THE ABC CONJECTURE AND ITS CONSEQUENCES

by

Büşra Budak

Submitted to Graduate School of Natural and Applied Sciences
in Partial Fulfillment of the Requirements
for the Degree of Master of Science in
Mathematics

Yeditepe University

2021

THE ABC CONJECTURE AND ITS CONSEQUENCES

APPROVED BY:

Assist. Prof. Dr. Erol Serbest . . . . . .
(Thesis Supervisor)
(Yeditepe University)

Prof. Dr. Ender Abadoğlu . . . . . .
(Yeditepe University)

Prof. Dr. Kazım İlhan İkeda . . . . . .
(Boğaziçi University)

DATE OF APPROVAL: . . . . . /. . . . . /2021

I hereby declare that this thesis is my own work and that all information in this thesis has been obtained and presented in accordance with academic rules and ethical conduct. I have fully cited and referenced all material and results as required by these rules and conduct, and this thesis study does not contain any plagiarism. If any material used in the thesis requires copyright, the necessary permissions have been obtained. No material from this thesis has been used for the award of another degree.

I accept all kinds of legal liability that may arise in case contrary to these situations.

Name, Last name ……

Signature …..…….……..

ACKNOWLEDGEMENTS

I would like to start my words by giving my deepest thanks to my dear thesis supervisor Asist. Prof. Dr. Erol Serbest whom I took my undergraduate courses from, contributed to my love of the algebra and my progress on this area. The way he leads me on how I can learn and teach Mathematics better will shine a light on my journey to become a better teacher throughout my life. I am very grateful to him for accompanying and supporting me sincerely to write my thesis at this process.

I thank the members of the Department of Mathematics at Yeditepe University.

I thank my friend Serdar Nair for sharing his experience in LaTeX with me.

I wholeheartedly thank my friend Gülcan Doğanay who is always there for me and encourages me to do what i can do in my life.

Finally, I present my gratitude to my family, especially my dearest brother Burak Budak, and my friends due to their support and belief in my success.

ABSTRACT

THE ABC CONJECTURE AND ITS CONSEQUENCES

The abc-conjecture is an integer analogue of Mason-Stothers theorem for polynomials which was proposed by J. Oesterle and D. Masser in number theory. It expresses a relation between multiplication and addition for integers. Stronger versions of this conjecture yield solutions of many important problems including Fermat's Last Theorem. Using his Inter-universal Teichmüller theory, S. Mochizuki obtained proofs of non-effective Vojta, Szpiro, and abc-conjectures over algebraic number fields. More recently, an effective abc-conjecture over $\mathbb{Q}$ or an imaginary quadratic number fields and the Szpiro conjecture have been proved by I. Fesenko, Y. Hoshi, A. Minamide ,S. Mochizuki and W. Porowski. In this thesis, the above developments are discussed in some detail.

ÖZET

ABC SANISI VE SONUÇLARI

abc-sanısı, polinomlar için olan Mason-Stothers teoreminin J. Oesterle ve D. Masser tarafından tamsayılar için önerilen sayılar kuramında bir sanıdır. Bu sanı tamsayılardaki çarpma ve toplama işlemleri arasındaki ilişkiyi ifade eder. Bu sanının daha güçlü versiyonları, Fermat'ın Son Teoremi de dahil olmak üzere birçok önemli problemin çözümlerini vermektedir. S. Mochizuki, kendisinin geliştirmiş olduğu Inter-universal Teichmüller teorisini kullanarak cebirsel sayı cisimleri üzerinde tanımlı efektif olmayan Vojta, Szpiro ve abc-sanılarının ispatlarını elde etmiştir. I. Fesenko, Y. Hoshi, A. Minamide ,S. Mochizuki ve W. Porowski yakın geçmişte, $\mathbb{Q}$ üzerinde veya sanal ikinci dereceden sayı cisimleri üzerinde tanımlı abc-sanısı ve Szpiro sanısının efektif versiyonlarını kanıtlamışlardır. Bu tezde, yukarıdaki gelişmeler ayrıntılı olarak tartışılmaktadır.

TABLE OF CONTENTS

LIST OF SYMBOLS/ABBREVIATIONS

$\mathbb{C}$	The set of complex numbers
$\mathbb{C}[t]$	The ring of the polynomial with complex coefficients
$D(f)$	The derivative of the polynomial $f \in \mathbb{C}[t]$
$\deg(f)$	The degree of the polynomial f
$\gcd(x, y)$	The largest positive integer that divides both x and y
$\max\{x, y\}$	The maximum of x and y
$\mathbb{N}$	The set of natural numbers
$\mathrm{ord}_p(a)$	The order of a modulo p
$\mathbb{Q}$	The set of rational numbers
$\mathbb{R}$	The set of real numbers
$\mathrm{Rad}(a)$	The radical of a
$\mathbb{Z}$	The set of integer numbers

1. INTRODUCTION

Integers are the most fundamental mathematical objects. Some of the most difficult problems in mathematics are about integers. We have two operations on the set of integers: addition and multiplication. Prime numbers can be viewed as atoms with respect to the multiplication. Many important problems in mathematics are about hidden relations between multiplication and addition for integers.

A version of abc-conjecture claims that:

There is an $n \in \mathbb{Z}_{>0}$ such that for each $\epsilon > 0$, there exist a positive number $C(\epsilon)$ such that, for any non-zero $a, b, c \in \mathbb{Z}$ with

$$\gcd(a, b, c) = 1 \quad \text{and} \quad a + b = c. \tag{1.1}$$

Then, we have

$$\max\{|a|, |b|, |c|\} < C(\epsilon)\,\mathrm{Rad}(abc)^{n+\epsilon} \tag{1.2}$$

where $\mathrm{Rad}(abc)$ denotes the radical of abc, namely, the product of distinct prime numbers dividing abc. In some stronger versions the number n is taken to be 1. Observe that the abc-conjecture describes a kind of balance or tension between multiplication and addition. This conjecture is an integer analogue of Mason-Stothers theorem for polynomials which was proposed by J. Oesterle (1988) and D. Masser (1985) in number theory. It has many applications in number theory. In particular, it implies the simplified proofs of many difficult results and important conjectures in Diophantine equations-including Fermat's Last Theorem and its variants.

As a result of 20 years work in anabelian geometry, Hodge-Arakelov theory and p-adic Teichmüller theory, S. Mochizuki has developed the Inter-universal Teichmüller Theory (IUT), also known as arithmetic deformation theory, in [1], to understand the abc-conjecture deeply. The papers related to his IUT theory were made public in 2012 and published in 2021. IUT theory studies such fundamental aspects as to which extent we can not separate the addition and multiplication on integers from each other. Using his IUT theory, S. Mochizuki proved non-effective Vojta, Szpiro and abc-conjectures over algebraic number fields.

More recently, in [2], based on IUT theory and its slight enhancement, S. Mochizuki, I. Fesenko, Y. Hoshi, A. Minamide A, and W. Porowski established effective abc and Szpiro conjectures. Moreover, they established the First Case of Fermat's Last Theorem for all primes $p > 2$ and the Second Case of Fermat's Last Theorem for all primes $p > 3.35 \cdot 10^9$.

The organization of the text is as follows:

In Chapter 2, we first give the proof of Mason-Stothers theorem, also known as the abc-theorem for polynomials. As a first application of this theorem, we give the proof of Fermat Last Theorem for polynomials. We also discuss its application to generalized Fermat Last Theorem for polynomials.

In Chapter 3, we first state the abc-conjecture for integers and its explicit version due to A. Baker for integers. Then we consider its various applications including Fermat's Last Theorem for exponent $n \geq 6$, generalized version Fermat Last Theorem for integers, powerful numbers, Wieferich primes, Erdös-Woods conjecture and some others.

In Chapter 4, following [2], we first state effective versions of the abc-conjecture over integers and Szpiro conjecture and then discuss in detail applications to Fermat's Last Theorem and its generalized version.

In this thesis, we claim no originality.

2. THE MASON-STOTHERS THEOREM

In this chapter, after the proof of Mason-Stothers theorem, we consider its applications to Fermat's Last Theorem and its generalized version for polynomials.

The main references for this chapter are [3] and [4].

2.1. THE MASON-STOTHERS THEOREM

First we consider the map

$$D : \mathbb{C}[t] \longrightarrow \mathbb{C}[t] \tag{2.1}$$

defined by

$$D : \sum_{j=0}^{n} a_j t^j \longmapsto \sum_{j=1}^{n} j a_j t^{j-1}. \tag{2.2}$$

The map D satisfy the following conditions:

- $D(\alpha f + \beta g) = \alpha D(f) + \beta D(g)$,
- $D(fg) = D(f)\, g + f D(g)$,

for all $\alpha, \beta \in \mathbb{C}$ and $f,\ g \in \mathbb{C}[t]$. From now on we write f' instead of $D(f)$.

It is well known that $\mathbb{C}[t]$ is a unique factorization domain (in short UFD). Therefore, if f is a non-zero polynomial in $\mathbb{C}[t]$ then there exist irreducible polynomials $p_1,\ p_2,\ \cdots,\ p_n \in \mathbb{C}[t]$, $k_1,\ k_2,\ \cdots,\ k_n \in \mathbb{N}$ and $a \in \mathbb{C}$ such that

$$f = a \prod_{j} p_j^{k_j}. \tag{2.3}$$

The radical of such a polynomial f is defined by

$$\mathrm{Rad}(f) = a \prod_{j} p_j. \tag{2.4}$$

W.W. Stothers [5] and, independently, R. Mason [6], [7] proved the following theorem. We give the elegant proof due to N. Synder [3].

Theorem 2.1.1 (The Mason-Stothers Theorem)**.** *Let f, g and h be three non-constant co-*

prime polynomials in $\mathbb{C}[t]$ *such that* $f + g = h$. *Then*

$$\max\{\deg(f), \deg(g), \deg(h)\} \leq \deg\big(\mathrm{Rad}(fgh)\big) - 1. \tag{2.5}$$

First, the following lemma must be established.

Lemma 2.1.2. *Let* f *be a non-zero polynomial in* $\mathbb{C}[t]$. *Then we have*

$$\deg\big(\gcd(f, f')\big) \geq \deg(f) - \deg\big(\mathrm{Rad}(f)\big). \tag{2.6}$$

Proof. Recall that $\mathbb{C}[t]$ is a UFD. Therefore, if f is a non-zero polynomial in $\mathbb{C}[t]$ then there exist irreducible polynomials $p_1, p_2, \cdots, p_n \in \mathbb{C}[t]$, $k_1, k_2, \cdots, k_n \in \mathbb{N}$ and $a \in \mathbb{C}$ such that

$$f = a\prod p_j^{k_j}. \tag{2.7}$$

For any $j = 1, 2, \cdots, n$ we write $f = p_j^{k_j} \cdot q_j$. Then

$$f' = k_j \cdot p_j^{k_j-1} \cdot p_j' \cdot q_j + p_j^{k_j} \cdot q_j' \tag{2.8}$$

$$= p_j^{k_j-1}(k_j \cdot p_j' \cdot q_j + p_j \cdot q_j'). \tag{2.9}$$

Therefore, $p_j^{k_j-1} \mid f'$ for each $j = 1, 2, \cdots, n$. Since $\gcd(p_1, p_2, \cdots, p_n) = 1$, we have

$$\prod_{j=1}^{n} p_j^{k_j-1} \,\Big|\, f'. \tag{2.10}$$

Since also

$$\prod_{j=1}^{n} p_j^{k_j-1} \,\Big|\, f, \tag{2.11}$$

it follows that

$$\prod_{j=1}^{n} p_j^{k_j-1} \,\Big|\, \gcd(f, f'). \tag{2.12}$$

Then

$$\deg\left(\prod_{j=1}^{n} p_j^{k_j-1}\right) \leq \deg\big(\gcd(f, f')\big). \tag{2.13}$$

Moreover, we have

$$\left(\prod_{j=1}^{n} p_j^{k_j-1}\right) \cdot \mathrm{Rad}(f) = f. \tag{2.14}$$

So, we get

$$\deg\left(\prod_{j=1}^{n} p_j^{k_j-1}\right) + \deg\big(\mathrm{Rad}(f)\big) = \deg(f). \tag{2.15}$$

Finally we obtain

$$\deg\big(\gcd(f, f')\big) \geq \deg\left(\prod_{j=1}^{n} p_j^{k_j-1}\right) = \deg(f) - \deg\big(\mathrm{Rad}(f)\big). \tag{2.16}$$

□

Proof of Theorem 2.1.1. Since $\gcd(f, g, h) = 1$ we get

$$\gcd(f, g) = \gcd(f, h) = \gcd(g, h) = 1. \tag{2.17}$$

Recall that we have

$$f + g = h. \tag{2.18}$$

Applying D, we get

$$f' + g' = h'. \tag{2.19}$$

If we multiply the equation (2.18) by g' and equation (2.19) by g we get

$$fg' + gg' = hg' \tag{2.20}$$

$$gf' + gg' = gh'. \tag{2.21}$$

Subtracting the equation (2.20) from the equation (2.21) we get

$$fg' - gf' = hg' - gh'. \tag{2.22}$$

Claim. We have $f'g \neq fg'$.

Assume, on the contrary, that $f'g = fg'$. Then $f \mid (f'g)$. Since $\gcd(f, g) = 1$ we conclude that $f \mid f'$. So $f' = 0$. Therefore f is constant which gives a contradiction since we assumed that f is non-constant.

Note that $\gcd(f,f') \mid (fg' - gf')$ and $\gcd(g,\, g') \mid (fg' - f'g)$. By equation (2.20), $\gcd(h,\, h') \mid (fg' - f'g)$. Since $\gcd(f,\, g,\, h) = 1$ we get

$$\gcd\Big(\gcd(f,f'),\, \gcd(g,\, g'),\, \gcd(h,h')\Big) = 1 \tag{2.23}$$

and hence

$$\gcd(f,f')\, \gcd(g,\, g')\, \gcd(h,h') \mid (f'g - fg'). \tag{2.24}$$

Moreover,

$$\deg(fg' - gf') \leq \deg(f) + \deg(g) - 1. \tag{2.25}$$

By Lemma 2.1.2 we have

- $\deg\big(\gcd(f,f')\big) \geq \deg(f) - \deg\big(\mathrm{Rad}(f)\big)$,
- $\deg\big(\gcd(g,\, g')\big) \geq \deg(g) - \deg\big(\mathrm{Rad}(g)\big)$,
- $\deg\big(\gcd(h,\, h')\big) \geq \deg(h) - \deg\big(\mathrm{Rad}(h)\big)$.

Therefore we obtain

$$\deg\big(\gcd(f,f')\, \gcd(g,\, g')\, \gcd(h,\, h')\big) \tag{2.26}$$

$$= \deg\big(\gcd(f,f')\big) + \deg\big(\gcd(g,\, g')\big) + \deg\big(\gcd(h,\, h')\big) \tag{2.27}$$

$$\geq \big(\deg(f) - \deg\big(\mathrm{Rad}(f)\big)\big) + \big(\deg(g) - \deg\big(\mathrm{Rad}(g)\big)\big) + \big(\deg(h) - \deg\big(\mathrm{Rad}(h)\big)\big). \tag{2.28}$$

It follows from the equation (2.24) that

$$\deg\big(\gcd(f,f')\, \gcd(g,\, g')\, \gcd(h,\, h')\big) \leq \deg(fg'-f'g) \leq \deg(f)+\deg(g)-1. \tag{2.29}$$

Hence we get

$$\deg(f) + \deg(g) - 1 \geq \deg\big(\gcd(f,f')\big) + \deg\big(\gcd(g,\, g')\big) + \deg\big(\gcd(h,\, h')\big) \tag{2.30}$$

$$\geq \deg(f) + \deg(g) + \deg(h) \tag{2.31}$$

$$- \deg\big(\mathrm{Rad}(f)\big) - \deg\big(\mathrm{Rad}(g)\big) - \deg\big(\mathrm{Rad}(h)\big). \tag{2.32}$$

If we rearrange then we obtain

$$\deg(h) \leq \deg\big(\mathrm{Rad}(f)\big) + \deg\big(\mathrm{Rad}(g)\big) + \deg\big(\mathrm{Rad}(h)\big) - 1 \tag{2.33}$$

$$= \deg\big(\mathrm{Rad}(fgh)\big) - 1. \tag{2.34}$$

Next using the above argument with the following equation

$$h + (-f) = g \tag{2.35}$$

we get

$$\deg(g) \leq \deg\big(\mathrm{Rad}(fgh)\big) - 1. \tag{2.36}$$

Finally using the above argument with the following equation

$$h + (-g) = f \tag{2.37}$$

we get

$$\deg(f) \leq \deg\big(\mathrm{Rad}(fgh)\big) - 1. \tag{2.38}$$

Thus we have shown that

$$\deg(f), \deg(g), \deg(h) \leq \deg\big(\mathrm{Rad}(fgh)\big) - 1 \tag{2.39}$$

and as a result we get

$$\max\{\deg(f), \deg(g), \deg(h)\} \leq \deg\big(\mathrm{Rad}(fgh)\big) - 1. \tag{2.40}$$

This completes the proof. □

2.2. TWO APPLICATIONS

In this section, it is possible to consider the applications of Mason-Stothers Theorem to Fermat's Last Theorem for polynomials and its generalized version.

2.2.1 Fermat's Last Theorem for Polynomials

Now, consider the non-constant co-prime solutions (if any) of the Fermat equation

$$f^n + g^n = h^n \tag{2.41}$$

in $\mathbb{C}[t]$.

When $n = 1$, the corresponding equation has infinitely many such solutions.

In the case $n = 2$:

Theorem 2.2.1. *The Fermat equation*

$$f^2 + g^2 = h^2 \tag{2.42}$$

has infinitely many non-constant co-prime solutions. Any solution of this equation is of the form

$$f = r^2 - s^2, \qquad g = 2rs, \qquad h = r^2 + s^2, \tag{2.43}$$

for some polynomials $r, s \in \mathbb{C}[t]$ *with* $\gcd(r, s) = 1$.

First the following proposition must be established which will be used frequently throughout the thesis.

Proposition 2.2.2. *Let R be a UFD. Let* $a, b \in R$ *such that*

$$\gcd(a, b) = 1 \quad \text{and} \quad ab = c^n \tag{2.44}$$

for some element $c \in R$ *and* $n \in \mathbb{N}$. *Then there are elements* $u, v \in R$ *and* $d \in R^*$ *such that*

$$a = du^n \quad \text{and} \quad b = d^{-1}v^n. \tag{2.45}$$

(R^* denotes the group of units of R.)

Proof. Put k denotes the number of prime factors of c. The proof is by induction on k.

- If $k = 0$, then c is a unit. In this case, a and b are also units. So we can write

$$a = a\,1_R^n \quad \text{and} \quad b = a^{-1}\,c^n. \tag{2.46}$$

- If $k \geq 1$, then there exist at least one prime element p such that $p \mid c$ and hence $p^n \mid c^n$. Since $c^n = ab$, it follows that $p^n \mid ab$. Therefore, $p^n \mid a$ or $p^n \mid b$, but not both since $\gcd(a, b) = 1$ and R is a UFD.

