INVESTIGATIONS ON SOME EXPONENTIAL CONGRUENCES

ARNAB BOSE
Master of Science, The University of Texas-Pan American, 2007

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

MASTER OF SCIENCE

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

INVESTIGATIONS ON SOME EXPONENTIAL CONGRUENCES

ARNAB BOSE

Date of Defense: June 10, 2016

Dr. Amir Akbary-Majdabadno Supervisor	Professor	Ph.D.
Dr. Habiba Kadiri Committee Member	Assistant Professor	Ph.D.
Dr. Pascal Ghazalian Committee Member	Associate Professor	Ph.D.
Dr. Hadi Kharaghani Chair, Thesis Examination Committee	Professor	Ph.D.

Abstract

Selfridge asked for what positive integers a and b with $a > b$, does $2^a - 2^b$ divide $n^a - n^b$ for all $n \in \mathbb{N}$. The problem was solved by various people who showed that the above problem is true only for $(a,b) \in S$, where $S =$

$$\big\{(2,1),(3,1),(4,2),(5,1),(5,3),(6,2),(7,3),(8,2),(8,4),(9,3),(14,2),(15,3),(16,4)\big\}.$$

In this thesis, we prove two generalizations of the above problem.

Theorem. *For a fixed positive integer m, $n^a - n^b \equiv 0 \pmod{m^a - m^b}$ has a solution in $(a,b) \in \mathbb{N}^2$ with $a > b$, for all integers $n > m$ if and only if $m = 2$ and $(a,b) \in S$, where S is as given above.*

Zaharescu and Vâjâitu considered a generalization of Selfridge's problem in algebraic number fields. Our second result makes their theorem explicit and provides explicit bounds for the solutions.

Next, we give a conditional resolution to a problem proposed by Ruderman which is related to Selfridge's problem and also investigate some generalizations.

Lastly, we use a particular case of the Schmidt Subspace Theorem and generalize a result proved by Bugeaud, Corvaja and Zannier [2].

Acknowledgments

A number of individuals should be acknowledged for their contributions to any academic success I have achieved during my two years at University of Lethbridge.

Firstly, my supervisor Prof. Amir Akbary is to be praised for his unending support and encouragement throughout the course of this thesis work. I sincerely thank Prof. Habiba Kadiri and Prof. Pascal Ghazalian for being a part of my thesis committee. A special mention should be made of Prof. Hadi Kharaghani for serving as Chair of my committee.

I will take this opportunity to thank some of the other people I came to know during my stay in Lethbridge. I thank Ram Dahal and Jayati Law for their support and friendship. My heartfelt gratitude goes to Allysa Lumley, Jeff Bleaney, Jim Parks, Adam Felix, Farzad Aryan, Sara Sasani, Forrest Francis, Sahar Siavashi, Dakota Duffy, Umair Arif, Mark Thom, Alia Hamieh, Manoj Kumar, to name a few.

My family deserves special mention for their continual support and love - my parents, my brother, and other extended family members. Also, I will take this chance to thank my in-laws, mainly for their daughter, but also for their encouragement and assistance. Lastly, my wife, Julia, is to be recognized for her unceasing love and support all along. My world is much more beautiful with her in it.

Contents

Contents **v**

1 Introduction **1**
1.1 A Problem of Selfridge 1
1.2 Ruderman's Problem 5
1.3 A generalization of the gcd bound 9
1.3.1 Notation and Definitions 9
1.3.2 The Schmidt Subspace Theorem 10

2 Generalizations of a Problem of Selfridge **12**
2.1 A Generalization 13
2.2 A Second Generalization 18
2.2.1 Notation 20
2.2.2 The Main Result 22
2.2.3 A Lower Bound for $\left|\mathrm{N}\left(\sum_{i=1}^{k}\alpha_i\beta^{a_i}\right)\right|$ 23
2.2.4 An Upper Bound for $\mathrm{N}(\mathcal{J})$ 24
2.2.5 Proof of Theorem 2.10 32
2.3 Applications 32
2.3.1 Problem 1.4 revisited 32
2.3.2 A Selfridge-type problem with $\mathcal{K}=\mathbb{Q}[i]$ 33

3 A Problem of Ruderman and some generalizations **35**
3.1 Conditional Resolution of Ruderman's Problem 35
3.2 A Generalization of Ruderman's Problem 39
3.3 The gcd bound via the *ABC*-Conjecture 42
3.4 A two dimensional version of Theorem 3.5 46

4 An application of the Schmidt Subspace Theorem **48**
4.1 Proof of the gcd Theorem 49
4.2 Proof of Lemma 4.5 53
4.3 A more general version of Theorem 3.4 55

Bibliography **57**

A Tables **59**

Chapter 1

Introduction

1.1 A Problem of Selfridge

Selfridge observed that 2^2-2 divides n^2-n, $2^{2^2}-2^2$ divides $n^{2^2}-n^2$, and $2^{2^{2^2}}-2^{2^2}$ divides $n^{2^{2^2}}-n^{2^2}$ for all $n \in \mathbb{N}$ and proposed the following problem.

Problem 1.1. *Find all positive integers a and b with $a > b$ such that $2^a - 2^b$ divide $n^a - n^b$ for all $n \in \mathbb{N}$.*

The above problem was first mentioned in the book "Unsolved Problems in Number Theory" by Richard Guy [4, page 57]. The problem was resolved by many people in different times, either in this context or while investigating some other related problems. In 1976, W. Velez observed in [10], that Problem 1.1 is true only for the pairs $(a,b) \in S$, where $S =$

$$\big\{(2,1),(3,1),(4,2),(5,1),(5,3),(6,2),(7,3),(8,2),(8,4),(9,3),(14,2),(15,3),(16,4)\big\}. \tag{1.1}$$

In fact, he proved the following characterization for the solutions (a,b) satisfying the condition of Problem 1.1.

Proposition 1.2 (Velez). *Write $c = a-b$. Let $c \geq 2$ and $2^c - 1 = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$, where p_i's are distinct primes with $e_i \geq 1$. Write $c = 2^k t$, where t is odd. Then $(2^a - 2^b) | (n^a - n^b)$ for all $n \in \mathbb{N}$ if and only if*

1. *$\phi(p_i^{e_i}) | c$, where ϕ is the Euler totient function.*

2. $e_i \leq b \leq k+2$.

In 1977, "The Mod Set Stanford University" and Carl Pomerance in [9] independently solved Problem 1.1. Their proof was based on Proposition 1.2 and a result by Schinzel [12, Lemma 3] where he showed that if $c \neq 1,2,4,6,12$, then $2^c - 1$ has a prime factor $\geq 2c+1$.

Unaware of these developments, in 1985, Qi Sun and Ming Zhi Zhang proved in [15] that Problem 1.1 is true only when $(a,b) \in S$. Their characterization for the solutions (a,b) was also identical to Proposition 1.2.

A natural generalization of Problem 1.1 is the following.

Problem 1.3. *For a fixed positive integer m, find all solutions $(a,b) \in \mathbb{N}^2$ with $a > b$ such that*

$$n^a - n^b \equiv 0 \pmod{m^a - m^b} \tag{1.2}$$

for all integers $n > m$.

Here we settle this problem by considering the following cases

(a) m is an even integer ≥ 4.

(b) m is an odd integer ≥ 3.

Our first result gives a complete solution to Problem 1.3. We have the following theorem.

Theorem 2.2. *For a fixed positive integer m, the congruence $n^a - n^b \equiv 0 \pmod{m^a - m^b}$ has a solution in $(a,b) \in \mathbb{N}^2$ with $a > b$, for all integers $n > m$ if and only if $m = 2$ and $(a,b) \in S$, where S is the set given in (1.1).*

One should note that Theorem 2.2 cannot be derived as a consequence of Schinzel's result (see Remark 2.3 in Chapter 2).

It is an easy exercise that Problem 1.1 can be equivalently stated as the following (see Proposition 2.7 in Chapter 2 for an explanation).

Problem 1.4. *Find all positive integers a and b with $a > b$ such that $2^a - 2^b$ divides $z^a - z^b$ for all $z \in \mathbb{Z}$.*

The above formulation paves a way to a natural generalization of Problem 1.1 in algebraic number fields. Recall that an algebraic number field $\mathcal{K}$ is a finite extension of $\mathbb{Q}$. We denote the integral closure of $\mathbb{Z}$ in $\mathcal{K}$ by $\mathcal{A}$, and $\mathcal{A}$ is called the ring of integers of $\mathcal{K}$. A. Zaharescu and M. Vâjâitu considered such a generalization in [16]. The problem they consider can be stated as follows.

Problem 1.5. *Let $\mathcal{A}$ be the ring of integers in an algebraic number field $\mathcal{K}$ and let $\alpha_1, \alpha_2, \cdots, \alpha_k$ and β be nonzero elements of $\mathcal{A}$, where β is not a unit. Then find all k-tuples $(a_1, a_2, \cdots, a_k) \in \mathbb{N}^k$ such that*

$$\sum_{i=1}^{k} \alpha_i \beta^{a_i} \quad \textit{divides} \quad \sum_{i=1}^{k} \alpha_i z^{a_i} \tag{1.3}$$

for any $z \in \mathcal{A}$, and

$$\sum_{i \in S} \alpha_i \beta^{a_i} \neq 0 \quad \textit{for any} \quad S \subseteq \{1, 2, ..., k\}. \tag{1.4}$$

Zaharescu and Vâjâitu proved that there are only finitely many k-tuples $(a_1, a_2, \cdots, a_k) \in \mathbb{N}^k$ satisfying (1.3) and (1.4), thereby showing that the finiteness result for Problem 1.1 is a special case of a more general situation. Here, we prove an explicit version of their theorem and provide bounds for the a_i's. First let us understand why we need some of the constraints that we have introduced in Problem 1.5. We observe that if β is a unit and $k = 1$, then (1.3) is true for all a_1. Therefore, to establish a non-trivial result we need to assume that β is not a unit. Moreover, to avoid other trivial solutions we need to assume (1.4). For example, if $\mathcal{A} = \mathbb{Z}$, $k = 3$, and $\alpha_1 = 1, \alpha_2 = 1$ and $\alpha_3 = -\beta$, then we have infinitely many solutions of the form $a_1 = n, a_2 = 0$ and $a_3 = n - 1$. A similar situation occurs in Problem 1.4 also, when $a = b$. Hence, to avoid these situations, we will consider only those solutions to (1.3) that also satisfy (1.4). Before we state our theorem, we will mention two lemmas which provides the necessary machinery to understand our result. The proofs of the following two lemmas are given in Chapter 2.

Lemma 2.7. *For a fixed positive integer k, the function* $f(x) = \frac{x^k}{(x-1)^{k-1}} - x$ *is bounded on* $[2,\infty]$.

Also, we have the following.

Lemma 2.8. *Let* $\alpha_1,\alpha_2,\cdots,\alpha_k$ *and* β *be nonzero complex numbers with* $|\beta| \neq 1$. *Then there exists a constant* $c = c(\alpha_1,\alpha_2,\cdots,\alpha_k,\beta) > 0$ *such that for any* $(a_1,a_2,\cdots,a_k) \in \mathbb{N}^k$ *satisfying* (1.4) *we have*

$$\left|\sum_{i=1}^{k} \alpha_i \beta^{a_i}\right| \geq c \max\left\{|\beta|^{a_1}, |\beta|^{a_2}, \cdots, |\beta|^{a_k}\right\}. \tag{1.5}$$

Our second result provides an explicit version of the theorem of Zaharescu and Vâjâitu. We denote $\mathrm{Norm}_{\mathcal{K}/\mathbb{Q}}(\cdot)$ by $\mathrm{N}(\cdot)$. Then we have the following theorem.

Theorem 2.9. *Assume the conditions of Problem 1.5. If* $(a_1,a_2,\cdots,a_k) \in \mathbb{N}^k$ *with* $a_1 > a_2 > \cdots > a_k$ *satisfy* (1.3) *and* (1.4)*, then we have*

$$\begin{aligned} a \leq \frac{1}{\log|N(\beta)|}\Bigg\{ & [\mathcal{K}:\mathbb{Q}]M\log 2 + (2^{k-1}+2M)\log|N(\alpha_1)| \\ & + M(k-1)[\mathcal{K}:\mathbb{Q}]a^{\frac{0.5414+1.06599(k-1)}{\log\log a}} + (2^{k-1}+M)(k-1)[\mathcal{K}:\mathbb{Q}]a^{\frac{0.5414}{\log\log a}} - \log c\Bigg\}, \end{aligned} \tag{1.6}$$

where $a = \max(a_1,3)$*, M is a positive integer such that* $f(x) < M$ *for* $x \geq 2$*, where* $f(x)$ *is given in Lemma 2.7, and* $c = \prod_{\sigma} c\big(\sigma(\alpha_1),\cdots,\sigma(\alpha_k),\sigma(\beta)\big)$*, where* σ *varies over all embeddings of* $\mathcal{K}$ *and* $c\big(\sigma(\alpha_1),\cdots,\sigma(\alpha_k),\sigma(\beta)\big)$ *is the constant derived from the application of Lemma 2.8 on* $\sigma(\alpha_1),\cdots,\sigma(\alpha_k)$*, and* $\sigma(\beta)$.

We prove Theorem 2.9 by finding constants d_1,d_2,d_3,d_4 such that

$$d_1 e^{d_2 \log a} \leq \mathrm{N}(\mathcal{J}) \leq d_3 e^{d_4 \frac{\log a}{\log\log a}}, \tag{1.7}$$

where $\mathcal{J}$ is the ideal of $\mathcal{A}$ generated by $\left\{ \sum_{i=1}^{k} \alpha_i z^{a_i} : z \in \mathcal{A} \right\}$. Observe that there are only finitely many a's that could satisfy (1.7).

In continuation we illustrate the usefulness of our Theorem 2.9, by providing two applications of it. Firstly, we give a concise alternative solution to Problem 1.1 using Theorem 2.9. As a second application, we obtain bounds for the solutions (a,b) for a Selfridge-type problem for the Gaussian integers $\mathcal{K} = \mathbb{Q}[i]$.

1.2 Ruderman's Problem

In 1974, Harry Ruderman [10] proposed the following as Problem E2468 in the problems section of the American Mathematical Monthly.

Problem 1.6. *If $a > b \geq 0$ are integers such that $(2^a - 2^b) | (3^a - 3^b)$, then $(2^a - 2^b) | (x^a - x^b)$ for all $x \in \mathbb{N}$.*

The problem is still unsolved to this day, but there has been some progress towards answering it. In fact, the remarks by Velez and Pomerance mentioned in the previous section, were primarily directed to provide some insight to Problem 1.6. In 2011, M. Ram Murty and V. Kumar Murty [6] proved the following theorem.

Theorem 1.7 (**Murty-Murty**). *There is a finite set S' such that $(2^a - 2^b) | (3^a - 3^b)$ for $a > b \geq 0$ if and only if $(a,b) \in S'$.*

Note that $S \cup \{(1,0)\} \subset S'$. In Chapter 3 we show the following.

Proposition 3.6. *Problem 1.6 is true if and only if $S' = S \cup \{(1,0)\}$.*

The above observations imply that if S' contains the same fourteen pairs as in $S \cup \{(1,0)\}$, then Problem 1.6 is true. But that is precisely where we hit a hurdle, since the proof of Theorem 1.7 is ineffective in the sense that it does not provide a way of computing the bounds for a and b. Thus, we cannot explicitly descibe the set S'. This is due to the application of the following ineffective theorem [2, Theorem 1] in the proof of Theorem 1.7.

Theorem 1.8 (**Bugeaud-Corvaja-Zannier**). *Let m and n be multiplicatively independent integers ≥ 2 with $m < n$. Then for $\varepsilon > 0$, we have*

$$\gcd(m^k - 1, n^k - 1) \ll m^{\varepsilon k}, \tag{1.8}$$

where the implied ineffective constant depends on ε.

Therefore, it is evident that in order to have an effective proof of Theorem 1.7, we need to come up with an effective version of (1.8) first. By fixing $\varepsilon = 0.74$ and looking at the values of $\frac{\gcd(2^k-1,3^k-1)}{2^{0.74k}}$ for $1 \leq k \leq 10^4$, we come up with the following conjecture.

