-conjecture we have*

$$|\{\textit{prime } \pi \in \mathbb{Z}[i] \,;\, N(\pi) \leq x \;\textit{ and }\; a^{N(\pi)-1} \not\equiv 1 \pmod{\pi^2}\}| \gg_a \log x.$$

Analogous to the concept of Wieferich numbers we can define the concept of K-Wieferich numbers in an algebraic number field K. An algebraic integer $\gamma \in \mathfrak{O}_K$ is called a *K-Wieferich*

number in base $\alpha \in \mathfrak{O}_K$ if $(\langle\gamma\rangle, \langle\alpha\rangle) = 1$ and

$$\alpha^{\varphi(\langle\gamma\rangle)} \equiv 1 \pmod{\langle\gamma^2\rangle}. \tag{1.6}$$

From now on for simplicity we denote $\varphi(\langle\gamma\rangle)$ by $\varphi(\gamma)$. Observe that (3.2) holds if and only if

$$\gamma^2 | \alpha^{\varphi(\gamma)} - 1.$$

Thus (1.6) can be written as

$$\alpha^{\varphi(\gamma)} \equiv 1 \pmod{\gamma^2}.$$

Next we define two notations. Let $\gamma \in \mathfrak{O}_K$, and $\pi \in \mathfrak{O}_K$ be one of its divisors. By $\nu_\pi(\gamma)$ we denote the largest power of π in γ. Moreover, let $\alpha \in \mathfrak{O}_K$. Similar to the integer case we consider the Euler quotient $(\alpha^{\varphi(\gamma)} - 1)/\gamma$ of γ in base α and we denote it by $q(\alpha, \gamma)$.

In [1, Theorem 5.5], T. Agoh, K. Dilcher, and L. Skula presented a criterion for Wieferich numbers. Analogously we prove the following result for K-Wieferich numbers in the case that K is a quadratic field of class number one.

Theorem 1.17. *Let $K = \mathbb{Q}(\sqrt{m})$ with $h_K = 1$. Let $\gamma = \pi_1^{a_1} \cdots \pi_\ell^{a_\ell} \in \mathfrak{O}_K$, where π_i's are primes above split or odd inert primes. Also let $\alpha \in \mathfrak{O}_K$ and $(\alpha, \gamma) = 1$. Then γ is a K-Wieferich number in base α if and only if π_i's satisfy the following conditions :*
(i) If π_i is a prime above an odd split prime p or if π_i is a prime above the split prime $p = 2$ and $\alpha \equiv 1 \pmod{\pi_i^2}$, then

$$a_i \leq \nu_{\pi_i}(\prod_{\pi|\gamma}(N(\pi) - 1)) + \nu_{\pi_i}(q(\alpha, \pi_i)).$$

(ii) If π_i is a prime above the split prime $p = 2$ and $\alpha \equiv 1 + \pi_i \pmod{\pi_i^2}$, then

$$a_i \leq \nu_{\pi_i}(\prod_{\pi|\gamma}(N(\pi) - 1)) + \nu_{\pi_i}(\alpha^{N(\pi_i)-1}) + 1) - 1.$$

(iii) *If π_i is a prime above an odd inert prime p, then*

$$2\nu_{\pi_i}(\prod_{\pi|\gamma}(N(\pi)-1))+\nu_{\pi_i}(q(\alpha,\pi_i))\geq 1$$

Note that the result of the above theorem remains the same if we consider another factorization of γ to product of primes. Observe that since $h_K = 1$, the prime factorization is unique up to units.

Recall that for ordinary integers it is not known that whether or not there are infinitely many Wieferich numbers. However by part (iii) of the above theorem we can show that there are infinitely many K-Wieferich numbers in certain bases, when $K = \mathbb{Q}(i)$. More precisely, if for a prime π above an odd inert prime, $\pi^a\omega$ is a K-Wieferich number in base α, then by part (iii) of Theorem 3.6, $\pi^{am}\omega$, for any integer $m \geq 1$, are K-Wieferich numbers. In such case the set of K-Wieferich numbers are infinite. For example we have the following.

Corollary 1.18. *There are infinitely many $\mathbb{Q}(i)$-Wieferich numbers in base $1+i$.*

Using this fact, in Table A.4 we present some examples of base α in which there are infinitely many K-Wieferich numbers in base α in $K = \mathbb{Q}(i)$. Moreover, in each base we present a Wieferich number which has an inert prime as a divisor.

As an application of Theorem 1.17 we prove an analogous of [1, Theorem 5.5] for the quadratic fields, which indicates that any prime divisor of maximum norm of certain K-Wieferich numbers are K-Wieferich primes.

Theorem 1.19. *Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field with $h_K = 1$. Let $\gamma = \pi_1^{a_1}\cdots\pi_k^{a_k} \in \mathfrak{O}_K$ be such that π_i, for $1 \leq i \leq k$, is a prime above an odd inert or on odd split prime p. Consider the set*

$$\Pi(\gamma) = \{\pi_i \ ; \ 1 \leq i \leq k \text{ and } \pi_i \text{ has the maximum norm among the prime divisors of } \gamma\}.$$

If γ is a K-Wieferich number in base $\alpha \in \mathfrak{O}_K$, then any $\pi_i \in \Pi(\gamma)$ that is above an odd split

prime, is a K-Wieferich prime in base α.

1.3 An exponential congruence in $\mathbb{C}[x]$

Let

$$\mathbb{C}[x] = \{f(x) = a_0 + a_1x + \cdots + a_nx^n \ ; \ a_i \in \mathbb{C} \text{ and } n \in \mathbb{N}\}$$

be the ring of polynomials with coefficients in the set of complex numbers $\mathbb{C}$. It is known that $\mathbb{C}[x]$ is a Euclidean domain, and consequently it is a principal ideal domain, and thus it is a unique factorization domain. Unlike the case of algebraic number fields analogies of Fermat's little theorem and Euler's theorem do not hold in the ring $\mathbb{C}[x]$. More precisely, for any prime ideal $\langle x-\alpha\rangle$ where $\alpha \in \mathbb{C}$ we have

$$\frac{\mathbb{C}[x]}{\langle x-\alpha\rangle} \cong \mathbb{C}.$$

Thus, we can not define norm of such ideals, since, the above quotient is infinite. Thus, we cannot generalize the concepts of Wieferich primes and Wieferich numbers to $\mathbb{C}[x]$. Instead in the final Chapter of this thesis, we study in $\mathbb{C}[x]$ an exponential congruence different from Wieferich congruences.

In 2011 M. Ram Murty and V. Kumar Murty [18] proved the following.

Theorem 1.20 (**Murty-Murty**). *There are only finitely many pairs* (m,n), *with* $m,n \geq 0 \in \mathbb{Z}$, *such that* $2^m - 2^n | 3^m - 3^n$.

This theorem originated from a problem proposed by Ruderman in 1974.

Problem 1.21 (**Ruderman**). *Let* $m > n \geq 0 \in \mathbb{Z}$, *such that* $2^m - 2^n | 3^m - 3^n$. *Then* $2^m - 2^n | x^m - x^n$, *for all natural numbers* x.

This problem has not been solved yet. In Chapter 3 we will find an analogue of Theorem 1.20 for polynomials in $\mathbb{C}[x]$.

Theorem 1.22. *Let $f,g \in \mathbb{C}[x]$, be two relatively prime polynomials with $\deg f \leq \deg g$. Then, there are only finitely many pairs (m,n), where $m > n \geq 0$, such that*

$$f^m - f^n | g^m - g^n. \tag{1.7}$$

One of the main ingredients of our proof is an upper bound for the degree of the greatest common divisor of $f^n - 1$ and $g^n - 1$, due to N. Ailon and Z. Rudnick [2, Theorem 1].

Theorem 1.23 (**Ailon-Rudnick**). *Let $f,g \in \mathbb{C}[x]$ be two multiplicatively independent polynomials. Then there exists an absolute constant, depending only on f and g, such that*

$$\deg(\gcd(f^n - 1, g^n - 1)) < C(f,g). \tag{1.8}$$

Unfortunately due to ineffectiveness of the upper bound in (1.8), our proof of Theorem 1.22 is ineffective. In other words given f and g in Theorem 1.22 we cannot explicitly write down all the possible solutions (m,n) of the congruence

$$f^m - f^n \equiv 0 \pmod{g^m - g^n}.$$

In order to remedy this situation, we employ a theorem due to Mason and following the ideas of [18], we prove an effective result related to Theorem 1.22.

Theorem 1.24. *Let $f,g \in \mathbb{C}[x]$ be two relatively prime polynomials with $\deg f \leq \deg g$. For a natural number k we have*

$$\deg(\gcd(f^k - 1, g^k - 1)) < \frac{k+2}{2} \deg g.$$

Using this theorem we find an explicit bound for $m - n$, where (m,n) is a solution of (1.7). In certain cases this enables us to find all pairs satisfying (1.7). More precisely, using the following theorem we can effectively solve the congruence (1.7) for such cases.

Theorem 1.25. *Let f and g be two polynomials in $\mathbb{C}[x]$ which are relatively prime and*

$$\frac{1}{2}\deg g < \deg f \leq \deg g.$$

If $m > n \geq 0$ be such that

$$f^m - f^n | g^m - g^n,$$

then we have

$$n < \frac{(\deg g + \deg(\mathrm{rad}(g))\deg f)\deg g}{(\deg f - \frac{1}{2}\deg g)\deg f}$$

and

$$m < \frac{\deg g + \deg(\mathrm{rad}(g))\deg f}{\deg f - \frac{1}{2}\deg g}\left(1 + \frac{\deg g}{\deg f}\right).$$

In the above theorem $\mathrm{rad}(g) = \prod_i (x - \alpha_i)$ if $g = \alpha \prod_i (x - \alpha_i)^{n_i}$ for $\alpha, \alpha_i \in \mathbb{C}$ and $n_i \in \mathbb{N}$, where α_i's are distinct. By employing Theorem 1.25 we have found all the pairs (m,n) for given polynomials $f, g \in \mathbb{Z}[x]$ of degrees less than 6 and with coefficients in $\mathbb{N} \cap [1,5]$, such that $\gcd(f,g) = 1$ and $f^m - f^n | g^m - g^n$. We recorded the cases with the only solution $(2,0)$ in Table A.5.

Chapter 2

Wieferich primes and Wieferich numbers

Recall that

$$W_{a,k}^{c}(x) = \{p \leq x;\ p \equiv 1 \pmod{k} \text{ and } a^{p-1} \not\equiv 1 \pmod{p^2}\}$$

is the set of non-Wieferich primes up to x, in the congruence class 1 mod k. Our first goal in this chapter is to give an improvement to the lower bound of Graves and Murty [9] for the size of the set $W_{a,k}^{c}(x)$.

2.1 An improvement of Graves-Murty lower bound

Here we describe an argument that improves the lower bound in the Graves-Murty result,

$$|W_{a,k}^{c}(x)| \gg_{a,k} \frac{\log x}{\log\log x},$$

to $\log x$. To start recall the common form of the *abc*-conjecture.

Conjecture 2.1 (**Masser**). Let a, b and c be such that $a+b=c$ and $(a,b,c)=1$. Then, for $\varepsilon > 0$, we have

$$\max\{|a|,|b|,|c|\} \ll_{\varepsilon} \mathrm{rad}(abc)^{1+\varepsilon}.$$

Under the assumption of the *abc*-conjecture we prove the following theorem.

Theorem 2.2. *Let $a > 1$ be a fixed non-zero integer. If the abc-conjecture is true, then we have*

$$|W_{a,k}^{c}(x)| \gg_{a,k} \log x,$$

as $x \to \infty$.

In order to prove this theorem, we need to set up our notation and state some lemmas. Let *the powerful part of n* be defined as

$$n_1 = \prod_{\nu_p(n)\geq 2} p^{\nu_p(n)}.$$

We call n/n_1 *the squarefree part* of the integer n. Every integer can be written uniquely as the product of its powerful part and its squarefree part.

Recall that

$$\Phi_n(x) = \prod_{\substack{1\leq k\leq n\\ \gcd(k,n)=1}} (x - e^{\frac{2k\pi i}{n}})$$

is *the n-th cyclotomic polynomial*. It can be shown that

$$\prod_{d|n} \Phi_d(x) = x^n - 1, \tag{2.1}$$

(see [14, Page 279] for a proof). For an integer $a > 1$ we write $U_n = \Phi_n(a)/V_n$ where V_n is the powerful part of $\Phi_n(a)$. Also we write $a^n - 1 = u_n v_n$, where u_n and v_n are powerful and squarefree part of $a^n - 1$. The next three lemmas give us information about the relation of the primes dividing U_{kn} with the set $W_{a,k}^{c}(x)$, which state that most of prime divisors of U_{kn} are in the set $W_{a,k}^{c}(x)$.

Lemma 2.3. *If $p \mid \Phi_n(a)$, then either $p \mid n$ or $p \equiv 1 \pmod{n}$.*

Proof. Suppose that p is a prime divisor of $\Phi_n(a)$ and $p \nmid n$. Since $p \mid \Phi_n(a)$ then

$$p \mid \prod_{d|n} \Phi_d(a) = a^n - 1.$$

Thus we have $a^n \equiv 1 \pmod{p}$. Hence, $\mathrm{ord}_p(a) \mid n$ (Note that $\mathrm{ord}_p(a)$ is the least non-negative integer k such that $a^k \equiv 1 \pmod{p}$). We claim that $\mathrm{ord}_p(a) = n$. Let $f = \mathrm{ord}_p(a)$, and $f < n$. Then we have $a^f \equiv 1 \pmod{p}$. This yields

$$p \mid a^f - 1 = \prod_{d \mid f} \Phi_d(a),$$

where the equality follows from (2.1). Therefore there exists $d_0 < n$ such that $d_0 \mid f$ and $p \mid \Phi_{d_0}(a)$. Moreover, $p \mid \Phi_n(a)$ and

$$a^n - 1 = \prod_{d \mid n} \Phi_d(a).$$

Thus we can conclude that $x^n - 1$ has a zero of order at least 2 in $\mathbb{Z}_p$, the integers mod p. However, since $p \nmid n$ we have $(x^n - 1, nx^{n-1}) = 1$ in $\mathbb{Z}_p[x]$. So $x^n - 1$ cannot have a multiple root. Thus $\mathrm{ord}_p(a) = n$. Therefore, we have $n \mid p - 1$ or equivalently $p \equiv 1 \pmod{n}$. □

Lemma 2.4. *If $p \nmid n$ and $p \mid U_n$, then* $\mathrm{ord}_p(a) = n$.