Assume that $p^n \mid b$. We get

$$a\left(\frac{b}{p^n}\right) = \left(\frac{c}{p}\right)^n. \tag{2.47}$$

Hence $\frac{c}{p}$ has clearly fewer prime divisors than c. Therefore, by induction, one gets

$$a = du^n \quad \text{and} \quad \frac{b}{p^n} = d^{-1}\, v^n \tag{2.48}$$

for some units $d,\ d^{-1} \in R^*$ and $u,\ v \in R$ so $b = d^{-1}\,(pv)^n$. □

Proof of Theorem 2.2.1. Let r and s be two polynomials in $\mathbb{C}[t]$ such that $\gcd(r,\ s) = 1$. Define

$$f := r^2 - s^2, \qquad g := 2rs, \qquad h := r^2 + s^2. \tag{2.49}$$

Claim 1 : We have $f^2 + g^2 = h^2$.

Indeed,

$$f^2 + g^2 = \left(r^2 - s^2\right)^2 + \left(2rs\right)^2 \tag{2.50}$$

$$= r^4 - 2r^2s^2 + s^4 + 4r^2s^2 \tag{2.51}$$

$$= r^4 + 2r^2s^2 + s^4 \tag{2.52}$$

$$= \left(r^2 + s^2\right)^2 \tag{2.53}$$

$$= h^2. \tag{2.54}$$

Claim 2 : We have $\gcd\left(f,\ g,\ h\right) = 1$.

It is enough to prove that $\gcd(f,\ h) = 1$. Assume, on the contrary, that $\gcd(f,\ h) \neq 1$. Any prime element $p \in \mathbb{C}[t]$ is takes the form $p = t - \alpha$ for some $\alpha \in \mathbb{C}$. Then there is a prime element $p \in \mathbb{C}[t]$ satisfying $p \mid f$ and $p \mid h$. This implies that $p \mid (h + f)$ and hence $p \mid 2r^2$. Similarly, $p \mid (h - f)$ and hence $p \mid 2s^2$. Therefore we see that $p \mid r$ and $p \mid s$ which contradicts the assumption $\gcd(r,\ s) = 1$. Hence $\gcd\left(f,\ g,\ h\right) = 1$.

Next, assume that there are non-constant polynomials $f,\ g,\ h \in \mathbb{C}[t]$ such that $f^2 + g^2 = h^2$ and $\gcd\left(f, g,\ h\right) = 1$. We want to show that there are polynomials $r,\ s \in \mathbb{C}[t]$ satisfying

$f = r^2 - s^2,\ g = 2rs$ and $h = r^2 + s^2$ with $\gcd(r, s) = 1$. Now we have

$$g^2 = h^2 - f^2 = (h + f)(h - f) \tag{2.55}$$

from which we get

$$\left(\frac{g}{2}\right)^2 = \left(\frac{h+f}{2}\right)\left(\frac{h-f}{2}\right). \tag{2.56}$$

Claim 3 : We have $\gcd\left(\frac{h+f}{2}, \frac{h-f}{2}\right) = 1$.

Suppose that

$$\gcd\left(\frac{h+f}{2}, \frac{h-f}{2}\right) \neq 1. \tag{2.57}$$

Then there is a prime element $p \in \mathbb{C}[t]$ satisfying

$$p \,\Big|\, \left(\frac{h+f}{2}\right) \quad \text{and} \quad p \,\Big|\, \left(\frac{h-f}{2}\right). \tag{2.58}$$

This implies

$$p \,\Big|\, \left[\left(\frac{h+f}{2}\right) + \left(\frac{h-f}{2}\right)\right] \quad \text{and} \quad p \,\Big|\, \left[\left(\frac{h+f}{2}\right) - \left(\frac{h-f}{2}\right)\right]. \tag{2.59}$$

Since

$$\left[\left(\frac{h+f}{2}\right) + \left(\frac{h-f}{2}\right)\right] = h \quad \text{and} \quad \left[\left(\frac{h+f}{2}\right) - \left(\frac{h-f}{2}\right)\right] = f, \tag{2.60}$$

we get $p \,|\, h$ and $p \,|\, f$. However, $\gcd(h, f) = 1$ as not equal to be as we assumed. So,

$$\gcd\left(\frac{h+f}{2}, \frac{h-f}{2}\right) = 1. \tag{2.61}$$

By Proposition 2.2.2, then there is a complex number $d \neq 0$ and polynomials $r_1,\ s_1 \in \mathbb{C}[t]$ satisfying

$$\frac{h+f}{2} = d\, r_1^2 \quad \text{and} \quad \frac{h-f}{2} = d^{-1}\, s_1^2. \tag{2.62}$$

Since every complex number is a square in $\mathbb{C}$ we get

$$\frac{h+f}{2} = r^2 \quad \text{and} \quad \frac{h-f}{2} = s^2 \tag{2.63}$$

for some polynomials $r,\ s \in \mathbb{C}[t]$. Solving the above equations for h and f we obtain

$$h = r^2 + s^2 \quad \text{and} \quad f = r^2 - s^2. \tag{2.64}$$

Since

$$g^2 = h^2 - f^2 = (h+f)(h-f) = 2r^2 2s^2 = 4r^2 s^2, \tag{2.65}$$

it follows that $g = \pm 2rs$. If necessary, replacing r with $-r$, we may suppose $g = 2rs$. Moreover, it is clear that $\gcd(r, s) = 1$. □

When $n \geq 3$, we have:

Theorem 2.2.3 (Fermat's Last Theorem for Polynomials)**.** *The Fermat equation*

$$f^n + g^n = h^n \tag{2.66}$$

does not have non-constant co-prime solutions in $\mathbb{C}[t]$ *for* $n \geq 3$.

Proof. Assume that such polynomials f, g and h exist. Applying Theorem 2.1.1 to the polynomials f^n, g^n and h^n we get

$$\begin{aligned} n\deg(f) = \deg(f^n) &\leq \deg\big(\mathrm{Rad}(f^n g^n h^n)\big) - 1 && (2.67)\\ &= \deg\big(\mathrm{Rad}(fgh)\big) - 1 && (2.68)\\ &= \deg\big(\mathrm{Rad}(f)\mathrm{Rad}(g)\mathrm{Rad}(h)\big) - 1 && (2.69)\\ &= \deg\big(\mathrm{Rad}(f)\big) + \deg\big(\mathrm{Rad}(g)\big) + \deg\big(\mathrm{Rad}(h)\big) - 1 && (2.70)\\ &\leq \deg(f) + \deg(g) + \deg(h) - 1. && (2.71) \end{aligned}$$

Similarly we get

$$\begin{aligned} n\deg(g) = \deg(g^n) &\leq \deg(f) + \deg(g) + \deg(h) - 1 && (2.72)\\ n\deg(h) = \deg(h^n) &\leq \deg(f) + \deg(g) + \deg(h) - 1. && (2.73) \end{aligned}$$

Summing up we get

$$n\big(\deg(f) + \deg(g) + \deg(h)\big) \leq 3\big(\deg(f) + \deg(g) + \deg(h)\big) - 3 \tag{2.74}$$

from which it follows that

$$(n-3)\big(\deg(f) + \deg(g) + \deg(h)\big) \leq -3 \tag{2.75}$$

which is not possible since $\deg(f) + \deg(g) + \deg(h) > 0$ and $n \geq 3$. This is a contradiction. This completes the proof. □

2.2.2 Generalized Fermat's Last Theorem for Polynomials

Theorem 2.2.4. *Let* $p, q, r \in \mathbb{N}$. *Then the generalized Fermat equation*

$$f^p + g^q = h^r \tag{2.76}$$

does not have non-constant co-prime solutions in $\mathbb{C}[t]$ *where*

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1. \tag{2.77}$$

Proof. Assume that such polynomials f, g, and h exist. Applying Theorem 2.1.1 to the polynomials f^p, g^q, and h^r we get

$$p \deg(f) = \deg(f^p) \leq \deg\left(\mathrm{Rad}(f^p g^q h^r)\right) - 1 \tag{2.78}$$

$$= \deg\left(\mathrm{Rad}(fgh)\right) - 1 \tag{2.79}$$

$$\leq \deg(fgh) - 1 \tag{2.80}$$

$$< \deg(fgh). \tag{2.81}$$

Similarly we get

$$q \deg(g) = \deg(g^q) < \deg(fgh) \tag{2.82}$$

$$r \deg(h) = \deg(h^r) < \deg(fgh). \tag{2.83}$$

Therefore we get

$$\frac{\deg(f)}{\deg(fgh)} < \frac{1}{p} \tag{2.84}$$

$$\frac{\deg(g)}{\deg(fgh)} < \frac{1}{q} \tag{2.85}$$

$$\frac{\deg(h)}{\deg(fgh)} < \frac{1}{r}. \tag{2.86}$$

Adding these inequalities we obtain

$$\frac{\deg(f) + \deg(g) + \deg(h)}{\deg(fgh)} < \frac{1}{p} + \frac{1}{q} + \frac{1}{r}. \tag{2.87}$$

Since $\deg(f) + \deg(g) + \deg(h) = \deg(fgh)$ we get

$$1 < \frac{1}{p} + \frac{1}{q} + \frac{1}{r}. \tag{2.88}$$

This is a contradiction which completes the proof. □

3. THE abc-CONJECTURE FOR INTEGERS

In this chapter, consider the abc-conjecture and its various applications.

The main references for this chapter are [4] and [8].

3.1. THE abc-CONJECTURE

Many results in number theory concerning polynomials have analogous results for integers. So, it is very natural to ask whether Mason-Stothers theorem has an integer version.

Every integer $n \neq 0, \pm 1$ can be expressed uniquely as a product

$$n = (-1)^e p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t} \tag{3.1}$$

where $p_1, p_2, \ldots, p_t$ are distinct primes, $e \in \{0, 1\}$ and $a_1, a_2, \ldots a_t \in \mathbb{N}$.

Definition 3.1.1. Let $n \in \mathbb{Z} - \{0, \pm 1\}$ and $n = (-1)^e p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ be its prime factorization. The radical of n is defined to be the product of all distinct primes which divide n:

$$\text{Rad}(n) = p_1 p_2 \cdots p_t. \tag{3.2}$$

Example 3.1. We have the following examples:

- $\text{Rad}(2^8 \cdot 13^9 \cdot 19^6) = 2 \cdot 13 \cdot 19 = 494$,
- $\text{Rad}(3^1 \cdot 5^7 \cdot 7^2 \cdot 23) = 3 \cdot 5 \cdot 7 \cdot 23 = 2415$.

Recall that prime factors of an integer correspond to irreducible factors of a polynomial. As a result, $\deg\big(\text{Rad}(f)\big)$ of a polynomial f corresponds to $\log\big(\text{Rad}(n)\big)$ of an integer n in this analogy.

J. Oesterle [9] and D. Masser [10] formulated the abc-conjecture for integers in the following way:

Conjecture 1 (The abc-conjecture)**.** *For each $\epsilon > 0$, there exists a positive number $C(\epsilon)$*

such that, for any $a, b, c \in \mathbb{Z} - \{0\}$ *with*

$$\gcd(a, b, c) = 1 \quad \text{and} \quad a + b = c \tag{3.3}$$

we have

$$\max\{|a|, |b|, |c|\} < C(\epsilon)\,\mathrm{Rad}(abc)^{1+\epsilon}. \tag{3.4}$$

For the details of this formulation from the Mason-Stother's theorem see [11]. In [12], it was shown that the abc-conjecture would not be true if $\epsilon = 0$.

In [13], A. Baker proposed the following explicit abc-conjecture.

Conjecture 2. *For any* $a, b, c \in \mathbb{Z} - \{0\}$ *with*

$$\gcd(a, b, c) = 1 \quad \text{and} \quad a + b = c \tag{3.5}$$

we have

$$\max\{|a|, |b|, |c|\} \leq \frac{6}{5} \cdot \mathrm{Rad}(abc) \cdot \frac{\left(\log \mathrm{Rad}(abc)\right)^{\omega}}{\omega!}, \tag{3.6}$$

where $\omega = \omega(abc)$ *denotes the number of distinct prime factors of* abc.

In [14], assuming the Conjecture 2, S. Laishram and T.N. Shorey established the following

Theorem 3.1.1 (Laishram-Shorey)**.** *For any* $a, b, c \in \mathbb{Z} - \{0\}$ *with*

$$\gcd(a, b, c) = 1 \quad \text{and} \quad a + b = c \tag{3.7}$$

we have

$$\max\{|a|, |b|, |c|\} < \mathrm{Rad}(abc)^{7/4}. \tag{3.8}$$

3.2. APPLICATIONS OF THE abc-CONJECTURE

In this section, consider various applications of the abc-conjecture.

3.2.1 Fermat's Last Theorem for Integers

The main reference for this section is [15]. In this section, as an application of Conjecture 3.1.1 we give the proof of Fermat's Last Theorem for the exponent $n \geq 6$. We also give the

proofs of the cases $n = 3, 4, 5$.

Let $n \in \mathbb{N}$. Now, consider the solutions (if any) of Fermat equation

$$x^n + y^n = z^n \tag{3.9}$$

in $\mathbb{Z}_{>0}$.

A solution (x, y, z) of the equation (3.9) is called a trivial solution if $xyz = 0$. Note that if there is a solution of the equation (3.9), then $(x/d, y/d, z/d)$ is also a solution where $d = \gcd(x, y, z)$. We call co-prime solutions as primitive solutions. So every non-trivial solution can be reduced to primitive solution.

3.2.1.1 The Case $n = 1$

In this case, there exist infinitely many non-trivial primitive solutions. In fact, let w be an integer $\neq 0, \pm 1$. Put

$$x := w \quad y := w + 1, \quad z := 2w + 1. \tag{3.10}$$

It is clear that $\gcd(w, w+1, 2w+1) = 1$ and $x + y = z$. For any such w there are infinitely many non-trivial primitive solutions.

3.2.1.2 The Case $n = 2$

The corresponding Fermat equation is

$$x^2 + y^2 = z^2. \tag{3.11}$$

A triple $(x, y, z) \in \mathbb{Z}_{>0}^3$ satisfying the equation (3.11) is called a Pythagorean triple.

Example 3.2. The triples $(3, 4, 5)$, $(20, 21, 29)$ and $(11, 60, 61)$ are all primitive Pythagorean triples.

Euclid gave a complete characterization of primitive Pythagorean triples. In particular, he showed that there are infinitely many Pythagorean triples. Below, you can find a modern proof of Euclid's characterization.

First, we need to establish the following lemmata.

Lemma 3.2.1. *Let* (x, y, z) *be a primitive Pythagorean triple, then it follows that*

$$\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1. \tag{3.12}$$

Proof. Let (x, y, z) be a primitive Pythagorean triple. Then

Claim 1. We have $\gcd(x, y) = 1$.

Assume that $\gcd(x, y) \neq 1$. In this case, there is a prime number p such that $p \mid x$ and $p \mid y$. We conclude that $p \mid x^2$ and $p \mid y^2$ and hence $p \mid (x^2 + y^2)$. Since $x^2 + y^2 = z^2$, so $p \mid z^2$ and hence $p \mid z$ which contradicts the assumption.

Claim 2. We have $\gcd(x, z) = 1$.

Assume that $\gcd(x, z) \neq 1$. In this case, there exist a prime number p such that $p \mid x$ and $p \mid z$. We conclude that $p \mid x^2$ and $p \mid z^2$ and hence $p \mid (z^2 - x^2)$. Since $z^2 - x^2 = y^2$, so $p \mid y^2$ and hence $p \mid y$ which contradicts the assumption.

Claim 3. We have $\gcd(y, z) = 1$.

Assume that $\gcd(y, z) \neq 1$. In this case, there exist a prime number p such that $p \mid y$ and $p \mid z$. We conclude that $p \mid y^2$ and $p \mid z^2$ and hence $p \mid (z^2 - y^2)$. Since $z^2 - y^2 = x^2$, so $p \mid x^2$ and hence $p \mid x$ which contradicts the assumption.

This proof is now complete. □

Lemma 3.2.2. *If* (x, y, z) *be a primitive Pythagorean triple then* x *and* y *are of opposite parity.*

Proof. Let (x, y, z) be a primitive Pythagorean triple. By Lemma 3.2.1, we have $\gcd(x, y) = 1$. So x and y can not be both even. Moreover, x and y can not be both odd. Assume, on the contrary, that x and y are both odd. Then there exist $w, u \in \mathbb{N}$ such that

$$x = 2w + 1 \quad \text{and} \quad y = 2u + 1. \tag{3.13}$$

Then

$$x^2 = (2w+1)^2 = 4w^2 + 4w + 1 \equiv 1 \pmod 4, \tag{3.14}$$

$$y^2 = (2u+1)^2 = 4u^2 + 4u + 1 \equiv 1 \pmod 4. \tag{3.15}$$

So we get

$$z^2 = x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod 4. \tag{3.16}$$

This is a contradiction since $z^2 \equiv 0 \pmod 4$ or $z^2 \equiv 1 \pmod 4$. So, we conclude that x and y are of opposite parity. □

Theorem 3.2.3. *The Fermat equation*

$$x^2 + y^2 = z^2 \tag{3.17}$$

has infinitely many positive integer solutions. Any solution (x, y, z) *is of the form*

$$x = 2rs, \qquad y = r^2 - s^2, \qquad z = r^2 + s^2, \tag{3.18}$$

where $r, s \in \mathbb{Z}_{>0}$ *are of opposite parity such that* $\gcd(r, s) = 1$ *and* $r > s$.

Proof. Let (x, y, z) be a primitive Pythagorean triple. Assume that x is even, y and z are odd. Write

$$x^2 = z^2 - y^2 = (z+y)(z-y). \tag{3.19}$$

Since $x, z+y$ and $z-y$ are both even integers, then there exist $a, b, c \in \mathbb{Z}_{>0}$ such that

$$x = 2a, \quad z + y = 2b, \quad \text{and} \quad z - y = 2c. \tag{3.20}$$

Then we get

$$(2a)^2 = (2b)(2c) \quad \text{or} \quad a^2 = bc. \tag{3.21}$$

Claim. We have $\gcd(b, c) = 1$.

Suppose that $\gcd(b, c) \neq 1$. So, there exist a prime number p such that $p \mid b$ and $p \mid c$. This implies that $p \mid (b + c)$. But

$$b + c = \frac{z+y}{2} + \frac{z-y}{2} = z \tag{3.22}$$

and hence $p \mid z$. Moreover, $p \mid (b - c)$. But

$$b - c = \frac{z + y}{2} - \left(\frac{z - y}{2}\right) = y \tag{3.23}$$

and hence $p \mid y$. This is a contradiction since by Lemma 3.2.1 we have $\gcd(y, z) = 1$.

Now, applying Proposition 2.2.2 with $R = \mathbb{Z}$ we get

$$b = r^2 \quad \text{and} \quad c = s^2 \tag{3.24}$$

for some $r, s \in \mathbb{N}$. Clearly, r and s are relatively prime because $\gcd(b, c) = 1$. Then

$$z = b + c = r^2 + s^2 \tag{3.25}$$

$$y = b - c = r^2 - s^2. \tag{3.26}$$

Since y is positive we must have $r > s$. Moreover, since z and y are both odd we conclude that r and s are of opposite parity. Finally,

$$x^2 = z^2 - y^2 \tag{3.27}$$

$$= \left(r^2 + s^2\right)^2 - \left(r^2 - s^2\right)^2 \tag{3.28}$$

$$= r^4 + 2r^2s^2 + s^4 - (r^4 - 2r^2s^2 + s^4) \tag{3.29}$$

$$= 4r^2s^2 \tag{3.30}$$

which it follows that $x = 2rs$.