Conjecture 1.9. For all $k \in \mathbb{N}$, we have

$$\gcd(2^k - 1, 3^k - 1) < 2^{0.74k}. \tag{1.9}$$

Our next result provides an effective proof of Theorem 1.7, assuming Conjecture 1.9. This enables us to compute the bounds for a and b. Next, we use these bounds to check which pairs (a,b) satisfy the condition $(2^a - 2^b) \big| (3^a - 3^b)$. Performing this we get the exact same fourteen pairs as given in $S \cup \{(1,0)\}$. In fact, we have the following theorem.

Theorem 3.8. *Conjecture 1.9 implies that Problem 1.6 is true.*

In order to prove a generalized version of Theorem 1.7 for bases $p-1$ and p (p prime) instead of 2 and 3, we need to have an effective version of Theorem 1.8 first. We turn to computations again. Fixing $\varepsilon = 0.74$ as before, but this time, we look at the values of $\frac{\gcd(m^k-1,(m+1)^k-1)}{m^{0.74k}}$ for $1 \leq k \leq 10^4$ and $m \in \mathbb{N}$ with $3 \leq m \leq 1000$. We propose the following conjecture.

Conjecture 1.10. For all $k, m \in \mathbb{N}$ with $m \geq 2$, we have

$$\gcd(m^k - 1, (m+1)^k - 1) < m^{0.74k}. \tag{1.10}$$

By employing Conjecture 1.10, we next give a generalization of Theorem 1.7.

Theorem 3.11. *Under the assumption of Conjecture 1.10, there is an effectively computable constant C such that if $b > C$, then $\left((p-1)^a - (p-1)^b\right) \nmid (p^a - p^b)$, where $(a,b) \in \mathbb{N} \times \mathbb{N} \cup \{0\}$ with $a > b$.*

In other words, all the finite number of pairs (a,b) satisfying $\left((p-1)^a-(p-1)^b\right)\big|(p^a-p^b)$ can be computed explicitly. In view of Theorem 3.11, we propose and investigate the following Ruderman-type problem for primes.

Problem 1.11. *For $p \neq 5$, if $a > b \geq 0$ are integers such that $\left((p-1)^a-(p-1)^b\right)\big|(p^a-p^b)$, then $\left((p-1)^a-(p-1)^b\right)\big|(x^a-x^b)$ for all $x \geq p$.*

Let us see why the condition $p \neq 5$ is needed. For $p = 5$, we observe that the pair $(a,b) = (3,1)$ satisfies the first divisibility condition in Problem 1.11. However, it does not satisfy the second condition even for the first choice of $x = 6$.

The case of $p = 3$ corresponds to the original problem of Ruderman (Problem 1.6) which we proved to be true, under the assumption of Conjecture 1.9. Moreover, by Theorem 2.2, we can say that the second divisibility condition has no solutions in (a,b) except when $p-1 = 2$, that is, when $p = 3$. Based on computations with the bounds for a and b derived from Theorem 3.11, we conclude that no pairs (a,b) will satisfy the first divisibility condition in Problem 1.11 for the primes $7 \leq p \leq 200$. This brings us to the conclusion that if Conjecture 1.10 holds, then for $7 \leq p \leq 200$, Problem 1.11 is trivially true, since no pair (a,b) satisfies both the divisibility conditions.

In continuation, we introduce the celebrated *ABC*-Conjecture and investigate how an explicit version of the conjecture due to A. Baker in [1] and Theorem 1 in [5] leads to an explicit upper bound for $\gcd(m^k-1,(m+1)^k-1)$.

We then concern ourselves with a possible generalization of Problem 1.6 in two dimensions. We start with a natural generalization of the problem of Selfridge (Problem 1.1) in two dimensions.

Problem 1.12. *Find all positive integers* $(t,u),(v,w) \in \mathbb{N}^2$ *with* $t > u$ *and* $v > w$ *such that* $(2^t - 2^u)(2^v - 2^w) \big| (x^t - x^u)(x^v - x^w)$ *for all* $x \in \mathbb{N}$.

Therefore, to propose and investigate a two-dimensional analogue of Problem 1.6, we need to establish a version of Theorem 1.7 in two dimensions. Our next result does this partially in a more general setting.

Theorem 3.17. *There is a finite set* S'' *such that for* $m < n$ *with* n *prime and* $\gcd(m,n) = 1$,

$$(m^t - m^u)(m^v - m^w) \big| (n^t - n^u)(n^v - n^w) \tag{1.11}$$

if and only if $(t,u),(v,w) \in S''$, *where* $(t,u),(v,w) \in \mathbb{N} \times \mathbb{N} \cup \{0\}$ *with* $t > u$ *and* $v > w$, *and moreover* $t - u \leq v - w \leq t - u + \ell$ *for a fixed non-negative integer* ℓ.

Theorem 3.17 is proved by using Theorem 1.8 and also Theorem 4.2, which is a generalization of Theorem 1.8. We mention Theorem 4.2 and the idea of its proof in the next section.

We observe that the pairs $(t,u) = (17,5)$ and $(v,w) = (20,2)$ satisfy (1.11) when $m = 2$ and $n = 3$. In fact, lots of such examples for (t,u) and (v,w) can be found which satisfy (1.11) for $m = 2$ and $n = 3$, but none of the pairs satisfy the condition in Problem 1.12 for various values of x (for example, say for $x = 17$). Another such example is when $(t,u) = (13,1)$ and $(v,w) = (24,6)$. Hence, with any of these counterexamples we can conclude that a Ruderman-type problem in the form

$$(2^t - 2^u)(2^v - 2^w) \big| (3^t - 3^u)(3^v - 3^w) \Rightarrow (2^t - 2^u)(2^v - 2^w) \big| (x^t - x^u)(x^v - x^w) \tag{1.12}$$

for all $x \in \mathbb{N}$, is not true in two dimensions.

In [3], A. Zaharescu and G. Choi considered another form of the generalization of Problem 1.1 in two dimensions.

Problem 1.13. *Find all positive integers* $(t,u),(v,w) \in \mathbb{N}^2$ *with* $t > u$ *and* $v > w$ *such that*

$(2^t-2^u)(2^v-2^w)\big|(x^t-x^u)(y^v-y^w)$ *for all* $x,y\in\mathbb{Z}$.

Observe that by choosing $y=2$ in the above problem, we have that (t,u) is a solution to Problem 1.1. Similarly, letting $x=2$ we see that (v,w) is a solution to Problem 1.1. Again, if both (t,u) and (v,w) are solutions of Problem 1.1, then (t,u) and (v,w) satisfy Problem 1.13. Hence, Problem 1.13 has exactly $14^2=196$ solutions in (t,u) and (v,w), since $|S\cup\{(1,0)\}|=14$.

However, with any of the counterexamples mentioned after Theorem 3.17, which satisfy (1.11) when $m=2$ and $n=3$, but are not in $S\cup\{(1,0)\}$, and referring to the above discussion, we can conclude that a Ruderman-type problem in the form

$$(2^t-2^u)(2^v-2^w)\big|(3^t-3^u)(3^v-3^w)\Rightarrow(2^t-2^u)(2^v-2^w)\big|(x^t-x^u)(y^v-y^w) \qquad (1.13)$$

for all $x,y\in\mathbb{Z}$, is also not true in two dimensions.

1.3 A generalization of the gcd bound

One of the main ingredients in the proof of Theorem 1.7 in the previous section is Theorem 1.8 for $m=2$ and $n=3$. We have already pointed out that Theorem 1.8 is a consequence of the Schmidt Subspace Theorem [13, Theorem 1A, page 176]. This theorem is a pioneering work in Diophantine Approximation Theory and has a vast number of applications and consequences. Here, we give an exposition of the Subspace Theorem and our generalization of Theorem 1.8.

1.3.1 Notation and Definitions

Definition 1.14. Let $n\in\mathbb{N}$ and $r\leq n$. We define $L_1=\sum_{j=1}^{n}\alpha_{1j}X_j,\cdots,L_r=\sum_{j=1}^{n}\alpha_{nj}X_j$ to be r linear forms with coefficients in $\mathbb{C}$. We say that $L_1,\cdots,L_r$ are linearly dependent if there exists $c_1,\cdots,c_r\in\mathbb{C}$, not all 0, such that $\sum_{i=1}^{r}c_iL_i=0$. Otherwise, they are called linearly independent. If $r=n$, then $L_1,\cdots,L_n$ are linearly independent if and only if $\det(L_1,\cdots,L_n)=\det(\alpha_{ij})_{1\leq i,j\leq n}\neq 0$.

Definition 1.15. A linear subspace T of $\mathbb{Q}^n$ of dimension r is defined as

$$T = \Big\{ \sum_{i=1}^{r} y_i \mathbf{a}_i : y_i \in \mathbb{Q} \Big\},$$

where $\mathbf{a}_1, \cdots, \mathbf{a}_r$ are linearly independent vectors in $\mathbb{Q}^n$.

Definition 1.16. We define the norm of $\mathbf{x} = (x_1, x_2, \cdots, x_n) \in \mathbb{Z}^n$ to be

$$\|\mathbf{x}\| = \max\big(|x_1|, \cdots, |x_n|\big).$$

1.3.2 The Schmidt Subspace Theorem

We are now ready to state the Schmidt Subspace Theorem [13, Theorem 1A, page 176].

Theorem 1.17 (Schmidt). *Let $n \geq 2$, and let $L_i(\boldsymbol{X}) = \alpha_{i1}X_1 + \alpha_{i2}X_2 + \cdots + \alpha_{in}X_n$ be n linearly independent linear forms with algebraic coefficients in $\mathbb{C}$, where $i = 1, 2, \cdots, n$. Let $\delta > 0$. Then the set of solutions of the inequality*

$$|L_1(\boldsymbol{x}) \cdots L_n(\boldsymbol{x})| \leq \|\boldsymbol{x}\|^{-\delta} \tag{1.14}$$

in $\boldsymbol{x} \in \mathbb{Z}^n$ is contained in a finite union $T_1 \cup T_2 \cup \cdots \cup T_t$ of proper linear subspaces of $\mathbb{Q}^n$.

The proof of Theorem 1.17 is ineffective, in the sense that it does not give a way to determine the subspaces T_i. However, there exists a version of the theorem that provides an explicit upper bound for the number of subspaces t. Nevertheless, Theorem 1.17 has many applications in Diophantine Approximation. Here, we mention one such application. First, we state the celebrated Roth's Theorem.

Theorem 1.18 (Roth). *Let $\alpha \in \mathbb{C}$ be an irrational algebraic number. Then for a given $\delta > 0$, the inequality*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\delta}} \tag{1.15}$$

has finitely many solutions in coprime integers p and q.

One of many well known applications of Theorem 1.17 is that it implies Theorem 1.18.

In Chapter 4, we employ a version of the subspace theorem to prove the following generalization of Theorem 1.8.

Theorem 4.2. *Let $\ell \in \mathbb{N} \cup \{0\}$ be fixed and $\varepsilon > 0$. Then if m and n are fixed multiplicatively independent integers ≥ 2 with $m < n$, and $a \leq b \leq a + \ell$, we have*

$$\gcd(m^a - 1, n^b - 1) < m^{\varepsilon a}, \tag{1.16}$$

for sufficiently large a.

It is not hard to show that (1.16) is equivalent to $d_{a,b} > m^{(1-\varepsilon)a}$, where $d_{a,b}$ is the denominator of $(n^b - 1)/(m^a - 1)$ (See Lemma 4.3). In order to prove Theorem 4.2, we assume that there exists $a \in \mathcal{B}$ and b such that $a \leq b \leq a + \ell$ for which $d_{a,b} \leq m^{(1-\varepsilon)a}$, where $\mathcal{B}$ is an infinite set of natural numbers, and then by an application of the subspace theorem we arrive at a contradiction.

Equipped with Theorem 4.2, we prove a further generalization of Theorem 1.7.

Theorem 4.6. *Let $\ell \in \mathbb{N} \cup \{0\}$ be fixed. If m and n are coprime integers ≥ 2 with n prime, then there are only finitely many pairs $(a,b) \in \mathbb{N}^2$ with $a > b$ such that $m^a - m^b \big| n^{a+\ell} - n^b$.*

The proof of Theorem 4.6 is not effective since it uses Theorem 4.2. However, we have performed some computations to get a flavor of the number of solutions (a,b) to $m^a - m^b \big| n^{a+\ell} - n^b$ for specific values of m, n, ℓ. We have included a table, at the end of Chapter 4, mentioning some values of (m,n) and ℓ and record the solutions (a,b) in each case for $1 \leq b < a \leq 10000$.

Chapter 2

Generalizations of a Problem of Selfridge

We start by mentioning the following problem proposed by Selfridge [4].

Problem 1.1. *Find all positive integers a and b with $a > b$ such that $2^a - 2^b$ divide $n^a - n^b$ for all $n \in \mathbb{N}$.*

In 1976, W. Velez published some remarks in [10], where he speculated that Problem 1.1 is true only for the pairs (a,b) mentioned in Theorem 2.2. In this context he proved Proposition 1.2, which is a characterization for the solutions (a,b) of Problem 1.1.

A year after, "The Mod Set Stanford University" and Carl Pomerance in [9] independently solved the above problem. Their argument were based on the following result proved by Schinzel [12, Lemma 3].

Theorem 2.1 (Schinzel). *If m and n are integers such that* $\gcd(m,n) = 1$ *and mn is either a square or twice a square, then $(m^c - n^c)$ has a prime factor $p \geq 2c+1$, provided one excludes the cases $c = 1,2,4,6,12$ when $m = 2$ and $n = 1$.*

By Proposition 1.2, we observe that any prime divisor p_i of c must satisfy $(p_i - 1)|c$ which gives $p_i \leq c+1$. But by Theorem 2.1 there is some p_i for which this inequality is not satisfied for $c \neq 1,2,4,6,12$. Therefore, the only choices for c are $1,2,4,6,12$.

Apparently unaware of these previous developments, Problem 1.1 was solved by Qi Sun and Ming Zhi Zhang [15] in 1985, where they showed that there exist only thirteen pairs (a,b) that satisfies the given condition. In this chapter we prove two generalizations

of Problem 1.1.

2.1 A Generalization

The next theorem gives a generalization of Problem 1.1.

Theorem 2.2. *For a fixed positive integer m, the congruence*

$$n^a - n^b \equiv 0 \pmod{m^a - m^b} \tag{2.1}$$

has a solution in $(a,b) \in \mathbb{N}^2$ *with* $a > b$ *for all integers n greater than m if and only if* $m = 2$ *and* $(a,b) \in S$*, where* $S =$

$$\big\{(2,1),(3,1),(4,2),(5,1),(5,3),(6,2),(7,3),(8,2),(8,4),(9,3),(14,2),(15,3),(16,4)\big\}.$$

The proof of Theorem 2.2 follows the method of Sun and Zhang for the case $m = 2$ in [15], and is realized by considering different cases for m. For $m = 1$ we observe that there is no solution. We prove the theorem for $m > 2$.

We call the pair (a,b) a solution of (2.1) if for this pair, (2.1) is true for all integers $n > m$.

Remark 2.3. Observe that Theorem 2.1 cannot be applied to give a proof of Theorem 2.2. However, C. L. Stewart in [14, Theorem 1.1, page 293], provided the following improvement of Theorem 2.1.

Theorem 2.4. *If a and b are integers with* $a > b > 0$ *then*

$$P(a^c - b^c) > c\exp(\log c/104\log\log c),$$

for c sufficiently large in terms of the number of distinct prime factors of ab.

Theorem 2.4 is effective, however the implied constants in the theorem are not given explicitly. An explicit version of Theorem 2.4 may give another approach in proving Theorem

2.2 which we keep for future work.

We start by proving two lemmas.

Lemma 2.5. *Suppose that* $\alpha \geq 3$. *Then* $\mathrm{ord}_{2^\alpha}(5) = 2^{\alpha-2}$.

Proof. We claim that for $\alpha \geq 3$,

$$5^{2^{\alpha-2}} = 1 + 2^\alpha + C \cdot 2^{\alpha+1}, \tag{2.2}$$

for some arbitrary constant C. We proceed by induction.