Proof. Since $p \mid U_n$, we have $p \mid \Phi_n(a)$. Since $p \nmid n$, from Lemma 2.3 we have $\mathrm{ord}_p(a) = n$. □

Lemma 2.5. *If $p \mid u_n$, then $a^{p-1} \not\equiv 1 \pmod{p^2}$.*

Proof. The proof is given in [23, Lemma 3]. We reproduce it here for completion. Since $a^{p-1} \equiv 1 \pmod{p}$, we have $\mathrm{ord}_p(a) \mid p - 1$. So we can write $a^{\mathrm{ord}_p(a)} = 1 + pt$, for some positive integer t. Since $p \mid u_n$ and u_n is the squarefree part of $a^n - 1$, we have $p^2 \nmid a^n - 1$. Thus $p \nmid t$. Therefore, we have

$$a^{p-1} = \left(a^{\mathrm{ord}_p(a)}\right)^{\frac{p-1}{\mathrm{ord}_p(a)}} = (1 + pt)^{\frac{p-1}{\mathrm{ord}_p(a)}} \equiv 1 + \frac{p-1}{\mathrm{ord}_p(a)} pt \pmod{p^2}.$$

Now, we have $p \nmid \frac{p-1}{\mathrm{ord}_p(a)} t$, which yields $a^{p-1} \not\equiv 1 \pmod{p^2}$. □

In the following lemma we find a lower bound for the set $W^c_{a,k}(x)$.

Lemma 2.6. *If $\Phi_{kn}(a) = U_{kn}V_{kn}$, where $k \geq 1$ is an integer, we have*

$$|W^c_{a,k}(x)| \geq |\{n \leq \frac{1}{k}\log_a(x);\ \ |U_{kn}| > akn\}|.$$

Proof. The proof is similar to [23, Lemma 4]. If $|U_{kn}| > akn$, considering the fact that U_{kn} is squarefree, then we can choose a prime p_n that divides U_{kn} but not akn. From Lemma 2.3 we have $p_n \equiv 1 \pmod{k}$. Also by Lemma 2.4 and Lemma 2.5, we have

$$\mathrm{ord}_{p_n}(a) = kn \ \text{ and } \ a^{p_n-1} \not\equiv 1 \pmod{p_n^2}.$$

Moreover, if we have $n \leq \frac{1}{k}\log_a x$, then $p_n \leq |U_{kn}| < a^{kn} \leq x$. Therefore we have

$$\{p_n;\ \ n \leq \frac{1}{k}\log_a x \ \text{ and } \ |U_{kn}| > akn\} \subseteq W^c_{a,k}(x).$$

Furthermore, p_n's are distinct. Since if $p_n = p_m$, then we have

$$kn = \mathrm{ord}_{p_n}(a) = \mathrm{ord}_{p_m}(a) = km.$$

This yields $m = n$. Therefore, we have

$$|W^c_{a,k}(x)| \geq |\{n \leq \frac{1}{k}\log_a(x);\ \ |U_{kn}| > akn\}|.$$

□

Next we prove a modified version of [23, Lemma 6].

Lemma 2.7. *Fix $\delta > 0$. Then*

$$|\{n \leq Y; \varphi(nk) \geq \delta kn\}| \gg Y.$$

Proof. It suffices to prove $\varphi(nk) \geq \varphi(n)\varphi(k)$, since then from [23, Lemma 6] we can con-

clude that

$$|\{n \leq Y : \varphi(n) \geq \frac{\delta kn}{\varphi(k)}\}| \gg Y.$$

To show $\varphi(nk) \geq \varphi(n)\varphi(k)$, suppose that $(n,k) \neq 1$ (otherwise $\varphi(nk) = \varphi(n)\varphi(k)$). Let $n = p_1^{\alpha_1} \cdots p_j^{\alpha_k} S$ and $k = p_1^{\beta_1} \cdots p_j^{\beta_k} T$, where p_i's are distinct primes dividing both n and k, also α_i's and β_i's are positive integers and S and T are integers such that $(S,T) = 1, (S, p_1 \cdots p_k) = (T, p_1 \cdots p_k) = 1$. We have

$$\begin{aligned}\varphi(nk) = \varphi(p_1^{\alpha_1+\beta_1} \cdots p_k^{\alpha_k+\beta_k})\varphi(S)\varphi(T) &= \prod_{i=1}^{j} p_i^{\alpha_i+\beta_i}\left(1-\frac{1}{p_i}\right)\varphi(S)\varphi(T) \\ &\geqslant \prod_{i=1}^{j}(1-\frac{1}{p_i})^2 p_i^{\alpha_i+\beta_i}\varphi(S)\varphi(T) = \varphi(n)\varphi(k).\end{aligned}$$

This gives us the desired result. □

Now we employ the *abc*-conjecture to show that V_n, the powerful part of $\Phi_n(a)$, is small.

Lemma 2.8. *If the abc-conjecture is true, then we have* $V_n \ll_{a,\varepsilon} a^{n\varepsilon}$.

Proof. The proof is from [23, Lemma 7]. We present the proof for v_n, then the result follows, since $V_n \mid v_n$. We have $u_n v_n + 1 = a^n$. Since $\max\{a^n, u_n v_n, 1\} = a^n$, applying the *abc*-conjecture yields

$$a^n \ll_\varepsilon \left(\prod_{p \mid a^n u_n v_n} p\right)^{1+\varepsilon} \ll_\varepsilon c(a)\left(u_n\sqrt{v_n}\right)^{1+\varepsilon},$$

where $c(a)$ is a constant depending only on a. The last inequality holds because for each $p \mid v_n$, we have $p^2 \mid v_n$. Now since we have $a^n < a^n/v_n$, we get

$$a_n \ll \left(\frac{a^n}{\sqrt{v_n}}\right)^{1+\varepsilon}.$$

From here we get $v_n \ll_{a,\varepsilon} a^{2n\varepsilon/(1+\varepsilon)}$. By adjusting ε, we get $v_n \ll_{a,\varepsilon} a^{n\varepsilon}$. □

Finally we use the following lemma due to R. Thangaduri and A. Vatwani [25] to obtain

a lower bound for the value of the n-th cyclotomic polynomial at a given point.

Lemma 2.9. *Let $a > 1$ and $n > 2$ be integers. Then we have*

$$\frac{1}{2}a^{\varphi(n)} \leq |\Phi_n(a)|, \tag{2.2}$$

where $\varphi(n)$ is the Euler totient function.

Proof. [25, Theorem 5]. □

Equipped with all the above ingredients we can now present the proof of Theorem 2.2.

Proof. We have $|U_{nk}| = |\Phi_{nk}(a)|/V_{nk}$. By employing Lemma 2.7 and Lemma 2.2, we have

$$|U_{nk}| \geq \frac{a^{\varphi(nk)}}{ca^{\varepsilon nk}},$$

for some constant c, depending on ε, obtained in the inequality of Lemma 2.8. Observe that if we have

$$(\varphi(nk) - \varepsilon nk)\log a + c_1 \geq \log n,$$

where $c_1 = \log(1/2ck)$, then we will have $|U_{nk}| > akn$. Let $\delta > 0$ be a fixed number and suppose $\varphi(nk) \geq \delta nk$, then we have

$$(\varphi(nk) - \varepsilon nk)\log a + c_1 - \log n > nk\log a(\delta - \varepsilon) - \log n + c_1. \tag{2.3}$$

By choosing $\varepsilon = \delta/2$, the right-hand side of (2.3) will become

$$\frac{1}{2}nc\delta k\log a - \log n + c_1.$$

Thus, there exists a constant $n_1(\delta, c_1, a)$ depending on c_1,δ, and a, such that if $n \geq n_1(\delta, c_1, a)$, then the right-hand side of (2.3) will be positive. Now by applying Lemma 2.7 and Lemma

2.6, we obtain

$$|W_{a,k}^c(x)| \geq |\{n_1(\delta,c_1,a) \leq n \leq \frac{1}{k}\log_a x\ ;\ \ \varphi(nk) \geq \delta nk\}| \geq \frac{c_2}{k}\log_a x - n_1(\delta,c_1,a),$$

where c_2 is the implied constant in Lemma 2.7. Therefore, we have

$$|W_{a,k}^c(x)| \gg_{a,k} \log x,$$

which is the desired assertion. □

2.2 An improvement of Theorem 1.3

In this section we give another proof of the lower bound for $W_{a,k}^c(x)$ in Theorem 2.2 under the assumption of a conjecture on the quality of $\Phi_n(a)$. Recall that

$$\lambda(n) = \frac{\log n}{\log \operatorname{rad} n},$$

is the quality of the integer n. The function $\lambda(n)$ was introduced by Jerzy Browkin [4] in order to present a weaker version of the *abc*-conjecture. We propose the following assumption.

Conjecture 2.10. Let $a > 1$ be an integer. For given $0 < \varepsilon < 1$, there exists integer $n_0 = n_0(a,\varepsilon)$, such that for $n \geq n_0$ we have

$$\lambda(|\Phi_n(a)|) < 2 - \varepsilon,$$

where $\Phi_n(a)$ is the value of the n-th cyclotomic polynomial at a.

Our aim in this section is to show that under the assumption of 2.10 there are at least $c\log_a x$ non-Wieferich primes in base a, where c is a constant. Our approach is analogous to De Koninck and Doyon's proof of Theorem 3 of [6]. As we discussed in the introduction

the new conjecture is a weaker assumption than the *abc*-conjecture in some cases. To justify our claim, we first present another version of the *abc*-conjecture which is proposed by Oesterlé [21] in 1986.

For non-zero integers, a, b and c, let

$$L(a,b,c) = \frac{\log \max\{|a|,|b|,|c|\}}{\log \mathrm{rad}(abc)}.$$

An statement equivalent to Conjecture 2.1 is the following.

Conjecture 2.11 (**Oesterlé**). As (a,b,c) varies over all relatively prime triples (a,b,c) with $a+b=c$, we have

$$\limsup L(a,b,c) \leq 1,$$

The following proposition establishes the equivalence of the two mentioned versions of the *abc*-conjecture.

Proposition 2.12. *Conjecture 2.1 is equivalent to Conjecture 2.11.*

Proof. First of all note that in the following proof whenever we talk about triple (a,b,c) we consider $a+b=c$ with $(a,b,c)=1$. Suppose that Conjecture 2.1 is true. Then we have

$$L(a,b,c) = \frac{\log \max\{|a|,|b|,|c|\}}{\log \mathrm{rad}(abc)} \leq \frac{\log(C(\varepsilon)(\mathrm{rad}(abc))^{1+\varepsilon})}{\log \mathrm{rad}(abc)} = \frac{\log C(\varepsilon)}{\log \mathrm{rad}(abc)} + 1 + \varepsilon,$$

where $C(\varepsilon)$ is a positive constant depending on ε. Now if we have

$$\frac{\log C(\varepsilon)}{\log \mathrm{rad}(abc)} \leq \varepsilon,$$

for a given $\varepsilon > 0$, then we have the desired result. We claim that

$$\mathrm{rad}(abc) \geq M,$$

for all but finitely many triple (a,b,c), where $M = e^{\log C(\varepsilon)/\varepsilon}$. This is true since from [13,

Chapter VI, Theorem 1.1] there are only finitely many triples (a,b,c) such that $\text{rad}(abc) \leq M$.

Assume that Conjecture 2.11 is true. Then for every $\varepsilon > 0$ we have $L(a,b,c) < 1+\varepsilon$, for all triples (a,b,c) except for finitely many of them. Therefore we conclude that

$$\max\{|a|,|b|,|c|\} \leq \text{rad}(abc)^{1+\varepsilon} \tag{2.4}$$

for all triples (a,b,c) except for finitely many of them. We set

$$I = \{(a,b,c)\ ;\ \max\{|a|,|b|,|c|\} > \text{rad}(abc)^{1+\varepsilon}\}.$$

For $(a,b,c) \in I$, let

$$c_\varepsilon = \frac{\max\{|a|,|b|,|c|\}}{\text{rad}(abc)^{1+\varepsilon}}.$$

Now let

$$C(\varepsilon) = \max_{(a,b,c)\in I}\{c(\varepsilon)\}.$$

Note that since I is finite, then $C(\varepsilon)$ is well-defined. Therefore for all triples (a,b,c) we have

$$\max\{|a|,|b|,|c|\} \leq C(\varepsilon)\text{rad}(abc)^{1+\varepsilon}.$$

This completes the proof. □

The following proposition indicates that Conjecture 2.10 is a weaker assumption than the *abc*-conjecture in some cases. Before stating the proposition, note that

$$\Phi_p(a) = \frac{a^p - 1}{a-1},$$

where p is a prime and $a > 1$ is an integer. Thus we have $|\Phi_p(a)| = \Phi_p(a)$, and $|U_p| = U_p$. Hence, in the following proposition we can drop the absolute value.

Proposition 2.13. *Let p be prime and $a > 1$ be an integer. Then Conjecture 2.11 implies that*

$$\lambda(\Phi_p(a)) < 1+\varepsilon,$$

for a given $\varepsilon > 0$ and sufficiently large p.

Proof. We note that $(a^p-1)+1 = a^p$. Thus, by Conjecture 2.11 we have

$$\frac{\log(a^p-1)}{\log \mathrm{rad}(a^p-1)} < 1+\varepsilon, \tag{2.5}$$

for large p. Also we have

$$\mathrm{rad}(a^p-1) - \mathrm{rad}(a-1) \leq \mathrm{rad}\left(\frac{a^p-1}{a-1}\right). \tag{2.6}$$

Thus, by an application of (2.6), we have

$$\begin{aligned}\lambda(\Phi_p(a)) = \frac{\log\left(\frac{a^p-1}{a-1}\right)}{\log \mathrm{rad}\left(\frac{a^p-1}{a-1}\right)} &\leq \frac{\log(a^p-1)-\log(a-1)}{\log\left(\mathrm{rad}(a^p-1)-\mathrm{rad}(a-1)\right)} \\ &= \frac{\log(a^p-1)}{\log \mathrm{rad}(a^p-1)} \frac{\left(1-\frac{\log(a-1)}{\log(a^p-1)}\right)}{\left(1+\frac{\log\left(1-\frac{\mathrm{rad}(a-1)}{\mathrm{rad}(a^p-1)}\right)}{\log \mathrm{rad}(a^p-1)}\right)}. \end{aligned} \tag{2.7}$$

Since $\mathrm{rad}(a^p-1) \to \infty$ as $p \to \infty$ (See [13, Theorem 1.1]), by applying (2.5) in (2.7) as sending p to ∞ we get the desired result. □

We now show that under the assumption of Conjecture 2.10 there are infinitely many non-Wieferich primes $p \equiv 1 \pmod{k}$. Observe that in Lemma 2.8 we used the *abc*-conjecture to obtain a lower bound for squarefree part of $\Phi_n(a)$. The proof of the following Lemma follows the arguments given in Lemma 5 of [6].