Conversely, given any pair (r, s) of positive integers such that r and s are relatively prime, $r > s$, r and s are of opposite parity. Then $\left(2rs, r^2 - s^2, r^2 + s^2\right)$ is a primitive Pythagorean triple. In fact, clearly

$$\left(2rs\right)^2 + \left(r^2 - s^2\right)^2 = \left(r^2 + s^2\right)^2. \tag{3.31}$$

Claim. We have $\gcd\left(2rs, r^2 - s^2, r^2 + s^2\right) = 1$.

Suppose, on the contrary, that $\gcd\left(2rs, r^2 - s^2, r^2 + s^2\right) \neq 1$. In this case, there exist a prime number p such that $p \mid 2rs$, $p \mid (r^2 - s^2)$ and $p \mid (r^2 + s^2)$. Since $r^2 - s^2$ and $r^2 + s^2$ are odd so $p \neq 2$. Since $p \mid 2rs$ we get $p \mid r$ or $p \mid s$ but not both since $\gcd(r, s) = 1$. Hence, it follows that $p \nmid (r^2 - s^2)$. This is a contradiction. □

3.2.1.3 The Case $n \geq 3$

In [16] , A. Wiles proved the following theorem:

Theorem 3.2.4 (Fermat's Last Theorem)**.** *The Fermat equation*

$$x^n + y^n = z^n \tag{3.32}$$

does not have solutions in positive integers when $n \geq 3$.

Using Theorem 3.1.1, we get

Theorem 3.2.5. *The Fermat equation*

$$x^n + y^n = z^n \tag{3.33}$$

does not have solutions in positive integers when $n \geq 6$.

Proof. Suppose that there exist co-prime $x, y, z \in \mathbb{Z}_{>0}$ satisfying the equation (3.33). Then, applying Theorem 3.1.1, with $a = x^n$, $b = y^n$, and $c = z^n$ we get

$$z^n \leq \text{Rad}(x^n y^n z^n)^{7/4} \tag{3.34}$$

$$= \text{Rad}(xyz)^{7/4} \tag{3.35}$$

$$\leq (xyz)^{7/4} \tag{3.36}$$

$$\leq z^{21/4}. \tag{3.37}$$

It then follows that $n \leq \frac{21}{4}$ which is a contradiction since by assumption $n \geq 6$. This completes the proof. □

Therefore, it remains to prove the cases $n = 3, 4, 5$. The proofs of these cases use Fermat's method of infinite descent which is applied to prove that a given Diophantine equation is not an insolvable in positive integers by proving that for each such solution, a smaller solution exists which contradicts the Well-Ordering Principle.

3.2.1.4 The Case $n = 4$

This case was proved by Fermat.

First of all, we will prove a more general theorem from which we get the proof of the case $n = 4$ as a corollary.

Theorem 3.2.6. *The Diophantine equation*

$$x^4 + y^4 = z^2 \tag{3.38}$$

does not have non-zero integer solutions.

Proof. Suppose that there exist $x, y, z \in \mathbb{Z} - \{0\}$ satisfying the equation (3.38). Assume that $x, y, z \in \mathbb{Z}_{>0}$.

In addition, x and y can be supposed to be relatively prime. In fact, letting $d = \gcd(x, y)$. Then, x and y can be expressed in the form

$$x = dx_1 \quad \text{and} \quad y = dy_1 \tag{3.39}$$

for some $x_1, y_1 \in \mathbb{Z}_{>0}$ with $\gcd(x_1, y_1) = 1$. Now, since $x^4 + y^4 = z^2$ we get

$$(dx_1)^4 + (dx_2)^4 = z^2 \tag{3.40}$$

and hence $d^4(x_1^4 + y_1^4) = z^2$. Therefore, $d^4 \mid z^2$ from which it follows that $d^2 \mid z$. Hence, there exist $z_1 \in \mathbb{Z}_{>0}$ satisfying $z = d^2 z_1$. Therefore

$$d^4(x_1^4 + y_1^4) = d^4 z_1^2 \tag{3.41}$$

which implies that

$$x_1^4 + y_1^4 = z_1^2. \tag{3.42}$$

So, we may assume that the equation (3.38) has a solution $(x_0, y_0, z_0) \in \mathbb{Z}_{>0}^3$ with x_0, y_0 and z_0 are pairwise relatively prime.

Our aim is to prove that there is another solution $(x_1, y_1, z_1) \in \mathbb{Z}_{>0}^3$ with $\gcd(x_1, y_1) = 1$ satisfying $z_1 < z_0$.

Claim. The triple (x_0^2, y_0^2, z_0) is a primitive Pythagorean triple.

First of all, since $x_0^4 + y_0^4 = z_0^2$ so we get $(x_0^2)^2 + (y_0^2)^2 = z_0^2$ this shows that (x_0^2, y_0^2, z_0) is a Pythagorean triple. Next , we need to show that $\gcd\left(x_0^2, y_0^2, z_0\right) = 1$.

Assume, on the contrary, that $\gcd\left(x_0^2, y_0^2, z_0\right) \neq 1$. So, there is a prime number p which divides x_0^2, y_0^2 and z_0. Then it follows that $p \mid x_0$ and $p \mid y_0$. This is a contradiction since $\gcd(x_0, y_0) = 1$. So, we conclude that (x_0^2, y_0^2, z_0) is a primitive Pythagorean triple. Hence, according to Theorem 3.2.3, interchanging x_0 and y_0, if necessary, we can write

$$x_0^2 = 2rs, \qquad y_0^2 = r^2 - s^2, \qquad z_0 = r^2 + s^2, \tag{3.43}$$

where $r, s \in \mathbb{Z}_{>0}$ such that r and s are relatively prime, one of the numbers r and s is even or odd but not both and $r > s$. Now, the second of these equations may be written as

$$y_0^2 + s^2 = r^2. \tag{3.44}$$

So $\gcd(r, s) = 1$ because $\gcd\left(y_0, s, r\right) = 1$. Hence we see that (y_0, s, r) is primitive Pythagorean triple. So, r is odd and since r and s are of opposite parity, s is even. Therefore, by Theorem 3.2.3

$$s = 2wu, \qquad y_0 = w^2 - u^2, \qquad r = w^2 + u^2, \tag{3.45}$$

where $w, u \in \mathbb{Z}_{>0}$ such that $\gcd(w, u) = 1$, one of the numbers w and u is even or odd but not both and $w > u$, we get

$$x_0^2 = 2rs = 2(w^2 + u^2)2wu = 4wu(w^2 + u^2). \tag{3.46}$$

Claim. We have $\gcd(wu, w^2 + u^2) = 1$.

Suppose, on the contrary, that $\gcd(wu, w^2 + u^2) \neq 1$. Then there exist a prime number p such that $p \mid wu$ and $p \mid (w^2 + u^2)$. So we get $\left(p \mid w \text{ and } p \mid \left(w^2 + u^2\right)\right)$ or $\left(p \mid u \text{ and } p \mid (w^2 + u^2)\right)$.

- Assume that $p \mid w$ and $p \mid (w^2 + u^2)$. It follows that $p \mid w^2$ and $p \mid (w^2 + u^2 - w^2)$ so $p \mid u^2$ and hence $p \mid u$. However, $\gcd(w, u) = 1$ as not equal to be as we assumed.

- Assume that $p \mid u$ and $p \mid (w^2 + u^2)$. It follows that $p \mid u^2$ and $p \mid (w^2 + u^2 - u^2)$ so $p \mid w^2$

and hence $p \mid w$. However, $\gcd(w, u) = 1$ as not equal to be as we assumed.

Hence, by Proposition 2.2.2, wu and $w^2 + u^2$ are squares. Moreover, since w and u are co-prime so by Proposition 2.2.2 we get $w = x_1^2$ and $u = y_1^2$ for some positive integers x_1 and y_1 . It is clear that $\gcd(x_1, y_1) = 1$. Therefore,

$$x_1^4 + y_1^4 = w^2 + u^2 = r \tag{3.47}$$

is a square. So there is $z_1 \in \mathbb{Z}_{>0}$ such that

$$x_1^4 + y_1^4 = w^2 + u^2 = r = z_1^2. \tag{3.48}$$

Moreover, we have $z_1 > z_0$ since

$$z_1 \leq z_1^4 = r^2 < r^2 + s^2 = z_0. \tag{3.49}$$

According to the method of infinite descent the solution (x, y, z) does not exist. This completes the proof. □

As a corollary we get

Corollary 3.2.6.1. *The Fermat equation*

$$x^4 + y^4 = z^4 \tag{3.50}$$

does not have solutions in positive integers.

Remark. For any $l \in \mathbb{Z}_{>0}$ the Fermat equation

$$x^{4l} + y^{4l} = z^{4l} \tag{3.51}$$

does not have solutions in $\mathbb{Z}_{>0}^3$. Otherwise, letting

$$(X, Y, Z) := (x^l, y^l, z^l) \tag{3.52}$$

would be a solution of

$$X^4 + Y^4 = Z^4 \tag{3.53}$$

which is not possible.

So, we conclude that for every $n \in \mathbb{Z}_{>0}$ divisible by 4 the equation (3.33) does not have

solutions in $\mathbb{Z}_{>0}^3$.

Let $n \in \mathbb{Z}_{\geq 2}$ which is not divisible by 4. So, n can not be a power of 2. Therefore, there is a prime number $p \neq 2$ which divides n. So there exist an integer $l \in \mathbb{Z}_{>0}$ such that $n = pl$. Therefore, to show that the equation (3.33) is not solvable in $\mathbb{Z}_{>0}$ it suffices to show that $x^p + y^p = z^p$ does not have solutions in $\mathbb{Z}_{>0}$.

3.2.1.5 The Case $n = 3$

In this case, we have

Theorem 3.2.7. *The Fermat equation*

$$x^3 + y^3 = z^3 \tag{3.54}$$

does not have solutions in positive integers.

We follow Euler's proof.

Proof. Suppose that there is $(x, y, z) \in \mathbb{Z}_{>0}^3$ satisfying the equation (3.54). It can be assumed that

$$\gcd(x, y) = 1, \qquad \gcd(x, z) = 1, \qquad \gcd(y, z) = 1. \tag{3.55}$$

Observe that, exactly one of the numbers must be even. Firstly, we suppose that x and y are odd and z is even. Then, necessarily the numbers $x + y$ and $x - y$ are both even. So, they can be expressed as

$$x + y = 2m \quad \text{and} \quad x - y = 2n \tag{3.56}$$

for some $m, n \in \mathbb{Z}$. This gives

$$x = m + n \quad \text{and} \quad y = m - n. \tag{3.57}$$

Then we can express $x^3 + y^3$ as:

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2) \tag{3.58}$$

$$= 2m[(m + n)^2 - (m + n)(m - n) + (m - n)^2] \tag{3.59}$$

$$= 2m[m^2 + 3n^2] = z^3. \tag{3.60}$$

Clearly, the integers m and n can not be both even or odd. Moreover,

Claim 1. We have $\gcd(m, n) = 1$.

Suppose that $\gcd(m, n) \neq 1$. So there is a prime number p such that $p \mid m$ and $p \mid n$. Hence $p \mid (m + n)$ and $p \mid (m - n)$. As $x = m + n$ and $y = m - n$ for this reason $p \mid x$ and $p \mid y$. However, $\gcd(x, y) = 1$ as not equal to be as we assumed.

In addition, we may suppose that $m, n \in \mathbb{Z}_{>0}$. In fact,

- If x is less than y, then interchanging x and y we get $n > 0$.
- The case $x = y$ is not possible. In fact, if it were true, then we would get $x = y = 1$ as $\gcd(x, y) = 1$. In addition, since $x^3 + y^3 = z^3$ we would get $z^3 = 2$ which is not possible since $z \in \mathbb{Z}_{>0}$.

Secondly, suppose that x and y are not both even or odd. Assume that, x is even and y is odd and z is odd. Therefore, $z + y$ and $z - y$ are both even. So, they can be expressed as

$$z - y = 2m \quad \text{and} \quad z + y = 2n. \tag{3.61}$$

for some $m, n \in \mathbb{Z}$. This gives

$$z = m + n \quad \text{and} \quad y = n - m. \tag{3.62}$$

Then we can express $z^3 - y^3$ as:

$$z^3 - y^3 = (z - y)(z^2 + zy + y^2) \tag{3.63}$$

$$= 2m[(m + n)^2 + (m + n)(n - m) + (m - n)^2] \tag{3.64}$$

$$= 2m(m^2 + 3n^2) = x^3. \tag{3.65}$$

It is clear that the integers m and n are not both even or odd with m and n are relatively prime. Since m and n have opposite parity it follows that $m^2 + 3n^2$ is odd. Since $2m(m^2 + 3n^2) = x^3$ and x is even, thus $4 \mid m$ and hence n is odd. Then,

Claim 2. We have $\gcd(2m, m^2 + 3n^2) = 1$ or 3.

Let $\gcd(2m, m^2 + 3n^2) = d$.

- Note that $d = 2$ is not possible, since $m^2 + 3n^2$ is odd.

- So, necessarily, $d \mid m$ as a result $d \mid m^2$. Since, $d \mid (m^2 + 3n^2)$ we conclude that $d \mid (m^2 + 3n^2 - m^2)$. That is $d \mid 3n^2$. Suppose that $d \neq 1$. Since $\gcd(m, n^2) = 1$ it follows that $d \nmid n^2$. So, $d \mid 3$ and hence $d = 3$. Hence $\gcd(2m, m^2 + 3n^2) = 1$ or 3.

Case 1. We have $\gcd(2m, m^2 + 3n^2) = 1$.

Recall that, $2m(m^2 + 3n^2)$ is a cube. So by Proposition 2.2.2 we see that both $2m$ and $m^2 + 3n^2$ must be cubes. By Lemma 3.2.8 there are $u, v \in \mathbb{Z}$ such that

$$m = u^3 - 9uv^2 \quad \text{and} \quad n = 3u^2v - 3v^3 \tag{3.66}$$

so that $m^2 + 3n^2 = (u^2 + 3v^2)^3$. Now, factorizing the expression for m and n, we obtain

$$m = u(u - 3v)(u + 3v) \quad \text{and} \quad n = 3v(u - v)(u + v). \tag{3.67}$$

Observe that $\gcd(u, v) = 1$. Moreover, we have

$$2m = 2u(u - 3v)(u + 3v) = \text{cube}. \tag{3.68}$$

Note that u and v are not both odd or even. Then

Claim 3. We have $\gcd(2u, u - 3v, u + 3v) = 1$.

Assume, on the contrary, that $\gcd(2u, u - 3v, u + 3v) \neq 1$. Then there must be a prime number p such that $p \mid 2u$, $p \mid (u - 3v)$ and $p \mid (u + 3v)$.

- Note that $p \neq 2$ since $u - 3v$ and $u + 3v$ are odd. Then, $p \mid u$. Since, $p \mid (u + 3v)$ then $p \mid (u + 3v - u)$ and hence $p \mid 3v$. Since $\gcd(u, v) = 1$ it follows that $p \nmid v$. So, we must have $p = 3$. Since $3 \mid u$ and $m = u^3 - 9uv^2$ it follows that $3 \mid m$. Since $3 \mid u$ and $n = 3u^2v - 3v^3$ it follows that $3 \mid n$. This is a contradiction because $\gcd(m, n) = 1$. So, by Proposition 2.2.2 there are $A, B, C \in \mathbb{Z}$ such that

$$2u = A^3, \quad u - 3v = B^3, \quad u + 3v = C^3. \tag{3.69}$$

Then,

$$B^3 + C^3 = A^3. \tag{3.70}$$

Observe that

- If z is even, then $0 < A^3B^3C^3 < z^3$.
- If x is even, then $0 < A^3B^3C^3 < x^3$.
- If y is even, then $0 < A^3B^3C^3 < y^3$.

The numbers A, B or C can be negative. But since $(-A)^3 = -A^3$ we can rearrange the negative cubes to get positive cubes. In this way, we get an equation of the form $X^3+Y^3 = Z^3$ in which the numbers $X, Y, Z \in \mathbb{Z}_{>0}$ such that $Z^3 < z^3$(if z is even). According to the method of infinite descent the solution (x, y, z) does not exist.

Case 2. We have $\gcd(2m, m^2 + 3n^2) = 3$.

In this case, since $3 \mid 2m$ we must have $3 \mid m$. Therefore, there exists $w \in \mathbb{Z}$ such that $m = 3w$. Then we get

$$2m(m^2 + 3n^2) = 3^2 2w(3w^2 + n^2). \tag{3.71}$$

As $\gcd(m, n) = 1$ for this reason $\gcd(n, w) = 1$. Since m is even (in fact $4 \mid m$), then w is also even. So, neither 3 nor 4 divide n. Therefore, we get $\gcd(18w, 3w^2 + n^2) = 1$. Therefore, by Proposition 2.2.2 both $18w$ and $3w^2 + n^2$ must be cubes. By Lemma 3.2.8, $3w^2 + n^2$ can be a cube if there exist $u, v \in \mathbb{Z}$ such that

$$n = u(u - 3v)(u + 3v) \tag{3.72}$$

$$w = 3v(u - v)(u + v). \tag{3.73}$$

Since we know that $18w$ is a cube then $3^3 2v(u - v)(u + v)$ is also a cube hence $2v(u - v)(u+v)$ is a cube. Then, clearly we have $\gcd(2v, u-v, u+v) = 1$. Hence, by Proposition 2.2.2 then there are $A, B, C \in \mathbb{Z}$ such that

$$2v = A^3, \quad u - v = B^3, \quad u + v = C^3. \tag{3.74}$$

As before, we can get an equation of the form $X^3 + Y^3 = Z^3$ in which $X, Y, Z \in \mathbb{Z}_{>0}$ such that $Z^3 < z^3$(if z is even). According to the method of infinite descent the solution (x, y, z)

does not exist. □

Lemma 3.2.8. *Let* $a, b \in \mathbb{Z}$ *such that*

$$\gcd(a, b) = 1 \quad \text{and} \quad a^2 + 3b^2 = \text{cube}. \tag{3.75}$$

Then there are $p, q \in \mathbb{Z}$ *such that*

$$a = p^3 - 9pq^2 \quad \text{and} \quad b = 3p^2q - 3q^3. \tag{3.76}$$

Proof. See [15]. □

3.2.1.6 The Case $n = 5$

We have:

Theorem 3.2.9. *The Fermat equation*

$$x^5 + y^5 = z^5 \tag{3.77}$$

does not have solutions in positive integers.

We follow Dirichlet's proof.

Proof of Theorem 3.2.9. Assume that there exist $x, y, z \in \mathbb{Z}_{>0}$ satisfying the equation (3.77). Then we clearly assume that

$$\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1. \tag{3.78}$$

Observe that, one of the integers x, y, and z must be divisible by 2. By Theorem 3.2.12, one of the integers x, y and z must be multiple of 5. Then, there are two cases:

Case 1: The integer which is a multiple 5 is also a multiple of 2, that is a multiple of 10.