For $\alpha = 3$, we have that $5^2 = (1+2^2)^2 = 1+2^3+2^4$. Let (2.2) hold. Then we have

$$\begin{aligned} 5^{2^{\alpha-1}} &= \left(5^{2^{\alpha-2}}\right)^2 \\ &= (1 + 2^\alpha + C \cdot 2^{\alpha+1})^2 \\ &= 1 + 2^{\alpha+1} + C' \cdot 2^{\alpha+2}, \end{aligned}$$

where C' is another constant. Hence, by induction the claim is true. Then, by (2.2) we have that $5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$, but $5^{2^{\alpha-3}} = 1 + 2^{\alpha-1} + C \cdot 2^\alpha \equiv 1 + 2^{\alpha-1} \not\equiv 1 \pmod{2^\alpha}$.

Therefore, $\mathrm{ord}_{2^\alpha}(5) = 2^{\alpha-2}$. □

The next lemma is a result regarding $d(n)$, the divisor function for n. We reproduce the proof given in [15, Lemma 6, page 220] here, as the result is not widely known.

Lemma 2.6. *For all positive integers n, we have* $d(n) \leq \sqrt{3n}$. *The coefficient* $\sqrt{3}$ *cannot be reduced further, since we have equality for* $n = 12$.

Proof. Let $n = \prod_{i=1}^{r} p_i^{\gamma_i}$ be the prime power factorization of n. Then we have $d(n) = \prod_{i=1}^{r} (\gamma_i + 1)$. Therefore, $\frac{d(n)}{\sqrt{n}} = \prod_{i=1}^{r} \frac{\gamma_i+1}{p_i^{\gamma_i/2}}$. Let $g(\gamma) = \frac{\gamma+1}{p^{\gamma/2}}$. Then we have that $g(\gamma)$ decreases when $\gamma \in [1,\infty)$ for $p > e$, and when $\gamma \in [2,\infty)$ for $p > e^{2/3}$. Therefore, we can conclude that $\frac{\gamma_i+1}{p_i^{\gamma_i/2}} \leq \frac{2}{\sqrt{3}}$ when $p_i \geq 3$ and $\frac{\gamma_i+1}{p_i^{\gamma_i/2}} \leq 1$ when $p_i \geq 5$. Also, we have that $\frac{\gamma_i+1}{2^{\gamma_i/2}} \leq \frac{3}{2}$. Hence, we have that $\frac{d(n)}{\sqrt{n}} \leq \frac{3}{2} \cdot \frac{2}{\sqrt{3}} = \sqrt{3}$, which shows that $d(n) \leq \sqrt{3n}$. □

Proof of Theorem 2.2. We consider two cases, according as m is even or odd.

Case 1. m is a fixed even integer ≥ 4.

Then $m^a - m^b = m^b(m^c-1) = m^b p_1^{\alpha_1}\cdots p_s^{\alpha_s}$, where p_i's are distinct odd primes, $\alpha_i \geq 0$, and $c = a-b$. Suppose (a,b) is a solution of (2.1).

Let n be a primitive root of $p_i^{\alpha_i}$. Since $p_i^{\alpha_i} | m^b(m^c-1) | n^b(n^c-1)$ and $(p_i, n) = 1$, we have that $n^c \equiv 1 \pmod{p_i^{\alpha_i}}$. Hence

$$\phi(p_i^{\alpha_i}) | c. \tag{2.3}$$

Since $(p_i - 1) | \phi(p_i^{\alpha_i})$, by (2.3) we have that $\frac{p_i-1}{2} | \frac{c}{2}$. This implies that

$$s \leq d(c/2), \tag{2.4}$$

where $d(c/2)$ denotes the number of divisors of $c/2$.

Let $M = p_r^{\alpha_r} = \max_{1\leq i\leq s}(p_i^{\alpha_i})$. If $s = 1$, then $M = m^c - 1$. In this case, we observe that $\phi(M) = \phi(p_r^{\alpha_r}) = M(1 - \frac{1}{p_r}) \geq \frac{2M}{3}$ since $p_r \geq 3$. Therefore, we have that

$$\phi(M) \geq \frac{2M}{3} = \frac{2}{3}(m^c - 1) > c$$

for $c \geq 2$ and $m \geq 4$, which is a contradiction to (2.3). Therefore, (a,b) is not a solution to (2.1) when $c \geq 2$ and $s = 1$. Note that $c \neq 1$, since c is even.

If $s > 1$, we have that $M^s > m^c - 1$. Since M is odd, we can say that $M^s > m^c$. Hence, by (2.4), we have

$$\phi(M) \geq \frac{2M}{3} > \frac{2}{3}\cdot m^{c/s} \geq \frac{2}{3}\cdot m^{c/d(c/2)}.$$

Therefore, if $m^{c/d(c/2)} > \frac{3c}{2}$, then $\phi(M) > \frac{2}{3}\cdot\frac{3c}{2} = c$, which, again contradicts (2.3). Hence (a,b) is not a solution of (2.1) if

$$m^{c/d(c/2)} > \frac{3c}{2}, \tag{2.5}$$

for $c \geq 1$ and $m \geq 4$. By Lemma 2.6 we have that $d(c/2) \leq \sqrt{3c/2}$, which gives $m^{c/d(c/2)} \geq$

$m^{\sqrt{2c/3}}$. Hence, by (2.5), we can say that (a,b) is not a solution of (2.1) when

$$m^{\sqrt{2c/3}} > \frac{3c}{2}.$$

Let $f_m(c) = m^{\sqrt{2c/3}} - \frac{3c}{2}$. Then $f_m(c) \geq 4^{\sqrt{2c/3}} - \frac{3c}{2} > 0$ for all $c \geq 1$, since $m \geq 4$. Therefore, for any fixed even integer $m \geq 4$, $f_m(c) > 0$ for all $c \geq 1$.

Hence, there are no solutions (a,b) that satisfy equation (2.1) when m is a fixed even integer ≥ 4.

Case 2. m is a fixed odd integer ≥ 3.

Then $m^a - m^b = m^b(m^c - 1) = m^b p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ with $p_1 = 2$, $p_2, \cdots p_s$ are distinct odd primes, $\alpha_i \geq 0$, and $c = a - b$.

Firstly, let $s \geq 2$. Suppose (a,b) is a solution of (2.1). Let n be a primitive root of $p_i^{\alpha_i}$, $2 \leq p_i \leq s$. Since $p_i^{\alpha_i} | n^b(n^c - 1)$, we have that $n^c \equiv 1 \pmod{p_i^{\alpha_i}}$. Hence

$$\phi(p_i^{\alpha_i}) | c, \tag{2.6}$$

for $2 \leq i \leq s$. Since $(p_i - 1) | \phi(p_i^{\alpha_i})$, by (2.6) we have that $\frac{p_i - 1}{2} | \frac{c}{2}$. This implies that

$$s - 1 \leq d(c/2). \tag{2.7}$$

Let $M = p_r^{\alpha_r} = \max_{1 \leq i \leq s}(p_i^{\alpha_i})$. We observe that $\phi(M) = M(1 - \frac{1}{p_r}) \geq \frac{M}{2}$ since $p_r \geq 2$. Then, since $s > 1$, we have that $M^s > m^c - 1$. This implies that $M^s \geq m^c$. Hence, by (2.7), we have

$$\phi(M) \geq \frac{M}{2} \geq \frac{1}{2} \cdot m^{c/s} \geq \frac{1}{2} \cdot m^{c/(d(c/2)+1)}.$$

Therefore, if $m^{c/(d(c/2)+1)} > 2c$, then $\phi(M) > \frac{1}{2} \cdot 2c = c$, which contradicts (2.6). Hence (a,b) is not a solution of (2.1) if

$$m^{c/(d(c/2)+1)} > 2c, \tag{2.8}$$

for $c \geq 1$ and $m \geq 3$. Using Lemma 2.6 we have that $m^{c/(d(c/2)+1)} \geq m^{c/(1+\sqrt{3c/2})}$. Therefore, by (2.8), we can say that (a,b) is not a solution of (2.1) when

$$m^{c/(1+\sqrt{3c/2})} > 2c.$$

Let $h_m(c) = m^{c/(1+\sqrt{3c/2})} - 2c$. Now $h_3(c) > 0$ for $c \geq 27$. Hence, we only need to consider $2 \leq c \leq 26$. Writing the prime factorization of $3^c - 1$ for $c = 2, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26$, we see that the condition (2.6) is not satisfied, and hence they are not possible.

For $m = 3$ and $c = 4$, equation (2.1) becomes $n^b(n^4 - 1) \equiv 0 \pmod{3^b(3^4 - 1)}$. Now, for $3 \nmid n$, this implies that $n^4 \equiv 1 \pmod{3^b}$. Hence, choosing n to be a primitive root of 3^b, we can conclude that $\phi(3^b)|4$. This gives $2 \cdot 3^{b-1}|4$, which is only possible if $b = 1$. Therefore, the only possible choice is $(a,b) = (5,1)$. Then (2.1) becomes $n^5 - n \equiv 0 \pmod{240}$, which is not true for all $n > 3$ (for example, $n = 4$). Hence, $c = 4$ is also ruled out.

Also, $h_5(c) > 0$ for $c \geq 7$. Therefore, we only need to check $2 \leq c \leq 6$. Writing the prime factorization of $5^c - 1$ for $c = 4, 6$, we observe that (2.6) is not satisfied, and hence they do not occur.

For $m = 5$ and $c = 2$, equation (2.1) takes the form $n^b(n^2 - 1) \equiv 0 \pmod{24 \cdot 5^b}$. For $5 \nmid n$, this implies that $n^2 \equiv 0 \pmod{5^b}$. Choosing n to be a primitive root of 5^b, we conclude that $\phi(5^b)|2$, which gives $4 \cdot 5^{b-1}|2$. This is impossible for any value of b. Therefore, $c = 2$ is also ruled out.

Next, for any fixed odd integer $m \geq 7$, $h_m(c) \geq 7^{c/(1+\sqrt{3c/2})} - 2c > 0$ for all $c \geq 1$.

Hence, there are no solutions (a,b) that satisfy equation (2.1), when m is a fixed odd integer ≥ 3 and $s \geq 2$.

Secondly, let $s = 1$. Then $m^c - 1 = 2^\alpha$, $\alpha \geq 1$. Therefore, equation (2.1) becomes $m^b \cdot 2^\alpha | n^b(n^c - 1)$, which implies that $2^\alpha | n^b(n^c - 1)$. For n odd, we have that

$$n^c \equiv 1 \pmod{2^\alpha}. \tag{2.9}$$

If $\alpha = 1$, then $m^c = 3$ which implies that $m = 3$ and $c = 1$. Then (2.1) becomes $n^b(n-1) \equiv 0 \pmod{2 \cdot 3^b}$. Choosing $n = 5$, we get $4 \cdot 5^b \equiv 0 \pmod{2 \cdot 3^b}$ which is not possible.

If $\alpha = 2$, we have $m^c = 5$. Therefore, $m = 5$ and $c = 1$. Then (2.1) takes the form $n^b(n-1) \equiv 0 \pmod{4 \cdot 5^b}$. Taking $n = 7$, we get $6 \cdot 7^b \equiv 0 \pmod{4 \cdot 5^b}$ which also, is not possible.

Finally, let $\alpha \geq 3$. Now, we choose $n \equiv 5 \pmod{2^\alpha}$. By Lemma 2.5, we know that $\text{ord}_{2^\alpha}(5) = 2^{\alpha-2}$. Then, by (2.9) we have that $2^{\alpha-2} | c$. This implies that $\frac{m^c-1}{4} | c$, and hence,

$$m^c - 1 \leq 4c. \tag{2.10}$$

We observe that for any fixed odd integer $m \geq 7$, $m^c - 1 > 4c$ for all $c \geq 1$. For $m = 3$, (2.10) only holds when $c = 1, 2$, and for $m = 5$ when $c = 1$. Since $2^{\alpha-2} | c$ where $\alpha \geq 3$, $c = 1$ is not possible.

For $m = 3$ and $c = 2$, (2.1) becomes $n^b(n^2-1) \equiv 0 \pmod{2^3 \cdot 3^b}$. For $3 \nmid n$, this implies that $n^2 \equiv 1 \pmod{3^b}$. Choosing n to be a primitive root of 3^b, we can conclude that $\phi(3^b) | 2$. This implies that $2 \cdot 3^{b-1} | 2$, which is only possible if $b = 1$.

Hence, the only possible choice is $(a, b) = (3, 1)$. Then (2.1) becomes $n^3 - n \equiv 0 \pmod{24}$ which is not true for all $n > 3$ (for example, $n = 4$). Consequently, $c = 2$ is also ruled out.

Therefore, there are no solutions (a, b) that satisfy equation (2.1), when m is a fixed odd integer ≥ 4 and $s = 1$.

The proof of Theorem 2.2 is now complete. □

2.2 A Second Generalization

In this section, we consider a further generalization of Problem 1.1.

Problem 1.4. *Find all positive integers a and b with $a > b$ such that $2^a - 2^b$ divides $z^a - z^b$ for all $z \in \mathbb{Z}$.*

It can be shown that Problem 1.4 is equivalent to Problem 1.1.

Proposition 2.7. *The solutions of Problem 1.1 coincide with the solutions of Problem 1.4.*

Proof. First of all, it is evident that any solution of Problem 1.4 is a solution of Problem 1.1. Conversely, assume that (a,b) satisfy the conditions of Problem 1.1. Then 2^a-2^b divides n^a-n^b for all $n\in\mathbb{N}$, that is, $2^b(2^c-1)|n^b(n^c-1)$ for all $n\in\mathbb{N}$ where $c=a-b$. Let $z=-n$. Then, we have that $2^b(2^c-1)|(-z)^b\big((-z)^c-1\big)$. However, from Proposition 1.2, we know that c is even. Therefore, we have that $2^b(2^c-1)|(-z)^b\big(z^c-1\big)$ which implies $2^a-2^b|z^a-z^b$ for all $z\in\mathbb{Z}$. Hence, (a,b) satisfies the condition of Problem 1.4. □

Problem 1.4 is, in fact, a special case of a further generalization in number fields considered by A. Zaharescu and M. Vâjâitu in [16]. First, we start by stating the problem.

Problem 1.5. *Let $\mathcal{A}$ be the ring of integers of an algebraic number field $\mathcal{K}$, and let $\alpha_1,\alpha_2,...,\alpha_k$, and β be nonzero elements of $\mathcal{A}$, where β is not a unit. Find all k-tuples $(a_1,a_2,\cdots,a_k)\in\mathbb{N}^k$ such that*

$$\sum_{i=1}^{k}\alpha_i\beta^{a_i} \quad \textit{divides} \quad \sum_{i=1}^{k}\alpha_i z^{a_i} \tag{2.11}$$

for all $z\in\mathcal{A}$, and

$$\sum_{i\in I}\alpha_i\beta^{a_i}\neq 0 \quad \textit{for any} \quad I\subseteq\{1,2,...,k\}. \tag{2.12}$$

We already mentioned in Chapter 1 why we need to assume (2.12) and the fact that β is not a unit (see discussion after Problem 1.5 in Chapter 1). Hence, we will consider only those solutions to (2.11) that also satisfy (2.12). Zaharescu and Vâjâitu has proved a finiteness theorem for the set of k-tuples satisfying (2.11) and (2.12) (see [16, Theorem 1]). In this section, we state and prove an explicit version of their theorem.

First, we start with a few notations that we use throughout this section.

2.2.1 Notation

Throughout this section, let $\mathcal{K}$ be an algebraic number field and $\mathcal{A} = \mathcal{A}_{\mathcal{K}}$ be its ring of integers. We denote $\mathrm{Norm}_{\mathcal{K}/\mathbb{Q}}(\cdot)$ by $\mathrm{N}(\cdot)$. Let $g(x) = \sum_{i=1}^{k} \alpha_i x^{a_i} \in \mathcal{A}[x]$, where $\alpha_1 \neq 0$, $a_1 > a_2 > \ldots > a_k$, $a = \max(a_1, 3)$, $\Delta = \prod_{i=2}^{k}(a_1 - a_i)$, and $\mathcal{J} = \mathcal{J}(g)$ be the ideal of $\mathcal{A}$ generated by the set $\{g(z) : z \in \mathcal{A}\}$.

We start by proving two lemmas.

Lemma 2.8. *For a fixed positive integer k, the function* $f(x) = \frac{x^k}{(x-1)^{k-1}} - x$ *is bounded on* $[2, \infty)$.