Lemma 2.14. *Let $n \geq 1$ and $a > 1$ be integers such that*

$$\lambda(|\Phi_n(a)|) < 2 - \varepsilon, \tag{2.8}$$

for some $0 < \varepsilon < 1$. Then we have

$$\log |U_n| > \varepsilon_0 \log(|\Phi_n(a)|),$$

where U_n is the squarefree part of $\Phi_n(a)$ and $\varepsilon_0 = \frac{2(1-\varepsilon)}{2-\varepsilon}$.

Proof. Recall that $\Phi_n(a) = U_n V_n$, where V_n is the squarefull part of $\Phi_n(a)$. Under the assumption 2.8, we have

$$\begin{aligned} 2 - \varepsilon > \lambda(|\Phi_n(a)|) = \lambda(|U_n|V_n) &= \frac{\log(|U_n|V_n)}{\log \mathrm{rad}(|U_n|V_n)} && (2.9) \\ &= \frac{\log(|U_n|V_n)}{\log(\mathrm{rad}(|U_n|)\mathrm{rad}(V_n))} && (2.10) \\ &> \frac{\log |U_n| + \log V_n}{\log |U_n| + \frac{1}{2}\log V_n}. && (2.11) \end{aligned}$$

Note that (2.9) implies (2.10), since rad is a multiplicative function and $(|U_n|, V_n) = 1$. Also since $\mathrm{rad}(|U_n|) \leq |U_n|$ and $\mathrm{rad}(V_n) \leq \frac{1}{2}V_n$ we obtain (2.11) from (2.10). Hence,

$$2 - \varepsilon > \frac{\log |U_n| \log V_n}{\log |U_n| + \frac{1}{2}\log V_n},$$

and thus,

$$(1-\varepsilon)\log |U_n| > \frac{\varepsilon \log V_n}{2}.$$

By employing the above inequality we deduce

$$\log(|\Phi_n(a)|) = \log |U_n| + \log V_n > \frac{\varepsilon \log V_n}{2(1-\varepsilon)} + \log V_n = \frac{2-\varepsilon}{2(1-\varepsilon)} \log V_n.$$

Thus,

$$\log V_n < \frac{2(1-\varepsilon)}{2-\varepsilon}\log(|\Phi_n(a)|),$$

which is the desired result. □

Note that Lemma 2.14 remain true if we consider logarithm in base a.

Lemma 2.15. *Under the assumption of Conjecture 2.10, we have*

$$\sum_{n\le \log_a x}\sum_{p\|\Phi_n(a)} \log_a p > \frac{3\varepsilon_0}{\pi^2}(\log_a x)^2\left(1+\mathrm{O}_a\left(\frac{\log\log x}{\log x}\right)\right),$$

where ε_0 *is given in Lemma 2.14.*

Proof. Note that $\sum_{p\|\Phi_n(a)} \log_a p = \log|U_n|$. Thus, from Lemma 2.14 and Conjecture 2.10 we have

$$\begin{aligned}\sum_{n\le \log_a x}\sum_{p\|\Phi_n(a)} \log_a p &= \sum_{n\le \log_a x} \log_a |U_n| \\ &\ge \sum_{n\le \log_a x} \varepsilon_0 \log_a(|\Phi_n(a)|).\end{aligned}$$

Applying the inequality (2.2) we have

$$\begin{aligned}\sum_{n\le \log_a x}\sum_{p\|\Phi_n(a)} \log_a p &\ge \sum_{n\le \log_a x} \varepsilon_0 \log_a\left(\frac{a^{\varphi(n)}}{2}\right) \\ &= -\sum_{n\le \log_a x} \varepsilon_0 \log 2 + \sum_{n\le \log_a x} \varepsilon_0\varphi(n) \qquad (2.12)\end{aligned}$$

From [16, Problem 1.4.2] we have

$$\sum_{n\le x}\varphi(n) = \frac{3x^2}{\pi^2} + \mathrm{O}(x\log x).$$

Applying this identity in (2.12) yields

$$\sum_{n\le \log_a x}\sum_{p\|\Phi_n(a)} \log_a p \ge \mathrm{O}(\log x) + \frac{3\varepsilon_0}{\pi^2}(\log_a x)^2 + \mathrm{O}_a((\log x)(\log\log x))$$
$$\ge \frac{3\varepsilon_0}{\pi^2}(\log_a x)^2\left(1+\mathrm{O}_a\left(\frac{\log\log x}{\log x}\right)\right).$$

□

Theorem 2.16. *Under the assumption of Conjecture 2.10 for* $0<\varepsilon<1$, *we have*

$$|W^c_{a,k}(x)| \gg_{\varepsilon,a,k} \log_a x.$$

More precisely, for any $\varepsilon>0$ *we have*

$$|W^c_{a,k}(x)| \ge \frac{9}{\pi^4}\frac{\varphi(k)^2}{k^4}\left(\frac{1-\varepsilon}{2-\varepsilon}\right)^2\left(1+\mathrm{O}_{a,k}\left(\frac{\log\log x}{\log x}\right)\right)\log_a x,$$

as $x\to\infty$.

Proof. First of all we observe that by replacing n to nk in Lemma 2.15 and employing the inequality $\varphi(nk)\ge\varphi(n)\varphi(k)$ obtained in Lemma 2.7, we get

$$\frac{3\varepsilon_0\varphi(k)}{\pi^2k^2}(\log_a x)^2\left(1+\mathrm{O}_{a,k}\left(\frac{\log\log x}{\log x}\right)\right) < \sum_{n\le\frac{1}{k}\log_a x}\sum_{p\|\Phi_{nk}(a)}\log_a p. \tag{2.13}$$

Observe that since $\Phi_{n,k}(a)|a^{nk}-1$ then each prime divisor of $\Phi_{nk}(a)$ is also a prime divisor of $a^{nk}-1$. Thus,

$$\sum_{n\le\frac{1}{k}\log_a x}\sum_{p\|\Phi_{nk}(a)}\log_a p \le \sum_{n\le\frac{1}{k}\log_a x}\sum_{\substack{p|a^{nk}-1\\ p\le x, p\in W^c_{a,k}}}\log_a p$$

Applying this inequality in (2.13) yields

$$\frac{3\varepsilon_0\varphi(k)}{\pi^2k^2}(\log_a x)^2\left(1+\mathrm{O}_{a,k}\left(\frac{\log\log x}{\log x}\right)\right) \le \sum_{n\le\frac{1}{k}\log_a x}\sum_{\substack{p\mid a^{nk}-1\\ p\le x, p\in W_{a,k}^c}}\log_a p$$

$$= \sum_{n\le\frac{1}{k}\log_a x}\sum_{s\mid nk}\sum_{\substack{\mathrm{ord}_p(a)=s\\ p\le x, p\in W_{a,k}^c}}\log_a p. \tag{2.14}$$

Let $nk = sm$. Then the right-hand side of the above inequality will be

$$\sum_{s\le\log_a x}\sum_{m=1}^{kn/s}\sum_{\substack{\mathrm{ord}_p(a)=s\\ p\le x, p\in W_{a,k}^c}}\log_a p = \sum_{s\le\log_a x}\left[\frac{\log_a x}{s}\right]\sum_{\substack{\mathrm{ord}_p(a)=s\\ p\le x, p\in W_{a,k}^c}}\log_a p. \tag{2.15}$$

By applying (2.15) in (2.14) we get

$$I = \sum_{s\le\log_a x}\sum_{m=1}^{kn/s}\sum_{\substack{\mathrm{ord}_p(a)=s\\ p\le x, p\in W_{a,k}^c}}\log_a p$$

$$= \sum_{s\le\log_a x}\left[\frac{\log_a x}{s}\right]\sum_{\substack{\mathrm{ord}_p(a)=s\\ p\le x, p\in W_{a,k}^c}}\log_a p > \frac{3\varepsilon_0\varphi(k)}{\pi^2k^2}(\log_a x)^2\left(1+\mathrm{O}_{a,k}\left(\frac{\log\log x}{\log x}\right)\right). \tag{2.16}$$

Next let $\varepsilon_1 = 3\varepsilon_0\varphi(k)/2\pi^2k^2$. We split I in the last inequality into two sums as follows.

$$I = \sum_{s=1}^{[\varepsilon_1\log_a x]}\left[\frac{\log_a x}{s}\right]\sum_{\substack{\mathrm{ord}_p(a)=s\\ p\le x, p\in W_{a,k}^c}}\log_a p + \sum_{s=[\varepsilon_1\log_a x]+1}^{[\log_a x]}\left[\frac{\log_a x}{s}\right]\sum_{\substack{\mathrm{ord}_p(a)=s\\ p\le x, p\in W_{a,k}^c}}\log_a p$$

$$= I_1 + I_2.$$

We now find an upper bound for I_1. We have

$$\sum_{\substack{\mathrm{ord}_p(a)=s\\ p\le x, p\in W_{a,k}^c}}\log_a p < \sum_{p\mid a^s-1}\log_a p < \log_a(a^s-1) < s.$$

Thus,

$$I_1 < \sum_{s=1}^{[\varepsilon_1 \log_a x]} \left[\frac{\log_a x}{s}\right] s < \varepsilon_1 (\log_a x)^2. \tag{2.17}$$

From (2.16) and (2.17) we have

$$I_2 \geq \frac{3\varepsilon_0 \varphi(k)}{k^2\pi^2} (\log_a x)^2 \left(1 + \mathrm{O}_{a,k}\left(\frac{\log\log x}{\log x}\right)\right) - I_1 > \varepsilon_1 (\log_a x)^2 \left(1 + \mathrm{O}_{a,k}\left(\frac{\log\log x}{\log x}\right)\right). \tag{2.18}$$

On the other hand, we have

$$\begin{aligned} I_2 &\leq \frac{1}{\varepsilon_1} \sum_{s=[\varepsilon_1 \log_a x]+1}^{[\log_a x]} \sum_{\substack{\mathrm{ord}_p(a)=s \\ p\leq x, p\in W_{a,k}^c}} \log_a p \\ &< \frac{1}{\varepsilon_1} \sum_{\substack{\mathrm{ord}_p(a)\in[\varepsilon_1 \log_a x, \log_a x] \\ p\leq x, p\in W_{a,k}^c}} \log_a p \\ &< \frac{1}{\varepsilon_1} \sum_{p\leq x, p\in W_{a,k}^c} \log_a p < \frac{\log_a x}{\varepsilon_1} |W_{a,k}^c(x)|. \end{aligned} \tag{2.19}$$

Thus, from (2.18) and (2.19) we have

$$|W_{a,k}^c(x)| \geq \varepsilon_1^2 \left(1 + \mathrm{O}_{a,k}\left(\frac{\log\log x}{\log x}\right)\right) \log_a x.$$

Or equivalently

$$|W_{a,k}^c(x)| \geq \frac{9}{\pi^4} \left(\frac{1-\varepsilon}{2-\varepsilon}\right)^2 \frac{\varphi(k)^2}{k^4} \left(1 + \mathrm{O}_{a,k}\left(\frac{\log\log x}{\log x}\right)\right) \log_a x,$$

which is the desired result. □

2.3 The largest known Wieferich numbers

Recall from the introduction that a Wieferich number in base $a > 1$ is a number m, relatively prime to a that satisfies the congruence

$$q(a,m) = \frac{a^{\varphi(m)} - 1}{m} \equiv 0 \pmod{m}.$$

We denoted the set of Wieferich numbers in base a by N_a. Following the method of [3, Theorem 9] one can show that

$$\max N_a \leq a^{w_a|W_a|} \prod_{p \leq w_a} (p-1), \tag{2.20}$$

where $w_a = \max W_a$. Our aim here is to improve the bound (2.20). To explain our method recall the following notations. A modified version of Fermat quotient is defined as follows.

$$\overline{q}(a,p) = \begin{cases} q(a,p) & \text{if } p \neq 2 \text{ or } p = 2 \text{ and } a \equiv 1 \pmod{4}, \\ \frac{a+1}{2} & \text{if } p = 2 \text{ and } a \equiv 3 \pmod{4}. \end{cases}$$

Also, we defined the sequence $S_a^{(n)}$ as follows. We set

$$S_a^{(0)} = \begin{cases} W_a \cup \{2\} & \text{if } \nu_2(\overline{q}(a,2)) \geq 1, \\ W_a & \text{otherwise.} \end{cases}$$

For $i \geq 1$, let

$$S_a^{(i)} = \{p;\ p|q-1, \text{ where } q \in S_a^{(i-1)}\}.$$

We called $S_a = \bigcup_{i=0}^{\infty} S_a^{(i)}$ the set of primes generated by the set of primes in W_a. In Lemma 2.20 we will show that every prime divisor of a Wieferich number in base a, is in S_a. This fact plays an important role in the proof of the main result of this section.

Theorem 2.17. *If W_a is a finite set, then N_a is also finite. Moreover, we have*

$$\begin{aligned}\max N_a &= \prod_{\substack{p\in S_a\\ p\nmid a}} p^{\nu_p(M)+\nu_p(\overline{q}(a,p))}\\ &= \prod_{p\in S_a^{(0)}} p^{\nu_p(M)+\nu_p(\overline{q}(a,p))} \prod_{\substack{p\in S_a\setminus S_a^{(0)}\\ p\nmid a}} p^{\nu_p(M)},\end{aligned}$$

where $M=\prod_{\substack{p\in S_a\\ p\nmid a}}(p-1)$.

Our method follows closely the proof of [3, Theorem 9]. The main tool in the proof of Theorem 2.17 is a criterion for Wieferich numbers. The following is [1, Theorem 5].

Theorem 2.18 (**Agoh-Dilcher-Skula**). *Let $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ and a be two relatively prime integers, with $m\geq 3$. Then $m\in N_a$ if and only if for every $1\leq i\leq k$, we have*

$$\alpha_i \leq \nu_{p_i}(\prod_{j=1}^{k}(p_j-1))+\nu_{p_i}(\overline{q}(a,p_i)).$$

Note that when $m=2$, by the definition of Wieferich numbers we have m is a Wieferich number in base $a>1$ if and only if we have $a\equiv 1 \pmod 4$.