Case 2: The integer which is a multiple of 2 is not divisible by 2.

The proof will be given 2 steps.

- Step 1: Case 1 is not possible.

The equation $x^5 + y^5 = z^5$ can be put in the following form

$$p^5 \pm q^5 = r^5 \tag{3.79}$$

where $p, q, r \in \mathbb{Z}_{>0}$ with $q < p$ and $10 \mid r$ such that

$$\gcd(p, q) = \gcd(p, r) = \gcd(q, r) = 1. \tag{3.80}$$

Since r is even and $\gcd(p, q) = 1$ then the integers p and q must be odd. So, necessarily, the integers $p + q$ and $p - q$ are both even. Therefore, there are $m, n \in \mathbb{Z} - \{0\}$ such that

$$p + q = 2m \quad \text{and} \quad p - q = 2n. \tag{3.81}$$

This gives

$$p = m + n \quad \text{and} \quad q = m - n. \tag{3.82}$$

Note that $\gcd(m, n) = 1$, $n < m$ and have opposite parity. We have $r^5 = 2^a 5^b r'$ where $a, b, r' \in \mathbb{N}$. Interchanging m and n, if necessary, we get

$$r^5 = 2^a 5^b r' = p^5 \pm q^5 = (m + n)^5 \pm (m - n)^5 = 2m\left(m^4 + 10m^2n^2 + 5n^4\right). \tag{3.83}$$

Hence $m \mid 5$. It follows that $m = 5\alpha$, for some positive integer α. Since $\gcd(m, n) = 1$, then $5 \nmid n$. We get

$$2m\left(m^4 + 10m^2n^2 + 5n^4\right) = 2(5\alpha)\left[(5\alpha)^4 + 10(5\alpha)^2n^2 + 5n^2\right] \tag{3.84}$$

$$= 2 \cdot 5^2 \cdot \alpha\left(125\alpha^4 + 50\alpha^2n^2 + n^4\right) \tag{3.85}$$

$$= 2 \cdot 5^2 \cdot \alpha\left(n^4 + 50\alpha^2n^2 + 125\alpha^4\right). \tag{3.86}$$

Claim. We have $\gcd\left(2 \cdot 5^2 \cdot \alpha,\ n^4 + 50\alpha^2n^2 + 125\alpha^4\right) = 1$.

Suppose $\gcd\left(2 \cdot 5^2 \cdot \alpha,\ n^4 + 50\alpha^2n^2 + 125\alpha^4\right) \neq 1$. So there exist a prime number p such that $p \mid \left(2 \cdot 5^2 \cdot \alpha\right)$ and $p \mid \left(n^4 + 50\alpha^2n^2 + 125\alpha^4\right)$. Next observe that

- $p \neq 2$ because $n^4 + 50\alpha^2n^2 + 125\alpha^4$ is odd.
- $p \neq 5$ since otherwise we would get $5 \mid n$ which is impossible because $\gcd(m, n) = 1$.
- $p \nmid \alpha$ since otherwise we would get $p \mid m$ and $p \mid n$ which is impossible because

$\gcd(m, n) = 1$.

By Proposition 2.2.2, the integers $2 \cdot 5^2 \cdot \alpha$ and $n^4 + 50\alpha^2 n^2 + 125\alpha^4$ are fifth powers. On the other hand

$$n^4 + 50\alpha^2 n^2 + 125\alpha^4 = \left(n^2 + 25\alpha^2\right)^2 - 5^4\alpha^4 + 5^3\alpha^4 \tag{3.87}$$

$$= \left(n^2 + 25\alpha^2\right)^2 - 5(10\alpha^2)^2 \tag{3.88}$$

$$= \theta_1^2 - 5\theta_2^2, \tag{3.89}$$

where $\theta_1 = n^2 + 25\alpha^2$ and $\theta_2 = 10\alpha^2$. Also,

$$\theta_1^2 - 5\theta_2^2 = (\theta_1 - \sqrt{5}\theta_2)(\theta_1 + \sqrt{5}\theta_2). \tag{3.90}$$

By Lemma 3.2.10, we get

$$\theta_1 + \sqrt{5}\theta_2 = (\delta_1 + \sqrt{5}\delta_2)^5 \tag{3.91}$$

for some integers δ_1 and δ_2. Then ,

$$\theta_1 = \delta_1^5 + 50\delta_1^3\delta_2^2 + 125\delta_1\delta_2^4 \tag{3.92}$$

$$\theta_2 = 5\delta_1^4\delta_2 + 50\delta_1^2\delta_2^3 + 25\delta_2^5. \tag{3.93}$$

Since $\theta_2 = 10\alpha^2$ and since $5^2 \cdot 2 \cdot \alpha$ is a fifth power,

$$\left(5^2 \cdot 2 \cdot \alpha\right)^2 = 5^3 \cdot 2 \cdot \theta_2 = 5^4 \cdot 2 \cdot \delta_2\left[\delta_1^4 + 10\delta_1^2\delta_2^2 + 5\delta_2^4\right] \tag{3.94}$$

is also a fifth power. Then

- $\gcd(\delta_1, \delta_2) = 1$ since $\gcd(\theta_1, \theta_2) = 1$.
- δ_1 and δ_2 are of opposite parity since θ_1 and θ_2 are not both even.
- $\gcd(2, \delta_1) = 1$ and $\gcd(5, \delta_1) = 1$ because $\gcd(2, \theta_1) = 1$ and $\gcd(5, \theta_1) = 1$.

Then, clearly we get $\gcd\left(5^4 \cdot 2 \cdot \delta_2\,,\, \delta_1^4 + 10^2\delta_2^2 + 5\delta_2^4\right) = 1$. Hence by Proposition 2.2.2

$$5^4 \cdot 2 \cdot \delta_2 \qquad \text{and} \qquad \delta_1^4 + 10^2\delta_2^2 + 5\delta_2^4 \tag{3.95}$$

are fifth powers. On the other hand completing the square we get

$$\delta_1^4 + 10^2\delta_2^2 + 5\delta_2^4 = (\delta_1^2 + 5\delta_2^2)^2 - 25\delta_2^4 + 5\delta_2^4 \tag{3.96}$$

$$=(\delta_1^2 + 5\delta_2^2)^2 - 5(2\delta_2^2)^2 \tag{3.97}$$

$$=\gamma_1^2 - 5\gamma_2^2. \tag{3.98}$$

where $\gamma_1 = \delta_1^2 + 5\delta_2^2$ and $\gamma_2 = 2\delta_2^2$. Moreover, we have

$$\gamma_1^2 - 5\gamma_2^2 = (\gamma_1 + \gamma_2\sqrt{5})(\gamma_1 - \gamma_2\sqrt{5}). \tag{3.99}$$

Then by Lemma 3.2.10, we have

$$\gamma_1 + \gamma_2\sqrt{5} = (\lambda_1 + \lambda_2\sqrt{5})^5 \tag{3.100}$$

for some integers λ_1 and λ_2. Then,

$$\gamma_1 = \lambda_1^5 + 50\lambda_1^3\lambda_2^2 + 125\lambda_1\lambda_2^4 \tag{3.101}$$

$$\gamma_2 = 5\lambda_1^4\lambda_2 + 50\lambda_1^2\lambda_2^3 + 25\lambda_2^5. \tag{3.102}$$

Since $\gamma_2 = 2 \cdot \delta_2^2$ and $5^4 \cdot 2 \cdot \delta_2$ is a fifth power, it follows that

$$(5^4 \cdot 2 \cdot \delta_2)^2 = 5^8 \cdot 2 \cdot \gamma_2 = 5^9 \cdot 2 \cdot \lambda_2[\lambda_1^4 + 10\lambda_1^2\lambda_2^2 + 5\lambda_2^4] = \text{fifth power.} \tag{3.103}$$

Since $\gcd\left(5^9 \cdot 2 \cdot \lambda_2,\ \lambda_1^4 + 10\lambda_1^2\lambda_2^2 + 5\lambda_2^4\right) = 1$, it follows from Proposition 2.2.2 that

$$5^9 \cdot 2 \cdot \lambda_2 \quad \text{and} \quad \lambda_1^4 + 10\lambda_1^2\lambda_2^2 + 5\lambda_1^4 \tag{3.104}$$

are fifth powers. Moreover, since

$$5^9 \cdot 2 \cdot \lambda_2 = 5^5 \cdot 5^4 \cdot 2 \cdot \lambda_2, \tag{3.105}$$

it follows that $5^4 \cdot 2 \cdot \lambda_2$ must be a fifth power. It is clear that λ_1 and λ_2 satisfy the same conditions provided by δ_1 and δ_2. In addition to the condition that

$$5^4 \cdot 2 \cdot \delta_2 \quad \text{and} \quad \delta_1^4 + 10\delta_1^2\delta_2^2 + 5\delta_2^4 \tag{3.106}$$

are fifth powers, we also have that δ_1 and δ_2 are of opposite parity and $\gcd(\delta_1,\ \delta_2) = 1$ such that $\gcd(\delta_1,\ 2) = \gcd(\delta_1,\ 5) = 1$. Hence we can repeat the same argument indefinitely and this leads to an infinite descent. The sequence of positive integers δ_2 decrease as

$$2\delta_2^2 = \gamma_2 = \lambda_2\left(5\lambda_1^4 + 50\lambda_1^2\lambda_2^2 + 25\lambda_2^4\right) \tag{3.107}$$

which gives

$$\lambda_2 > 0 \quad \text{and} \quad 2\delta_2^2 > 25\lambda_2^4 \quad \text{and} \quad \delta_2 > \lambda_2. \tag{3.108}$$

Finally, by the method of infinite descent the Case 1 was not possible. This proves Step 1.

- Step 2: Case 2 is not possible.

Note that the equation $x^5 + y^5 = z^5$ can be put in the following form

$$p^5 \pm q^5 = r^5 \tag{3.109}$$

where $p, q, r \in \mathbb{Z}_{>0}$ with $q < p$, $5 \mid r$ and $2 \nmid r$ such that

$$\gcd(p, q) = \gcd(p, r) = \gcd(q, r) = 1. \tag{3.110}$$

Since $2 \nmid r$, p and q are of opposite parity. We set

$$m := p + q \quad \text{and} \quad n := p - q. \tag{3.111}$$

This gives

$$p = \frac{m+n}{2} \quad \text{and} \quad q = \frac{m-n}{2}. \tag{3.112}$$

Then

$$p^5 \pm q^5 = \left(\frac{m+n}{2}\right)^5 \pm \left(\frac{m-n}{2}\right)^5 \tag{3.113}$$

and, interchanging m and n, if necessary, we get

$$r^5 = 2^{-5}2\left(m^5 + 10m^3n^2 + 5mn^4\right), \tag{3.114}$$

$$2^4r^5 = m\left(m^4 + 10m^2n^2 + 5n^4\right). \tag{3.115}$$

Since $5 \mid r$, m must be divisible by 5, say $m = 5\alpha$ for some $\alpha \in \mathbb{Z}_{>0}$. As $\gcd(m, n) = 1$ for this reason $5 \nmid n$. Since $m = 5\alpha$ we get

$$2^4r^5 = 5^2\alpha\left(n^4 + 50\alpha^2n^2 + 125\alpha^4\right). \tag{3.116}$$

Claim. We have $\gcd\left(5^2\alpha, n^4 + 50\alpha^2n^2 + 125\alpha^4\right) = 1$.

Assume, on the contrary, that $\gcd\left(5^2\alpha, n^4 + 50\alpha^2n^2 + 125\alpha^4\right) \neq 1$. Let t be a prime number such that $t \mid \left(5^2\alpha\right)$ and $t \mid \left(n^4 + 50\alpha^2n^2 + 125\alpha^4\right)$. Then $t = 5$ or $t \mid \alpha$.

- If $t = 5$, then we would get $5 \mid n$ which is a contradiction since $5 \mid m$ and $\gcd(m, n) = 1$.
- If $t \mid \alpha$, then we would get $t \mid n$ which is impossible since $t \mid m$ and $\gcd(m, n) = 1$.

So, $\gcd\left(5^2\alpha, n^4 + 50\alpha^2n^2 + 125\alpha^4\right) = 1$.

Since α is odd, $5^2\alpha$ must be a fifth power. On the other hand we have

$$n^4 + 50\alpha^2n^2 + 125\alpha^4 = \left(n^2 + 25\alpha^2\right)^2 - 5^4\alpha^4 + 5^3\alpha^4 \tag{3.117}$$

$$= \left(n^2 + 25\alpha^2\right)^2 - 5(10\alpha^2)^2 \tag{3.118}$$

$$= 2^4 \cdot (\text{fifth power}). \tag{3.119}$$

For an odd integer a we have $a^2 \equiv 1 \pmod 8$. Since n and α are odd numbers it follows that

$$n^2 + 25\alpha^2 = n^2 + \left(5\alpha\right)^2 \equiv 1 + 1 = 2 \pmod 8 \tag{3.120}$$

so $n^2 + 25\alpha^2$ is divisible by 2 but not by 2^2. So

$$\left(n^2 + 25\alpha^2\right)^2 - 5\left(10\alpha^2\right)^2 = \left(\frac{\theta_1}{2}\right)^2 - 5\left(\frac{\theta_2}{2}\right)^2 \tag{3.121}$$

is a fifth power where $\theta_1 = \dfrac{(n^2 + 25\alpha^2)}{2}$ and $\theta_2 = 5\alpha^2$ are both odd numbers. Note that $5 \mid \theta_2$. By Lemma 3.2.11 there exist δ_1 and δ_2 such that

$$\frac{\theta_1}{2} + \frac{\theta_2}{2}\sqrt{5} = \left(\frac{\delta_1}{2} + \frac{\delta_2}{2}\sqrt{5}\right)^5. \tag{3.122}$$

This gives,

$$\frac{\theta_1}{2} = \frac{\delta_1^5}{2^5} + 50\frac{\delta_1^3\delta_2^2}{2^5} + 125\frac{\delta_1\delta_2^4}{2^5} \tag{3.123}$$

and

$$\frac{\theta_2}{2} = 5\frac{\delta_1^4\delta_2}{2^5} + 50\frac{\delta_1^2\delta_2^3}{2^5} + 5^2\frac{\delta_2^5}{2^5}. \tag{3.124}$$

Since $5^2\alpha$ is a fifth power we get

$$\left(5^2\alpha\right)^2 = 5^3\theta_2 = 5^4\delta_2\left[\frac{\delta_1^4}{2^4} + 10\frac{\delta_1^2\delta_2^2}{2^4} + 5\frac{\delta_2^4}{2^4}\right], \tag{3.125}$$

and hence

$$5^4\delta_2\left[\delta_1^4 + 10\delta_1^2\delta_2^2 + 5\delta_2^4\right] = 2^4 \cdot (\text{fifth power}). \tag{3.126}$$

Observe that $\gcd(\delta_1, \delta_2) = 1$ and $5 \nmid \delta_1$.

Claim. We have $\gcd\left(5^4\delta_2, \delta_1^4 + 10\delta_1^2\delta_2^2 + 5\delta_2^4\right) = 1$.

Assume, on the contrary, that $\gcd\left(5^4\delta_2, \delta_1^4 + 10\delta_1^2\delta_2^2 + 5\delta_2^4\right) \neq 1$. Let t be a prime number such that $t \mid \left(5^4\delta_2\right)$ and $t \mid \left(\delta_1^4 + 10\delta_1^2\delta_2^2 + 5\delta_2^4\right)$. Then $t = 5$ or $t \mid \delta_2$.

- If $t = 5$, then we would get $5 \mid \delta_1$ which is a contradiction since $5 \nmid \delta_1$.
- If $t \mid \delta_2$, then we would get $t \mid \delta_1$ which is a contradiction since $t \mid \delta_2$ and $\gcd(\delta_1, \delta_2) = 1$.

So, $\gcd\left(5^4\delta_2, \delta_1^4 + 10\delta_1^2\delta_2^2 + 5\delta_2^4\right) = 1$.

Since δ_2 is odd it follows that $5^4\delta_2$ is a fifth power and hence $5 \mid \delta_2$. Moreover,

$$\delta_1^4 + 10\delta_1^2\delta_2^2 + 5\delta_2^4 = 2^4 \cdot (\text{fifth power}). \tag{3.127}$$

The equation (3.127) can be written as

$$\left(\frac{\delta_1^2 + 5\delta_2^2}{2^2}\right)^2 - 5\left(\frac{\delta_2^2}{2}\right)^2 = (\text{fifth power}). \tag{3.128}$$

Since δ_1 and δ_2 are both odd so we get $\delta_1^2 + 5\delta_2^2 \equiv 6 \pmod 8$. Therefore the equation (3.128) can be written as

$$\left(\frac{\gamma_1}{2}\right)^2 - 5\left(\frac{\gamma_2}{2}\right)^2 = (\text{fifth power}) \tag{3.129}$$

where γ_1 and γ_2 are odd integers with $\gcd(\gamma_1, \gamma_2) = 1$ such that $5 \mid \gamma_2$. Also by Lemma 3.2.11 we get

$$\frac{\gamma_1}{2} + \frac{\gamma_2}{2}\sqrt{5} = \left(\frac{\lambda_1}{2} + \frac{\lambda_2}{2}\sqrt{5}\right)^5 \tag{3.130}$$

for some numbers λ_1 and λ_2. Similarly, as above, we get

$$\lambda_1^4 + 10\lambda_1^2\lambda_2^2 + 5\lambda_2^4 = 2^4 \cdot (\text{fifth power}).$$

So we get an infinitely decreasing sequence of fifth powers. This gives a contradiction. Finally, the Case 2 was not possible by the method of infinite descent. This proves Step 2. □

Lemma 3.2.10. *Let $R, S \in \mathbb{Z}$ satisfying*

(i) $5 \mid S$,

(ii) $\gcd(R, S) = 1$,

(iii) *are of opposite parity,*

(iv) $R^2 - 5S^2$ *is a fifth power.*

Then there are $C, D \in \mathbb{Z}$ *such that*

$$R + S\sqrt{5} = \left(C + D\sqrt{5}\right)^5. \tag{3.131}$$

Proof. See [15]. □

Lemma 3.2.11. *Let* $R, S \in \mathbb{Z}$ *be two odd numbers satisfying*

(i) $5 \mid S$,

(ii) $\gcd(R, S) = 1$,

(iii) $\left(\frac{R}{2}\right)^2 - 5\left(\frac{S}{2}\right)^2 =$ fifth power.

Then there are two odd integers C, D *such that*

$$\frac{R}{2} + \frac{S}{2}\sqrt{5} = \left(\frac{C}{2} + \frac{D}{2}\sqrt{5}\right)^5. \tag{3.132}$$

Proof. See [15]. □

Theorem 3.2.12. *If there exist integers* x, y, z *satisfying the equation* (3.77) *, then one of them must be a multiple of 5.*

Proof. See [15]. □

3.2.2 Generalized Fermat's Last Theorem for Integers

Now, we follow [4].

Consider the generalized Fermat equation

$$x^\alpha + y^\beta = z^\gamma \tag{3.133}$$

$x, y, z, \alpha, \beta, \gamma \in \mathbb{Z}_{>0}$ such that $\gcd(x, y, z) = 1$ and α, β, γ are ≥ 2.