Proof. We have

$$f(x) = \frac{x^k - x(x-1)^{k-1}}{(x-1)^{k-1}} = \frac{\binom{k-1}{1}x^{k-1} - \binom{k-1}{2}x^{k-2} + \cdots + (-1)^k x}{x^{k-1} - \binom{k-1}{1}x^{k-2} + \cdots + (-1)^{k-1}}.$$

Dividing the numerator and denominator of the above expression by x^{k-1} we can conclude that $f(x) \to \binom{k-1}{1}$ as $x \to \infty$. Therefore, $f(x)$ is bounded on $[2, \infty)$. □

The next lemma is [16, Lemma 1]. Here we state and give its proof for completeness.

Lemma 2.9. *Let* $\alpha_1, \alpha_2, \cdots, \alpha_k$ *and* β *be nonzero complex numbers with* $|\beta| \neq 1$. *Then there exists a constant* $c = c(\alpha_1, \alpha_2, \cdots, \alpha_k, \beta) > 0$ *such that for any* $(a_1, a_2, \cdots, a_k) \in \mathbb{N}^k$ *satisfying* (2.12) *we have*

$$\left| \sum_{i=1}^{k} \alpha_i \beta^{a_i} \right| \geq c \max\left\{ |\beta|^{a_1}, |\beta|^{a_2}, \cdots, |\beta|^{a_k} \right\}. \tag{2.13}$$

Proof. First, we observe that the case $|\beta| < 1$ reduces to the case $|\beta| > 1$. Because, we have that

$$\sum_{i=1}^{k} \alpha_i \beta^{a_i} = \beta^{\max\{a_1, \cdots . a_k\}+1} \sum_{i=1}^{k} \alpha_i \frac{1}{\beta^{\max\{a_1, \cdots, a_k\}+1-a_i}}.$$

Now if $|\beta| < 1$, then using the established inequality for $|\beta| > 1$, we have

$$\sum_{i=1}^{k} \alpha_i \beta^{a_i} \geq c\beta^{\max\{a_1,\cdots.a_k\}+1} \max\left\{ \frac{1}{|\beta|^{\max\{a_1,\cdots,a_k\}+1-a_1}}, \cdots, \frac{1}{|\beta|^{\max\{a_1,\cdots,a_k\}+1-a_1}} \right\}$$
$$\geq c \max\left\{ |\beta|^{a_1}, |\beta|^{a_2}, \cdots, |\beta|^{a_k} \right\}.$$

Therefore, let us assume $|\beta| > 1$. We divide (2.13) by $|\beta|^{\max\{a_1,a_2,\cdots,a_k\}}$ and denote $b_i = \max\{a_1,a_2,\cdots,a_k\} - a_i$ for each i. Then (2.13) means that if $b_1,b_2,\cdots,b_k \in \mathbb{N}\cup\{0\}$ then $\left| \sum_{i=1}^{k} \alpha_i \beta^{-b_i} \right| \geq c$ for some $c > 0$. Towards a contradiction, we assume that such a $c > 0$ does not exist. Then there exists a sequence $(x_m) = \left(\sum_{i=1}^{k} \alpha_i \beta^{-b_{i,m}} \right)$ where $b_{i,m} \in \mathbb{N}\cup\{0\}$, $\min_{1\leq i\leq k} b_{i,m} = 0$, and $\lim_{m\to\infty} x_m = 0$.

Since each k-tuple $(b_{1,m}, b_{2,m}, \cdots, b_{k,m})$ has at least one zero entry, then there exists some $1 \leq i_0 \leq k$ such that $(b_{i_0,m})$ has infinitely many zeros. That is, there exists a subsequence (x_{m_j}) of (x_m) such that $b_{i_0,m_j} = 0$ for some $1 \leq i_0 \leq k$. This means that there exists $1 \leq i_0 \leq k$ and an infinite subset of natural numbers A such that $b_{i_0,m} = 0$ for all $m \in A$. Now let $1 \leq i \leq k$, $i \neq i_0$. Then either there is a non-negative integer that repeats infinitely many times or $\lim_{\substack{m\to\infty \\ m\in A}} b_{i,m} = \infty$. Suppose that the former case occurs. Then there exists an infinite subset B of natural numbers such that $b_{i,m} = \gamma_i$ for $m \in B$, where γ_i is a number that repeats infinitely many times. Continuing this argument we can arrive at a collection of non-negative integers γ_i for $i \in J \subset \{1,2,\cdots,k\}$, and an infinite subset of integers C such that $b_{i,m} = \gamma_i$ for all $i \in J$ and $m \in C$, and $\lim_{\substack{m\to\infty \\ m\in C}} b_{i,m} = \infty$ for $i \notin J$. Therefore, we have

$$0 = \lim_{\substack{m\to\infty \\ m\in C}} x_m = \lim_{\substack{m\to\infty \\ m\in C}} \sum_{i=1}^{k} \alpha_i \beta^{-b_{i,m}} = \sum_{i\in J} \alpha_i \beta^{-\gamma_i},$$

which implies that for some a_i's, we have $\sum_{i\in J} \alpha_i \beta^{a_i - \max\{a_1,\cdots,a_k\}} = 0$. Hence, we have that $\sum_{i\in J} \alpha_i \beta^{a_i} = 0$, which contradicts (2.12). Therefore, the lemma is proved. □

2.2.2 The Main Result

The following explicit version of Theorem 1 in [16] is the main result of this section.

Theorem 2.10. *Let $\mathcal{A}$ be the ring of integers of an algebraic number field $\mathcal{K}$, and let $\alpha_1, \alpha_2, ..., \alpha_k$, and β be nonzero elements of $\mathcal{A}$, where β is not a unit. If $(a_1, a_2, \cdots, a_k) \in \mathbb{N}^k$ with $a_1 > a_2 > \cdots > a_k$ satisfy* (2.11) *and* (2.12)*, then we have*

$$a \leq \frac{1}{\log|N(\beta)|}\Bigg\{[\mathcal{K}:\mathbb{Q}]M\log 2 + (2^{k-1}+2M)\log|N(\alpha_1)| \\ + M(k-1)[\mathcal{K}:\mathbb{Q}]a^{\frac{0.5414+1.06599(k-1)}{\log\log a}} + (2^{k-1}+M)(k-1)[\mathcal{K}:\mathbb{Q}]a^{\frac{0.5414}{\log\log a}} - \log c\Bigg\},$$

where $a = \max(a_1, 3)$, M is a positive integer such that $f(x) < M$ for $x \geq 2$, where $f(x)$ is given in Lemma 2.8, and $c = \prod_{\sigma} c\big(\sigma(\alpha_1), \cdots, \sigma(\alpha_k), \sigma(\beta)\big)$, where σ varies over all embeddings of $\mathcal{K}$ and $c\big(\sigma(\alpha_1), \cdots, \sigma(\alpha_k), \sigma(\beta)\big)$ is the constant derived from the application of Lemma 2.9 on $\sigma(\alpha_1), \cdots, \sigma(\alpha_k)$, and $\sigma(\beta)$.

The proof of this theorem is achieved by combining two estimates that are obtained by different means. In the first estimate, we establish a lower bound for the norm of $\sum_{i=1}^{k} \alpha_i \beta^{a_i}$ where $(a_1, a_2, \cdots, a_k)$ satisfy (2.11) and (2.12). In the second estimate, we give an upper bound for $\mathrm{N}(\mathcal{J})$. Since $\sum_{i=1}^{k} \alpha_i \beta^{a_i}$ divides $\sum_{i=1}^{k} \alpha_i z^{a_i}$ for any $z \in \mathcal{A}$, we have that $\Big\langle \sum_{i=1}^{k} \alpha_i \beta^{a_i} \Big\rangle$ divides the ideal $\mathcal{J}$, and hence, $\mathrm{N}\Big(\sum_{i=1}^{k} \alpha_i \beta^{a_i}\Big)$ divides $\mathrm{N}(\mathcal{J})$. This furnishes a lower bound for $\mathrm{N}(\mathcal{J})$ upon establishing a lower bound for the norm of $\sum_{i=1}^{k} \alpha_i \beta^{a_i}$. Using our estimates, we find explicit constants d_1, d_2, d_3, d_4 such that

$$d_1 e^{d_2 \log a} \leq \mathrm{N}(\mathcal{J}) \leq d_3 e^{d_4 \frac{\log a}{\log\log a}}. \tag{2.14}$$

Then by taking the natural logarithm of (2.14), we obtain an upper bound for a similar to

the one in Theorem 2.10. In the next two sections, we establish the inequality (2.14).

2.2.3 A Lower Bound for $\left|\mathrm{N}\Big(\sum_{i=1}^{k}\alpha_i\beta^{a_i}\Big)\right|$

A lower bound for $\left|\mathrm{N}\Big(\sum_{i=1}^{k}\alpha_i\beta^{a_i}\Big)\right|$ is given by the following assertion, which is Proposition 1 of [16].

Proposition 2.11. *Given $\mathcal{K},\alpha_1,\alpha_2,\cdots,\alpha_k$, and a non-unit β as before, there exists a constant $c=c(\alpha_1,\alpha_2,...\alpha_k,\beta,\mathcal{K})>0$ such that for any $(a_1,a_2,...,a_k)\in\mathbb{N}^k$ satisfying* (2.12) *we have*

$$\left|N\Big(\sum_{i=1}^{k}\alpha_i\beta^{a_i}\Big)\right|\geq c|N(\beta)|^{\max\{a_1,a_2,...,a_k\}}. \tag{2.15}$$

Moreover, $c=\prod_{\sigma}c\big(\sigma(\alpha_1),\cdots,\sigma(\beta)\big)$, where σ varies over all embeddings of $\mathcal{K}$ and $c\big(\sigma(\alpha_1),\cdots,\sigma(\beta)\big)$ is the constant derived from the application of Lemma 2.9 on $\sigma(\alpha_1),\cdots,\sigma(\alpha_k)$ and $\sigma(\beta)$.

Proof. We apply inequality (2.13) to $\sigma(\alpha_i)$ for $i=1,2,\cdots k$, and $\sigma(\beta)$ for any embedding $\sigma:\mathcal{K}\to\mathbb{C}$. We observe that if $|\sigma(\beta)|=1$, then we have $\sigma(\beta)\overline{\sigma(\beta)}=1$ since any $\mathbb{Q}$-monomorphism of $\mathcal{K}$ commutes with complex conjugation. This implies that $\sigma(\beta\overline{\beta})=1$. Therefore, we have $\beta\overline{\beta}=1$ which means that β is a unit. This contradicts the hypothesis of Proposition 2.11. Since β is not a unit then $|\sigma(\beta)|\neq 1$. Hence, we can employ Lemma 2.9 to get

$$\left|\sum_{i=1}^{k}\sigma(\alpha_i\beta^{a_i})\right|=\left|\sum_{i=1}^{k}\sigma(\alpha_i)\sigma(\beta)^{a_i}\right|\geq c\big(\sigma(\alpha_1),\cdots\sigma(\alpha_k),\sigma(\beta)\big)\max\{|\sigma(\beta)|^{a_1},\cdots,|\sigma(\beta)|^{a_k}\},$$

for a positive constant $c\big(\sigma(\alpha_1),\cdots\sigma(\alpha_k),\sigma(\beta)\big)$. By multiplying the above inequalities for all possible embeddings σ we obtain

$$\left|\mathrm{N}\Big(\sum_{i=1}^{k}\alpha_i\beta^{a_i}\Big)\right|=\prod_{\sigma}\left|\sum_{i=1}^{k}\sigma(\alpha_i\beta^{a_i})\right|\geq\prod_{\sigma}c\big(\sigma(\alpha_1),\cdots,\sigma(\alpha_k),\sigma(\beta)\big)\prod_{\sigma}\max\{|\sigma(\beta)|^{a_1},\cdots,|\sigma(\beta)|^{a_k}\}.$$

Now, it is enough to observe that

$$\prod_{\sigma} \max\{|\sigma(\beta)|^{a_1}, \cdots, |\sigma(\beta)|^{a_k}\} \geq \prod_{\sigma} |\sigma(\beta)|^{\max\{a_1, \cdots a_k\}} = |\mathrm{N}(\beta)|^{\max\{a_1, \cdots a_k\}}.$$

The proof is complete. □

2.2.4 An Upper Bound for $\mathrm{N}(\mathcal{J})$

The following proposition gives an upper bound for $\mathrm{N}(\mathcal{J})$.

Proposition 2.12. *We have*

$$N(\mathcal{J}) \leq 2^{[\mathcal{K}:\mathbb{Q}]M} |N(\alpha_1)|^{M+M'} \exp\Big(M(k-1)[\mathcal{K}:\mathbb{Q}]a^{\frac{0.5413+1.06599(k-1)}{\log\log a}}$$

$$+M'(k-1)[\mathcal{K}:\mathbb{Q}]a^{\frac{0.5413}{\log\log a}}\Big),$$

where $M' = 2^{k-1} + M$, and M is a positive integer such that $f(x) < M$ for $x \geq 2$, where $f(x)$ is given in Lemma 2.8.

Proposition 2.12 is proved using two lemmas. Lemma 2.14 establishes a bound for the power of $\mathfrak{p}$ in $\tilde{\mathcal{J}}$ where $\tilde{\mathcal{J}} = \tilde{\mathcal{J}}(g) = \langle\{g(z) : z \in \mathcal{A} \setminus \mathfrak{p}\}\rangle$, and Lemma 2.17 gives an upper bound for the norm of any prime ideal $\mathfrak{p}$ dividing $\mathcal{J}$. Let p be a prime number and $\mathfrak{p}$ be a prime ideal of $\mathcal{A}$ which lies above p. Let $v_{\mathfrak{p}}(z)$ be the exponent of $\mathfrak{p}$ that occurs in the prime power factorization of $\langle z\rangle$. Recall that $\Delta = \prod_{i=2}^{k}(a_1 - a_i)$. First, we state and prove a result which we will use in proving Lemma 2.14.

Lemma 2.13. *Let $f(x) = g(x)x^{-a_k}$. For all $z \in \mathcal{A} \setminus \mathfrak{p}$ suppose that*

$$v_{\mathfrak{p}}(f(z)) \geq \eta$$

for a fixed non-negative integer η. *Then we have*

$$v_{\mathfrak{p}}(f'(z)) \geq \frac{N(\mathfrak{p})-1}{N(\mathfrak{p})}\eta,$$

for all $z \in \mathcal{A} \setminus \mathfrak{p}$.