Before presenting the proof of Theorem 2.17 we need to establish the connection of Wieferich numbers with the set S_a. Lemma 2.20 which is a consequence of Theorem 2.18 is for this purpose. We also need a lemma regarding the largest prime divisor of a Wieferich number. The following is basically Lemma 2 of [3] which is written for Wieferich numbers in a general base a (instead of base 2).

Lemma 2.19. *Let m be a Wieferich number in base a. Let $P(m)$ be the largest prime divisor of m. Then $P(m)\in S_a^{(0)}$.*

Proof. Let $m=2$ be a Wieferich number in base a. Then we have $P(m)=2$ is a Wieferich

prime in base a. So let $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k} > 2$ be a Wiefriech number in base a. Observe that

$$P(m) \nmid \prod_{j=1}^{k} (p_j - 1).$$

Hence,

$$\nu_{P(m)}(\prod_{i=1}^{k} (p_i - 1)) = 0.$$

Therefore by Theorem 2.18 we have

$$\nu_{P(m)}(\overline{q}(a, P(m))) \geq 1. \tag{2.21}$$

Now if $P(m) = 2$ and $a \equiv 1 \pmod 4$ or $p \neq 2$ then (2.21) yields $\nu_{P(m)}(\overline{q}(a,p)) = \nu_p(q(a,p)) = \nu_{P(m)}(a^{P(m)-1} - 1) \geq 2$. Therefore $P(m) \in W_a$. Thus $P(m) \in S_a^{(0)}$. If $P(m) = 2$ and $a \equiv 3 \pmod 4$, then by (2.21) and the definition of $S_a^{(0)}$ we have $P(m) = 2 \in S_a^{(0)}$. □

Lemma 2.20. *Let m be a Wieferich number in base a. Then for every prime divisor p of m we have $p \in S_a$.*

Proof. First of all note that if $m = 2$ is a Wieferich number in base a, then by Lemma 2.19 it is a Wieferich prime. Thus $2 \in S_a$. So, let p_1 be a prime divisor of a Wieferich number $m > 2$. If $p_1 \in S_a^{(0)}$, then $p_1 \in S_a$. Otherwise, if $p_1 \notin S_a^{(0)}$, we have $\nu_{p_1}(\overline{q}(a, p_1)) = 0$. Hence, by the fact that $\nu_{p_1}(m) > 0$ and employing Theorem 2.18, we have

$$\nu_{p_1}(\prod_{p|m} (p - 1)) > 0.$$

Therefore there exists a prime divisor of m like p_2 such that p_1 divides $p_2 - 1$. Now we consider cases.

If $p_2 \in S_a^{(0)}$ then we have $p_1 \in S_a^{(1)}$. Consequently we have $p_1 \in S_a$.

If $p_2 \notin S_a^{(0)}$, by the similar argument there exists a prime divisor of m like p_3 such that $p_2 | p_3 - 1$.If $p_3 \in S_a^{(0)}$ then $p_2 \in S_a^{(1)}$ and $p_1 \in S_a^{(2)}$ (Since $p_1 | p_2 - 1$).

If $p_3 \notin S_a^{(0)}$ then we continue this process. However the process terminates with a prime in $S_a^{(0)}$. This is true since $p_1 < p_2 < \cdots$ is an increasing sequence. Thus, either at some point we hit a prime which is in $S_a^{(0)}$ or we reach to the largest prime divisor of m, which is, by Lemma 2.19 also is in $S_a^{(0)}$. Thus $p_1 \in S_a^{(\ell)} \subseteq S_a$, for some integer ℓ and therefore $p_1 \in S_a$. □

Corollary 2.21. *If $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is a Wieferich number in base a and $m \geq 3$, then for every $1 \leq i \leq k$ we have*

$$\alpha_i \leq \nu_{p_i}\Big(\prod_{\substack{p_i \in S_a \\ p_i \nmid a}} (p_i - 1)\Big) + \nu_{p_i}(\overline{q}(a, p_i))$$

Proof. By Lemma 2.20 each $p_i \in S_a$ for $1 \leq i \leq k$. On the other hand since $(a,m) = 1$, then $p_i \nmid a$. Therefore the result follows from Theorem 2.18. □

We are ready to prove the main theorem of this section.

Proof of Theorem 2.17. Let

$$M = \prod_{\substack{p \in S_a \\ p \nmid a}} (p-1) = \prod_{\substack{p \in S_a \\ p \mid a}} p^{\nu_p(M)} \prod_{\substack{p \in S_a \\ p \nmid a}} p^{\nu_p(M)} = M_1 M_2.$$

Observe that using Corollary 2.21 and the fact that $\nu_p(\overline{q}(a,p)) = 0$, if $p \notin S_a^{(0)}$, we have

$$\begin{aligned} \max N_a &\leq \prod_{p \in S_a^{(0)}} \left(p^{\nu_p(\overline{q}(a,p))} p^{\nu_p(M_2)} \right) \prod_{\substack{p \in S_a \setminus S_a^{(0)} \\ p \nmid a}} p^{\nu_p(M_2)} \\ &= \prod_{p \in S_a^{(0)}} p^{\nu_p(\overline{q}(a,p))} \prod_{\substack{p \in S_a \\ p \nmid a}} p^{\nu_p(M_2)} \\ &= M_2 \prod_{p \in S_a^{(0)}} p^{\nu_p(\overline{q}(a,p))}. \end{aligned} \tag{2.22}$$

Now let

$$m = M_2 \prod_{p \in S_a^{(0)}} p^{\nu_p(\overline{q}(a,p))} = \prod_{p \in S_a^{(0)}} \left(p^{\nu_p(\overline{q}(a,p))} p^{\nu_p(M_2)} \right) \prod_{\substack{p \in S_a \setminus S_a^{(0)} \\ p \nmid a}} p^{\nu_p(M_2)} \tag{2.23}$$

Then from (2.22) we have $\max N_a \leq m$. Thus, it remains to show that m is a Wieferich number. By Theorem 2.18 it is enough to show that for every prime divisor of m

$$\nu_p(m) \leq \nu_p(M) + \nu_p(\overline{q}(a,m)). \tag{2.24}$$

Suppose that $p|m$ and $p \in S_a^{(0)}$. In this case from (2.23) we have

$$\nu_p(m) = \nu_p(M_2) + \nu_p(\overline{q}(a,p)). \tag{2.25}$$

Since $p \in S_a^{(0)}$ and thus $p \nmid a$, then $\nu_p(M_2) = \nu_p(M)$. Therefore equality occurs in (2.24). Next suppose that $p|m$ and $p \notin S_a^{(0)}$. Then from (2.23) we have

$$\nu_p(m) = \nu_p(M_2) \leq \nu_p(M) = \nu_p(M) + \nu_p(\overline{q}(a,p)).$$

Thus, (2.24) holds in this case too.

Since (2.24) holds in both cases, then m is a Wieferich number. □

2.4 Density of Wieferich numbers

Recall that in the introduction we discussed a heuristic, which predicts

$$|W_a(x)| \approx \log\log x.$$

Inspired by this heuristic, we find a conditional lower bound for the number of Wieferich numbers. Our method here closely follows the proof of Theorem 8 of [3]. However the

condition considered in [3, Theorem 8] for the number of Wieferich primes is different from our condition.

Theorem 2.22. *For integer $a > 1$ and real $x > 0$, if*

$$c_a \log\log x \leq |W_a(x)| \leq d_a \log\log x,$$

then

$$|N_a(x)| \geq (\log x)^{c_a \log 2 + o(1)} - 1,$$

where c_a and d_a are positive constants.

Proof. Let $y = x^{\frac{1}{|W_a(x)|}}$. Observe that $y \leq x$. We define

$$A_a(x) = \{n \leq x;\ \ n \text{ is squarefree and if } \ \ p|n \ \text{ then } \ \ p \in W_a(y)\}.$$

First note that $|A_a(x)| = 2^{|W_a(y)|} - 1$. Secondly, if $n \in A_a(x)$, then $n \in N_a(x)$. This is true, since for every prime divisor p of n we have $\nu_p(q(a,p)) \geq 1$. Therefore by Theorem 2.18 we conclude that n is a Wieferich number. Moreover, we have $n \leq y^{|W_a(y)|} \leq y^{|W_a(x)|} = x$. Therefore $n \in N_a(x)$, and consequently

$$|N_a(x)| \geq 2^{|W_a(y)|} - 1. \tag{2.26}$$

Moreover, by the assumption on $|W_a(x)|$ we have

$$\begin{aligned} |W_a(y)| \geq c_a \log\log y &= c_a \log\log x^{\frac{1}{|W_a(x)|}} \\ &= c_a (\log\log x - \log|W_a(x)|) \\ &= (c_a + o(1)) \log\log x. \end{aligned}$$

Thus by applying the above lower bound for $|W_a(y)|$ in (2.26), we have

$$|N_a(x)| \geq (\log x)^{c_a \log 2 + o(1)} - 1.$$

□

2.5 Density of non-Wieferich numbers

In this section we prove an unconditional lower bound for the number of non-Wieferich prime in base a. Our result is a generalization of [3, Theorem 5] to any base. For odd prime p, let

$$T_p(x) = \{k \leq x; \text{ If } \text{ prime } q|k \text{ then } q \not\equiv 1 \pmod{p}\}.$$

The following is a version of a Theorem of Wirsing [27].

Theorem 2.23. *For any positive real integer x and any odd prime $p \leq \log\log x$ we have*

$$T_p(x) \geq x \exp\left(-\frac{\log\log x}{p-1} + \mathrm{O}\left(\log\log\log x\right)\right).$$

Following the proof of Theorem 5 of [3], here, we employ Theorem 2.23 to obtain a lower bound for the number of non-Wieferich numbers in any base. The following is the main result of this section. Note that the O-term in Theorem 5 of [3] is $\mathrm{O}((\log\log x)^{\frac{1}{3}})$. We were unable to verify this O-term.

Theorem 2.24. *We have*

$$|N_a^c(x)| \geq x \exp\left(-2(\log a)^{1/2}(\log\log x)^{1/2} + \mathrm{O}(\log\log\log x)\right).$$

Proof. Let p be any prime in the interval $[y, y+y^{2/3}]$, where $y = \left(\frac{\log\log x}{\log a}\right)^{1/2}$. (Such a prime exists by the existence of prime in short intervals, see [11] for more information.) Moreover, let $e = \nu_p(a^{p-1}-1)$ and suppose $n \in T_p(x/p^e)$. We show that $m = np^e$ is a non-

Wieferich number, thus the number of non-Wieferich numbers is bigger than the numbers of integers in the set $T_p(x/p^e)$. Note that since $p \nmid n$ we have $\nu_p(\prod_{p|m}(p-1)) = 0$. Thus $\nu_p(a^{p-1}-1) - 1 + \nu_p(\prod_{p|m}(p-1)) = e - 1 < \nu_p(m)$. Hence, by Theorem 2.18 m is a non-Wieferich number. Therefore by Theorem 2.23 we have

$$|N_a^c(x)| \geq T_p\left(\frac{x}{p^e}\right) \geq \frac{x}{p^e}\exp\left(-\frac{\log\log(x/p^e)}{p-1} + \mathrm{O}(\log\log\log(x/p^e))\right). \tag{2.27}$$

Observe that

$$\begin{aligned}\log\log\left(\frac{x}{p^e}\right) &= \log\left(\log x\left(1 - \frac{e\log p}{\log x}\right)\right)\\ &= \log\log x + \mathrm{O}\left(\frac{\log p}{\log x}\right)\\ &= \log\log x + \mathrm{O}\left(\frac{\log\log\log x}{\log x}\right)\end{aligned} \tag{2.28}$$

In above, we used the facts that $\log(1+x) = \mathrm{O}(x)$ and $p \leq 2y$, for $y = \frac{(\log\log x)}{\log a}^{1/2}$. Since $e = \nu_p(a^{p-1}-1)$, we have $p^e < a^{p-1}$. Thus,

$$p^{-e} > \exp(-(p-1)\log a). \tag{2.29}$$

Applying (2.28) and (2.29) in (2.27) yields

$$|N_a^c(x)| \geq x\exp\left(-(p-1)\log a - \frac{\log\log x}{p-1} + \mathrm{O}(\log\log\log x)\right).$$

Now the minimum of the right-hand side of the above inequality happens when

$$p - 1 = \left(\frac{\log\log x}{\log a}\right)^{1/2}.$$

Therefore we have

$$|N_a^c(x)| \geq x \geq x \exp\left(-2(\log a \log\log x)^{1/2} + \mathrm{O}(\log\log\log x)\right).$$

□

Chapter 3

K-Wieferich primes and numbers

3.1 Wieferich primes in a quadratic field

Recall the definition of a K-Wieferich from Section 1.2.

Definition 3.1. Let K be a number field with the ring of integers $\mathfrak{O}_K$. A prime $\pi \in \mathfrak{O}_K$ is called a K- *Wieferich prime in base* $\alpha \in \mathfrak{O}_K$ if

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi^2}.$$

We prove the following Theorem on the relation between Wieferich primes in an integer base a and K-Wieferich primes in base a, where K is a quadratic field.

Theorem 3.2. *Let $K = \mathbb{Q}(\sqrt{m})$ with $h_K = 1$. Then the following assertion holds.*

(i) *Any prime of $\mathfrak{O}_K$ above a Wieferich prime p in an integer base a is a K-Wieferich prime in base a.*

(ii) *If π is a K-Wieferich prime in an integer base a such that $N(\pi) = p$ for a prime p, then p is a Wieferich prime in base a.*

Proof. (i) From the fact that p is a Wieferich prime we have

$$p^2 | a^{p-1} - 1. \tag{3.1}$$

Now let π be a prime with $N(\pi) = p$. In other words, π is a prime above a split or ramified

prime p, then for an integer a we have

$$a^{N(\pi)-1} - 1 = a^{p-1} - 1.$$

Since $N(\pi) = p = |\pi\pi'|$, where π' is the non-trivial conjugate of π in $\mathbb{Q}(\sqrt{m})$, we have $\pi^2 | p^2$. Therefore by (3.1), we have

$$a^{N(\pi)-1} \equiv 1 \pmod{\pi^2}.$$

Thus π is a K-Wieferich prime.

Now suppose that $N(\pi) = p^2$, so π is a prime above an inert prime p. We have $a^{N(p)-1} = a^{p^2-1} = a^{(p-1)(p+1)}$. From (3.1) we have $a^{(p-1)(p+1)} \equiv 1 \pmod{p^2}$. Thus, $a^{N(p)-1} \equiv 1 \pmod{p^2}$, and p is a K-Wieferich prime.