Theorem 3.2.13. *Assuming the truth of the conjecture 1 the generalized Fermat equation*

$$x^{\alpha} + y^{\beta} = z^{\gamma} \tag{3.134}$$

has finitely many co-prime positive integer solutions if

$$\alpha^{-1} + \beta^{-1} + \gamma^{-1} < 1. \tag{3.135}$$

First of all, we need to establish the following:

Lemma 3.2.14. *If $\alpha, \beta, \gamma \in \mathbb{Z}_{>0}$ such that*

$$\alpha^{-1} + \beta^{-1} + \gamma^{-1} < 1 \tag{3.136}$$

then

$$\alpha^{-1} + \beta^{-1} + \gamma^{-1} \leq 41/42. \tag{3.137}$$

Proof. We may suppose, without loss of generality, that $\alpha \leq \beta \leq \gamma$.

If $\alpha = 1$, then $\beta^{-1} + \gamma^{-1} < 0$ which is not possible. So, we necessarily we have $\alpha \geq 2$.

- **Case 1:** $\alpha = 2$.

  Then,

  $$\alpha^{-1} + \beta^{-1} + \gamma^{-1} = 2^{-1} + \beta^{-1} + \gamma^{-1} < 1 \Rightarrow \beta^{-1} + \gamma^{-1} < 2^{-1} \tag{3.138}$$

  and hence, $\beta \geq 3$.

  – $\beta = 3$: Then,

  $$\alpha^{-1} + \beta^{-1} + \gamma^{-1} = 2^{-1} + 3^{-1} + \gamma^{-1} < 1 \Rightarrow \gamma^{-1} < 6^{-1}. \tag{3.139}$$

  This implies that $\gamma \geq 7$ and hence

  $$\alpha^{-1} + \beta^{-1} + \gamma^{-1} = 2^{-1} + 3^{-1} + \gamma^{-1} \leq 2^{-1} + 3^{-1} + 7^{-1} = 41/42. \tag{3.140}$$

– $\beta = 4$: Then,

$$\alpha^{-1} + \beta^{-1} + \gamma^{-1} = 2^{-1} + 4^{-1} + \gamma^{-1} < 1 \Rightarrow \gamma^{-1} < 4^{-1}. \quad (3.141)$$

This implies that $\gamma \geq 5$ and hence

$$\alpha^{-1} + \beta^{-1} + \gamma^{-1} = 2^{-1} + 4^{-1} + \gamma^{-1} \leq 2^{-1} + 4^{-1} + 5^{-1} = 19/20 < 41/42. \quad (3.142)$$

– $\beta \geq 5$: Since $\gamma \geq \beta$ it follows that $\gamma \geq 5$ and hence

$$\alpha^{-1} + \beta^{-1} + \gamma^{-1} \leq 2^{-1} + 5^{-1} + 5^{-1} = 9/10 < 41/42. \quad (3.143)$$

- **Case 2:** $\alpha = 3$.

Then,

$$\alpha^{-1} + \beta^{-1} + \gamma^{-1} = 3^{-1} + \beta^{-1} + \gamma^{-1} < 1 \Rightarrow \beta^{-1} + \gamma^{-1} < 2/3. \quad (3.144)$$

Since $\alpha \leq \beta \leq \gamma$ and $\alpha = 3$ we have $\beta, \gamma \geq 3$

– $\beta = 3$: Then,

$$\alpha^{-1} + \beta^{-1} + \gamma^{-1} = 3^{-1} + 3^{-1} + \gamma^{-1} < 1. \quad (3.145)$$

This implies that $\gamma^{-1} < 1/3$, that is, $\gamma \geq 4$. Hence,

$$\alpha^{-1} + \beta^{-1} + \gamma^{-1} \leq 3^{-1} + 3^{-1} + 4^{-1} = 11/12 < 41 < 42. \quad (3.146)$$

– $\beta \geq 4$: Then, since $\gamma \geq \beta$, and $\gamma \geq 4$ it follows that $\gamma \geq 4$. Hence

$$\alpha^{-1} + \beta^{-1} + \gamma^{-1} \leq 3^{-1} + 4^{-1} + 4^{-1} = 5/6 < 41/42. \quad (3.147)$$

- **Case 3:** $\alpha \geq 4$.

Since $\gamma \geq \beta \geq \alpha$ and $\alpha \geq 4$ it follows that $\beta, \gamma \geq 4$. Hence,

$$\alpha^{-1} + \beta^{-1} + \gamma^{-1} \leq 4^{-1} + 4^{-1} + 4^{-1} = 3/4 < 41/42. \quad (3.148)$$

This proves the lemma. □

Now we can prove the Theorem 3.2.13.

Proof of Theorem 3.2.13. Let $x, y, z \in \mathbb{Z}_{>0}$ be three co-prime numbers satisfying the equation (3.134). Applying the Conjecture 1 with

$$a := x^{\alpha}, \quad b := y^{\beta}, \qquad c := z^{\gamma}, \tag{3.149}$$

we get:

$$\max\{a, b, c\} = \max\{x^{\alpha}, y^{\beta}, z^{\gamma}\} = z^{\gamma} \leq C(\epsilon)\mathrm{Rad}\left(x^{\alpha}y^{\beta}z^{\gamma}\right)^{1+\epsilon} \tag{3.150}$$

$$= C(\epsilon)\mathrm{Rad}\left(\left(x^{\alpha}\right)^{\frac{1}{\alpha}}\left(y^{\beta}\right)^{\frac{1}{\beta}}\left(z^{\gamma}\right)^{\frac{1}{\gamma}}\right)^{1+\epsilon} \tag{3.151}$$

$$\leq C(\epsilon)\left(z^{\gamma}\right)^{\left(\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}\right)(1+\epsilon)} \tag{3.152}$$

$$\leq C(\epsilon)\left(z^{\gamma}\right)^{\frac{41}{42}(1+\epsilon)}, \tag{3.153}$$

from which it follows that

$$\left(z^{\gamma}\right)^{\frac{1}{42}-\frac{41\epsilon}{42}} \leq C(\epsilon). \tag{3.154}$$

This implies that

$$z^{\gamma} \leq C(\epsilon)^{\frac{42}{1-41\epsilon}}. \tag{3.155}$$

Hence if we take $\epsilon < \frac{1}{41}$ we have a finite bound, $C(\epsilon)^{\frac{42}{1-41\epsilon}}$, for x^{α}, y^{β}, and z^{γ}. This completes the proof. □

3.2.3 Powerful Numbers

Definition 3.2.1. A powerful number is a positive integer m which is a multiple of $\mathrm{Rad}(m)^2$.

Such a number m can be expressed as $n = a^2b^3$ for some $a, b \in \mathbb{Z}_{>0}$. Such numbers were studied by P.Erdös and G.Szekeres.

Example 3.3. Here are some examples of powerful numbers:

1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, ...

Lemma 3.2.15. *Let m be a powerful number, then*

$$\mathrm{Rad}(m) \leq \sqrt{m}. \tag{3.156}$$

Proof. Let m be a powerful number. Consider its prime factorization

$$m = p_1^{a_1} \cdots p_k^{a_k}. \tag{3.157}$$

Then

$$\text{Rad}(m)^2 = p_1^2 \cdots p_k^2. \tag{3.158}$$

Therefore, $\text{Rad}(m)^2 \mid m$ and hence $\text{Rad}(m)^2 \leq m$. So $\text{Rad}(m) \leq \sqrt{m}$. □

It is known that there are infinitely many pairs of consecutive powerful numbers. For example,

$(8, 9), (288, 289), (675, 676), (9800, 9801), \ldots$

The following conjecture was made by P. Erdös, R. A. Mollin and P. Walsh.

Conjecture 3. *[Erdös-Mollin-Walsh] There are no three consecutive powerful numbers.*

This conjecture has a very surprising consequence. First recall that

Definition 3.2.2. Let p a prime number such that

$$2^{p-1} \equiv 1 \pmod{p^2} \tag{3.159}$$

is called a Wieferich prime to the base 2, otherwise it is called a non-Wieferich prime.

Theorem 3.2.16. *Assuming the conjecture 3 there are infinitely many non-Wieferich primes.*

Proof. See a reference [17]. □

Concerning the conjecture of Erdös-Mollin-Walsh we have:

Theorem 3.2.17. *Assuming the truth of Conjecture 1, there are only finitely many triples of consecutive powerful numbers.*

Proof. Let m, n and l be three consecutive powerful numbers with $m > n > l > 1$. Then $n = l + 1$ and $m = n + 1 = l + 2$. So,

$$ml + 1 = l^2 + 2l + 1 = n^2. \tag{3.160}$$

It is clear that $\gcd\left(ml,\ 1,\ n^2\right) = 1$.

Applying Conjecture 1, with

$$a := ml, \quad b := 1, \quad c = n^2, \tag{3.161}$$

we get

$$\begin{aligned} n^2 &\leq C(\epsilon)\,\mathrm{Rad}\left(mln^2\right)^{1+\epsilon} && (3.162)\\ &= C(\epsilon)\,\mathrm{Rad}\left(mln\right)^{1+\epsilon} && (3.163)\\ &\leq C(\epsilon)\left[\mathrm{Rad}(m)\mathrm{Rad}(l)\mathrm{Rad}(n)\right]^{1+\epsilon} && (3.164)\\ &\leq C(\epsilon)\left[m^{\frac{1}{2}}l^{\frac{1}{2}}n^{\frac{1}{2}}\right]^{1+\epsilon} && (3.165)\\ &= C(\epsilon)\left(mln\right)^{\frac{1+\epsilon}{2}} && (3.166)\\ &\leq C(\epsilon)\left(n^3\right)^{\frac{1+\epsilon}{2}} && (3.167)\\ &= C(\epsilon)\,n^{\frac{3(1+\epsilon)}{2}} && (3.168) \end{aligned}$$

where we used the fact that $ml < n^2$. So we get

$$n^{\left(\frac{1-3\epsilon}{2}\right)} \leq C(\epsilon). \tag{3.169}$$

Finally, taking ϵ small enough we see that n (and hence m and l) is bounded. This completes the proof. □

Definition 3.2.3. Let $k \in \mathbb{Z}_{\geq 2}$. A k-powerful number is a positive integer m which is a multiple of $\mathrm{Rad}(m)^k$.

Conjecture 4 (Erdös)**.** *The following equation*

$$x + y = z \tag{3.170}$$

has only finitely many solutions with $\gcd(x,\ y) = 1$ *and* x, y *and* z *all 4-powerful.*

Theorem 3.2.18. *The truth of the Conjecture 1 implies Conjecture 4.*

Proof. Assume that there exist three powerful numbers x, y and z with $\gcd(x,\ y) = 1$ such

that $x + y = z$. Clearly $\gcd(x, y, z) = 1$. Applying Conjecture 1 to the following situation

$$a := x, \quad b := y, \quad c := z \tag{3.171}$$

we get

$$z \leq C(\epsilon)\text{Rad}(xyz)^{1+\epsilon} \tag{3.172}$$
$$\leq C(\epsilon)\big(\text{Rad}(x)\text{Rad}(y)\text{Rad}(z)\big)^{1+\epsilon} \tag{3.173}$$
$$\leq C(\epsilon)\big(x^{\frac{1}{4}}y^{\frac{1}{4}}z^{\frac{1}{4}}\big)^{1+\epsilon} \tag{3.174}$$
$$= C(\epsilon)\big(xyz\big)^{\frac{1+\epsilon}{4}} \tag{3.175}$$
$$\leq C(\epsilon)\big(z^3\big)^{\frac{1+\epsilon}{4}} \tag{3.176}$$
$$= C(\epsilon)z^{\frac{3(1+\epsilon)}{4}} \tag{3.177}$$

from which it follows that

$$z^{\frac{1-3\epsilon}{4}} \leq C(\epsilon). \tag{3.178}$$

Finally, taking ϵ small enough we conclude that z (and hence x and y) is bounded. This completes the proof. □

3.2.4 Wieferich Primes

The main reference is [4].

In 1909, Arthur Wieferich obtained the following result [18].

Theorem 3.2.19. *For an odd prime number p if the congruence*

$$2^{p-1} \equiv 1 \pmod{p^2} \tag{3.179}$$

is not satisfied then the First Case of Fermat's Last Theorem is true.

Definition 3.2.4. A prime number p satisfies the congruence in equation (3.179) is called a Wieferich prime to the base 2, otherwise it is called a non-Wieferich prime.

Remark. As of March 2021, 1093 and 3511 are the only known Wieferich-primes.

Problem 1. To decide whether the number of Wieferich or non-Wieferich primes is finite or

not.

In [19], the following theorem was proved by J. H. Silverman.

Theorem 3.2.20. *Let p an odd prime number. Assuming the truth of Conjecture 1 with $\epsilon \in (0,1)$ the set S of non-Wieferich primes is infinite.*

Proof. The proof is by contradiction. So, suppose that S is finite. We denote the set of Wieferich primes by T.

Consider the sequence (a_k) of positive integers defined as follows:

- If $k = 1$, we define a_1 as follows:

For every $p \in S$, $p \nmid a_1$ and it is the smallest integer having this property.

- If $k = 2$, we define a_2 as follows:

For every $p \in S$, $p \nmid a_2$ and it is the smallest integer $> a_1$ having this property and so on.

Clearly, the sequence (a_k) is a positive, increasing, and unbounded above.

Next, consider the sequence $(2^{a_k} - 1)$ which is also positive, increasing, and unbounded above. Now, write

$$2^{a_k} - 1 = s_k t_k, \tag{3.180}$$

where the prime divisors of s_k are in S and the prime divisors of t_k are in T.

Our strategy is to show that the sequences (s_k) and (t_k) are bounded which will lead to a contradiction since their product $(2^{a_k} - 1)$ is unbounded above.

Let $\mathrm{ord}_p(a)$ denote the order of a modulo p. It is defined as the smallest positive integer satisfying

$$a^{\mathrm{ord}_p(a)} \equiv 1 \pmod{p}. \tag{3.181}$$

We set $n_1 := \mathrm{ord}_p(2)$ and $n_2 := \mathrm{ord}_{p^2}(2)$. Then,

$$2^{n_1} \equiv 1 \pmod{p} \Leftrightarrow p \mid (2^{n_1} - 1) \Leftrightarrow 2^{n_1} = 1 + \alpha p \tag{3.182}$$

for some positive integer α. So,

$$2^{n_1 p} = (1+\alpha p)^p \tag{3.183}$$

$$= \sum_{i=1}^{p} \binom{p}{i} (\alpha p)^i \tag{3.184}$$

$$\equiv 1 \pmod{p^2}. \tag{3.185}$$

Since $n_2 = \text{ord}_{p^2}(2)$ it follows that $n_2 \mid n_1 p$. On the other hand,

$$2^{n_2} \equiv 1 \pmod{p^2} \Leftrightarrow p^2 \mid (2^{n_2} - 1). \tag{3.186}$$

Moreover, it follows that p divides $2^{n_2}-1$, that is, $2^{n_2}-1 \equiv 0 \pmod{p}$. Since $n_1 = \text{ord}_p(2)$, we conclude that $n_1 \mid n_2$. Now

- $n_2 \mid n_1 p \Rightarrow n_1 p = n_2 l$ for some $l \in \mathbb{N}$.
- $n_1 \mid n_2 \Rightarrow n_2 = n_1 l'$ for some $l' \in \mathbb{N}$.

It follows that $n_1 p = n_1 l' l$. So, $l' l = p$ implies that ($l = 1$ and $l' = p$) or ($l = p$ and $l' = 1$).

- If $l = 1$ and $l' = p$ then $n_1 p = n_2$.
- If $l = p$ and $l' = 1$, $n_1 = n_2$.

So, we have either $n_1 = n_2$ or $n_2 = n_1 p$.

Next, we have

- **Claim 1.** If $p \mid s_k$, then $p^2 \nmid s_k$.

  Assume that $p \mid s_k$. We have two cases:

  – Suppose that $n_1 = n_2$. Recall that Fermat's Little Theorem says that

  $$2^{p-1} \equiv 1 \pmod{p}. \tag{3.187}$$

  As $n_1 = \text{ord}_p(2)$, it follows that $n_1 \mid (p-1)$. As $n_1 = n_2$, we also have $n_2 \mid (p-1)$ and hence $2^{p-1} \equiv 1 \pmod{p^2}$. This contradicts the assumption that if $p \mid s_k$ then $p \in S$.

  – Suppose that $n_2 = n_1 p$. As $p \mid s_k$, we have, by assumption, $p \in S$ and $p \nmid a_k$.

This implies that $n_2 \nmid a_k$. Therefore, $2^{a_k} \not\equiv 1 \pmod{p^2}$ and so $p^2 \nmid s_k$.

Hence, we have shown that if $p \mid s_k$ then $p^2 \nmid s_k$.

This proves **Claim 1**.

- **Claim 2.** If $p \mid t_k$, then $p^2 \mid t_k$.

  Assume that $p \mid t_k$. We have two cases:

  – Suppose that $n_2 = n_1 p$. As $p \mid t_k$, we have by assumption, $p \in T$, that is, $2^{p-1} \equiv 1 \pmod{p^2}$. As $n_2 = \mathrm{ord}_{p^2}(2)$, it implies that $n_2 \mid (p-1)$ and hence, $p \nmid n_2$. This is a contradiction since we assumed that $n_2 = n_1 p$.

  – Suppose that $n_1 = n_2$. As $p \mid t_k$ and $t_k \mid (2^{a_k} - 1)$ it follows that $p \mid (2^{a_k} - 1)$ or equivalently $2^{a_k} \equiv 1 \pmod{p}$. Since $n_1 = \mathrm{ord}_p(2)$, we have $n_1 \mid a_k$ and hence $n_2 \mid a_k$. Finally, since $n_2 = \mathrm{ord}_{p^2}(2)$ we get $2^{a_k} \equiv 1 \pmod{p^2}$. Note that $p^2 \mid (2^{a_k} - 1)$ or $p^2 \mid s_k t_k$ so $p^2 \mid t_k$ since $p \mid t_k$. Hence we have shown that if $p \mid t_k$ then $p^2 \mid t_k$.

  This proves **Claim 2**.

Next, we set

$$m := \prod_{p \in S} p. \tag{3.188}$$

As S is a finite set we conclude that $m \in \mathbb{Z}_{>0}$.

By **Claim 1** we know that if $p \mid s_k$ then $p^2 \nmid s_k$. So we have

$$s_k = \prod_{p \mid s_k} p \leq m. \tag{3.189}$$

Therefore, (s_k) is bounded.