Proof. Let $1 \leq r \leq \mathrm{N}(\mathfrak{p})-1$ be a fixed positive integer. Let $m = \left\lceil \frac{\eta}{r+1} \right\rceil$. By Taylor's theorem, for $z, y \in \mathcal{A}$ we have

$$f(z+y) = f(z) + f'(z)y + \cdots + \frac{f^{(r)}(z)}{r!}y^r + \cdots.$$

Let $y_1, \cdots, y_r \in \mathfrak{p}^m \setminus \mathfrak{p}^{m+1}$ be such that $\overline{y_i} \neq \overline{y_j}$ for $1 \leq i, j \leq r$, $i \neq j$, where $\overline{y}$ is the image of y in $\mathfrak{p}^m/\mathfrak{p}^{m+1}$. By applying Taylor's theorem to $y_1, \cdots, y_r$ and $z \in \mathcal{A} \setminus \mathfrak{p}$, we arrive at the following linear system of equations:

$$\begin{aligned}
f'(z)y_1 + \cdots + \frac{f^{(r)}(z)y_1^r}{r!} &= t_1, \\
f'(z)y_2 + \cdots + \frac{f^{(r)}(z)y_2^r}{r!} &= t_2, \\
&\cdots\cdots\cdots\cdots\cdots \\
f'(z)y_r + \cdots + \frac{f^{(r)}(z)y_r^r}{r!} &= t_r.
\end{aligned}$$

By solving this system using Cramer's rule, we obtain

$$f'(z) = \frac{\begin{vmatrix} t_1 & y_1^2 & y_1^3 & \cdots & y_1^r \\ t_2 & y_2^2 & y_2^3 & \cdots & y_2^r \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ t_r & y_r^2 & y_r^3 & \cdots & y_r^r \end{vmatrix}}{\prod_{i=1}^r y_i \prod_{1 \leq i < j \leq r}(y_j - y_i)}. \tag{2.16}$$

Observe that

$$t_i = f(z+y_i) - f(z) - \frac{f^{(r+1)}(z)}{(r+1)!}y_i^{r+1} - \cdots \tag{2.17}$$

Now, we know that $v_{\mathfrak{p}}(f(z)) \geq \eta$ and also $v_{\mathfrak{p}}(f(z+y_i)) \geq \eta$. Moreover, for $n > r$, we have that

$$v_{\mathfrak{p}}\Big(\frac{f^n(z)}{n!}y^n\Big) = v_{\mathfrak{p}}\Big(\frac{f^n(z)}{n!}\Big) + v_{\mathfrak{p}}(y^n) \geq v_{\mathfrak{p}}(y^n) \geq mn = \Big\lceil \frac{\eta}{r+1} \Big\rceil n \geq \eta.$$

Here $v_{\mathfrak{p}}\Big(\frac{f^n(z)}{n!}\Big) \geq 0$ since $\frac{f^n(z)}{n!}$ is an algebraic integer. Therefore, by applying these facts in (2.17) we deduce that $v_{\mathfrak{p}}(t_i) \geq \eta$. Next, we observe that the the exponent of $\mathfrak{p}$ in the denominator of (2.16) is $mr + m\frac{r(r-1)}{2} = \frac{mr(r+1)}{2}$. Also, in the numerator of (2.16), we can obtain $\mathfrak{p}^{\eta}$ from the first column, $\mathfrak{p}^{2m}$ from the second column and similarly, $\mathfrak{p}^{rm}$ from the last column. Hence, the total exponent of $\mathfrak{p}$ in the numerator of (2.16) is $\geq \eta + 2m + \cdots + rm = \eta + m\big(\frac{r(r+1)}{2} - 1\big)$. Therefore, we have that

$$v_{\mathfrak{p}}(f'(z)) \geq \eta - m \geq \frac{r}{r+1}\eta,$$

for all $1 \leq r \leq \mathrm{N}(\mathfrak{p}) - 1$. Therefore, taking the largest value of r, we have that

$$v_{\mathfrak{p}}(f'(z)) \geq \frac{\mathrm{N}(\mathfrak{p}) - 1}{\mathrm{N}(\mathfrak{p})}\eta,$$

for all $z \in \mathcal{A} \setminus \mathfrak{p}$. □

Equipped with the previous lemma, the following crucial result is proved in [16, Lemma 3]. We provide the detailed proof here for completeness.

Lemma 2.14. *With the above notations, we have*

$$v_{\mathfrak{p}}(\tilde{\mathcal{J}}) \leq \Big(1 + \frac{1}{N(\mathfrak{p}) - 1}\Big)^{k-1}\Big(v_{\mathfrak{p}}(\alpha_1\Delta) + N(\mathfrak{p})\Big) - N(\mathfrak{p}). \tag{2.18}$$

Proof. We prove the result by induction on k. For $k = 1$, we see that the right hand side of (2.18) equals $v_{\mathfrak{p}}(\alpha_1)$. We will prove that in this case $v_{\mathfrak{p}}(\tilde{\mathcal{J}}) = v_{\mathfrak{p}}(\alpha_1)$. Observe that

$\tilde{\mathcal{J}} = \langle\{\alpha_1 z^{a_1} : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle$. We claim that $\tilde{\mathcal{J}} = \langle\alpha_1\rangle\langle\{z^{a_1} : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle$. To see this, we take any element $\sum_i r_i\alpha_1 z_i^{a_1} \in \tilde{\mathcal{J}}$, where $r_i \in \mathcal{A}$ and $z_i \in \mathcal{A}\setminus\mathfrak{p}$. Since $\sum_i r_i\alpha_1 z_i^{a_1} = \alpha_1\sum_i r_i z_i^{a_1} \in \langle\alpha_1\rangle\langle\{z^{a_1} : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle$, we conclude that $\tilde{\mathcal{J}} \subseteq \langle\alpha_1\rangle\langle\{z^{a_1} : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle$. To see the other direction, we take an element $\sum_i r_i\alpha_1 r_i' z_i^{a_1} \in \langle\alpha_1\rangle\langle\{z^{a_1} : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle$, where $r_i, r_i' \in \mathcal{A}$ and $z_i \in \mathcal{A}\setminus\mathfrak{p}$. Since $\mathcal{A}$ is a ring, we have that $\sum_i r_i\alpha_1 r_i' z_i^{a_1} \in \tilde{\mathcal{J}}$, and hence $\langle\alpha_1\rangle\langle\{z^{a_1} : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle \subseteq \tilde{\mathcal{J}}$. Thus

$$\tilde{\mathcal{J}} = \langle\alpha_1\rangle\langle\{z^{a_1} : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle.$$

Next, we prove that $\mathfrak{p} \not| \langle\{z^{a_1} : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle$. For, if $\mathfrak{p}\big|\langle\{z^{a_1} : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle$, then $\langle\{z^{a_1} : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle \subseteq \mathfrak{p}$. This implies that $z^{a_1} \in \mathfrak{p}$ and hence we have $z \in \mathfrak{p}$, which is a contradiction. Hence, $\mathfrak{p} \not| \langle\{z^{a_1} : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle$ and therefore, $v_\mathfrak{p}(\tilde{\mathcal{J}}) = v_\mathfrak{p}(\alpha_1)$. This shows that (2.18) is true for $k = 1$.

For general k, our approach is to reduce the number of terms in $g(x)$ so that we can use the induction hypothesis. In order to do this, we divide $g(x)$ by x^{a_k} and then take the derivative of the resulting polynomial. We set $f(x) = g(x)x^{-a_k}$. It should be noted here that $f(x)$ and $g(x)$ have the same value of $\alpha_1\Delta$.

Next, we note that since $v_\mathfrak{p}(f(z)) \geq v_\mathfrak{p}(\tilde{\mathcal{J}})$ for all $z \in \mathcal{A}\setminus\mathfrak{p}$, then by Lemma 2.13, taking $\eta = v_\mathfrak{p}(\tilde{\mathcal{J}}(g))$, we have that

$$v_\mathfrak{p}(f'(z)) \geq \frac{\mathrm{N}(\mathfrak{p})-1}{\mathrm{N}(\mathfrak{p})} v_\mathfrak{p}(\tilde{\mathcal{J}}(g)), \tag{2.19}$$

for all $z \in \mathcal{A}\setminus\mathfrak{p}$. If we denote $\tilde{\mathcal{J}}(f') = \langle\{f'(z) : z \in \mathcal{A}\setminus\mathfrak{p}\}\rangle$, then from (2.19) we conclude that

$$v_\mathfrak{p}(\tilde{\mathcal{J}}(f')) \geq \frac{\mathrm{N}(\mathfrak{p})-1}{\mathrm{N}(\mathfrak{p})} v_\mathfrak{p}(\tilde{\mathcal{J}}(g)). \tag{2.20}$$

By the induction hypothesis,we have

$$v_\mathfrak{p}(\tilde{\mathcal{J}}(f')) \leq \Big(1+\frac{1}{\mathrm{N}(\mathfrak{p})-1}\Big)^{k-2}\Big(v_\mathfrak{p}(\alpha_1\Delta)+\mathrm{N}(\mathfrak{p})\Big) - \mathrm{N}(\mathfrak{p}). \tag{2.21}$$

Hence, by applying (2.21) in (2.20), we infer that

$$v_{\mathfrak{p}}(\tilde{\mathcal{J}}(g)) \leq \left(1+\frac{1}{\mathrm{N}(\mathfrak{p})-1}\right)^{k-1}\Big(v_{\mathfrak{p}}(\alpha_1\Delta)+\mathrm{N}(\mathfrak{p})\Big)-\frac{\big(\mathrm{N}(\mathfrak{p})\big)^2}{\mathrm{N}(\mathfrak{p})-1}.$$

Therefore, we conclude that

$$v_{\mathfrak{p}}(\tilde{\mathcal{J}}) \leq \Big(1+\frac{1}{\mathrm{N}(\mathfrak{p})-1}\Big)^{k-1}\Big(v_{\mathfrak{p}}(\alpha_1\Delta)+\mathrm{N}(\mathfrak{p})\Big)-\mathrm{N}(\mathfrak{p}).$$

□

The following corollary is a direct consequence of the fact that $\mathcal{J}\big|\tilde{\mathcal{J}}$, and so $v_{\mathfrak{p}}(\mathcal{J}) \leq v_{\mathfrak{p}}(\tilde{\mathcal{J}})$.

Corollary 2.15. *We have*

$$v_{\mathfrak{p}}(\mathcal{J}) \leq \Big(1+\frac{1}{N(\mathfrak{p})-1}\Big)^{k-1}\Big(v_{\mathfrak{p}}(\alpha_1\Delta)+N(\mathfrak{p})\Big)-N(\mathfrak{p}). \tag{2.22}$$

The above corollary furnishes an explicit bound for the $\mathfrak{p}$-adic valuation of $\mathcal{J}$.

Corollary 2.16. *We have*

$$v_{\mathfrak{p}}(\mathcal{J}) \leq (2^{k-1}+M)v_{\mathfrak{p}}(\alpha_1\Delta)$$

for any $\mathfrak{p}$ for which $v_{\mathfrak{p}}(\mathcal{J}) \geq M$, where M is a positive integer such that $f(x)=\frac{x^k}{(x-1)^{k-1}}-x<M$ for $x\in[2,\infty)$.

Proof. We observe that $\Big(1+\frac{1}{\mathrm{N}(\mathfrak{p})-1}\Big)^{k-1} \leq 2^{k-1}$. Also, by Lemma 2.8 we know that $f(x)$ is bounded as $x\to\infty$. Therefore, we can say that $0 \leq \Big(1+\frac{1}{\mathrm{N}(\mathfrak{p})-1}\Big)^{k-1}\mathrm{N}(\mathfrak{p})-\mathrm{N}(\mathfrak{p})<M$ for some positive integer M. Hence, from (2.22) we have that $v_{\mathfrak{p}}(\mathcal{J}) \leq 2^{k-1}v_{\mathfrak{p}}(\alpha_1\Delta)+M$. Since $v_{\mathfrak{p}}(\mathcal{J}) \geq M$, then $v_{\mathfrak{p}}(\alpha_1\Delta)\neq 0$. Thus we have $v_{\mathfrak{p}}(\mathcal{J}) \leq v_{\mathfrak{p}}(\alpha_1\Delta)\Big(2^{k-1}+\frac{1}{v_{\mathfrak{p}}(\alpha_1\Delta)}M\Big)$. Therefore, we conclude that $v_{\mathfrak{p}}(\mathcal{J}) \leq v_{\mathfrak{p}}(\alpha_1\Delta)(2^{k-1}+M)$ for any $\mathfrak{p}$ for which $v_{\mathfrak{p}}(\mathcal{J}) \geq M$.

□

The following is Lemma 2 of [16].

Lemma 2.17. *Let $\alpha_1, \alpha_2, ..., \alpha_k$, $g(x)$, Δ and $\mathcal{J}$ be as defined before, and let $\mathfrak{p}$ be a prime dividing $\mathcal{J}$. Then at least one of the following holds:*

(i) $\mathfrak{p}$ *divides* α_1.

(ii) $N(\mathfrak{p}) - 1$ *divides* Δ.

Proof. Let $\pi : \mathcal{A} \to \mathcal{A}/\mathfrak{p}$ be the canonical homomorphism from the ring of integers $\mathcal{A}$ to the finite field $\mathcal{A}/\mathfrak{p}$ of order $q = \mathrm{N}(\mathfrak{p})$, where we have $\mathcal{A}/\mathfrak{p} \cong \mathbb{F}_q$, the finite field of q elements. We observe that for any $z \in \mathcal{A}$, $\pi(g(z)) = 0$. This is true since $\mathfrak{p}|\mathcal{J} = \langle \{g(z) : z \in \mathcal{A}\} \rangle$ and so $g(z) \in \mathfrak{p}$. On the other hand $\pi(g(z)) = \sum_{i=0}^{q-1} q_i \big(\pi(z)\big)^i$, where $q_i \in \mathbb{F}_q$. Thus, $\pi(g(z))$ is a polynomial of degree less than q with coefficients in $\mathbb{F}_q$, that has exactly q roots. Therefore, this polynomial should be identically zero in $\mathbb{F}_q[\pi(z)]$. So, $q_i = 0$ in $\mathbb{F}_q$ for $0 \leq i \leq q-1$. Now, we note that $\pi(g(z)) = \pi(\alpha_1)\pi(z)^{a_1} + \cdots + \pi(\alpha_k)\pi(z)^{a_k}$. From here, we have that $\sum_{a_i \equiv a_1 \pmod{q-1}} \pi(\alpha_1) = q_{i_0}$ where $i_0 \equiv a_1 \pmod{q-1}$. Since $q_{i_0} = 0$ in $\mathbb{F}_q$, we conclude that $\sum_{a_i \equiv a_1 \pmod{q-1}} \pi(\alpha_i) = 0$ in $\mathbb{F}_q$.

Now, if there exists $i > 2$ such that $a_i \equiv a_1 \pmod{q-1}$, then we have that $(q-1)|(a_i - a_1)$ and hence $(q-1)|\Delta$. Otherwise $\pi(\alpha_1) = 0$, which implies that $\mathfrak{p}$ divides α_1. This completes the proof. □

Lastly, state and prove a result from elementary number theory which we will use in the proof of Proposition 2.12.

Lemma 2.18. *For any positive divisor d of Δ, we have*

$$\prod_{d|\Delta} d = \Delta^{\frac{1}{2}\sigma_0(\Delta)},$$

where $\sigma_0(\Delta)$ is the number of divisors of Δ.

Proof. Let $t = \sigma_0(\Delta)$. Let the positive divisors of Δ be $a_1, a_2, \cdots, a_t$ with $a_1 < a_2 < \cdots < a_t$. If Δ is not a perfect square, then t is even and we can write

$$\begin{aligned}\Delta &= a_1 a_t = a_2 a_{t-1} \\ &= \cdots\cdots = a_t a_{t/2+1}.\end{aligned}$$

Then $\prod_{d|\Delta} d = a_1 a_2 \cdots a_t = \Delta^{t/2} = \Delta^{\frac{1}{2}\sigma_0(\Delta)}$.
If Δ is a perfect square, then t is odd. In this case, we have

$$\begin{aligned}\Delta &= a_1 a_t = a_2 a_{t-1} \\ &= \cdots\cdots = a_{\frac{t-1}{2}} a_{\frac{t+3}{2}},\end{aligned}$$

and $\Delta^{1/2} = a_{\frac{t-1}{2}+1} = a_{\frac{t+1}{2}}$. Hence, in this case, we have that $\prod_{d|\Delta} d = a_1 a_2 \cdots a_t = \Delta^{\frac{t-1}{2}} \cdot \Delta^{1/2} = \Delta^{t/2} = \Delta^{\frac{1}{2}\sigma_0(\Delta)}$.

Therefore, for any positive divisor d of Δ we have $\prod_{d|\Delta} d = \Delta^{\frac{1}{2}\sigma_0(\Delta)}$. □

Now, we are ready to prove Proposition 2.12.