(ii) Since π is a K-Wieferich prime in base a, then there exists $\beta \in \mathfrak{O}_k$ such that

$$a^{p-1} - 1 = \beta\pi^2. \tag{3.2}$$

Hence, we have

$$\pi^2 | a^{p-1} - 1. \tag{3.3}$$

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$ be the non-trivial monomorphism. From (3.2) we have

$$\sigma(a^{p-1} - 1) = \sigma(\beta)\sigma(\pi^2).$$

Since $a^{p-1} - 1$ is an integer, we have $a^{p-1} - 1 = \sigma(\beta)\sigma(\pi^2)$. Hence,

$$\sigma(\pi^2) | a^{p-1} - 1. \tag{3.4}$$

From (3.3) and (3.4) and the fact that π and $\sigma(\pi)$ are distinct primes we have

$$p^2 = N(\pi)^2 = \pi^2\sigma(\pi^2)|a^{p-1}-1.$$

Therefore p is a Wieferich prime in base a. □

Corollary 3.3. *Let $a>1$ be an integer and $h_K = 1$, for $K = \mathbb{Q}(\sqrt{m})$. If there are infinitely many Wieferich primes in base a, then there are infinitely many K-Wieferich primes.*

Note that based on the heuristic for the set $W_a(x)$, the set of Wieferich primes up to a real number x, there are at least $\log\log x$ Wieferich primes up to x. Therefore by Corollary 3.3 we expect that there are at least $\log\log x$, K-Wieferich primes in any integer base a. Combining Theorem 2.2 from Chapter 2 and Theorem 3.2 we have the following result for $K = \mathbb{Q}(i)$.

Corollary 3.4. *Let $K = \mathbb{Q}(i)$, and $a>1$ be an integer. Assuming the abc-conjecture we have*

$$|\{\textit{prime } \pi \in \mathbb{Z}[i] \ ; \ N(\pi) \leq x \ \textit{ and } \ a^{N(\pi)-1} \not\equiv 1 \pmod{\pi^2}\}| \gg_a \log x.$$

Proof. First of all note that by [19, Theorem 4.39] p is a split prime in $\mathbb{Q}(i)$ if and only if $p \equiv 1 \pmod 4$. Thus, we have

$$\begin{aligned} &\{\text{prime } \pi \in \mathbb{Z}[i] \ ; \ N(\pi) = p \leq x, \ p \equiv 1 \pmod 4, \ \pi \in W_a^c(\mathbb{Q}(i),x)\} \\ &\subseteq \{\text{prime } \pi \ \in \mathbb{Z}[i] \ ; \ N(\pi) \leq x, \ \pi \in W_a^c(\mathbb{Q}(i),x)\} \end{aligned} \tag{3.5}$$

Note that by part (i) of Theorem 3.2 we conclude that for any integer a and k and any quadratic field K with $h_K = 1$ we have $W_{a,k}^c(x) \subseteq W_{a,k}^c(K,x)$. Especially for $K = \mathbb{Q}(i)$ and $k = 4$. Thus we have

$$W_{a,4}^c(x) \subseteq W_{a,4}^c(\mathbb{Q}(i),x). \tag{3.6}$$

Hence, employing (3.6) in (3.5) and using Theorem 2.2 yield

$$|\{\text{prime } \pi \in \mathbb{Z}[i]\ ;\ N(\pi) = p \le x,\ p \equiv 1 \pmod 4,\ \pi \in W_a^c(\mathbb{Q}(i), x)\}| = 2|W_{a,4}^c(x)| \gg_a \log x.$$

This proves the corollary. □

We would like to point out that it is not clear whether or not part (ii) of Theorem 3.1 remains true for a non-split prime p. We have done some experiment on this in the field $\mathbb{Q}(i)$. We checked all primes with norm non-exceeding 4000 for integer bases between 2 and 3. All the K-Wieferich prime found in our experiment were proven to be Wieferich primes.

3.2 Wieferich numbers in a quadratic field

The main result of this section provides a characterization for Wieferich numbers in quadratic fields with unique factorization property. The following generalization of Proposition 5.4 of [1] to quadratic fields plays an important role in the proof of the main result of this section. Recall that $\nu_p(\gamma)$ denotes the multiplicity of π in γ.

Lemma 3.5. *Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field of class number 1. Let $\beta \in \mathfrak{O}_K$ and $\pi \in \mathfrak{O}_K$ be a prime such that $\beta \equiv 1 \pmod \pi$. Then for any natural number n the following assertion holds:*

(i) If π is a prime above an odd split prime p or if π is a prime above the split prime $p = 2$ and $\beta \equiv 1 \pmod{\pi^2}$, we have

$$\nu_\pi(\beta^{N(\pi)^n} - 1) = \nu_\pi(\beta - 1) + n. \tag{3.7}$$

(ii) If π is a prime above a split prime $p = 2$ and $\beta \equiv \pi + 1 \pmod{\pi^2}$, we have

$$\nu_\pi(\beta^{N(\pi)^n} - 1) = \nu_\pi(\beta + 1) + n. \tag{3.8}$$

(iii) If π is a prime above an odd inert prime p we have

$$\nu_\pi(\beta^{N(\pi)^n} - 1) = \nu_\pi(\beta - 1) + 2n. \tag{3.9}$$

Proof. (i) Let π be a prime above an odd split prime p. Note that this implies $N(\pi) = p$. We will establish (3.7) by induction on n. For $n = 1$, note that by the assumption we have $\beta = \pi\delta + 1$ for some $\delta \in \mathfrak{O}_K$. Thus, for every $0 \le m \le N(\pi) - 1$, we have

$$\beta^m = (\pi\delta + 1)^m \equiv m\delta\pi + 1 \pmod{\pi^2}.$$

Consequently, we have

$$\begin{aligned}\frac{\beta^{N(\pi)} - 1}{\beta - 1} = \sum_{m=0}^{N(\pi)-1} \beta^m &\equiv \sum_{m=0}^{N(\pi)-1} (m\delta\pi + 1) \pmod{\pi^2} \\ &\equiv \frac{\delta\pi N(\pi)(N(\pi) - 1)}{2} + N(\pi) \pmod{\pi^2}.\end{aligned}$$

Since $N(\pi) = p$ we conclude

$$\frac{\beta^{N(\pi)} - 1}{\beta - 1} = \sum_{m=0}^{N(\pi)-1} \beta^m = \eta\pi^2 + \frac{\delta\pi p(p-1)}{2} + \pi\pi', \tag{3.10}$$

for some $\eta \in \mathfrak{O}_K$, where π' is the conjugate of π or $-\pi$. Therefore, from (3.10), we have

$$\begin{aligned}\nu_\pi(\beta^{N(\pi)} - 1) &= \nu_\pi(\beta - 1) + \nu_\pi(\pi(\pi\eta + \frac{\delta p(p-1)}{2}) + \pi')) \\ &= \nu_\pi(\beta - 1) + \nu_\pi(\pi) + \nu_\pi(\pi\eta + \frac{\delta p(p-1)}{2} + \pi').\end{aligned}$$

Since $\pi \neq \pi'$, in the latter identity, the last term is zero. (Note that $(p-1)/2$ is an integer, since p is an odd prime.) Thus,

$$\nu_\pi(\beta^{N(\pi)} - 1) = \nu_\pi(\beta - 1) + 1.$$

Hence, (3.7) holds for $n = 1$.

Now let $n > 1$ and assume (3.7) holds for $n-1$. We have

$$\beta^{N(\pi)^n} - 1 = (\beta^{N(\pi)^{n-1}} - 1)(\sum_{j=0}^{N(\pi)-1} (\beta^{N(\pi)^{n-1}})^{N(\pi)-j}),$$

which implies

$$\nu_\pi(\beta^{N(\pi)^n} - 1) = \nu_\pi(\beta^{N(\pi)^{n-1}} - 1) + \nu_\pi(\sum_{j=0}^{N(\pi)-1} (\beta^{N(\pi)^{n-1}})^{N(\pi)-j}). \tag{3.11}$$

Note that for every $0 \leq j \leq N(\pi) - 1$, we have

$$\begin{aligned}(\beta^{N(\pi)^{n-1}})^{N(\pi)-j} &\equiv \left((\pi\delta + 1)^{N(\pi)^{n-1}}\right)^{N(\pi)-j} \pmod{\pi^2} \\ &\equiv \sum_{k=0}^{(N(\pi))^{n-1}(N(\pi)-j)} \binom{N(\pi)^{n-1}(N(\pi)-j)}{k} (\pi\delta)^k \pmod{\pi^2}. \end{aligned} \tag{3.12}$$

Observe that since $N(\pi) = p$, from (3.12) we get

$$\begin{aligned}(\beta^{N(\pi)^{n-1}})^{p-j} &\equiv 1 + p^{(n-1)(p-j)}\pi\delta \pmod{\pi^2} \\ &\equiv 1 \pmod{\pi^2}.\end{aligned}$$

(The last congruence holds because $n > 1$ and $p = \pi\pi'$.) Therefore, for every $0 \leq j \leq N(\pi) - 1$, we have

$$(\beta^{N(\pi)^{n-1}})^{N(\pi)-j} = \sigma_j\pi^2 + 1,$$

for some $\sigma_j \in \mathfrak{O}_K$ depending on j. Hence,

$$\nu_\pi\left(\sum_{j=0}^{N(\pi)-1}(\beta^{N(\pi)^{n-1}})^{N(\pi)-j}\right)=\nu_\pi\left(\sum_{j=0}^{p-1}(\sigma_j\pi^2+1)\right)=\nu_\pi\left(\pi\left(\sum_{j=0}^{p-1}\sigma_j\pi+\pi'\right)\right)=1. \tag{3.13}$$

Moreover, by the induction assumption we have

$$\nu_\pi(\beta^{N(\pi)^{n-1}}-1)=\nu_\pi(\beta-1)+n-1. \tag{3.14}$$

Applying (3.13) and (3.14) in (3.11) yields (3.7) for the case that p is an odd prime.

Now suppose that π is a prime above the splitting prime $p=2$ and $\beta \equiv 1 \pmod{\pi^2}$. To prove (3.7) for this case, again we use induction on n. For $n=1$ we have

$$\frac{\beta^{N(\pi)}-1}{\beta-1}=\sum_{m=0}^{N(\pi)-1}\beta^m=N(\pi)=2.$$

Therefore,

$$\nu_\pi(\beta^2-1)=\nu_\pi(\beta-1)+\nu_\pi(\sum_{m=0}^{N(\pi)-1}\beta^m)=\nu_\pi(\beta-1)+1.$$

This proves (3.7) for $n=1$. Now, for $n>1$, let (3.7) be true for $n-1$. We have

$$\nu_\pi(\beta^{2^n}-1)=\nu_\pi(\beta^{2^{n-1}}-1)+\nu_\pi(\beta^{2^{n-1}}+1). \tag{3.15}$$

Since $\beta \equiv 1 \pmod{\pi^2}$ we have $\beta^{2^{n-1}} \equiv 1 \pmod{\pi^2}$ and thus,

$$\beta^{2^{n-1}}+1=\pi^2\sigma+2=\pi^2\sigma+\pi\pi'=\pi(\pi\sigma+\pi'), \tag{3.16}$$

for $\sigma \in \mathfrak{O}_K$ and π' defined as before. Therefore, $\nu_\pi(\beta^{2^{n-1}}+1)=1$. Recall that by the

induction assumption we have

$$\nu_\pi(\beta^{2^{n-1}} - 1) = \nu_\pi(\beta - 1) + n - 1. \tag{3.17}$$

Thus (3.15), (3.16), and (3.17) yields (3.7) for the case $p = 2$.

(ii) Let π be a prime above the split prime $\pi = 2$ and $\beta \equiv \pi + 1 \pmod{\pi^2}$. Again we use induction on n to prove (3.9). For $n = 1$, we have

$$\nu_\pi(\beta^2 - 1) = \nu_\pi(\beta - 1) + \nu_\pi(\beta + 1). \tag{3.18}$$

Moreover, by the assumption of part (ii) of our lemma we have

$$\beta - 1 = \pi^2\sigma + \pi = \pi(\pi\sigma + 1), \tag{3.19}$$

for some $\sigma \in \mathfrak{O}_K$. Therefore by (3.18) and (3.19) we have

$$\nu_\pi(\beta^2 - 1) = \nu_\pi(\beta - 1) + 1.$$

Now let (3.8) be true for $n - 1$. We have

$$\begin{aligned} \beta^{2^{n-1}} + 1 &\equiv (1 + \pi)^{2^{n-1}} + 1 \pmod{p^2} \\ &\equiv 2 + 2^{n-1}\pi \pmod{\pi^2} \\ &\equiv 2 \pmod{\pi^2}. \end{aligned}$$

The last congruence holds, since $n > 1$. Thus, by the fact that $2 = \pi\pi'$, we have

$$\beta^{2^{n-1}} + 1 = \pi^2\sigma + \pi\pi' = \pi(\pi\sigma + \pi'), \tag{3.20}$$

for some $\sigma \in \mathfrak{O}_K$. Therefore, by applying (3.20) and the induction assumption in the identity

(3.15), we get

$$\nu_\pi(\beta^{2^{n-1}} - 1) = \nu_\pi(\beta - 1) + n,$$

which yields (3.8).