By **Claim 2**, we know that if $p \mid t_k$, then $p^2 \mid t_k$. So all the prime factors of t_k are powers of 2, from which we conclude that

$$\mathrm{Rad}(t_k) \leq t_k^{1/2}. \tag{3.190}$$

Applying Conjecture 1 with $a = s_k t_k = 2^{a_k} - 1$, $b = 1$, and $c = 2^{a_k}$, we get

$$2^{a_k} \leq C(\epsilon)\, \mathrm{Rad}(s_k t_k \cdot 1 \cdot 2^{a_k})^{1+\epsilon} \tag{3.191}$$

$$\leq C(\epsilon)\, 2^{1+\epsilon}\, \mathrm{Rad}(s_k t_k)^{1+\epsilon} \tag{3.192}$$

$$= C(\epsilon)\, 2^{1+\epsilon}\, \mathrm{Rad}(s_k)^{1+\epsilon}\, \mathrm{Rad}(t_k)^{1+\epsilon} \tag{3.193}$$

$$\leq C(\epsilon)\, 2^{1+\epsilon}\, m^{1+\epsilon}\, t_k^{\frac{1+\epsilon}{2}}. \tag{3.194}$$

Hence,

$$t_k < s_k t_k + 1 = 2^{a_k} \leq C(\epsilon)\, 2^{1+\epsilon}\, m^{1+\epsilon}\, t_k^{\frac{1+\epsilon}{2}} \tag{3.195}$$

from which it follows that

$$t_k \leq \left(2^{1+\epsilon}\, C(\epsilon)\, m^{1+\epsilon}\right)^{\frac{2}{1-\epsilon}}. \tag{3.196}$$

We see that (t_k) is bounded. It is contradiction since $(2^{a_k} - 1) = (s_k)(t_k)$ is unbounded. This completes the proof. □

3.2.5 Erdös-Woods Conjecture

The main references are [4] and [20].

In this section, we consider the following problem:

Problem 2. Does there exist a positive constant l such that if $\theta,\ \delta \in \mathbb{Z}_{>0}$ satisfying

$$\mathrm{Rad}(\theta + i) = \mathrm{Rad}(\delta + i) \tag{3.197}$$

for $j = 0, 1, \ldots, l-1$ then $\theta = \delta$?

- It is clear that $l > 1$.
- For $l = 2$, we have:

Theorem 3.2.21. *There are infinitely many pairs $(\theta, \delta) \in \mathbb{Z}_{>0}^2$ with $\theta < \delta$ such that*

$$\mathrm{Rad}(\theta + j) = \mathrm{Rad}(\delta + j) \tag{3.198}$$

for $j = 0, 1$.

Proof. Let $m \in \mathbb{Z}_{>0}$. Define the following numbers θ and δ as follows:

$$\theta = 2^m - 2 = 2(2^{m-1} - 1), \quad \delta = (2^m - 1)^2 - 1 = 2^{m+1}\,(2^{m-1} - 1). \tag{3.199}$$

Clearly θ and δ are positive with $\theta < \delta$.

We have

$$\theta + 1 = 2^{m-1} \quad \text{and} \quad \delta + 1 = (2^{m-1})^2, \tag{3.200}$$

and hence

$$\text{Rad}(\theta) = \text{Rad}\big(2(2^{m-1} - 1)\big) = \text{Rad}(2)\,\text{Rad}(2^{m-1} - 1) = 2\text{Rad}(2^{m-1} - 1), \tag{3.201}$$

$$\text{Rad}(\delta) = \text{Rad}\big(2^{m+1}(2^{m+1} - 1)\big) = \text{Rad}(2^{m+1})\,\text{Rad}(2^{m-1} - 1) = 2\text{Rad}(2^{m-1} - 1). \tag{3.202}$$

So, $\text{Rad}(\theta) = \text{Rad}(\delta)$. Moreover, we have

$$\text{Rad}(\theta + 1) = \text{Rad}(2^m - 1), \tag{3.203}$$

$$\text{Rad}(\delta + 1) = \text{Rad}\big((2^m - 1)^2\big) = \text{Rad}(2^m - 1), \tag{3.204}$$

and hence, $\text{Rad}(\theta + 1) = \text{Rad}(\delta + 1)$.

This completes the proof. □

Remark. We have another example of a pair of integers (θ, δ) with $\theta < \delta$ that is not in the above form. Consider the pair $(\theta, \delta) = (75, 1215)$. Then

- $\text{Rad}(75) = \text{Rad}(2 \cdot 5^2) = 3 \cdot 5 = 15$
- $\text{Rad}(1215) = \text{Rad}(3^5 \cdot 5) = 3 \cdot 5 = 15$ so $\text{Rad}(75) = \text{Rad}(1215)$.
- $\text{Rad}(75 + 1) = \text{Rad}(76) = \text{Rad}(2^2 \cdot 19) = 2 \cdot 19 = 38$
- $\text{Rad}(1215 + 1) = \text{Rad}(1216) = \text{Rad}(2^6 \cdot 19) = 2 \cdot 19 = 38$ so $\text{Rad}(76) = \text{Rad}(1216)$.

There are no other further examples. In addition, no one has yet found two positive integers θ, δ with $\theta \neq \delta$ which satisfies

$$\text{Rad}(\theta + j) = \text{Rad}(\delta + j) \tag{3.205}$$

for $j = 0, 1, 2$.

Therefore, we come to the Erdös-Woods conjecture.

Conjecture 5. *There exist an absolute constant $l > 2$ such that if $\theta, \delta \in \mathbb{Z}_{>0}$ which satisfy*

$$\text{Rad}(\theta + j) = \text{Rad}(\delta + j) \tag{3.206}$$

for $j = 0, 1, 2, \ldots, l - 1$ then $\theta = \delta$.

In [2], Langevin showed that Conjecture 1 implies that the Conjecture 5 holds when $l = 3$ for all but finitely many θ.

Theorem 3.2.22. *Assuming the truth of Conjecture 1, there exist finitely many positive integers θ, δ with $\delta < \theta$ such that*

$$\text{Rad}(\theta + j) = \text{Rad}(\delta + j) \tag{3.207}$$

for $j = 0, 1, 2$.

Proof. First of all observe that

$$\theta + j \equiv 0 \pmod{\text{Rad}(\theta + j)} \quad \text{and} \quad \delta + j \equiv 0 \pmod{\text{Rad}(\delta + j)} \tag{3.208}$$

for $j = 0, 1, 2$. Then

$$\theta - \delta = (\theta + j) - (\delta + j) \equiv 0 \pmod{\text{Rad}(\delta + j)} \tag{3.209}$$

for $j = 0, 1, 2$.

Observe that the greatest common divisor of any two integers $\text{Rad}(\theta), \text{Rad}(\theta + 1)$ and $\text{Rad}(\theta + 2)$ is either 1 or 2. Therefore

$$2(\theta - \delta) \equiv 0 \pmod{\text{Rad}((\theta)(\theta + 1)(\theta + 2))}. \tag{3.210}$$

Next, we apply Conjecture 1 with

$$a = \theta(\theta + 2), \quad b = 1, \quad c = (\theta + 1)^2 \tag{3.211}$$

to get

$$c = (\theta + 1)^2 \leq C(\epsilon)\text{Rad}\big(\theta(\theta + 2)1(\theta + 1)^2\big)^{1+\epsilon}. \tag{3.212}$$

Note that

- $(\theta + 1)^2 \geq \theta^2$,
- $\text{Rad}\big(\theta(\theta + 2)(\theta + 1)^2\big) = \text{Rad}\big(\theta(\theta + 2)(\theta + 1)\big)$,
- $\text{Rad}\big(\theta(\theta + 2)(\theta + 1)\big) \leq 2(\theta - \delta)$ by the equation (3.210).

Finally, combining above the observations we get

$$\theta^2 \leq \big(\theta+1\big)^2 \leq C(\epsilon)\mathrm{Rad}\big(\theta(\theta+2)1(\theta+1)^2\big)^{1+\epsilon} \tag{3.213}$$

$$\leq C(\epsilon)\big(2(\theta-\delta)\big)^{1+\epsilon} \tag{3.214}$$

$$\leq C(\epsilon)(2\theta)^{1+\epsilon}. \tag{3.215}$$

Hence we get

$$\theta \leq \big(C(\epsilon)2^{1+\epsilon}\big)^{\frac{1}{1-\epsilon}}. \tag{3.216}$$

Therefore, θ is bounded (and so is δ).

This completes the proof. □

3.2.6 Other Applications

In this section, we give further applications of Conjecture 1 following [21].

(i) Weak Version of The Hall's Conjecture:

This conjecture states that for any $\epsilon > 0$, there is a positive number $C(\epsilon)$ such that for every $x, y \in \mathbb{Z}_{>0}$ such that $x^3 - y^2 \neq 0$ then

$$|x^3 - y^2| > C(\epsilon)\max\{x^3, y^2\}^{\frac{1}{6}-\epsilon}. \tag{3.217}$$

In [22] and [23], it was shown that the weak version Hall's conjecture follows from Conjecture 1.

(ii) Mordell's Conjecture:

This conjecture states the following:

Let F be an algebraic number field. Every curve of genus > 1 over F has only finitely many F-rational points. It was proved by Faltings in 1984. In [24], Elkies proved this conjecture over F follows from Conjecture 1 over F.

(iii) Roth's Theorem:

It states that for every algebraic number α the inequality

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^{2+\epsilon}} \tag{3.218}$$

with $\epsilon > 0$ has only finitely many solutions. In [25], Bombieri, using Conjecture 1, proved that one has the inequality

$$\left|\alpha - \frac{r}{s}\right| > \frac{1}{s^{2+l}} \tag{3.219}$$

except for finitely many fractions $\frac{r}{s}$ with $\gcd(r, s) = 1$ where

$$l = C(\log s)^{\frac{-1}{2}} \left(\log(\log s)\right)^{-1} \tag{3.220}$$

for a suitable constant C which depends only on α.

(iv) Dressler's Conjecture:

For any $x, y \in \mathbb{Z}_{>0}$ with $x < y$ such that $\mathrm{Rad}(x) = \mathrm{Rad}(y)$ then there exist a prime number between them. In [26], Cochrane and Dressler showed that Conjecture 1 yields that for any $\epsilon > 0$ there is a suitable constant $C(\epsilon)$, then

$$y - x > C(\epsilon)\, x^{\frac{1}{2}-\epsilon}. \tag{3.221}$$

(v) The Schinzel-Tijdeman Conjecture:

Let $g(x) \in \mathbb{Q}[x]$ having at least three simple zeros. Then the Diophantine equation

$$g(x) = y^3 z^2 \tag{3.222}$$

has finitely many solutions $(x, y, z) \in \mathbb{Z}^3$ such that $xyz \neq 0$. In [27], Walsh proved that this conjecture follows from Conjecture 1.

4. RECENT ADVANCES

In [1], using his Inter-universal Teichmüller Theory (IUT), S. Mochizuki proved non-effective Vojta, Szpiro and abc-conjectures over algebraic number fields. Recently, in [2], I. Fesenko, Y. Hoshi, A. Minamide , S. Mochizuki and W. Porowski verified numerically effective versions of the abc- conjecture over mono-complex number fields and Szpiro conjecture. In addition, they get, as an application, an explicit estimate for Fermat's Last Theorem.

In this chapter, following [2], we state effective abc and Szpiro conjectures over integers and discuss in detail applications to Fermat's Last Theorem and its generalized version. The main references for this chapter are [1] and [2].

4.1. EFFECTIVE abc AND EFFECTIVE SZPIRO CONJECTURES

In this section, we state effective versions of abc and Szpiro conjectures.

Theorem 4.1.1 (Effective abc-conjecture)**.** *Let* $a, b, c \in \mathbb{Z} - \{0\}$ *such that*

$$\gcd(a, b, c) = 1 \quad \text{and} \quad a + b + c = 0. \tag{4.1}$$

Let $\epsilon \in (0, 1]$. *Then*

$$\max\{|a|, |b|, |c|\} \leq 2^{\frac{5}{2}} \max\left\{\exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30} \cdot \epsilon^{\frac{-166}{81}}\right), \left(\mathrm{Rad}(abc)^{\frac{3(1+\epsilon)}{2}}\right)\right\} \tag{4.2}$$

$$\leq 2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30} \cdot \epsilon^{\frac{-166}{81}}\right)\left(\mathrm{Rad}(abc)^{\frac{3(1+\epsilon)}{2}}\right). \tag{4.3}$$

Proof. See [2]. □

Remark. In [2], a version of this theorem is also proved over imaginary quadratic number fields.

Theorem 4.1.2 (Effective Szpiro conjecture)**.** *Let* $a, b, c \in \mathbb{Z} - \{0\}$ *such that*

$$\gcd(a, b, c) = 1 \quad \text{and} \quad a + b + c = 0. \tag{4.4}$$

Let $\epsilon \in (0,1]$. *Then*

$$|abc| \leq 2^4 \max\left\{\exp(1.7 \cdot 10^{30}\epsilon^{\frac{-166}{81}}), \operatorname{Rad}(abc)^{3(1+\epsilon)}\right\} \tag{4.5}$$

$$\leq 2^4 \exp\left(1.7 \cdot 10^{30}\epsilon^{\frac{-166}{81}}\right)\left(\operatorname{Rad}(abc)\right)^{\frac{3(1+\epsilon)}{2}}. \tag{4.6}$$

Proof. See [2]. □

Remark. In [28], Theorem 4.1.2 was stated as a conjecture by Szpiro.

Remark. Note that Theorem 4.1.1 follows from Theorem 4.1.2 but not conversely.

4.2. APPLICATIONS TO ASYMPTOTIC FERMAT'S LAST THEOREM AND ITS GENERALIZED VERSION

In this section, following [2], as applications of Theorem 4.1.1 and Theorem 4.1.2 we consider asymptotic Fermat's Last Theorem and its generalized version. First we need to establish the following lemmata.

Lemma 4.2.1. *Let* $x, y \in \mathbb{Z}$ *such that* $x + y \neq 0$. *Let* $n \in \mathbb{Z}_{\geq 3}$ *be an odd integer. Then*

$$(x^n + y^n)(x+y)^{-1} = ny^{n-1} - (x+y)\sum_{j=0}^{n-2}(-1)^{j+1}(j+1)x^{n-2-j}y^j. \tag{4.7}$$

Proof. Without loss of generality, we may assume, that $x \neq 0$. Multiplying both sides of the equation (4.7) by x^{1-n} we get

$$\left(1+\left(\frac{y}{x}\right)^n\right)\left(1+\left(\frac{y}{x}\right)\right)^{-1} = n\left(\frac{y}{x}\right)^{n-1} - \left(1+\frac{y}{x}\right)\sum_{j=0}^{n-2}(-1)^{j+1}(j+1)\left(\frac{y}{x}\right)^j. \tag{4.8}$$

We set $t := \frac{y}{x}$. Hence we need to verify the following equality

$$(1+t^n)(1+t)^{-1} = nt^{n-1} - (1+t)\sum_{j=0}^{n-2}(-1)^{j+1}(j+1)t^j. \tag{4.9}$$

We will need following the fact:

Fact. For every $n \in \mathbb{Z}_{\geq 3}$ clearly we have

$$(1+x^n)(1+x)^{-1} = \sum_{j=-1}^{n-2} (-1)^{j+1} x^{j+1}. \tag{4.10}$$

This fact can be proved easily by induction on n:

- If $n = 3$, then we get

$$(1+x^3)(1+x)^{-1} = 1 - x + x^2 = \sum_{j=-1}^{1} (-1)^{j+1} x^{j+1}. \tag{4.11}$$

Therefore the equation (4.10) is true in the case $n = 3$.

- Assume that the equation (4.10) is true for $n = k > 3$. Now,

$$(1+x^{k+1})(1+x)^{-1} = x^k + (1-x^k)(1+x)^{-1} = x^k + (1+(-x)^k)(1+x)^{-1} \tag{4.12}$$

$$= x^k + \sum_{j=-1}^{k-2} (-1)^{j+1}(-x)^{j+1} \tag{4.13}$$

$$= x^k + \sum_{j=-1}^{k-2} (-1)^{j+1}(-1)^{j+1} x^{j+1} \tag{4.14}$$

$$= x^k + \sum_{j=-1}^{k-2} x^{j+1} \tag{4.15}$$

$$= x^k + 1 + x + x^2 + \ldots + x^{k-1} \tag{4.16}$$

$$= x^k + \sum_{j=-1}^{k-1} x^{j+1} = \sum_{j=-1}^{(k+1)-2} x^{j+1}, \tag{4.17}$$

so the equation (4.10) is true for $n = k+1$. By induction (4.10) is true for all $n \geq 3$. Now, we have

$$nt^{n-1} = \frac{d}{dt}(1+t^n)\frac{d}{dt}\left\{\left[(1+t^n)(1+t)^{-1}\right](1+t)\right\} \tag{4.18}$$

$$= 1.\left[(1+t^n)(1+t)^{-1}\right] + (1+t)\frac{d}{dt}\left[(1+t^n)(1+t)^{-1}\right] \tag{4.19}$$

$$= \left[(1+t^n)(1+t)^{-1}\right] + (1+t)\frac{d}{dt}\left(\sum_{j=-1}^{n-2}(-1)^{j+1}t^{j+1}\right) \tag{4.20}$$

$$= \left[(1+t^n)(1+t)^{-1}\right] + (1+t)\sum_{j=0}^{n-2}(-1)^{j+1}(j+1)t^j. \tag{4.21}$$

□

Lemma 4.2.2. *Let $p \geq 3$ be a prime number and $x, y, z \in \mathbb{Z} - \{0\}$ such that*

$$\gcd(x, y, z) = 1 \qquad \text{and} \qquad x^p + y^p + z^p = 0. \tag{4.22}$$

Then,

(i) If q is a prime number such that $q \mid (x + y)$ and $q \mid (x^p + y^p)(x + y)^{-1}$ then $q = p$.

(ii) Assume that $p \nmid z$, then $\gcd\left(x + y, (x^p + y^p)(x + y)^{-1}\right) = 1$. In particular, there are $m, m' \in \mathbb{Z}$ such that

$$x + y = m^p, \quad (x^p + y^p)(x + y)^{-1} = (m')^p, \quad z = -mm'. \tag{4.23}$$

(iii) Assume that $p \mid z$. Then $p \mid (x+y)$, $p \mid (x^p+y^p)(x+y)^{-1}$ and $p^2 \nmid (x^p+y^p)(x+y)^{-1}$. In particular, if we write $z = p^l a$ for some $l, a \in \mathbb{Z}_{>0}$ with $\gcd(p, a) = 1$, then there are $n, n' \in \mathbb{Z}$ with $\gcd(p, n) = \gcd(p, n') = 1$ satisfying

$$x + y = p^{lp-1}n^p, \quad (x^p + y^p)(x + y)^{-1} = p(n')^p, \quad a = -nn'. \tag{4.24}$$

Proof. (i) Let q be a prime number such that $q \mid (x + y)$ and $q \mid (x^p + y^p)(x + y)^{-1}$. By Lemma 4.2.1 ,

$$(x^p + y^p)(x + y)^{-1} = py^{p-1} - (x + y)\sum_{j=0}^{p-2}(-1)^{j+1}(j + 1)x^{p-2-j}y^j \tag{4.25}$$

from which we conclude that $q \mid py^{p-1}$. Hence, if $q \neq p$, then necessarily $q \mid y^{p-1}$ as a result $q \mid y$. Moreover, since $x = (x + y) - y$, we conclude that $q \mid x$.

Clearly, $q \mid x^p$ and $q \mid y^p$, hence $q \mid (x^p + y^p)$. Since $x^p + y^p = -z^p$ we get $q \mid (-z^p)$ and hence $q \mid z$ which contradicts the assumption so we must have $q = p$. This proves (i).