Proof of Proposition 2.12. We write $\mathcal{J} = \mathcal{J}_1\mathcal{J}_2$ where $\mathcal{J}_1$ consists of the prime ideals $\mathfrak{p}$ such that $v_\mathfrak{p}(\mathcal{J}) < M$ and $\mathcal{J}_2$ contains the prime ideals $\mathfrak{p}$ for which $v_\mathfrak{p}(\mathcal{J}) \geq M$. Then, by Corollary 2.16 we have that $\mathcal{J}_2 \big| (\alpha_1\Delta)^{M'}$. Therefore,

$$\mathrm{N}(\mathcal{J}_2) \leq |\mathrm{N}(\alpha_1\Delta)|^{M'} = |\mathrm{N}(\alpha_1)|^{M'} |\Delta|^{M'[\mathcal{K}:\mathbb{Q}]}.$$

Now $|\Delta| = \left| \prod_{i=2}^{k} (a_1 - a_i) \right| \leq a^{k-1} = \exp((k-1)\log a)$. Also, we have that $\log a \leq a^{\frac{c'}{\log\log a}}$ uniformly in a for $c' > \frac{4}{e^2} = 0.5413$. Therefore, putting all these together, we have

$$\mathrm{N}(\mathcal{J}_2) \leq |\mathrm{N}(\alpha_1)|^{M'} |\Delta|^{M'[\mathcal{K}:\mathbb{Q}]} \leq |\mathrm{N}(\alpha_1)|^{M'} \exp\left((k-1)M'[\mathcal{K}:\mathbb{Q}]a^{\frac{0.5414}{\log\log a}}\right).$$

Now, we find an upper bound for $\mathrm{N}(\mathcal{J}_1)$. Let $\mathcal{J}_0 = \prod_{\substack{\mathfrak{p} \text{ prime} \\ \mathfrak{p}|\mathcal{J}_1}} \mathfrak{p}$. Since $\mathcal{J}_1 \big| \mathcal{J}_0^M$, we have $\mathrm{N}(\mathcal{J}_1) \leq (\mathrm{N}(\mathcal{J}_0))^M$. Hence, it suffices to find an upper bound for $\mathrm{N}(\mathcal{J}_0)$. We start by removing all the divisors of 2 (if any) from $\mathcal{J}_0$. Let m denote the number of divisors of 2 in $\mathcal{J}_0$. Then $m \leq [\mathcal{K}:\mathbb{Q}]$. Also, we remove any divisor of α_1 from $\mathcal{J}_0$. The product of them divides α_1 and so its norm is $\leq |\mathrm{N}(\alpha_1)|$. Therefore, we obtain a square free divisor of $\mathcal{J}$, say $\mathcal{J}_3$. Observe that $\mathcal{J}_3$ is relatively prime to $2\alpha_1$. Now, by Lemma 2.17 we have that $\mathrm{N}(\mathfrak{p})-1$ divides Δ for any prime divisor $\mathfrak{p}$ of $\mathcal{J}_3$. Since the numbers $\mathrm{N}(\mathfrak{p})-1$ are not relatively prime, we cannot say that their product divides Δ. Nevertheless, we know that if d be any positive divisor of Δ, then $d = \mathrm{N}(\mathfrak{p})-1$ for at most $[\mathcal{K}:\mathbb{Q}]$ prime ideals $\mathfrak{p}$. Therefore, $\prod_{\mathfrak{p}|\mathcal{J}_3} (\mathrm{N}(\mathfrak{p})-1)$ divides $\big(\prod_{d|\Delta} d\big)^{[\mathcal{K}:\mathbb{Q}]}$ and by Lemma 2.18 we have $\big(\prod_{d|\Delta} d\big)^{[\mathcal{K}:\mathbb{Q}]} = \Delta^{\frac{1}{2}[\mathcal{K}:\mathbb{Q}]\sigma_0(\Delta)}$. Now, for $\sigma_0(\Delta)$ we have the following upper bound from [7]:

$$\sigma_0(\Delta) \leq \Delta^{\frac{1.5379 \log 2}{\log\log \Delta}}.$$

Also, since $\mathrm{N}(\mathfrak{p}) \geq 3$ if $\mathfrak{p}$ divides $\mathcal{J}_3$, we have that $\mathrm{N}(\mathfrak{p}) < \big(\mathrm{N}(\mathfrak{p})-1\big)^2$. Therefore, $\mathrm{N}(\mathcal{J}_3) < \Big(\prod_{\mathfrak{p}|\mathcal{J}_3} (\mathrm{N}(\mathfrak{p})-1)\Big)^2 \leq \Delta^{[\mathcal{K}:\mathbb{Q}]\sigma_0(\Delta)}$. Using the the bounds for $\sigma_0(\Delta)$, Δ and $\log a$ obtained earlier, we conclude that

$$\mathrm{N}(\mathcal{J}_3) \leq \exp\Big((k-1)[\mathcal{K}:\mathbb{Q}] a^{\frac{0.5414+1.06599(k-1)}{\log\log a}}\Big).$$

Now, since $\mathrm{N}(\mathcal{J}_1) \leq \big(\mathrm{N}(\mathcal{J}_0)\big)^M \leq \Big(2^{[\mathcal{K}:\mathbb{Q}]} \cdot |\mathrm{N}(\alpha_1)| \cdot \mathrm{N}(\mathcal{J}_3)\Big)^M$, we obtain

$$\mathrm{N}(\mathcal{J}_1) \leq 2^{[\mathcal{K}:\mathbb{Q}]M} \cdot |\mathrm{N}(\alpha_1)|^M \cdot \exp\Big(M(k-1)[\mathcal{K}:\mathbb{Q}] a^{\frac{0.5414+1.06599(k-1)}{\log\log a}}\Big).$$

Finally, since $\mathrm{N}(\mathcal{J}) = \mathrm{N}(\mathcal{J}_1)\mathrm{N}(\mathcal{J}_2)$, we have

$$\mathrm{N}(\mathcal{J}) \leq 2^{[\mathcal{K}:\mathbb{Q}]M} |\mathrm{N}(\alpha_1)|^{M+M'} \exp\Big(M(k-1)[\mathcal{K}:\mathbb{Q}] a^{\frac{0.5414+1.06599(k-1)}{\log\log a}}$$

$$+M'(k-1)[\mathcal{K}:\mathbb{Q}] a^{\frac{0.5414}{\log\log a}}\Big).$$

□

2.2.5 Proof of Theorem 2.10

Proof. Let $(a_1, a_2, ..., a_k)$ satisfy (2.11) and (2.12). Let $g(x) = \sum_{i=1}^{k} \alpha_i x^{a_i}$. Then, by (2.11) we have that $g(\beta)$ divides $\mathcal{J}(g)$. Therefore, from (2.14), Proposition 2.11 and Proposition 2.12, we conclude that

$$c|\mathrm{N}(\beta)|^a \leq 2^{[\mathcal{K}:\mathbb{Q}]M}|\mathrm{N}(\alpha_1)|^{M+M'} \exp\Big(M(k-1)[\mathcal{K}:\mathbb{Q}]a^{\frac{0.5414+1.06599(k-1)}{\log\log a}}$$

$$+M'(k-1)[\mathcal{K}:\mathbb{Q}]a^{\frac{0.5414}{\log\log a}}\Big).$$

Since $|\mathrm{N}(\beta)| > 1$, we can take the natural logarithm on both sides of the above inequality and obtain

$$a\log|\mathrm{N}(\beta)| \leq [\mathcal{K}:\mathbb{Q}]M\log 2 + (M+M')\log|\mathrm{N}(\alpha_1)| + M(k-1)[\mathcal{K}:\mathbb{Q}]a^{\frac{0.5414+1.06599(k-1)}{\log\log a}}$$

$$+M'(k-1)[\mathcal{K}:\mathbb{Q}]a^{\frac{0.5414}{\log\log a}} - \log c.$$

The above inequality shows that a is finite. Hence we conclude that the set of solutions $(a_1, a_2, ..., a_k)$ of (2.11) and (2.12) is finite. □

2.3 Applications of Theorem 2.10

We end this chapter with some applications of Theorem 2.10. In particular, we use Theorem 2.10 to provide a solution of Problem 1.4 and calculate bounds for the solutions (a, b) for a Selfridge-type problem with $\mathcal{K} = \mathbb{Q}[i]$.

2.3.1 Problem 1.4 revisited

In Section 2.1, we proved Theorem 2.2, which shows that Problem 1.1 is satisfied only for the thirteen pairs as listed in the set S. Also, we showed in Proposition 2.7 that the solutions of Problem 1.1 coincide with the solutions of Problem 1.4. Here, we revisit Problem

1.4 again, using Theorem 2.10.

For Problem 1.4, we have $k = 2$, $\beta = 2$, $\alpha_1 = 1$, $\alpha_2 = -1$ with $a > b > 0$. Here, $\mathcal{K} = \mathbb{Q}$ and therefore $\mathcal{A} = \mathbb{Z}$. Hence $[\mathcal{K} : \mathbb{Q}] = 1$ and since we are working in $\mathbb{Z}$, we have $\mathrm{N}(z) = z$ for any $z \in \mathbb{Z}$.

Now, by Proposition 2.11, we have $2^a - 2^b \geq c \cdot 2^a$, which gives $1 - \frac{1}{2^{a-b}} \geq c$. Also, we observe that $1 - \frac{1}{2^{a-b}} \geq \frac{1}{2}$. Therefore, we can conclude that for any $c \leq 0.5$, we have $2^a - 2^b \geq c \cdot 2^a$.

Lastly, we need to calculate M. In this case, $f(x) = \frac{x}{x-1}$ and for $x \geq 2$, we have $f(x) \leq 2$. Hence, we can choose $M = 2$. Therefore, by Theorem 2.10 we have

$$a \log 2 \leq 2a^{\frac{0.5414 + 1.06599 \cdot 1}{\log\log a}} + 4a^{\frac{0.5414}{\log\log a}} + 3\log 2.$$

Letting

$$f(a) = 2a^{\frac{1.60729}{\log\log a}} + 4a^{\frac{0.5414}{\log\log a}} - a\log 2 + 3\log 2,$$

we observe that $f(a) > 0$ for $1 < a \leq 911$. Therefore, $0 < b < a \leq 911$ which gives the bounds for a and b. Using the characterization in Proposition 1.2, we performed computations in SAGE and obtained the exact thirteen pairs listed in S, as given in Theorem 2.2. Hence, we are done.

2.3.2 A Selfridge-type problem with $\mathcal{K} = \mathbb{Q}[i]$

Next, we look at a Selfridge-type problem in $\mathcal{K} = \mathbb{Q}[i]$. Then $\mathcal{A} = \mathbb{Z}[i]$. Hence $[\mathcal{K} : \mathbb{Q}] = [\mathbb{Q}[i] : \mathbb{Q}] = 2$, and since we are working in $\mathbb{Z}[i]$, we have $\mathrm{N}(z) = |z|^2$ for any $z \in \mathbb{Z}[i]$. We state the problem as follows.

Problem 2.19. *For any fixed $\beta \in \mathbb{Z}[i]$, not a unit, find all positive integers a and b with $a > b$ such that $\beta^a - \beta^b$ divides $z^a - z^b$ for all $z \in \mathbb{Z}[i]$.*

Here, we have $k = 2$, $\alpha_1 = 1$, $\alpha_2 = -1$ with $a > b > 0$.

By Proposition 2.11, we have $\left|\beta^a - \beta^b\right|^2 \geq c|\beta|^{2a}$ which implies that $\left|1 - \frac{1}{\beta^{a-b}}\right|^2 \geq c$. Now

$$\left|1 - \frac{1}{\beta^{a-b}}\right| \geq 1 - \frac{1}{|\beta|^{a-b}} \geq 1 - \frac{1}{2^{a-b}},$$

since $|\beta| \geq 2$ and $a-b \geq 1$. Therefore, we must have $\left|1 - \frac{1}{\beta^{a-b}}\right|^2 \geq \left(1 - \frac{1}{2^{a-b}}\right)^2 \geq c$, which results in $c \leq \frac{1}{4}$.

In this case also, since $k = 2$ we can choose $M = 2$. Therefore, by Theorem 2.10 we have

$$a \log |\beta| \leq \log 2 + 2a^{\frac{1.60729}{\log\log a}} + 4a^{\frac{0.5414}{\log\log a}}.$$

Let

$$f(a) = 2a^{\frac{1.60729}{\log\log a}} + 4a^{\frac{0.5414}{\log\log a}} + \log 2 - a \log |\beta|.$$

By [16, Theorem 2, page 2226], we have that $|\beta| \leq 8$. Therefore, $f(a) \geq 2a^{\frac{1.60729}{\log\log a}} + 4a^{\frac{0.5414}{\log\log a}} + \log 2 - 3a \log 2 > 0$ for $1 < a \leq 154$. Hence, $1 \leq b < a \leq 154$, which provides the bounds for a and b.

We can perform computations to list all $\beta \in \mathbb{Z}[i]$ such that $|\beta| \leq 8$. With these choices of β, and along with the bounds for a and b obtained above, we can check the divisibility condition of Problem 2.19. We may also need a characterization, similar to Proposition 1.2, for the solutions (a,b) satisfying the conditions of the problem. This we keep for future work.

Chapter 3

A Problem of Ruderman and some generalizations

In this chapter, we consider the following problem due to Ruderman.

Problem 1.6. *If $a > b \geq 0$ are integers such that $(2^a - 2^b)|(3^a - 3^b)$, then $(2^a - 2^b)|(x^a - x^b)$ for all $x \in \mathbb{N}$.*

Our first goal is to give a conditional resolution of this problem.

3.1 Conditional Resolution of Ruderman's Problem

In this section we make an explicit conjecture about the upper bound of $\gcd(2^k - 1, 3^k - 1)$, $k \in \mathbb{N}$, and use it to give a solution of Problem 1.6. We start by reviewing some results that will be needed subsequently. Recall that an integer g is called a primitive root modulo an integer m, if g generates the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^{\times}$. A celebrated theorem of Gauss states that $m = 2, 4, p^{\alpha}, 2p^{\alpha}$ where p is an odd prime and α is a positive integer, are the only moduli for which primitive roots exist. We have the following lemma on the construction of primitive roots.

Lemma 3.1. *If p is an odd prime and g is a primitive root $\pmod{p^2}$, then g is a primitive root $\pmod{p^{\alpha}}$ for all $\alpha \geq 2$.*

Proof. See [8, Theorem 2.40, pages 102–103] □

Based on Lemma 3.1, we have the following observation.

Corollary 3.2. *2 is a primitive root* $\pmod{3^\alpha}$ *for all* $\alpha \geq 1$.

Proof. We know that 2 is a primitive root $\pmod{3^2}$. Hence, using Lemma 3.1, we have the result. □

The next theorem, due to Bugeaud, Corvaja, and Zannier, gives a result which is obtained as one of the applications of the Schmidt Subspace Theorem (See Chapter 4 for a more detailed discussion on this important theorem).

Theorem 3.3. *For any* $\varepsilon > 0$*, we have* $\gcd(2^k - 1, 3^k - 1) < 2^{\varepsilon k}$*, for sufficiently large k.*

Proof. See [2, Theorem 1, page 80] □

Based on Lemma 3.1 and Theorem 3.3, the following is proved by M. Ram Murty and V. Kumar Murty in [6, Theorem 1].

Theorem 3.4. *There is a finite set* S' *such that* $(2^a - 2^b) | (3^a - 3^b)$ *if and only if* $(a,b) \in S'$*, where* $(a,b) \in \mathbb{N} \times \mathbb{N} \cup \{0\}$ *with* $a > b$*.*

Proof. Let $0 < \varepsilon < 1$. Since $(2^a - 2^b) | (3^a - 3^b)$, we have that

$$2^b(2^{a-b} - 1) \Big| 3^b(3^{a-b} - 1).$$

Then, we can say that $2^{a-b} - 1 = AB$, where $A = 3^r$ for some non-negative integer r and $B | (3^{a-b} - 1)$. Hence, $B | \gcd(2^{a-b} - 1, 3^{a-b} - 1)$. Therefore, by Theorem 3.3, we have $B \ll 2^{\varepsilon(a-b)}$, which gives $A \gg \frac{2^{a-b}-1}{2^{\varepsilon(a-b)}} \gg 2^{\varepsilon(a-b)}$. Since $A | (2^{a-b} - 1)$, we have that $2^{a-b} \equiv 1 \pmod{3^r}$. By Corollary 3.2, we have that 2 is a primitive root $\pmod{3^r}$. Therefore, $\phi(3^r) \Big| (a-b)$. Since $\phi(3^r) = 2 \cdot 3^{r-1} = \frac{2A}{3}$, we have that $A \leq \frac{3(a-b)}{2}$. Hence, we conclude that

$$2^{\varepsilon(a-b)} \ll A \leq \frac{3(a-b)}{2}. \tag{3.1}$$

This shows that $a - b$ is bounded. Also, we have $2^b \Big| (3^{a-b} - 1)$, which shows that b is bounded and hence, a is also bounded. □

Remark 3.5. We note here, that $S \cup \{(1,0)\} \subset S'$, where S is as given in Theorem 2.2.

Since the above proof of Theorem 3.4 uses Theorem 3.3, the proof is ineffective. Hence, in order to make Theorem 1.7 effective and compute the bounds for a and b, we need to have an explicit version of Theorem 3.3. Before doing so,we prove a result which establishes a connection between Problem 1.1 and Problem 1.6.

Proposition 3.6. *Problem 1.6 is true if and only if* $S' = S \cup \{(1,0)\}$.