(*iii*) Let $\pi = p$ be an odd inert prime. We claim that

$$\nu_p(\beta^{p^n} - 1) = \nu_p(\beta - 1) + n, \tag{3.21}$$

for any integer $n \geq 1$. We prove the identity (3.21) by induction on n. Let $n = 1$ and write $\beta = p\delta + 1$ for some $\delta \in \mathfrak{O}_K$. Then, for $0 \leq m \leq p-1$, we have $\beta^m \equiv m\delta p + 1 \pmod{p^2}$. Hence,

$$\begin{aligned} \sum_{m=0}^{p-1} \beta^m &\equiv \frac{(p-1)p^2\delta}{2} + p \pmod{p^2} \\ &\equiv p \pmod{p^2}. \end{aligned}$$

Thus, we can write

$$\frac{\beta^p - 1}{\beta - 1} = \sum_{m=0}^{p-1} \beta^m = \eta p^2 + p,$$

for some integer $\eta \in \mathfrak{O}_K$. Therefore

$$\nu_p(\beta^p - 1) = \nu_p(\beta - 1) + \nu_p(\eta p^2 + p) = \nu_p(\beta - 1) + 1.$$

This proves the case $n = 1$. Now let $n > 1$. Since

$$\beta^{p^n} - 1 = (\beta^{p^{n-1}} - 1)\left(\sum_{j=0}^{p-1} (\beta^{p^{n-1}})^{p-j}\right),$$

we have

$$\nu_p(\beta^{p^n}-1) = \nu_p(\beta^{p^{n-1}}-1) + \nu_p(\sum_{j=0}^{p-1}(\beta^{p^{n-1}})^{p-j}). \tag{3.22}$$

By the induction assumption we have

$$\nu_p(\beta^{p^{n-1}}-1) = \nu_p(\beta-1)+n-1. \tag{3.23}$$

Moreover, from the fact that $\beta = p\delta+1$, and using binomial theorem for every $0 \le j \le p$ we have

$$\begin{aligned}
(\beta^{p^{n-1}})^{p-j} &\equiv \left((p\delta+1)^{p^n-1}\right)^{p-j} \pmod{p^2} \\
&\equiv \sum_{k=0}^{(p-j)p^{n-1}} \binom{p^{n-1}(p-j)}{k} (p\delta)^k \pmod{p^2} \\
&\equiv \binom{p^{n-1}(p-j)}{1} p\delta+1 \pmod{p^2} \\
&\equiv 1 \pmod{p^2}.
\end{aligned}$$

for every $0 \le j \le p-1$, the above congruence yields

$$(\beta^{p^{n-1}})^{p-j} = \eta_j p^2 + 1,$$

where η_j is an integer depending on j. Therefore we have

$$\nu_p\left(\sum_{j=1}^{p}(\beta^{p^{n-1}})^{p-j}\right) = \nu_p\left(p\left(p\sum_{j=1}^{p}\eta_j + p\right)\right) = 1. \tag{3.24}$$

Hence, from (3.22), (3.23) and (3.24) we have

$$\nu_p(\beta^{p^n}-1) = \nu_p(\beta-1)+n-1+1 = \nu_p(\beta-1)+n.$$

Thus we proved (3.21) by induction. Now we replace n with $2n$ in (3.21), to obtain

$$\nu_p(\beta^{p^{2n}} - 1) = \nu_p(\beta - 1) + 2n. \tag{3.25}$$

Since $\pi = p^2$ and $N(\pi) = p^2$. The identity (3.25) can be written

$$\nu_\pi(\beta^{N(\pi)^n} - 1) = \nu_\pi(\beta - 1) + 2n.$$

□

Before stating our main theorem of this section, recall that for $\alpha, \gamma \in \mathfrak{O}_K$, we set $q(\alpha, \gamma) = (\alpha^{\varphi(\gamma)} - 1)/\gamma$.

Theorem 3.6. *Let $K = \mathbb{Q}(\sqrt{m})$ with $h_K = 1$. Let $\gamma = \pi_1^{a_1} \cdots \pi_\ell^{a_\ell} \in \mathfrak{O}_K$, where π_i's are primes above split or inert primes. Also let $\alpha \in \mathfrak{O}_K$ and $(\alpha, \gamma) = 1$. Then γ is a K-Wieferich number in base α if and only if π_i's satisfy the following conditions :*

(i) If π_i is a prime above an odd split prime p or if π_i is a prime above the split prime $p = 2$ and $\alpha \equiv 1 \pmod{\pi_i^2}$, then

$$a_i \leq \nu_{\pi_i}(\prod_{\pi|\gamma}(N(\pi) - 1)) + \nu_{\pi_i}(q(\alpha, \pi_i)). \tag{3.26}$$

(ii) If π_i is a prime above the split prime $p = 2$ and $\alpha \equiv 1 + \pi_i \pmod{\pi_i^2}$, then

$$a_i \leq \nu_{\pi_i}(\prod_{\pi|\gamma}(N(\pi) - 1)) + \nu_{\pi_i}(\alpha^{N(\pi_i)-1} + 1) - 1. \tag{3.27}$$

(iii) If π_i is a prime above an odd inert prime p, then

$$2\nu_{\pi_i}(\prod_{\pi|\gamma}(N(\pi) - 1)) + \nu_{\pi_i}(q(\alpha, \pi_i)) \geq 1 \tag{3.28}$$

Proof. Let $R = \prod_{\pi|\gamma}(N(\pi)-1)$. For every $1 \leq i \leq \ell$ we have

$$\varphi(\gamma) = \theta_i \varphi(\pi_i^{a_i}) N(\pi_i)^{\nu_{\pi_i}(R)},$$

where $(\theta_i, N(\pi_i)) = 1$ and consequently $(\theta_i, \pi_i) = 1$. Now let

$$\rho = \alpha^{\varphi(\pi_i^{a_i}) N(\pi_i)^{\nu_{\pi_i}(R)}}.$$

Thus, we have

$$\alpha^{\varphi(\gamma)} - 1 = \rho^{\theta_i} - 1 = (\rho - 1) \sum_{j=0}^{\theta_i - 1} \rho^j. \tag{3.29}$$

Since

$$\rho = \alpha^{N(\pi_i)^{a_i - 1}(N(\pi_i)-1) N(\pi_i)^{\nu_\pi(R)}} = \alpha^{(N(\pi_i)-1) N(\pi_i)^{a_i + \nu_{\pi_i}(R) - 1}}, \tag{3.30}$$

and $\alpha^{N(\pi_i)-1} \equiv 1 \pmod{\pi_i}$, then $\rho \equiv 1 \pmod{\pi_i}$. Hence,

$$\sum_{j=0}^{\theta_i - 1} \rho^j \equiv \theta_i \pmod{\pi_i}.$$

Thus, from the fact that $(\theta_i, \pi_i) = 1$ and (3.29) we obtain

$$\nu_{\pi_i}(\alpha^{\varphi(\gamma)} - 1) = \nu_{\pi_i}(\rho - 1) + \nu_{\pi_i}\Big(\sum_{j=0}^{\theta_i - 1} \rho^j\Big) = \nu_{\pi_i}(\rho - 1).$$

Now let π and α satisfy the conditions of part (i) in the statement of the theorem. By employing the equality (3.7) of Lemma 3.5 for $n = a_i + \nu_{\pi_i}(R) - 1$ and $\beta = \alpha^{N(\pi_i)-1}$ we deduce from (3.30) that

$$\nu_{\pi_i}(\rho - 1) = \nu_{\pi_i}(\alpha^{N(\pi_i)-1} - 1) + a_i + \nu_{\pi_i}(R) - 1.$$

Subtracting a_i from both side of the above identity yields

$$\nu_{\pi_i}(q(\alpha,\gamma)) = \nu_{\pi_i}(q(a,\pi_i)) + \nu_{\pi_i}(R).$$

Now since γ is a K-Wieferich number if and only if γ divides $q(a,\gamma)$, the inequality (3.26) follows.

Next let π_i and α satisfy conditions of part (ii) in the statement of the theorem. We employ the equality (3.8) of Lemma 3.5 for $n = a_i + \nu_{\pi_i}(R) - 1$ and $\beta = \alpha^{N(\pi_i)-1}$ to conclude from (3.30)

$$\nu_{\pi_i}(q(\alpha,\gamma)) = \nu_{\pi_i}(\alpha^{N(\pi)-1} + 1) - 1 + \nu_{\pi_i}(R).$$

Since γ divides $q(a,\gamma)$ we obtain (3.27).

Lastly if π satisfies the condition of (iii) of the theorem, by employing (3.9) of Lemma 3.5 for $n = a_i + \nu_{\pi_i}(R) - 1$ and $\beta = \alpha^{N(\pi_i)-1}$ and using the equality (3.30) we obtain

$$\nu_{\pi_i}(\alpha^{\varphi(\gamma)} - 1) = \nu_{\pi_i}(\rho - 1) = \nu_{\pi_i}(\alpha^{N(\pi_i)-1} - 1) + 2a_i + 2\nu_{\pi_i}(R) - 2.$$

By subtracting a_i from both side of the above equality, we establish

$$\nu_{\pi_i}(q(\alpha,\gamma)) = \nu_{\pi_i}(q(\alpha,\pi_i)) + a_i + 2\nu_{\pi_i}(R) - 1.$$

Now by employing the fact that $a_i \leq \nu_{\pi_i}(q(\alpha,\gamma))$ for every $1 \leq i \leq \ell$ if and only if γ is a K-wieferich number we obtain (3.28).

□

Using Theorem 3.6, we can derive a property of K-Wieferich numbers which is analogous to Lemma 2.19.

Theorem 3.7. *Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field with $h_K = 1$. Let $\gamma = \pi_1^{a_1} \cdots \pi_k^{a_k} \in \mathfrak{O}_K$ be such that π_i, for $1 \leq i \leq k$, is a prime above an odd inert or and split prime p. Consider*

the set

$$\Pi(\gamma) = \{\pi_i \ ; \ 1 \leq i \leq k \text{ and } \pi_i \text{ has the maximum norm among the prime divisors of } \gamma\}.$$

If γ is a K-Wieferich number in base $\alpha \in \mathfrak{O}_K$, then any $\pi_i \in \Pi(\gamma)$ that is above an split prime, is a K-Wieferich prime in base α.

Proof. Let $\pi_i \in \Pi(\gamma)$ be a prime above a split prime p_i. Then we have $N(\pi_i) = \pi_i\pi_i' = p$, where π' is the non-trivial conjugate of π_i or $-\pi_i$. We show that $\nu_{\pi_i}(\prod_{i=1}^{k}(N(\pi_i)-1)) = 0$. We consider two cases.

First suppose $N(\pi_j) = p_j^2$, where $1 \leq j \leq k$ is fixed and $p_j \in \mathbb{Z}$ is an inert prime. Since $\pi_i \in \Pi(\gamma)$, we have $p_i > p_j^2 > p_j^2 - 1$. Thus,

$$p_i \nmid N(\pi_j) - 1. \tag{3.31}$$

Moreover, we show that $\pi_i \nmid N(\pi_j) - 1$. Otherwise

$$N(\pi_j) - 1 = \pi_i\eta \tag{3.32}$$

for some $\eta \in \mathfrak{O}_K$. We know that there exists a $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$ such that $\sigma(\pi_i) = \pi_i'$ or $-\pi_i'$. Applying σ in both sides of the equality, (3.32) we obtain $N(\pi_j) - 1 = \sigma(\eta')\pi_i'$, where $\eta' = \eta$ or $-\eta$. Therefore, π_i' also divides $N(\pi_j) - 1$. Consequently we have $p_i = \pi_i\pi_i'$ divides $N(\pi_j) - 1$, which is in contradiction with (3.31). Thus, $\pi_i \nmid N(\pi_j) - 1$.

Next we assume that $N(\pi_j) = p_j$, where $1 \leq j \leq k$ and $p_j \in \mathbb{Z}$ is an odd split prime. Then we have $p_i > p_j - 1$, since $\pi_i \in \Pi(\gamma)$. Thus, $p_i \nmid N(\pi_j) - 1$. Now an argument identical to the first case shows that $\pi_i \nmid N(\pi_j) - 1$. Hence,

$$\nu_{\pi_i}(\prod_{j=1}^{k} N(\pi_j) - 1) = 0.$$

Next we observe that since γ is a K-Wieferich number then by (3.26) in Theorem 3.6 we have $\nu_{\pi_i}(q(\alpha,\pi_i)) \geq 1$. Thus, we have $\nu_{\pi_i}(\alpha^{N(\pi_i)-1}-1) \geq 2$ or equivalently π_i is a K-Wieferich prime. □

Chapter 4

An exponential congruence in $\mathbb{C}[x]$

4.1 A finiteness theorem in $\mathbb{C}[x]$

In [18, Theorem 1] M. Ram Murty and V. Kumar Murty proved that the congruence

$$3^m - 3^n \equiv 0 \pmod{2^m - 2^n},$$

has only finitely many integer solutions (m,n), where $m > n \geq 0$. One of the main ingredients of their proof is a result proved in [5]. More precisely, Bugeaud, Corvaja and Zannier [5] showed that for any two multiplicatively independent integers a, and b, with $2 \leq a < b$ and given $\varepsilon > 0$, there exists an integer $n_0 > 0$ such that for all $n \geq n_0$ we have

$$\gcd(a^n - 1, b^n - 1) \leq a^{\varepsilon n}.$$

An analogous result in $\mathbb{C}[x]$ is a theorem of Ailon and Rudnick [2, Theorem 1].

Theorem 4.1 (**Ailon-Rudnick**). *Let $f, g \in \mathbb{C}[x]$ be two multiplicatively independent polynomials. Then there exists an absolute constant, depending only on f and g, such that*

$$\deg(\gcd(f^n - 1, g^n - 1)) < C(f,g). \tag{4.1}$$

In this section we employ Theorem 4.1 to prove an analogous result to [18, Theorem 1] in $\mathbb{C}[x]$. More precisely we prove the following.

Theorem 4.2. *Let f and g be two polynomials in $\mathbb{C}[x]$, which are relatively primes and $\deg f \leq \deg g$. Then, there are only finitely many integer pairs (m,n), where $m > n \geq 0$, such that*

$$f^m - f^n | g^m - g^n. \tag{4.2}$$

We need two lemmas and a proposition for proving Theorem 4.2. The following two lemmas are necessary for the proof of Proposition 4.5. We denote the k-th derivative of a polynomial f by $f^{(k)}$. Proposition 4.5 together with the inequality (4.1) will imply Theorem 4.2.