(ii) Assume, one the contrary that, $\gcd\left(x + y, (x^p + y^p)(x + y)^{-1}\right) \neq 1$. Hence, there is a prime number q such that $q \mid (x + y)$ and $q \mid (x^p + y^p)(x + y)^{-1}$. By part (i) , we have $q = p$. Observe that $p \mid (x + y)(x^p + y^p)(x + y)^{-1}$, that is, $p \mid (x^p + y^p)$. Since $x^p + y^p = -z^p$ we conclude that $p \mid z$ which contradicts the assumption that $p \nmid z$. So $\gcd\left(x + y, (x^p + y^p)(x + y)^{-1}\right) = 1$.

Next, since $\gcd\left(x+y,\ (x^p+y^p)(x+y)^{-1}\right)=1$ and $(x+y)(x^p+y^p)(x+y)^{-1}=(-z)^p$ then, by Proposition 2.2.2, there are m and m' such that

$$x+y=m^p,\quad (x^p+y^p)(x+y)^{-1}=(m')^p,\quad z=-mm'. \tag{4.26}$$

This proves (ii).

(iii) First of all, since $p \mid z$ it follows that

$$(x+y)^p \equiv x^p+y^p=(-z)^p \equiv 0 \pmod{p}. \tag{4.27}$$

So $p \mid (x+y)$. Recall that by Lemma 4.2.1 we have

$$(x^p+y^p)(x+y)^{-1}=py^{p-1}-(x+y)\sum_{j=0}^{p-2}(-1)^{j+1}(j+1)x^{p-2-j}y^j \tag{4.28}$$

from which we have $p \mid (x^p+y^p)(x+y)^{-1}$. Therefore we need to prove that $p^2 \nmid (x^p+y^p)(x+y)^{-1}$. As $p \mid (x+y)$, we can express $x+y=p\alpha$ for some integer α. Moreover, since

$$(x^p+y^p)(x+y)^{-1}=(x^p+(p\alpha-x)^p)\,(p\alpha)^{-1} \tag{4.29}$$

$$=\left(x^p+\sum_{j=0}^{p}\binom{p}{j}(p\alpha)^{p-j}(-x)^j\right)(p\alpha)^{-1} \tag{4.30}$$

$$=\sum_{j=0}^{p-1}\binom{p}{j}(p\alpha)^{p-j-1}(-x)^j \tag{4.31}$$

$$=p\,(p\alpha)^{p-1}+\cdots+p\,(-x)^{p-1}, \tag{4.32}$$

we conclude that $p^2 \mid px^{p-1}$, and hence $p \mid x$. Since $y=(y+x)-x$, we get $p \mid y$ and hence $p \mid z$ which contradicts the assumption. Hence,

$p^2 \nmid (x^p+y^p)(x+y)^{-1}$. Next we get

$$(x+y)(x^p+y^p)(x+y)^{-1}=(-z)^p=(-p^la)^p=p^{lp}(-a)^p. \tag{4.33}$$

Therefore, we can write

$$x+y=p^{lp-1}A \quad \text{and} \quad (x^p+y^p)(x+y)^{-1}=pB, \tag{4.34}$$

for some $A, B \in \mathbb{Z}$, with $\gcd(p,\ A)=\gcd(p,\ B)=1$ and $AB=(-a)^p$.

Claim. We have $\gcd(A, B) = 1$.

Suppose, on the contrary, that $\gcd(A, B) \neq 1$. Then there exist a prime number q such that $q \mid A$ and $q \mid B$. It implies that $q \mid (x + y)$ and $q \mid (x^p + y^p)(x + y)^{-1}$. By part (i) we get $q = p$ which contradicts the assumption that $\gcd(p, A) = \gcd(p, B) = 1$. By Proposition 2.2.2, there are n and n' such that

$$A = n^p, \quad B = (n')^p, \quad \text{and} \quad a = -nn'. \tag{4.35}$$

This proves (iii).

□

Lemma 4.2.3. *Let p be an odd prime number; $X, Y, Z \in \mathbb{Z}_{>0}$ such that*

$$\gcd(X, Y, Z) = 1 \qquad \text{and} \qquad X^p + Y^p = Z^p. \tag{4.36}$$

Then we have

$$Z > \frac{(p+1)^p}{2}. \tag{4.37}$$

Proof. The proof splits into three cases: $p \mid XY$, $p \mid Z$ and $p \nmid XYZ$.

- Case 1: $p \mid XY$.

  Suppose that $p \mid XY$.

  Claim 1. We have $p \nmid Z$.

  Assume, on the contrary, that $p \mid Z$. Then $p \mid XY$ and $p \mid Z \Rightarrow (p \mid X$ and $p \mid Z)$ or $(p \mid Y$ and $p \mid Z)$.

  If $p \mid X$ and $p \mid Z$, then $p \mid X^p$ and $p \mid Z^p$. So, $p \mid (Z^p - X^p)$. Since, $Z^p - X^p = Y^p$ we get $p \mid Y^p$ and hence $p \mid Y$ which contradicts since the assumption that $\gcd(X, Y, Z) = 1$.

  If $p \mid Y$ and $p \mid Z$, then $p \mid Y^p$ and $p \mid Z^p$. So, $p \mid (Z^p - Y^p)$. Since, $Z^p - Y^p = X^p$ we get $p \mid X^p$ and hence $p \mid X$ which contradicts since the assumption that $\gcd(X, Y, Z) = 1$.

  Therefore, we conclude that $p \nmid Z$.

  Next, since $p \mid XY$, we may suppose that $p \mid X$.

Claim 2. We have $p \nmid Y$.

Suppose that $p \mid Y$. Then $p \mid X^p$ and $p \mid Y^p$. So, $p \mid (X^p + Y^p)$. Since $X^p + Y^p = Z^p$, then $p \mid Z^p$ and hence $p \mid Z$. This is a contradiction.

Since $X^p + Y^p = Z^p$ and p is odd we have $X^p + Y^p + (-Z)^p = 0$. Moreover, by assumption $p \nmid Z$. So , applying Lemma 4.2.2 (ii) with

$$x := X, \qquad y := Y, \qquad z := -Z \tag{4.38}$$

it follows that

$$X + Y = \alpha^p \tag{4.39}$$

for some positive integer α. (The positivity of α follows from the facts that $X, Y \in \mathbb{Z}_{>0}$ and p is odd.)

Since $X^p + Y^p = Z^p$ and p is odd, we have $Z^p + (-X)^p + (-Y)^p = 0$. Applying again Lemma 4.2.2 (ii) with

$$x := Z, \qquad y := -X, \qquad z := -Y \tag{4.40}$$

we get

$$Z - X = \beta^p \tag{4.41}$$

for some positive integer β. (The positivity of β follows from the facts that $Z > X$ and p is odd.)

Since, $p \mid X$ we get

$$(Z - Y)^p \equiv Z^p - Y^p = X^p \equiv 0 \pmod{p} \tag{4.42}$$

and hence $p \mid (Z - Y)$. Therefore, we have

$$(\beta - \alpha)^p \equiv \beta^p - \alpha^p = (Z - X) - (X + Y) = (Z - Y) - 2X \equiv 0 \pmod{p} \tag{4.43}$$

and hence $p \mid (\beta - \alpha)$.

Claim 3. We have $\max\{\alpha, \beta\} \geq p + 1$.

Assume, on the contrary, that $\max\{\alpha, \beta\} < p + 1$ or, equivalently $\max\{\alpha, \beta\} \leq p$.

Since, $p \mid (\beta - \alpha)$ we must have $\beta = \alpha$. In this case, we get

$$X + Y = \alpha^p = \beta^p = Z - X. \tag{4.44}$$

So $Z = 2X + Y$. Then, taking the p^{th} powers we get

$$Z^p = (2X + Y)^p > X^p + Y^p. \tag{4.45}$$

This is a contradiction, since, we assumed that $Z^p = X^p + Y^p$. Now, using Claim 3, and the fact that $Z > Y$, we get

$$2Z > Z + Y = \alpha^p + \beta^p > \max\{\alpha, \beta\}^p \geq (p+1)^p, \tag{4.46}$$

from which we conclude that $Z > \dfrac{(p+1)^p}{2}$.

This proves Case 1.

- Case 2: $p \mid Z$.

  Suppose that, $p \mid Z$.

  Claim 4. We have $p \nmid XY$.

  Suppose, on the contrary, that $p \mid XY$. Then $p \mid X$ or $p \mid Y \Rightarrow (p \mid X$ and $p \mid Z)$ or $(p \mid Y$ and $p \mid Z)$.

  If $p \mid X$ and $p \mid Z$, then $p \mid X^p$ and $p \mid Z^p$. So $p \mid (Z^p - X^p)$. Since $Z^p - X^p = Y^p$ we get $p \mid Y^p$ and hence $p \mid Y$ which contradicts since the assumption.

  If $p \mid Y$ and $p \mid Z$, then $p \mid Y^p$ and $p \mid Z^p$. So $p \mid (Z^p - Y^p)$. Since $Z^p - Y^p = X^p$ we get $p \mid X^p$ and hence $p \mid X$ which contradicts since the assumption.

  Therefore, we conclude that, $p \nmid XY$.

  Since $X^p + Y^p = Z^p$ and p is odd we get $Z^p + (-Y)^p + (-X)^p = 0$. Moreover, $p \nmid X$ by assumption. So, applying Lemma 4.2.2 (ii) with

  $$x := Z, \qquad y := -Y, \qquad z := -X \tag{4.47}$$

  we get

  $$Z - Y = \gamma^p \tag{4.48}$$

for some positive integer γ. (The positivity of γ follows from the facts that $Z > Y$ and p is odd.)

Since $X^p + Y^p = Z^p$ and p is odd, we have $X^p + Y^p + (-Z)^p = 0$. Moreover, $p \mid Z$ by assumption. So, applying again Lemma 4.2.2 (iii) with

$$x := X, \qquad y := Y, \qquad z := -Z \tag{4.49}$$

we get

$$X + Y = p^{lp-1}n^p \quad \text{and} \quad Z = -p^l a, \tag{4.50}$$

for some $n, l \in \mathbb{Z}_{>0}$ with $\gcd(p, n) = 1$ and negative integer a with $\gcd(p, a) = 1$.

Since $p \mid (X + Y)$ and $p \mid Z$, we have

$$(\beta + \gamma)^p \equiv \beta^p + \gamma^p = (Z - X) + (Z - Y) = 2Z - X - Y \equiv 0 \pmod{p} \tag{4.51}$$

and hence $p \mid (\beta + \gamma)$.

Recall that by Lemma 4.2.1, we have

$$(\beta^p + \gamma^p)(\beta + \gamma)^{-1} = p\gamma^{p-1} - (\beta + \gamma)\sum_{j=1}^{p-2}(-1)^{j+1}(j+1)\beta^{p-2-j}\gamma^j. \tag{4.52}$$

Multiplying both sides by $(\beta + \gamma)$ we get

$$\beta^p + \gamma^p = p\gamma^{p-1}(\beta + \gamma) - (\beta + \gamma)^2\sum_{j=1}^{p-2}(-1)^{j+1}(j+1)\beta^{p-2-j}\gamma^j \tag{4.53}$$

from which it follows that

$$p^2 \mid (\beta^p + \gamma^p). \tag{4.54}$$

Therefore, since we have

$$-2p^l a = 2Z = (Z - X) + (Z - Y) + (X + Y) \tag{4.55}$$

$$= \beta^p + \gamma^p + p^{lp-1}n^p \equiv 0 \pmod{p^2} \tag{4.56}$$

we get $l \geq 2$.

We have the following fact:

Remark. For all real numbers $\theta \geq 3$, $\theta^{2\theta-1} > (\theta + 1)^\theta$.

Finally, using the above fact we get

$$2Z = Z + Z > X + Y = p^{lp-1}n^p \geq p^{2p-1}n^p > (p+1)^p \tag{4.57}$$

and hence $Z > \frac{(p+1)^p}{2}$.

This proves Case 2.

- Case 3: $p \nmid XYZ$.

Since $X^p + Y^p = Z^p$ and p is odd we have $X^p + Y^p + (-Z)^p = 0$. Moreover, by assumption $p \nmid (-Z)$. So, applying Lemma 4.2.2 (ii) with

$$x := X, \qquad y := Y, \qquad z := -Z \tag{4.58}$$

we have

$$X + Y = \alpha^p, \quad (X^p + Y^p)(X + Y)^{-1} = (\alpha')^p, \quad Z = \alpha\alpha' \tag{4.59}$$

for some $\alpha, \alpha' \in \mathbb{Z}_{>0}$.

Since $X^p + Y^p = Z^p$ and p is odd, we have $Z^p + (-X)^p + (-Y)^p = 0$. Moreover, by assumption $p \nmid (-Y)$.So, applying again Lemma 4.2.2 (ii) with

$$x := Z, \qquad y := -X, \qquad z := -Y \tag{4.60}$$

we get

$$Z - X = \beta^p, \quad (Z^p + (-X)^p)(Z + (-X))^{-1} = (\beta')^p, \quad Y = \beta\beta', \tag{4.61}$$

for some $\beta, \beta' \in \mathbb{Z}_{>0}$.

Since $X^p + Y^p = Z^p$ and p is odd, we have $Z^p + (-Y)^p + (-X)^p = 0$. Moreover, by assumption $p \nmid (-Z)$.So, applying again Lemma 4.2.2 (ii) with

$$x := Z, \qquad y := -Y, \qquad z := -X \tag{4.62}$$

we get

$$Z - Y = \gamma^p, \quad (Z^p + (-Y)^p)(Z + (-Y))^{-1} = (\gamma')^p, \quad X = \gamma\gamma', \tag{4.63}$$

for some $\gamma, \gamma' \in \mathbb{Z}_{>0}$.

Since $X^p + Y^p = Z^p$ we get

$$(Z - X - Y)^p \equiv Z^p - X^p - Y^p = 0 \pmod{p} \tag{4.64}$$

from which we conclude that $p \mid (Z - X - Y)$. Therefore,

$$(\beta + \gamma - \alpha)^p \equiv \beta^p + \gamma^p - \alpha^p = (Z - X) + (Z - Y) - (X + Y) \tag{4.65}$$

$$= 2(Z - X - Y) \equiv 0 \pmod{p} \tag{4.66}$$

and hence $p \mid (\beta + \gamma - \alpha)$.

Claim 5. We have $\alpha \geq p + 1$.

Suppose that $\alpha \leq p$. Since

$$(2X + Y)^p > X^p + Y^p = Z^p \quad \text{and} \quad (X + 2Y)^p > X^p + Y^p = Z^p, \tag{4.67}$$

it follows that

$$2X + Y > Z \quad \text{and} \quad X + 2Y > Z. \tag{4.68}$$

Then we get

$$X + Y > Z - X \quad \text{and} \quad X + Y > Z - Y \tag{4.69}$$

from which we conclude that

$$\alpha^p > \beta^p \quad \text{and} \quad \alpha^p > \gamma^p. \tag{4.70}$$

Hence

$$\alpha > \beta \quad \text{and} \quad \alpha > \gamma. \tag{4.71}$$

Therefore,

$$-p \leq -\alpha < \beta + \gamma - \alpha < \alpha + \alpha - \alpha \leq p. \tag{4.72}$$

Since $p \mid (\beta + \gamma - \alpha)$ we must have $\beta + \gamma - \alpha = 0$.

Claim 6. Exactly one of the numbers α, β and γ must be even.

First of all, the equality $\beta + \gamma = \alpha$ shows that at least one of the numbers α, β and γ must be even. Assume, on the contrary that, that at least two of them are even. Since $\beta + \gamma = \alpha$ we conclude that all of them must be even.

Recall $X + Y = \alpha^p$ and $X^p + Y^p = Z^p$.

Since $(X + Y) \mid (X^p + Y^p)$ and $2 \mid \alpha$ it follows that $2 \mid \alpha^p$. Also, $\alpha^p \mid Z^p$ and hence $2 \mid Z$. So, Z is even.

Since Z and β are even it follows from the equality $Z - X = \beta^p$ that X is also even.

Since Z and γ are even it follows from the equality $Z - Y = \gamma^p$ that Y is also even.

It contradicts because the assumption.

Now, suppose that α is even. Since, $\alpha = \beta + \gamma$ we get

$$(\beta^p + \gamma^p)(\beta + \gamma)^{-1} = (\beta^p + \gamma^p)\alpha^{-1} \tag{4.73}$$

$$= (Z - X + Z - Y)\alpha^{-1} \tag{4.74}$$

$$= (2Z - X - Y)\alpha^{-1} \tag{4.75}$$

$$= (2\alpha\alpha' - \alpha^p)\alpha^{-1} \tag{4.76}$$

$$= 2\alpha' - \alpha^{p-1} \tag{4.77}$$

from which it follows that $(\beta^p + \gamma^p)(\beta + \alpha)^{-1}$ is even.

On the other hand, we have

$$(\beta^p + \gamma^p)(\beta + \alpha)^{-1} = \sum_{j=0}^{p-1} (-1)^j \beta^{p-j-1}\gamma^j. \tag{4.78}$$

Since each term $\beta^{p-j-1}\gamma^j$ in the above sum is odd we see that $(\beta^p + \gamma^p)(\beta + \alpha)^{-1}$ is also odd. This is a contradiction.

Suppose that β is even, since $\alpha = \beta + \gamma$ we get

$$(\alpha^p - \gamma^p)(\alpha - \gamma)^{-1} = (\alpha^p - \gamma^p)\beta^{-1} \tag{4.79}$$

$$= [(X + Y) - (Z - Y)]\,\beta^{-1} \tag{4.80}$$

$$= (2Y + X - Z)\beta^{-1} \tag{4.81}$$

$$= (2\beta\beta' - \beta^p)\beta^{-1} \tag{4.82}$$

$$= 2\beta' - \beta^{p-1}, \tag{4.83}$$

from which it follows that $(\alpha^p - \gamma^p)(\alpha - \gamma)^{-1}$ is also even.

On the other hand, we have

$$(\alpha^p - \gamma^p)(\alpha - \gamma)^{-1} = \sum_{j=0}^{p-1} \alpha^{p-j-1}\gamma^j. \tag{4.84}$$

Since each term $\alpha^{p-j-1}\gamma^j$ in the above sum is odd we see that $(\alpha^p - \gamma^p)(\alpha - \gamma)^{-1}$ is also odd. This is a contradiction.

Finally suppose that γ is even, since $\alpha = \beta + \gamma$ we get

$$\begin{aligned}(\alpha^p - \beta^p)(\alpha - \beta)^{-1} &= (\alpha^p - \beta^p)\gamma^{-1} && (4.85)\\ &= [(X + Y) - (Z - X)]\gamma^{-1} && (4.86)\\ &= (2X + Y - Z)\gamma^{-1} && (4.87)\\ &= (2\gamma\gamma' - \gamma^p)\gamma^{-1} && (4.88)\\ &= 2\gamma' - \gamma^{p-1}, && (4.89)\end{aligned}$$

from which it follows that $(\alpha^p - \beta^p)(\alpha - \beta)^{-1}$ is also even.

On the other hand, we have

$$(\alpha^p - \beta^p)(\alpha - \beta)^{-1} = \sum_{j=0}^{p-1} \alpha^{p-j-1}\beta^j. \tag{4.90}$$

Since each term $\alpha^{p-j-1}\beta^j$ in the above sum is odd we see that $(\alpha^p - \beta^p)(\alpha - \beta)^{-1}$ is also odd. This is a contradiction.