Proof. First, we observe that $(a,0)$ does not satisfy Problem 1.1 except the solution $(1,0)$. To see this, let $n = 2^a - 1$. Then, if $(a,0)$ is a solution of equation (2.1), we must have that $(2^a-1)|((2^a-1)^a-1)$ which is possible only when $a = 1$. Hence $S \cup \{(1,0)\}$ is the set of fourteen pairs that satisfies Problem 1.1, when we assume that b is non-negative. If Problem 1.6 is true, then for integers $a > b \geq 0$ satisfying $(2^a - 2^b)\big|(3^a - 3^b)$, we have that $(2^a - 2^b)\big|(x^a - x^b)$ for all $x \in \mathbb{N}$. Thus, if $(a,b) \in S'$, then $(a,b) \in S \cup \{(1,0)\}$. Hence, $S' \subset S \cup \{(1,0)\}$. From Remark 3.5, we have that $S \cup \{(1,0)\} \subset S'$. Therefore $S' = S \cup \{(1,0)\}$.

For the converse, since $S' = S \cup \{(1,0)\}$, we have that $S' \subset S \cup \{(1,0)\}$. This means that $(a,b) \in S'$ implies $(a,b) \in S \cup \{(1,0)\}$. Therefore for integers $a > b \geq 0$, $(2^a - 2^b)\big|(3^a - 3^b)$ implies that $(2^a - 2^b)\big|(x^a - x^b)$ for all $x \in \mathbb{N}$. Hence, Problem 1.6 is true. □

Proposition 3.6 shows that if $(2^a - 2^b)\big|(3^a - 3^b)$ is true only for the fourteen pairs (a,b) as listed in $S \cup \{(1,0)\}$, then Problem 1.6 is true. In order to show this, we need to have an effective upper bound for $\gcd(2^k - 1, 3^k - 1)$ in Theorem 3.3.

We fix $\varepsilon = 0.74$ and compute the value of $q_3(k) = \frac{\gcd(2^k-1,3^k-1)}{2^{0.74k}}$ for $1 \leq k \leq 10^4$. Table A.1 gives the values of $q_3(k)$ for the first 40 values of k.

As we see in Table A.1, all the values of $q_3(k)$ are smaller than 1, with the largest value being $q_3(12) = 0.96575$. Hence, we propose the following conjecture.

Conjecture 1.9. *For all* $k \in \mathbb{N}$*, we have that* $\gcd(2^k - 1, 3^k - 1) < 2^{0.74k}$.

Remark 3.7. Our choice of $\varepsilon = 0.74$ is the optimal one, since for any $\varepsilon < 0.74$, we find that $q_3(k) > 1$ for some values of k.

Assuming Conjecture 1.9, we give an effective proof of Theorem 3.4 and hence, show that Problem 1.6 is true.

Theorem 3.8. *Conjecture 1.9 implies that Problem 1.6 is true.*

Proof. We follow the proof of Theorem 3.4, but instead of Theorem 3.3, we use Conjecture 1.9 to obtain $B < 2^{0.74(a-b)}$ which gives $A > \frac{2^{a-b}-1}{2^{0.74(a-b)}}$. Then, by (3.1), we conclude that

$$\frac{2^{a-b}-1}{2^{0.74(a-b)}} < A \leq \frac{3(a-b)}{2}, \tag{3.2}$$

which shows that $a-b$ is bounded. Let $a-b=c$. Then, from (3.2), we have that

$$\frac{2^c-1}{2^{0.74c}} < \frac{3c}{2}.$$

Let $h(c) = 2^c - 1 - \frac{3c}{2} \cdot 2^{0.74c}$. It can be verified that $h(c) \geq h(19) > 0$ for $c \geq 19$. Therefore, we only need to consider $1 \leq c \leq 19$. Also, from Theorem 3.4, we have $2^b | (3^c - 1)$ which implies that $2^b < 3^c$. Therefore, we have $b < \frac{c \log 3}{\log 2}$.

Performing relevant computations in SAGE, for each value of c in $1 \leq c \leq 19$, we compute the values of b such that $0 \leq b < \lfloor \frac{c \log 3}{\log 2} \rfloor$, and calculate $a = b + c$. Subsequently, we check that, out of all these pairs (a,b) obtained by the above process, which ones satisfy the condition $(2^a - 2^b) \big| (3^a - 3^b)$. It turns out that we obtain the exact fourteen pairs as listed in $S \cup \{(1,0)\}$, where S is as given in Theorem 2.2. This proves that $S' = S \cup \{(1,0)\}$, and therefore, Problem 1.6 is true. □

Remark 3.9. We can strengthen Theorem 3.8 by weakening Conjecture 1.9. For example, taking $\varepsilon = 0.99$, we observe that $h(c) = 2^c - 1 - \frac{3c}{2} \cdot 2^{0.99c} \geq h(1065) > 0$ for $c \geq 1065$. Therefore, repeating the same computations as above with $1 \leq c \leq 1065$, we still obtain the same fourteen pairs as in $S \cup \{(1,0)\}$. This also confirms that Problem 1.6 is true.

3.2 A Generalization of Ruderman's Problem

In this section, we propose a generalization of Conjecture 1.9 by replacing 2 and 3 with m and $m+1$ for all $m \in \mathbb{N}$. Using the conjecture, we prove a conditional effective analogue of Theorem 3.4 for primes. Further, we formulate and investigate a version of Problem 1.6 for primes.

As in the previous section, we fix $\varepsilon = 0.74$ and compute the value of $q_{m+1}(k) = \frac{\gcd(m^k-1,(m+1)^k-1)}{m^{0.74k}}$ for $1 \leq k \leq 10^4$ and $m \in \mathbb{N}$, $3 \leq m \leq 1000$. Table A.2 gives the values of $q_{m+1}(k)$ for $3 \leq m \leq 7$ and $1 \leq k \leq 20$.

We notice in Table A.2 that the values of $q_{m+1}(k)$ are all less than 1, and as k and m increase, $q_{m+1}(k)$ decreases further. Based on these observations, we propose the following conjecture for the upper bound of $\gcd(m^k-1,(m+1)^k-1)$ for all $k,m \in \mathbb{N}$ with $m \geq 2$.

Conjecture 1.10. *For all $k,m \in \mathbb{N}$ with $m \geq 2$, we have that*

$$\gcd\left(m^k-1,(m+1)^k-1\right) < m^{0.74k}.$$

Remark 3.10. As in the remark mentioned in the previous section, here also our choice of $\varepsilon = 0.74$ turns out to be the optimal one, since for any $\varepsilon < 0.74$, we find that $q_{m+1}(k) > 1$ for some values of k and m.

Our goal here, is to state and prove an analogue of Theorem 3.4 for $(p-1)^k - 1$ and $p^k - 1$, where p is prime. More precisely, we aim to prove that there are only finitely many pairs $(a,b) \in \mathbb{N} \times \mathbb{N} \cup \{0\}$ with $a > b$ such that $(p-1)^a - (p-1)^b$ divides $p^a - p^b$. Since Corollary 3.2 is not applicable in this general case, we start by reproducing a result of Robert J. Rundle in [11] which will play a crucial role in our generalization. Let $t = \mathrm{ord}_n(m)$, where n is prime. This implies $m^t \equiv 1 \pmod{n}$. Also, let s be such that $n^s \mid m^t - 1$ but $n^{s+1} \nmid m^t - 1$. Then, we have the following lemma.

Lemma 3.11 ([11, Lemma 1])**.** *n^{r-s} divides $\mathrm{ord}_{n^r}(m)$ with $r > s$.*

Proof. We do induction on r. Let $r = s+1$. Also, let $J = \mathrm{ord}_{n^r}(m)$. Then, we have that $t|J$. Also, since $m^t \equiv 1 \pmod{n^s}$, we have

$$m^J = \left(m^t\right)^{J/t} = (1+vb^s)^{J/t} \equiv 1 + (J/t)vb^s \pmod{n^{2s}}.$$

Again, since $n^r = n^{s+1}\big|m^J - 1$, we have that $n^{s+1}\big|(J/t)vn^s$. Therefore, $n\big|(J/t)v$. Since $\gcd(v,n) = 1$, we conclude that $n|J$. Hence, the result is proved for $r = s+1$. We will now see that there exists $\ell \geq 1$ such that $n^\ell\big|(J/t)$ but $n^{\ell+1} \nmid (J/t)$, which implies that $m^J = 1 + v'b^{\ell+s}$ and $\gcd(v',n) = 1$. Then $J = J_{s+1} = J_{s+2} = \cdots = J_{s+\ell}$. Therefore, we have that $n^{r-s}\big|J_r$ for $s+1 \leq r \leq s+\ell$. Hence, for the main induction step, we will assume the result for $r = s+\ell$ and prove it for $r = s+\ell+1$. Let $J_r = \mathrm{ord}_{n^r}(m)$. We assume that $n^{r-s}\big|J_r$. We will also assume that $m^{J_r} = 1 + v_2 n^{r-s}$, where $\gcd(v_2,n) = 1$.

Let $J_{r+1} = \mathrm{ord}_{n^{r+1}}(m)$. Then $m^{J_{r+1}} \equiv 1 \pmod{n^{r+1}}$, and hence $m^{J_{r+1}} = 1 + v_1 n^{r+1}$. Therefore, $m^{J_{r+1}} \equiv 1 \pmod{n^r}$. This shows that $J_r\big|J_{r+1}$. Then we have

$$m^{J_{r+1}} = \left(m^{J_r}\right)^{J_{r+1}/J_r} = (1+v_2n^r)^{J_{r+1}/J_r} \equiv 1 + \frac{J_{r+1}}{J_r}v_2n^r \pmod{n^{2r}}.$$

But since $n^{r+1}\big|m^{J_{r+1}} - 1$, we have that $n^{r+1}\big|\left(\frac{J_{r+1}}{J_r}v_2n^r\right)$. Since $n \nmid v_2$, we have $n\big|\frac{J_{r+1}}{J_r}$. Therefore, $n^{r+1-s}\big|J_{r+1}$. Next, we find an ℓ for which $n^\ell\big|\frac{J_{r+1}}{J_r}$, but $n^{\ell+1} \nmid \frac{J_{r+1}}{J_r}$. Then as shown above, J_{r+i} satisfies $n^{r+i-s}\big|J_{r+i}$ for $1 \leq i \leq \ell$ and $J_{r+\ell}$ satisfies the induction hypothesis. Hence, the lemma is proved. □

We now state and prove a conditional effective analogue of Theorem 3.4 for $(p-1)^a - (p-1)^b$ and $p^a - p^b$, where p is prime. We will use Conjecture 1.10 to produce an explicit result. A more general ineffective version of the following result is proved in [11, Proof 2, page 22].

Theorem 3.12. *Under the assumption of Conjecture 1.10, there is an effectively computable constant C such that if $b > C$, then $\left((p-1)^a - (p-1)^b\right) \nmid (p^a - p^b)$ where $(a,b) \in \mathbb{N}^2$ with*

$a > b$.

Proof. Let $c = a - b$. Then, since $(p-1)^b\big((p-1)^c - 1\big)\big|p^b(p^c-1)$, we have that $(p-1)^c - 1 = AB$, where $A|p^b$, $B|(p^c-1)$ and $\gcd(B,p) = 1$. Since p is prime, then $A = p^j$ for some j. By Conjecture 1.10, we have that $\gcd((p-1)^c - 1, p^c - 1) < (p-1)^{0.74c}$. Therefore,

$$B < (p-1)^{0.74c}.$$

Hence, we have $(p-1)^c - 1 = AB < A(p-1)^{0.74c}$ which gives

$$p^j = A > \frac{(p-1)^c - 1}{(p-1)^{0.74c}}.$$

Since $(p-1)^c \equiv 1 \pmod{p^j}$, this implies that $\mathrm{ord}_{p^j}(p-1)\big|c$. By Lemma 3.11, we know that $p^{j-s}\big|\mathrm{ord}_{p^j}(p-1)$. Then we have that $p^{j-s} < c$, and so $p^j < cp^s$. Therefore, we have that

$$\frac{(p-1)^c - 1}{(p-1)^{0.74c}} < p^j < cp^s. \tag{3.3}$$

Since s is fixed, the above inequality shows that $c = a - b$ is bounded. Also, since $(p-1)^b\big|(p^c-1)$, we conclude that b is bounded and hence, a is also bounded. □

Let us look at some applications of Theorem 3.12 by taking particular values for the prime p. For $p = 5$, we observe that $t = \mathrm{ord}_5(4) = 2$, and $s = 1$. Then from (3.3) we have that

$$\frac{4^c - 1}{4^{0.74c}} < 5c.$$

Let $f(c) = 4^c - 1 - 5c \cdot 4^{0.74c}$. Then we can verify that $f(c) \geq f(12) > 0$ for $c \geq 12$. Hence, we only need to consider $1 \leq c \leq 12$. Also, from Theorem 3.12, we have that $4^b|(5^c-1)$ which implies that $4^b < 5^c$. Therefore, we have $b < \frac{c\log 5}{\log 4}$.

We perform the relevant computations in SAGE. For each value of c in $1 \leq c \leq 12$, we compute the values of b such that $1 \leq b < \lfloor \frac{c\log 5}{\log 4} \rfloor$ and calculate $a = b + c$. Next, we check that, out of all these pairs (a,b) obtained by the above process, which ones satisfy

the condition $(4^a - 4^b)\big|(5^a - 5^b)$. It turns out that we obtain exactly one pair $(a,b) = (3,1)$.

Performing similar calculations for primes $7 \leq p \leq 200$, we see that no pair $(a,b) \in \mathbb{N}^2$ with $a > b$ satisfies $\big((p-1)^a - (p-1)^b\big)\big|(p^a - p^b)$.

In view of Theorem 3.12 and the above examples, we may be inclined to propose and investigate the following Ruderman-type problem for primes.

Problem 1.11. *If $a > b \geq 0$ are integers such that $\big((p-1)^a - (p-1)^b\big)\big|(p^a - p^b)$ for $p \neq 5$, then $\big((p-1)^a - (p-1)^b\big)\big|(x^a - x^b)$ for all $x \geq p$.*

Let us see why the condition $p \neq 5$ is needed. For $p = 5$, it is mentioned above that the pair $(a,b) = (3,1)$ satisfies the first divisibility condition in Problem 1.11. However, it does not satisfy the second condition even for the first choice of $x = 6$.

The case of $p = 3$ corresponds to the original problem of Ruderman (Problem 1.6) which we proved to be true, under the assumption of Conjecture 1.9. Moreover, by Theorem 2.2, we can say that the second divisibility condition has no solutions in (a,b) except when $p - 1 = 2$, that is, when $p = 3$. Also, based on computations using Theorem 3.12 as mentioned above, we conclude that no pairs (a,b) will satisfy the first divisibility condition in Problem 1.11 for the primes $7 \leq p \leq 200$. This brings us to the conclusion that if Conjecture 1.10 holds, then for $7 \leq p \leq 200$, Problem 1.11 is trivially true, since no pair (a,b) satisfies both the divisibility conditions.

3.3 The gcd bound via the *ABC*-Conjecture

In this section, we state the *ABC*-Conjecture and investigate its connection with Conjecture 1.10. The *ABC*-Conjecture, first proposed by J. Osterlé and D. Masser in 1985, is an integer analogue of Mason's theorem for polynomials. The conjecture is stated as follows.

Conjecture 3.13. For every $\varepsilon > 0$, there is a constant $K(\varepsilon)$ such that for any coprime integers A, B, C satisfying $A + B = C$, we have

$$\max(|A|, |B|, |C|) \leq K(\varepsilon) N^{1+\varepsilon},$$

where

$$N = \mathrm{rad}(ABC) = \prod_{\substack{\text{p prime} \\ p|ABC}} p,$$

the 'radical' of ABC, is the product of all distinct prime factors of ABC.

In Lemma 3.3, we noted that the implied constant, which depends on ε, is ineffective. In this context, M. Ram Murty and V. Kumar Murty in [6] observed that Conjecture 3.13 implies a bound for $\gcd(2^k-1, 3^k-1)$ where the implied constant depends effectively on ε. Based on their ideas, we prove the following theorem.