Lemma 4.3. *Let $f \in \mathbb{C}[x]$ and β be a root of f with multiplicity $k \geq 1$. Then we have*

$$f^{(0)}(\beta) = f^{(1)}(\beta) = \cdots = (f)^{(k-1)}(\beta) = 0 \tag{4.3}$$

and

$$f^{(k)}(\beta) \neq 0. \tag{4.4}$$

Proof. We can write

$$f(x) = g(x)h(x),$$

where $h(\beta) \neq 0$ and $g(x) = (x-\beta)^t$ for $t \geq 1$. Taking the s-th derivative from both side (using Leibnitz rule for derivative), we have

$$f^{(s)}(x) = \sum_{m=0}^{s} \binom{s}{m} g^{(m)}(x) h^{(s-m)}(x). \tag{4.5}$$

Observe that $g^{(m)}(\beta) = 0$ for $0 \leq m < k$. Therefore $f^{(s)}(\beta) = 0$, for $0 \leq s \leq k-1$, which

proves (4.3). Also since $g^{(k)}(\beta) = k!$, considering (4.5) for $s = k$ will result

$$f^{(k)}(\beta) = k!h(\beta).$$

Since $h(\beta) \neq 0$ we get (4.4). □

Lemma 4.4. *Let $f(x) \in \mathbb{C}[x]$, $c \in \mathbb{N}$, and $\beta \in \mathbb{C}$. Moreover, let $f^c(\beta) = 1$, for some $\beta \in \mathbb{C}$ and $f^{(i)}(\beta) = 0$, for $1 \leq i \leq k$, with $k \geq 1$. Then we have*

$$(f^c - 1)^{(k+1)}(\beta) = \frac{cf^{(k+1)}(\beta)}{f(\beta)}.$$

Proof. First note that, since $f^c(\beta) = 1$, we have

$$(f^c - 1)'(\beta) = cf^{c-1}(\beta)f'(\beta).$$

Moreover, for $k \geq 1$ using Leibnitz rule for derivative we have

$$\begin{aligned}(f^c - 1)^{(k+1)} &= (cf^{c-1}f')^{(k)} \\ &= \sum_{i=0}^{k} \binom{k}{i} (cf^{c-1})^{(k-i)} (f')^{(i)}. \end{aligned} \tag{4.6}$$

Now, according to the assumption, we have $(f')^{(i)}(\beta) = 0$, for $i < k$. By evaluating (4.6) at $x = \beta$ we find out that only for $i = k$ we obtain a nonzero term and all other terms are zero. Hence, $(f^c(x) - 1)^{(k+1)}$ at $x = \beta$ is equal to

$$cf^{c-1}(\beta)f^{(k+1)}(\beta) = \frac{cf^{(k+1)}(\beta)}{f(\beta)},$$

which is the desired result. □

Proposition 4.5. *Let f, g and $h \in \mathbb{C}[x]$. Suppose that*

$$f^c - 1 = gh,$$

where $c \in \mathbb{N}$ and

$$g(x) = \gamma \prod_i (x - \alpha_i)^{\beta_i},$$

with $\gamma \in \mathbb{C}$ and β_i's $\in \mathbb{N}$. Then $\beta_i \leq \deg f$, for each i.

Proof. Without loss of generality we show that $\beta_1 \leq \deg f$. To this aim let $t \geq \beta_1$ be the multiplicity of α_1 in $f^c - 1$. Thus we can write

$$f^c - 1 = (x - \alpha_1)^t h_1 = g_1 h_1,$$

where $g_1 = (x - \alpha_1)^t$ and $h_1 = (f^c - 1)/(x - \alpha_1)^t$. Applying Leibnitz rule for derivative we have

$$(f^c - 1)^{(s)} = \sum_{\ell=0}^{s} \binom{s}{\ell} g_1^{(\ell)} h_1^{(s-\ell)}. \tag{4.7}$$

We observe that $g_1^{(\ell)}(\alpha_1) = 0$, if $0 \leq \ell < s$. Thus, from (4.7) we deduce

$$(f^c - 1)^{(s)}(\alpha_1) = g_1^{(s)}(\alpha_1) h_1^{(0)}(\alpha_1). \tag{4.8}$$

For $s = 1$ the identity (4.8) becomes

$$c f^{c-1}(\alpha_1) f'(\alpha_1) = g_1'(\alpha_1) h_1(\alpha_1). \tag{4.9}$$

Observe that $g_1'(x) = t(x - \alpha_1)^{t-1}$. Thus, if $t = 1$, from (4.9) we conclude that $f'(\alpha_1) \neq 0$. Otherwise, if $t > 1$ we have $f'(\alpha_1) = 0$. In other words α_1 is a root of f'. Let α_1 have the

multiplicity k, with $k \geq 1$, in f'. In other words

$$f' = (x-\alpha_1)^k h_2,$$

where $h_2 \in \mathbb{C}[x]$. Thus, applying Lemma 4.3 for f', we have

$$(f')^{(0)}(\alpha_1) = (f')^{(1)}(\alpha_1) = \cdots = (f')^{(k-1)}(\alpha_1) = 0 \text{ and } (f')^{(k)}(\alpha_1) \neq 0. \tag{4.10}$$

Now by Lemma 4.4 and (4.8) we have

$$\frac{cf^{(k+1)}(\alpha_1)}{f(\alpha_1)} = (f^c-1)^{(k+1)}(\alpha_1) = g_1^{(k+1)}(\alpha_1)h_1^{(0)}(\alpha_1). \tag{4.11}$$

Since by (4.10) we have

$$f^{(k+1)}(\alpha_1) = (f')^{(k)}(\alpha_1) \neq 0,$$

from (4.11) we conclude that

$$g_1^{(k+1)}(\alpha_1) \neq 0.$$

Therefore we should have $t = k+1 \leq \deg f' + 1 = \deg f$. Since $\beta_1 \leq t$, we are done. □

We also need the concept of radical of a polynomial $f \in \mathbb{C}[x]$. For $f = \alpha\prod_i (x-\alpha_i)^{n_i} \in \mathbb{C}[x]$, with distinct $\alpha_i's \in \mathbb{C}$, we define the radical of f by

$$\mathrm{rad}(f) = \prod_i (x-\alpha_i).$$

Having Proposition 4.5 in hand, we can prove the main theorem of this section.

Proof. From (4.2), we have

$$f^n(f^{m-n}-1) | g^n(g^{m-n}-1). \tag{4.12}$$

From here we can deduce that

$$f^{m-n} - 1 = ab, \tag{4.13}$$

where a divides g^n and b divides $g^{m-n} - 1$. Thus,

$$b | gcd(f^{m-n} - 1, g^{m-n} - 1). \tag{4.14}$$

Now from (4.1) we have $\deg(\gcd(f^{m-n} - 1, g^{m-n} - 1)) \leq C(f,g)$. Thus, applying (4.14) we have $\deg b \leq C(f,g)$. Hence,

$$\deg a \geq (m-n)\deg f - C(f,g). \tag{4.15}$$

On the other hand, we can write

$$g = \alpha \prod_i (x - \alpha_i)^{n_i},$$

where α and α_i's belong to $\mathbb{C}$ and n_i's are natural numbers. Since a divides g^n, we can write

$$a = \gamma \prod_i (x - \alpha_i)^{\beta_i},$$

where γ divides α^n, and for each i we have $0 \leq \beta_i \leq n_i n$. Thus, from (4.13) we have

$$f^{m-n} - 1 = \gamma \prod_i (x - \alpha_i)^{\beta_i} b.$$

Applying Proposition 4.5, for each β_i we have $\beta_i \leq \deg f$. Hence, we have

$$\deg a \leq \deg(\mathrm{rad}(a)) \deg f \leq \deg(\mathrm{rad}(g)) \deg f, \tag{4.16}$$

where the last inequality holds, since a divides g^n. Combining (4.15) with (4.16) yields

$$(m-n)\deg f - C(f,g) \leq \deg(\mathrm{rad}(g))\deg f. \tag{4.17}$$

Thus $m-n$ is bounded by an absolute constant. Now from (4.12) and the fact that f and g are relatively primes, we deduce that f^n divides $g^{m-n}-1$. Thus,

$$n \leq \frac{(m-n)\deg g}{\deg f}. \tag{4.18}$$

So n is also bounded and consequently m is bounded.

□

4.2 An effective finiteness result

The bound that we have found for $m-n$ in the proof of Theorem 4.2 is not effective. Our goal in this section is to present a method that enables us to calculate all the pairs satisfying the relation (4.2). As we have seen in the proof of Theorem 4.2, if we can find an effective bound for $\deg(\gcd(f^k-1, g^k-1))$, then we can calculate all the pairs (m,n) explicitly. Unfortunately, we can not make the constant $C(f,g)$ in Theorem 4.2 effective. However, in this section we obtain a weaker effective bound for $\deg(\gcd(f^k-1, g^k-1))$.

In order to prove this effective result we need to use Mason's theorem which is analogous to the *abc*-conjecture.

Theorem 4.6 (Mason). *Let f, g, and h be three polynomials in $\mathbb{C}[x]$ which are nonzero, relatively primes, and are not simultaneously constants. Then we have*

$$\max\{\deg(f(x))\deg(g(x))\deg(h(x))\} \leq \deg(\mathrm{rad}(f(x)g(x)h(x))) - 1.$$

Proof. See [20, Section 5.3]. □

Equipped with Mason's Theorem, we establish an effective upper bound for the $\gcd(f^k -$

$1, g^k - 1)$. The method of the proof of the following theorem is inspired by the proof of Theorem 4 of [18].

Theorem 4.7. *Let $f, g \in \mathbb{C}[x]$ be two relatively prime polynomials with* $\deg f \leq \deg g$. *Also let $k > 0$ be a natural number. We have*

$$\deg(\gcd(f^k - 1, g^k - 1)) < \frac{k+2}{2} \deg g.$$

Proof. Let $\gcd(f^k - 1, g^k - 1) = d$. Thus, there are $u, v \in \mathbb{C}[x]$ such that $(u, v) = 1$ and we have

$$f^k - 1 = ud \tag{4.19}$$

and

$$g^k - 1 = vd. \tag{4.20}$$

Multiplying (4.19) by v and (4.20) by u and subtracting them, we get

$$ug^k - vf^k = u - v. \tag{4.21}$$

Our goal is to apply Mason's theorem for ug^k, vf^k, and $u - v$. Thus, we claim that ug^k, vf^k and $u - v$ are pairwise relatively prime. First we show $\gcd(vf^k, ug^k) = 1$. Let $\gcd(v, g^k) = \delta$. Since $\delta | v$, and by (4.19) $v | g^k - 1$, we have $\delta | g^k - 1$. Moreover, $\delta | g^k$. Thus, $\delta | \gcd(g^k, g^k - 1) = 1$. Hence,

$$\gcd(v, g^k) = 1. \tag{4.22}$$

With the same argument as above we have

$$\gcd(u, f^k) = 1. \tag{4.23}$$

Also by our assumptions we have

$$\gcd(f^k, g^k) = 1. \tag{4.24}$$

Now by the fact that $(u,v) = 1$ together with (4.22), (4.23), and (4.24) we conclude that $\gcd(vf^k, ug^k) = 1$.

Next we show that $\gcd(vf^k, u-v) = 1$. Let $\gcd(vf^k, u-v) = \delta$. Since $\delta | u-v$ and $\delta | vf^k$, we have $\delta | u-v+vf^k$, and thus, by (4.21) we have $\delta | ug^k$. Hence $\delta | \gcd(vf^k, ug^k) = 1$. With the same argument one can show that $(ug^k, u-v) = 1$. Therefore ug^k, vf^k and $u-v$ are pairwise relatively prime.

Now, we find $\max\{\deg\,(u-v), \deg\,(vf^k), \deg\,(ug^k)\}$. Observe that from (4.19) we have

$$vf^k = uvd + v,$$

and from (4.20) we have

$$ug^k = uvd + u.$$

From these two identities we obtain

$$\deg(vf^k) = \deg(ug^k). \tag{4.25}$$

Moreover by (4.21) we have

$$u - v = vf^k - ug^k.$$

Thus, $\deg(u-v) \leq \deg(ug^k)$. Therefore by (4.25) we have

$$\max\{\deg(u-v), \deg(vf^k), \deg(ug^k)\} = \deg(vf^k) = \deg(ug^k).$$

Hence, applying Theorem 4.6 on $u-v, vf^k$, and ug^k yields

$$\max\{\deg(u-v), \deg(vf^k), \deg(ug^k)\} = \deg(ug^k) < \deg\left(\operatorname{rad}\left(uv(u-v)f^k g^k\right)\right).$$

From here, we obtain

$$k\deg g + \deg u < \deg(u-v) + \deg f + \deg v + \deg g + \deg u. \tag{4.26}$$

Observe that by (4.25) and the assumption $\deg f \leq \deg g$, we conclude that $\deg u \leq \deg v$, and thus $\deg(u-v) \leq \deg v$. Applying this inequality in (4.26) implies

$$k\deg g < 2\deg v + \deg f + \deg g.$$

Now note that by employing (4.20) in the above inequality we have

$$2\deg d < k\deg f + \deg f + \deg g.$$

Since $\deg f \leq \deg g$, this implies

$$\deg d < \frac{k+2}{2}\deg g,$$

which is the desired result. □

Combining Theorem 4.2 and Theorem 4.7, we are able to solve the congruence $g^m - g^n \equiv 0 \pmod{f^m - f^n}$ effectively, for polynomials f and g such that $\frac{1}{2}\deg g < \deg f \leq \deg g$.

Theorem 4.8. *Let f and g be two polynomials in $\mathbb{C}[x]$ that are relatively prime and*

$$\frac{1}{2}\deg g < \deg f \leq \deg g. \tag{4.27}$$

If $m > n \geq 0$ be such that

$$f^m - f^n | g^m - g^n,$$

then we have

$$n < \frac{(\deg g + \deg(\mathrm{rad}(g))\deg f)\deg g}{(\deg f - \frac{1}{2}\deg g)\deg f} \tag{4.28}$$

and

$$m < \frac{\deg g + \deg(\mathrm{rad}(g))\deg f}{\deg f - \frac{1}{2}\deg g}\left(1 + \frac{\deg g}{\deg f}\right). \tag{4.29}$$

Proof. First of all note that from (4.14) we have

$$\deg b \leq \deg(\gcd(f^{m-n} - 1, g^{m-n} - 1)).$$

Applying Theorem 4.7 yields

$$\deg b < \frac{(m-n)+2}{2}\deg g. \tag{4.30}$$

Recall from the proof of Theorem (4.2) that $f^{m-n} - 1 = ab$. Hence, we have

$$\deg a = (m-n)\deg f - \deg b.$$

Thus, by (4.30) we deduce

$$\deg a > (m-n)\deg f - \frac{(m-n)+2}{2}\deg g.$$

Combining this with (4.16) yields

$$(m-n)\deg f - \frac{(m-n)+2}{2}\deg g < \deg(\mathrm{rad}(g))\deg f.$$

Hence, we have

$$m-n < \frac{\deg g + \deg(\mathrm{rad}(g))\deg f}{\deg f - \frac{1}{2}\deg g}. \tag{4.31}$$

Now from (4.18) and (4.31) we conclude

$$n < \frac{(\deg g + \deg(\mathrm{rad}(g))\deg f)\deg g}{(\deg f - \frac{1}{2}\deg g)\deg f}.$$

This proves (4.28). Moreover, from (4.28) and (4.31), we obtain (4.29).