The proof of Claim 5 is completed.

According to the Claim 5 we get

$$2Z > X + Y = \alpha^p > (p + 1)^p \tag{4.91}$$

from which we have

$$Z > \frac{(p + 1)^p}{2}. \tag{4.92}$$

This proves Case 3.

This proves Lemma 4.2.3. □

Corollary 4.2.3.1. *The Fermat equation*

$$X^p + Y^p = Z^p \tag{4.93}$$

does not have positive integer solutions for any odd prime $p > 1.615 \cdot 10^{14}$.

Proof. We proceed by contradiction. So, suppose that there are positive integers X, Y, Z such that $X^p + Y^p = Z^p$. We may assume, without loss of generality, that $\gcd(X, Y, Z) = 1$. By Lemma 4.2.3 we get

$$Z > \frac{(p+1)^p}{2}. \tag{4.94}$$

Since $X^p + Y^p = Z^p$ and p be an odd number we have $X^p + Y^p + (-Z)^p = 0$. We apply Theorem 4.1.1 with

$$a := X^p, \quad b := Y^p, \quad c := (-Z)^p, \quad \text{and} \quad \epsilon = 1, \tag{4.95}$$

to get

$$\max\{|X|^p, |Y|^p, |(-Z)|^p\} = Z^p \leq 2^{\frac{5}{2}} \max\left\{\exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right), \text{Rad}(X^p Y^p Z^p)^3\right\} \tag{4.96}$$

$$\leq 2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right) \text{Rad}(XYZ)^3 \tag{4.97}$$

$$\leq 2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right) (XYZ)^3 \tag{4.98}$$

$$\leq 2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right) (Z^3)^3 \tag{4.99}$$

from which it follows that

$$Z^{p-9} \leq 2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right). \tag{4.100}$$

Using Lemma 4.2.3 we get

$$\left[\frac{(p+1)^p}{2}\right]^{p-9} < Z^{p-9} \leq 2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right). \tag{4.101}$$

Taking logarithms to the base 2 we get

$$\log_2 \left[\frac{(p+1)^p}{2}\right]^{p-9} = (p-9)[\log_2 (p+1)^p - \log_2 2] = (p-9)[p \log_2 (p+1) - 1], \tag{4.102}$$

and

$$\log_2 \left(2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right)\right) = \frac{5}{2} + \frac{1}{4} \cdot 3.4 \cdot 10^{30} \cdot \log_2 e. \tag{4.103}$$

Then we get

$$(p-9)(p\log_2(p+1)-1) < \frac{5}{2} + \frac{1}{4}\cdot 3.4\cdot 10^{30}\cdot \log_2 e < 1.227\cdot 10^{30}. \quad (4.104)$$

Consider the function

$$f(x) = (x-9)(-1+1.44x\cdot \log(x+1)). \quad (4.105)$$

If we take the derivative of $f(x)$, we get

$$f'(x) = -1+1.44x\cdot\log(x+1)+(x-9)\left(1.44\cdot\log(x+1)+1.44x\cdot\frac{1}{x+1}\right)\geq 0 \quad (4.106)$$

for every real $x \geq 9$.

So, f is monotone increasing for every real $x \geq 9$. Moreover, since $\frac{1}{\log 2} > 1.44$ and $p > 1.615\cdot 10^{14}$ we get

$$(p-9)(-1+p\log_2(p+1)) = (p-9)\left(-1+\frac{1}{\log 2}p\log(p+1)\right) \quad (4.107)$$

$$> (p-9)(-1+1.44p\log(p+1)) \quad (4.108)$$

$$> 1.227\cdot 10^{30}. \quad (4.109)$$

Hence we get

$$1.227\cdot 10^{30} < (p-9)(-1+1.44p\log(p+1)) < 1.227\cdot 10^{30}. \quad (4.110)$$

This is a contradiction. This proves the Corollary 4.2.3.1. □

Corollary 4.2.3.2 (The First Case of Fermat's Last Theorem)**.** *The Fermat equation*

$$X^p + Y^p = Z^p \quad (4.111)$$

does not have solutions $X, Y, Z \in \mathbb{Z}_{>0}$ *for any odd prime* p *such that* $p \nmid XYZ$.

Proof. In [29] it was shown that the first case of Fermat's Last Theorem is true for every odd prime number $p < 7.568\cdot 10^{17}$. Also, by Corollary 4.2.3.1 we know that the first case of Fermat's Last Theorem is true for every odd prime number $p > 1.615\cdot 10^{14}$. Since $7.568\cdot 10^{17} > 1.615\cdot 10^{14}$ we get the first case of Fermat's Last Theorem is true for every odd prime p. This completes the proof. □

In the second case of Fermat's Last Theorem using the very recent estimate due to Mihăilescu (see below), we get a better lower bound then the one given in Corollary 4.2.3.1.

First we have:

Lemma 4.2.4. *Keeping the notation of Lemma 4.2.3. Assume further that* $p \mid XYZ$. *Then*

$$Z > (2p)^{p^2}. \tag{4.112}$$

Proof. See [30]. □

Corollary 4.2.4.1 (The Second Case of Fermat's Last Theorem)**.** *The Fermat equation*

$$X^p + Y^p = Z^p \tag{4.113}$$

does not have solutions $X, Y, Z \in \mathbb{Z}_{>0}$ *for any odd prime* $p > 3.35 \cdot 10^9$ *such that* $p \mid XYZ$.

Proof. We proceed by contradiction. So, suppose that there are $X, Y, Z \in \mathbb{Z}_{>0}$ such that $X^p + Y^p = Z^p$. We may assume, without loss of generality, that $\gcd(X, Y, Z) = 1$. By Lemma 4.2.4 we have

$$Z > (2p)^{p^2}. \tag{4.114}$$

Since $X^p + Y^p = Z^p$ and p be an odd number we have $X^p + Y^p + (-Z)^p = 0$. We apply Theorem 4.1.1 with

$$a := X^p, \quad b := Y^p, \quad c := (-Z)^p \quad \text{and} \quad \epsilon = 1, \tag{4.115}$$

to get

$$\max\{|X|^p, |Y|^p, |(-Z)|^p\} = Z^p \leq 2^{\frac{5}{2}} \max\left\{\exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right), \mathrm{Rad}(X^p Y^p Z^p)^3\right\} \tag{4.116}$$

$$\leq 2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right) \mathrm{Rad}(XYZ)^3 \tag{4.117}$$

$$\leq 2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right) (XYZ)^3 \tag{4.118}$$

$$\leq 2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right) (Z^3)^3 \tag{4.119}$$

from which it follows that

$$Z^{p-9} \leq 2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right). \tag{4.120}$$

Using Lemma 4.2.4 we get

$$\left((2p)^{p^2}\right)^{p-9} < Z^{p-9} \leq 2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right). \tag{4.121}$$

Taking logarithms to the base 2 we get

- $\log_2 \left((2p)^{p^2}\right)^{p-9} = (p-9)p^2 \log_2 (2p)$,
- $\log_2 (2^{\frac{5}{2}} \exp\left(\frac{1}{4} \cdot 3.4 \cdot 10^{30}\right)) = \frac{5}{2} + \frac{1}{4} \cdot 3.4 \cdot 10^{30} \cdot \log_2 e$.

Then we get

$$(p-9)p^2 \log_2 (2p) < \frac{5}{2} + \frac{1}{4} \cdot 3.4 \cdot 10^{30} \cdot \log_2 e < 1.227 \cdot 10^{30}. \tag{4.122}$$

Consider the function

$$f(x) = (x-9)x^2 \log_2 (2x) \tag{4.123}$$

whose derivative is

$$f'(x) = 3x(x-6) \log_2 (2x) + x(x-9)\frac{1}{2} \log_2 e \geq 0 \tag{4.124}$$

for every real $x \geq 9$.

So, f is monotone increasing for every real $x \geq 9$. Moreover, since $\frac{1}{\log 2} > 1.44$ and $p > 3.35 \cdot 10^9$ we get

$$(p-9)p^2 \log_2 (2p) > 1.227 \cdot 10^{30}. \tag{4.125}$$

Hence we get

$$1.227 \cdot 10^{30} < (p-9)p^2 \log_2 (2p) < 1.227 \cdot 10^{30}. \tag{4.126}$$

This is a contradiction. This completes the proof. □

Finally, we consider an application of Theorem 4.1.2 to the generalized Fermat's Last Theorem.

Corollary 4.2.4.2 (A Generalized Fermat's Last Theorem)**.** *Let* $A, B, C \in \mathbb{Z} - \{0\}$ *be such*

that

$$\gcd(A,\, B) = \gcd(B,\, C) = \gcd(A,\, C) = 1. \tag{4.127}$$

Let $r, s, t \in \mathbb{Z}_{>0}$ *such that*

$$\min\{r, s, t\} > \max\{2.453 \cdot 10^{30},\, \log_2 |ABC|,\, 10 + 5\log_2 \mathrm{Rad}(ABC)\}. \tag{4.128}$$

Then the generalized Fermat equation

$$AX^r + BY^s + CZ^t = 0 \tag{4.129}$$

does not have any co-prime $X, Y, Z \in \mathbb{Z}$ *with* $|XYZ| \geq 2$.

Proof. We proceed by contradiction. So, assume, on the contrary, that there are integers X, Y, Z with $|XYZ| \geq 2$ such that

$$\gcd(X,\, Y,\, Z) = 1 \quad \text{and} \quad AX^r + BY^s + CZ^t = 0. \tag{4.130}$$

Claim: We have $\gcd(AX^r,\, BY^s,\, CZ^t) = 1$.

Assume, on the contrary, that $\gcd(AX^r,\, BY^s,\, CZ^t) \neq 1$. Hence there is a prime number p such that $p \mid AX^r, p \mid BY^s$ and $p \mid CZ^t$. Let $P = \{X, Y, Z\}$ and Q a subset of P consisting of those elements of P which are divisible by p. Since, by assumption, $\gcd(X,\, Y,\, Z) = 1$, we conclude that the number of elements of Q must be at most 2. Next, observe that $Q \neq \emptyset$. Suppose, on the contrary, that Q is the empty set. Then

(i) $p \nmid X$ and $p \mid AX^r$ implies $p \mid A$.

(ii) $p \nmid Y$ and $p \mid BY^s$ implies $p \mid B$.

(iii) $p \nmid Z$ and $p \mid CZ^t$ implies $p \mid C$.

This is a contradiction since we assumed that the integers $A, B, C \in \mathbb{Z}$ are pairwise relatively prime. Therefore, $Q \neq \emptyset$. Next, note that the number of elements of Q can not be 1. Assume, on the contrary, that the cardinality of Q is 1. We may suppose, without loss of generality, that $Q = \{Y\}$. Then

(i) $p \nmid X$ and $p \mid AX^r$ implies $p \mid A$.

(ii) $p \nmid Z$ and $p \mid CZ^t$ implies $p \mid C$.

It contradicts since the assumption that $\gcd(A, C) = 1$. As a result, we conclude that the cardinality of Q must be 2. We may suppose, without loss of generality, that $Q = \{X, Z\}$. Put $k := \min\{r, s, t\}$. Then we conclude that $p^k \mid AX^r$ and $p^k \mid CZ^t$. Hence $p^k \mid (AX^r + CZ^t)$. Since $AX^r + CZ^t = -BY^s$, it follows that $p^k \mid (-BY^s)$. Since $Y \notin Q$ we conclude that $p \mid B$. Therefore

$$\log_2 |ABC| \geq \log_2 |B| \geq \log_2 p^k = k \log_2 p \geq k \tag{4.131}$$

which contradicts. This proves the **Claim**.

We apply Theorem 4.1.2 with

$$a := AX^r, \quad b := BY^s, \quad c := CZ^t \quad \text{and} \quad \epsilon = 1 \tag{4.132}$$

then we get

$$|ABC| \cdot |XYZ|^k \leq |ABC||X^rY^sZ^t| \tag{4.133}$$

$$= |AX^rBY^sCZ^t| \tag{4.134}$$

$$\leq 2^4 \max\left\{\exp(1.7 \cdot 10^{30}), \operatorname{Rad}\left(AX^rBY^sCZ^t\right)^6\right\} \tag{4.135}$$

$$= 2^4 \max\left\{\exp(1.7 \cdot 10^{30}), \operatorname{Rad}\left(ABCXYZ\right)^6\right\}. \tag{4.136}$$

Recall that

$$k > 10 + 5 \log_2 \operatorname{Rad}(ABC) = 4 + (6-1) \log_2 \operatorname{Rad}(ABC) + 6 \tag{4.137}$$

$$\Leftrightarrow k - 6 > 4 + (6-1) \log_2 \operatorname{Rad}(ABC) > 0 \tag{4.138}$$

$$\Leftrightarrow 2^{k-6} > 2^{4+(6-1)\log_2 \operatorname{Rad}(ABC)} = 2^4 2^{\log_2 \operatorname{Rad}(ABC)^5} = 2^4 \operatorname{Rad}(ABC)^5. \tag{4.139}$$

Also, recall that $|XYZ| \geq 2$. Now, we have

$$|ABC|.|XYZ|^k \geq \operatorname{Rad}(ABC)|XYZ|^{k-6}|XYZ|^6 \tag{4.140}$$

$$\geq \operatorname{Rad}(ABC)2^{k-6}|XYZ|^6 \tag{4.141}$$

$$> \operatorname{Rad}(ABC)2^4 \operatorname{Rad}(ABC)^5|XYZ|^6 \tag{4.142}$$

$$= 2^4 \operatorname{Rad}(ABC)^6|XYZ|^6 \tag{4.143}$$

$$\geq 2^4 \operatorname{Rad}(ABC)^6 \operatorname{Rad}(XYZ)^6 \tag{4.144}$$

$$\geq 2^4 \operatorname{Rad}(ABCXYZ)^6. \tag{4.145}$$

So, we get

$$2^k \leq |ABC|.|XYZ|^k \leq 2^4 \exp(1.7 \cdot 10^{30}) \tag{4.146}$$

from which it follows that

$$k \leq 2.453 \cdot 10^{30}. \tag{4.147}$$

This is a contradiction. This completes the proof. □

REFERENCES

1. Mochizuki SH. Inter-universal Teichmüller theory I: Constructions of Hodge theaters. *Publ. Res. Inst. Math. Sci.* 2021; 57: 3–207; II: Hodge-Arakelov. Theoretic Evaluation. *Publ. Res. Inst. Math. Sci.* 2021; 57: 209–401; III: Canonical splittings of the log-theta-lattice, *Publ. Res. Inst. Math. Sci.* 2021; 57: 403–626; IV : Log-volume computations and set-theoretic foundations. *Publ. Res. Inst. Math. Sci.* 2021; 57: 627–723.

2. Mochizuki SH, Fesenko I, Hoshi Y, Minamide A, Porowski W. *Explicit estimates in inter-universal Teichmüller theory RIMS Preprint 1*. 1933.

3. Snyder N. An Alternate Proof of Mason's Theorem *Elem. Math. 55*. 2000; 93-94.

4. Sheppard K. The abc-conjecture and its applications. Kansas State University; 2016.

5. Stothers WW. Polynomial identities and Hauptmoduln *Quart. J. Math. Oxford Ser. 2*. 1981; 32(127): 349-370.

6. Mason RC. *Diophantine Equations over Function Fields, London Mathematical Society Lecture Notes Series, vol. 96. Cambridge University Press*. Cambridge; 1984.

7. Mason RC. *Diophantine Equations over Function Fields, London Mathematical Society Lecture Notes Series, vol. 96. Cambridge University Press. In: New Advances in Transcendence Theory.* Cambridge University Press: Cambridge; 1988.

8. Waldschmidt M. Lecture on the abc conjecture and some of its consequences. *Abdus Salam School of Mathematical Sciences (ASSMS), Lahore 6th World Conference on 21st Century Mathematics Universite Pierre et Marie Curie-Paris*. 2013.

9. Oesterle J. Nouvelles approaches du "theoreme" de Fermat. Asterisque. *Seminaire Bourbaki, Vol. 1987/88. no. 161-162, Exp. No. 694*. 1988; 4, 165-186.

10. Masser DW. Open problems. *In: Chen, W.W.L. (ed.) Proceedings of the Symposium on Analytic Number Theory*. Imperial College: London; 1985.

11. Granville A. Tucker T. J. It's as easy as abc, *Notices Amer. Math. Soc. 49*. 2002; 1224–1231.

12. Stewart C. L. Tijdeman R. On the Oesterl´e–Masser conjecture. *Monatsh. Math. 102* 1986 ;251–257.

13. Baker A. Experiments on the abc-conjecture. *Publ. Math. Debrecen*. 2004; 65(3-4):253-260.

14. Laishram S, Shorey TN. Baker's explicit abc-conjecture and applications. *Acta Arith.* 2012; 155(4): 419-429.

15. Edwards HM. *A Genetic Introduction to Algebraic Number Theorey*. Springer: Verlag ; 1977.

16. Wiles A. Modular elliptic curves and Fermat's Last Theorem *Annals of Mathematics*. 1995; 141: 443-551.

17. Granville A. Powerful Numbers and Fermat's Last Theorem. *C. R. Math. Acad. Sci. Canada*. 1986; 8: 215-218.

18. Wieferich A. Zum Letzten Fermat' Schen Theorem. *J. Reine Angew. Math.* 1909; 136 : 293-302.

19. Silverman JH. Wieferich's Criterion and the abc-conjecture. *J. Number Theory 30.* 1988; No.2, 226-237.

20. Pei-Chu Hu, Chung-Chun Yang. *Distribution Theory of Algebraic Numbers, de Gruyter Expositions in Mathematics*; 2000.

21. Nitaj A. The abc-Conjecture [cited 2021 24 July] Avaliable from: https://ni-taj.users.lmno.cnrs.fr/abc.html

22. Nitaj A. La conjecture abc. The abc conjecture. *Enseign. Math.II. Ser. 42.* 1996; No.1-2, 3-24.

23. Schmidt W. M. *Diophantine approximations and diophantine equations.* Springer: Verlag; 1991.

24. Elkies N.D. abc *implies Mordell. Int. Math. Res. Not.* 1991; No.7, 99-109.

25. Bombieri E. Roth's theorem and the abc-conjecture. 1994; preprint.

26. Cochrane T. Dressler M. Robert E. Gaps between integers with the same prime factors. *Math. Comput. 68*, 1999; No.225, 395-401.

27. Walsh P. G. On a conjecture of Schinzel and Tijdeman. Gyoery, Kalman (ed.) et al., *Number theory in progress Proceedings of the international conference organized by the Stefan Banach International Mathematical Center in honor of the 60th birthday of Andrzej Schinzel, Zakopane, Poland, Volume 1: Diophantine problems and polynomials.* 1999; 577-582.

28. Szpiro L. *Discriminant et conducteur des courbes elliptiques, Astérisque.*1990.

29. Coppersmith D. Fermat's Last Theorem (Case 1) and Wieferich Criterion. *Math. Comp. 54.* 1990; 895-902.

30. Mihăilescu P. Improved lower bounds for possible solutions in the Second Case of the Fermat Last Theorem and in the Catalan Equation, *J. Number Theory 225* 2021 ; 151-173.