□

Chapter 5

Concluding Remark

In this thesis properties of a special type of prime numbers, the so-called Wieferich primes, have been investigated. We provided a heuristic that predicts that there are approximately $\log\log x$ Wieferich primes among the primes up to x. This is a very thin subset of primes. Despite the prediction that almost all primes are non-Wieferich primes, the infinitude of the set of non-Wieferich primes has not been proven unconditionally. In Chapter 2, some conjectural theorems on the size of the set of non-Wieferich primes in certain arithmetic progressions are proved. They are Theorems 2.2 and 2.16. We then investigated a generalization of the notion of Wieferich primes to integers greater than one. Heuristically, the set of Wieferich numbers up to x has order of magnitude $\log x$. Similar to the set of Wieferich primes, no unconditional result on the size of the set of Wieferich numbers are known. However, we described a relation between the size of the set of Wieferich primes and the set of Wieferich numbers. We presented the largest element of the set of Wieferich numbers, assuming that the set of Wieferich primes is finite. In Theorem 2.17 we stated and proved this fact. It is shown unconditionally in Theorem 2.24 that the size of the set of non-Wieferich numbers in any base is infinite, although the lower bound obtained is far from the expected size of the set of Wieferich numbers.

In another direction we explored the notion of Wieferich primes and Wieferich numbers in quadratic fields of class number one, a special type of number fields. In Theorem 3.2 we proved a relation between Wieferich primes in $\mathbb{Z}$ and Wieferich primes in quadratic fields of class number one. Speaking of Wieferich numbers, a criterion for Wieferich numbers in

quadratic fields of class number one has been proved in Theorem 3.6. From the criterion we concluded that, in $\mathbb{Q}(i)$ there are infinitely many Wieferich numbers in certain bases.

In the last chapter we proved that there are only finitely many pairs (m,n) such that the congruence $g^m - g^n \equiv 0 \pmod{f^m - f^n}$ is satisfied for given polynomials f and $g \in \mathbb{C}[x]$, with $\deg f \leq \deg g$. Moreover, in Theorem 4.8 we showed how to find these pairs explicitly when f and g satisfy the relation $(1/2)\deg g < \deg f \leq \deg g$.

In continuation of the topics considered in the thesis, one may consider the following :

- Studying the size of the set of non-Wieferich primes in the arithmetic progression $p \equiv a \pmod{k}$.
- Investigating the size of the set of Wieferich numbers (respectively, non-Wieferich numbers) in a fixed congruence class.
- Investigating the relation of Conjecture 2.10 with the *abc*-conjecture for composite n.
- Studying Wieferich primes and non-Wieferich primes in other number fields (such as cubic fields).
- Exploring possible generalization of Theorems 3.2 and 3.6 to quadratic fields of class number greater than one and general number fields.
- Investigating the possibility of an effective version of Theorem 4.2 for two given polynomials f and g with $\deg f \leq \deg g$.

Bibliography

[1] Takashi Agoh, Karl Dilcher, and Ladislav Skula. Fermat quotients for composite moduli. *J. Number Theory*, 66(1):29–50, 1997.

[2] Nir Ailon and Zéev Rudnick. Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$. *Acta Arith.*, 113(1):31–38, 2004.

[3] William D. Banks, Florian Luca, and Igor E. Shparlinski. Estimates for Wieferich numbers. *Ramanujan J.*, 14(3):361–378, 2007.

[4] Jerzy Browkin. The *abc*-conjecture for algebraic numbers. *Acta Math. Sin. (Engl. Ser.)*, 22(1):211–222, 2006.

[5] Pietro Corvaja and Umberto Zannier. Some new applications of the subspace theorem. *Compositio Math.*, 131(3):319–340, 2002.

[6] J.-M. DeKoninck and N. Doyon. On the set of wieferich primes and of its complement. *Ann. Univ. Sci. Budapest. Sect. Comput.*, 27:3–13, 2007.

[7] Andrea Del Centina. Unpublished manuscripts of Sophie Germain and a revaluation of her work on Fermat's last theorem. *Arch. Hist. Exact Sci.*, 62(4):349–392, 2008.

[8] Euclid. *Euclid's Elements*. Green Lion Press, Santa Fe, NM, 2002. All thirteen books complete in one volume, The Thomas L. Heath translation, Edited by Dana Densmore.

[9] Hester Graves and M. Ram Murty. The abc conjecture and non-Wieferich primes in arithmetic progressions. *J. Number Theory*, 133(6):1809–1813, 2013.

[10] K. Győry. On the *abc* conjecture in algebraic number fields. *Acta Arith.*, 133(3):281–295, 2008.

[11] Henryk Iwaniec and János Pintz. Primes in short intervals. *Monatsh. Math.*, 98(2):115–143, 1984.

[12] Srinivas Kotyada and Subramani Muthukrishnan. Non-wieferich primes in number fields and abc conjecture in number fields. arXiv:1610.00488 [math.NT]., October 2016.

[13] Serge Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, 1978.

[14] Serge Lang. *Algebra*. Addison-Wesley publishing company, third edition, 1993.

[15] D. W. Masser. Open problems. In Chen, W. W. L. Proceedings of the Symposium on Analytic Number Theory. London: Imperial College, 1985.

[16] M. Ram Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2008. Readings in Mathematics.

[17] M. Ram Murty and Jody Esmonde. *Problems in algebraic number theory*, volume 190 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2005.

[18] M. Ram Murty and V. Kumar Murty. On a problem of Ruderman. *Amer. Math. Monthly*, 118(7):644–650, 2011.

[19] Władysł aw Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[20] Melvyn B. Nathanson. *Elementary methods in number theory*, volume 195 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[21] Joseph Oesterlé. Nouvelles approches du "théorème" de Fermat. *Astérisque*, (161-162):Exp. No. 694, 4, 165–186 (1989), 1988. Séminaire Bourbaki, Vol. 1987/88.

[22] Michael Rosen. A generalization of Mertens' theorem. *J. Ramanujan Math. Soc.*, 14(1):1–19, 1999.

[23] Joseph H. Silverman. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory*, 30(2):226–237, 1988.

[24] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem*. CRC Press, Boca Raton, FL, fourth edition, 2016.

[25] R. Thangadurai and A. Vatwani. The least prime congruent to one modulo *n*. *Amer. Math. Monthly*, 118(8):737–742, 2011.

[26] Arthur Wieferich. Zum letzten Fermatschen Theorem. *J. Reine Angew. Math.*, 136:293–302, 1909.

[27] Eduard Wirsing. Über die Zahlen, deren Primteiler einer gegebenen Menge angehören. *Arch. Math.*, 7:263–272, 1956.

Appendix A

Tables

Table A.1: Values of $\lambda(\Phi_n(a)) \geq 2$ for $1 \leq a \leq 100$

a	n	$\lambda(\Phi_n(a))$
3	2	2
3	5	2
5	1	2
8	2	2
9	1	3
10	1	2
15	2	4
17	1	4
18	3	3
19	6	3
24	2	2
26	1	2
26	2	3
28	1	3
31	2	5
33	1	5
35	2	2
37	1	2
47	2	2.16056
48	2	2
49	1	2.16056
50	1	2
53	2	2.22629
55	1	2.22629

a	n	$\lambda(\Phi_n(a))$
63	2	6
65	1	6
71	2	2.38685
73	1	2.38685
80	2	4
82	1	4
95	2	2.54741
97	1	2.54741
99	2	2
101	1	2
107	2	2.61315

Table A.2: The largest known Wieferich numbers in some bases $2 \leq a \leq 30$.

a	Wieferich primes p base a	Largest Wieferich number
2	1093, 3511	$3^6 \times 5 \times 7 \times 13^2 \times 1093 \times 3511$
3	11, 1006003	$2^{14} \times 5^2 \times 7 \times 11 \times 41 \times 83 \times 499 \times 55889 \times 1006003$
4	1093, 3511	$3^6 \times 5 \times 7 \times 13^2 \times 1093 \times 3511$
6	66161, 281409, 534851	$5^6 \times 7^3 \times 11 \times 17 \times 19 \times 23 \times 29 \times 41 \times 47 \times 59 \times 281 \times 409 \times 563 \times 827 \times 3152573 \times 66161 \times 281409 \times 534851$
7	5, 491531	$2^9 \times 3^5 \times 5^3 \times 11 \times 13 \times 19 \times 199 \times 491531$
8	3, 1093, 3511	$3^7 \times 5 \times 7 \times 13^2 \times 1093 \times 3511$
9	2, 11, 1006003	$2^{16} \times 5^2 \times 7 \times 11 \times 41 \times 83 \times 499 \times 55889 \times 1006003$
10	3, 487, 56598313	$3^{12} \times 7 \times 11 \times 13 \times 23 \times 31 \times 127 \times 487 \times 599 \times 56598313$
11	71	$2^6 \times 3^3 \times 5 \times 7 \times 71$
12	2693, 123653	$5 \times 7 \times 19 \times 271 \times 673 \times 1627 \times 2693 \times 123653$
13	2, 863, 1747591	$2^{17} \times 3^4 \times 5^3 \times 7^2 \times 43 \times 431 \times 863 \times 4481 \times 1747591$
18	5, 7, 37, 331, 33923, 1284043	$5^4 \times 7^4 \times 11 \times 13 \times 17 \times 37 \times 43 \times 137 \times 331 \times 823 \times 2423^2 \times 8231 \times 214007 \times 33923 \times 1284043$
19	3, 7, 13, 43, 137, 63061489	$2^{23} \times 3^9 \times 7^4 \times 13^2 \times 17 \times 43 \times 53 \times 73 \times 107 \times 137 \times 857 \times 63061489$
20	281, 46457, 9377747, 122959073	$3^{10} \times 7^4 \times 17 \times 29^3 \times 59 \times 281 \times 433 \times 883 \times 1451 \times 2903 \times 46457 \times 132499 \times 122959073$
21	2	2
24	5, 25633	$5^2 \times 43 \times 89 \times 25633$
27	11, 1006003	$2^{14} \times 5^2 \times 7 \times 11 \times 41 \times 83 \times 499 \times 55889 \times 1006003$
28	3, 19, 23	$3^4 \times 5 \times 11 \times 19 \times 23$
29	2	2

Table A.3: $\mathbb{Q}(i)$-Wieferich primes π in base a where $N(\pi) \leq 4000$ and $N(a) \leq 30$

Norm	Base	K-Wieferich primes
2	$1+i$	$33-2i, 33+2i$
	$1-i$	$33-2i, 33+2i$
4	$2i$	$33-2i, 33+2i$
	2	$33-2i, 33+2i$
5	$1+2i$	$1-4i,-15-4i,-19-10i$
	$1-2i$	$1+4i,-15+4i,-19+10i$
	$2+i$	$1+4i,-15+4i,-19+10i$
	$2-i$	$1-4i,-15-4i,-19-10i$
8	$2i+2$	$3,33-2i,33+2i$
	$2i-2$	$3,33-2i,33+2i$
9	$3i$	11
	3	11
10	$3+i$	$5+8i, -7+10i$
	$3-i$	$5-8i, -7-10i$
	$3i+1$	$5-8i, -7-10i$
	$3i-1$	$5+8i, -7+10i$
13	$2+3i$	$-19+16i$
	$2-3i$	$-19-16i$
	$3+2i$	$-19-16i$
	$3-2i$	$-19+16i$
16	$4i$	$33-2i,33+2i$
	4	$33-2i,33+2i$
17	$1+4i$	*
	$1-4i$	*
	$i+4$	*
	$i-4$	*
18	$3+3i$	$7, 1+2i, 1-2i, 1+6i, 1-6i$
	$3-3i$	$7, 1+2i, 1-2i, 1+6i, 1-6i$
20	$2+4i$	$1-2i$
	$2-4i$	$1+2i$
	$4+2i$	$1+2i$
	$4-2i$	$1-2i$
25	$5i$	*
	$3+4i$	$1+4i,-15+4i,-19+10i$
	$3-4i$	$1-4i,-15-4i,-19-10i$
	$4+3i$	$1-4i,-15-4i,-19-10i$
	$4-3i$	$1+4i,-15+4i,-19+10i$
	5	*
26	$1+5i$	*
	$1-5i$	*
	$5+i$	*
	$5-i$	*
29	$2+5i$	$5-4i,9+10i,5+36i$
	$2+5i$	$5+4i,9-10i,5-36i$
	$5+2i$	$5-4i,9+10i,5+36i$
	$5-2i$	$5-4i,9+10i,5+36i$

Table A.4: Some $\mathbb{Q}(i)$-Wieferich numbers with prime divisors above inert primes

Norm	Base	K-Wieferich number with inert prime divisors
2	$1+i$	$3(33+2i)$
	$1-i$	$3(33+2i)i$
4	$2i$	$3(33+2i)$
	2	$3(33+2i)$
5	$1+2i$	$3(1-2i)(15+4i)$
	$1-2i$	$3(1-2i)(15+4i)$
	$2+i$	$3(1+i)(15-4i)$
	$2-i$	$3(1-2i)(1-4i)(15+4i)$
8	$2i+2$	$3(33+2i)$
	$2i-2$	$3(33+2i)$
9	$3i$	$(1+i)^3 11(1-2i)$
	3	$(1+i)^3 11(1-2i)$
10	$3+i$	$11(5+8i)$
	$3i-1$	$3(33+2i)$
16	4	$3(3+2i)(33+2i)$
	4i	$3(3+2i)(33+2i)$
18	$3+3i$	$7(1+6i)$
	$3-3i$	$7(1+6i)$
20	$2+4i$	$47+72i$
	$4-2i$	$47+72i$
25	$3+4i$	$3(1+i)(15-4i)$
	$3-4i$	$3(1+i)^3(1-2i)(15+4i)$
	$4+3i$	$3(1+i)^3(1-2i)(15+4i)$
	$4-3i$	$3(1+i)(15-4i)$
29	$2+5i$	$3i(1+i)^2(9+10i)$
	$2-5i$	$3(1-2i)(-5+36i)$
	$5+2i$	$3(1-2i)(-5+36i)$
	$5-2i$	$3i(1+i)^2(9+10i)$

Table A.5: All solutions (m,n) of $f^m - f^n | g^m - g^n$

f	g	(m,n)
x^2+x+1	x^3+x^2+2x+1	$(2,0)$
x^2+x+1	x^3+2x^2+3x+1	$(2,0)$
$2x^2+x+1$	$4x^3+4x^2+5x+1$	$(2,0)$
$2x^2+x+1$	$4x^3+2x^2+4x+1$	$(2,0)$
$2x^2+2x+1$	$2x^3+2x^2+2x+1$	$(2,0)$
$2x^2+2x+1$	$2x^3+4x^2+4x+1$	$(2,0)$