Theorem 3.14. *Let $n > m \geq 2$ be two relatively prime integers. Assuming Conjecture 3.13, we have for large enough k and any $\varepsilon > 0$,*

$$\gcd(m^k-1, n^k-1) \leq (mn)^{1/2}\sqrt{K(\varepsilon/2)} \cdot m^{(\frac{(1+\varepsilon)\log n}{2\log m}k},$$

where $K(\varepsilon)$ is the constant given in Conjecture 3.13.

Proof. Let $d := d_{m,n} = \gcd(m^k-1, n^k-1)$. Write $m^k-1 = dU$ and $n^k-1 = dV$, with $(U,V) = 1$. Then, $U(n^k-1) = V(m^k-1)$ and therefore, we have the equation,

$$Un^k - Vm^k = U - V.$$

Since $U|(m^k-1)$, we have that $\gcd(U, m^k) = 1$. Similarly, $\gcd(V, n^k) = 1$. Then, we have that $\gcd(U, Vm^k) = 1$ since $\gcd(U,V) = 1$. Also $\gcd(n^k, Vm^k) = 1$, since $\gcd(n^k, V) = 1$ and $\gcd(m,n) = 1$. Therefore, $\gcd(Un^k, Vm^k) = 1$. Now, let us suppose that $\gcd(U-V, Un^k) = d'$, where $d' \neq 1$. Then $d'|(U-V)$ and $d'|Un^k$. Since $Un^k - Vm^k = U - V$, we have that $d'|(Un^k - Vm^k)$ and $d'|Un^k$ which implies that $d'|Vm^k$. This is only possible if $d' = 1$ since we proved above that $\gcd(Un^k, Vm^k) = 1$. Therefore $\gcd(U-V, Un^k) = 1$. Similarly, we can prove that $\gcd(U-V, Vm^k) = 1$. Therefore, Un^k, Vm^k and $U-V$ are mutually coprime.

Now applying Conjecture 3.13 to the above equation with $\varepsilon/2$ and $A = Un^k$, $B = -Vm^k$

and $C = U - V$, we have

$$Un^k \leq K(\varepsilon/2)[rad(UVm^k n^k(U-V))]^{1+\varepsilon/2} \leq K(\varepsilon/2)[U\mathrm{rad}(mnV(U-V))]^{1+\varepsilon/2}.$$

Since $U \leq dU = m^k - 1 < n^k$, we have

$$n^k \leq K(\varepsilon/2) \cdot U^{\varepsilon/2}[\mathrm{rad}(mnV(U-V))]^{1+\varepsilon/2} \leq K(\varepsilon/2) \cdot n^{k\varepsilon/2}[\mathrm{rad}(mnV(U-V))]^{1+\varepsilon/2}.$$

Therefore, we get

$$n^{k(1-\varepsilon/2)} \leq K(\varepsilon/2)[\mathrm{rad}(mnV(U-V))]^{1+\varepsilon/2},$$

which gives

$$mn \cdot \mathrm{rad}(V(U-V)) \geq \frac{n^{k(1-\varepsilon/2)/(1+\varepsilon/2)}}{(K(\varepsilon/2))^{1/(1+\varepsilon/2)}} \geq \frac{n^{k(1-\varepsilon)}}{(K(\varepsilon/2))^{1/(1+\varepsilon/2)}}.$$

Also, we have

$$\mathrm{rad}(V(U-V)) = \mathrm{rad}(V)rad(U-V) \leq V(V-U) \leq V^2.$$

Hence, we conclude that

$$V \geq \frac{n^{(k/2)(1-\varepsilon)}}{\sqrt{mn}(K(\varepsilon/2))^{1/(2+\varepsilon)}}.$$

Thus, $n^k \geq dV \geq d \cdot \frac{n^{(k/2)(1-\varepsilon)}}{\sqrt{mn}(K(\varepsilon/2))^{1/(2+\varepsilon)}}$, which implies that

$$d = \gcd(m^k - 1, n^k - 1) \leq \sqrt{mn}(K(\varepsilon/2))^{1/(2+\varepsilon)} \cdot n^{(k/2)(1+\varepsilon)} \leq \sqrt{mn}\sqrt{K(\varepsilon/2)} \cdot n^{(k/2)(1+\varepsilon)}.$$

Therefore, we have that

$$\gcd(m^k - 1, n^k - 1) \leq (mn)^{1/2}\sqrt{K(\varepsilon/2)} \cdot m^{(\frac{(1+\varepsilon)\log n}{2\log m}k}$$

□

Corollary 3.15. *Under the assumptions of Theorem 3.14, for an integer $m \geq 2$ and large enough k, we have*

$$\gcd(m^k-1,(m+1)^k-1) \leq \sqrt{(m^2+m)K(\varepsilon/2)} \cdot m^{(\frac{(1+\varepsilon)\log(m+1)}{2\log m}k}.$$

Since $\frac{\log(m+1)}{\log m} \leq \frac{\log 3}{\log 2} = 1.585$ for all $m \geq 2$. From the above corollary we conclude that under the assumptions of Theorem 3.14, we have

$$\gcd(m^k-1,(m+1)^k-1) \leq \sqrt{(m^2+m)K(\varepsilon/2)} \cdot m^{0.7925(1+\varepsilon)k}. \tag{3.4}$$

We observe that the above conditional upper bound is weaker than the unconditional upper bound given in Theorem 3.3. However, upon formulating an explicit version of Conjecture 3.13 the above upper bound will furnish an explicit upper bound for $\gcd(m^k-1,(m+1)^k-1)$. Such an explicit version of Conjecture 3.13 has been proposed by Baker [1].

Conjecture 3.16 (Baker). Following the notations of Conjecture 3.13, we have

$$\max(|A|,|B|,|C|) < \frac{6}{5}N\frac{(\log N)^{\omega}}{\omega!},$$

where $\omega(N)$ is the number of distinct prime divisors of N.

In [5, Theorem 1], Laishram and Shorey proved that under the assumption of Conjecture 3.16, for $\varepsilon > 0$ and A,B,C triples with $N(ABC)$ large enough (depending on ε), one can choose $\frac{6}{5\sqrt{2\pi}} = 0.4787$ as an admissible value for $K(\varepsilon)$. Hence, we have the following.

Proposition 3.17. *Under the assumption of Conjecture 3.16, for $m \geq 2$ and large enough k we have*

$$\gcd(m^k-1,(m+1)^k-1) \leq \sqrt{\frac{6(m^2+m)}{5\sqrt{2\pi}}}m^{0.8004k}$$

Proof. This is a consequence of taking $\varepsilon = 0.001$ in (3.4) and the argument given above. □

3.4 A two dimensional version of Theorem 3.5

In this section, we prove a two dimensional generalization of the result of Murty and Murty [6, Theorem 1].

Theorem 3.18. *There is a finite set S'' such that for $m < n$ with n prime and $\gcd(m,n) = 1$, $(m^t - m^u)(m^v - m^w) \big| (n^t - n^u)(n^v - n^w)$ if and only if $(t,u),(v,w) \in S''$, where $(t,u),(v,w) \in \mathbb{N} \times \mathbb{N} \cup \{0\}$ with $t > u$ and $v > w$, and moreover $t - u \leq v - w \leq t - u + \ell$ for a fixed non-negative integer ℓ.*

Proof. Since $m^{u+w}(m^{t-u} - 1)(m^{v-w} - 1)$ divides $n^{u+w}(n^{t-u} - 1)(n^{v-w} - 1)$, we can say that $m^{t-u} - 1 = n^{\alpha} A_1 A_2$, $m^{v-w} - 1 = n^{\beta} B_1 B_2$, where $\alpha + \beta \leq u + w$ for some $\alpha, \beta \geq 0$ and $A_1, B_1 \big| (n^{t-u} - 1)$ and $A_2, B_2 \big| (n^{v-w} - 1)$. Therefore, we have $A_1 \big| \gcd(m^{t-u} - 1, n^{t-u} - 1)$, $A_2 \big| \gcd(m^{t-u}, n^{v-w} - 1)$, $B_1 \big| \gcd(m^{v-w} - 1, n^{t-u} - 1)$, and $B_2 \big| \gcd(m^{v-w} - 1, n^{v-w} - 1)$.

By [2, Theorem 1] with $\varepsilon/3$, we have that $A_1 \ll m^{\frac{\varepsilon}{3}(t-u)}$, $B_2 \ll m^{\frac{\varepsilon}{3}(v-w)}$. Also, by Theorem 4.2, we have that $A_2 \ll m^{\frac{\varepsilon}{3}(t-u)}$ and $B_1 \ll m^{\frac{\varepsilon}{3}(v-w)} \ll m^{\frac{\varepsilon}{3}(t-u)}$. Hence, we conclude that $(m^{t-u} - 1)(m^{v-w} - 1) = n^{\alpha+\beta} A_1 A_2 B_1 B_2 \ll n^{\alpha+\beta} \cdot m^{\frac{\varepsilon}{3}(3(t-u)+v-w)}$ which gives

$$\frac{(m^{t-u} - 1)(m^{v-w} - 1)}{m^{\frac{\varepsilon}{3}(3(t-u)+v-w)}} \ll n^{\alpha+\beta}.$$

On the other hand, since $n^{\alpha} \big| (m^{t-u} - 1)$ and $n^{\beta} \big| (m^{v-w} - 1)$, we have that $m^{t-u} \equiv 1 \pmod{n^{\alpha}}$ and $m^{v-w} \equiv 1 \pmod{n^{\beta}}$. Hence, $\mathrm{ord}_{n^{\alpha}}(m) \big| (t-u)$ and $\mathrm{ord}_{n^{\beta}}(m) \big| (v-w)$. By Lemma 3.11, we can say that $n^{\alpha-s} \big| \mathrm{ord}_{n^{\alpha}}(m)$ and $n^{\beta-s} \big| \mathrm{ord}_{n^{\beta}}(m)$, where s is the largest power of n that divides $m^k - 1$, $k = \mathrm{ord}_n(m)$. Therefore, $n^{\alpha-s} \big| (t-u)$ and $n^{\beta-s} \big| (v-w)$. This gives

$$n^{\alpha+\beta} \leq (t-u)(v-w)n^{2s}.$$

Hence, we have that

$$\frac{(m^{t-u}-1)(m^{v-w}-1)}{m^{\frac{\varepsilon}{3}(3(t-u)+v-w)}} \ll n^{\alpha+\beta} \leq (t-u)(v-w)n^{2s}.$$

Since s is fixed, the above inequality shows that $t-u$ and $v-w$ are bounded. Again, since $m^{u+w}\big|(n^{t-u}-1)$, we conclude that $u+w$ is bounded. Therefore, t,u,v and w are all bounded. □

Chapter 4

An application of the Schmidt Subspace Theorem

In Chapter 3, we stated an upper bound for the greatest common divisor of $a^k - 1$ and $b^k - 1$, where a and b are two multiplicatively independent integers (see Chapter 3, Theorem 3.3). This bound was crucial in proving Theorem 3.4. Theorem 3.3 is obtained by an application of the Schmidt Subspace Theorem [13, Theorem 1A, page 176]. The Schmidt Subspace Theorem is a higher dimensional generalization of Roth's Theorem in Diophantine Approximation and has a vast number of applications and consequences. In this chapter, we propose and prove a generalization of Theorem 1 in [2], and use it to prove a more general version of Theorem 3.4. In fact, we will prove our generalization by employing a particular case of the Subspace Theorem as given in [13, Theorem 1D, page 177].

Theorem 4.1. *Let S be a finite set of absolute values of $\mathbb{Q}$, including ∞ (normalized so that $|p|_p = p^{-1}$) and let $N \in \mathbb{N}$. For $\nu \in S$, let $L_{1,\nu}, \cdots, L_{N,\nu}$ be linearly independent linear forms in N variables, with coefficients in $\mathbb{Q}$ and also, let $\delta > 0$. Then the solutions $\boldsymbol{x} = (x_1, \cdots, x_N) \in \mathbb{Z}^N$ to the inequality*

$$\prod_{\nu \in S} \prod_{i=1}^{N} |L_{i,\nu}(\boldsymbol{x})|_\nu < \|\boldsymbol{x}\|^{-\delta} \tag{4.1}$$

are contained in finitely many proper subspaces of $\mathbb{Q}^N$.

4.1 Proof of the gcd Theorem

In this section and the next, we prove a more general version of Theorem 1 in [2]. The proof of our theorem follows closely the proof given in [2, Theorem 1], however that proof should be suitably adjusted to our case. We will use the version of the Subspace theorem, as given in Theorem 4.1 and prove the following theorem.

Theorem 4.2. *Let $\ell \in \mathbb{N} \cup \{0\}$ be fixed and $\varepsilon > 0$. Then if m and n are multiplicatively independent integers ≥ 2 with $m < n$, and $a \leq b \leq a + \ell$, we have*

$$\gcd(m^a - 1, n^b - 1) < m^{\varepsilon a}, \tag{4.2}$$

for sufficiently large a.

Setup. For a positive integer j, let

$$z_j(a,b) = \frac{n^{jb}-1}{m^a-1} = \frac{(n^b-1)/g_{a,b} \cdot (n^{(j-1)b} + \cdots + 1)}{(m^a-1)/g_{a,b}} = \frac{c_{j,a,b}}{d_{a,b}},$$

where $g_{a,b} = \gcd(m^a - 1, n^b - 1)$. □

Next, we state and prove several lemmas that will establish Theorem 4.2.

Lemma 4.3. *Theorem 4.2 follows if $d_{a,b} > m^{(1-\varepsilon)a}$.*

Proof. We have $d_{a,b} = \frac{m^a-1}{g_{a,b}} < \frac{m^a}{g_{a,b}}$. Therefore, if $d_{a,b} > m^{(1-\varepsilon)a}$, we have that $m^{(1-\varepsilon)a} < \frac{m^a}{g_{a,b}}$ from which the theorem follows. □

We will now assume that there exist integers $a \in \mathcal{B}$ and b such that $a \leq b \leq a + \ell$ for which $d_{a,b} \leq m^{(1-\varepsilon)a}$, where $\mathcal{B}$ is an infinite set of natural numbers, and arrive at a contradiction which will prove Theorem 4.2.

Lemma 4.4. *For a fixed integer $h > 0$, we have*

$$\left| z_j(a,b) + \sum_{s=1}^{h} \frac{1}{m^{sa}} - \sum_{r=1}^{h} \frac{n^{jb}}{m^{ra}} \right| = O\big(n^{jb} m^{-(h+1)a}\big). \tag{4.3}$$

Proof. We have

$$\frac{1}{m^a-1} = \frac{1}{m^a}\cdot(1-\frac{1}{m^a})^{-1} = \sum_{r=1}^{\infty}\frac{1}{m^{ra}} = \sum_{r=1}^{h}\frac{1}{m^{ra}} + \frac{1}{m^{(h+1)a}}\cdot\frac{m^a}{m^a-1}.$$

Since $\frac{m^a}{m^a-1} = 1+\frac{1}{m^a-1} \leq 2$ for all a, we conclude that

$$\frac{1}{m^a-1} = \sum_{r=1}^{h}\frac{1}{m^{ra}} + O\Big(\frac{1}{m^{(h+1)a}}\Big).$$

Then

$$z_j(a,b) = \frac{n^{jb}-1}{m^a-1} = \sum_{r=1}^{h}\frac{n^{jb}-1}{m^{ra}} + O\Big((n^{jb}-1)m^{-(h+1)a}\Big),$$

which gives

$$z_j(a,b) = \sum_{r=1}^{h}\frac{n^{jb}}{m^{ra}} - \sum_{s=1}^{h}\frac{1}{m^{sa}} + O\Big(n^{jb}m^{-(h+1)a}\Big).$$

Therefore,

$$\Big|z_j(a,b) + \sum_{s=1}^{h}\frac{1}{m^{sa}} - \sum_{r=1}^{h}\frac{n^{jb}}{m^{ra}}\Big| = O\big(n^{jb}m^{-(h+1)a}\big).$$

□

We will apply Theorem 4.1 by looking at the left hand side of the equation (4.3) as a linear form in the variables $z_j(a,b)$, $\frac{n^{jb}}{m^{ra}}$ and $\frac{1}{m^{sa}}$. The idea is to consider a set of linear forms, for various values of j.

Setup (Cont.) We fix a positive integer k. Let S be the set of all prime divisors of mn and ∞. Also, we let $N = hk+h+k$. Writing the vectors $x \in \mathbb{Z}^N$ as

$$x = (x_1, x_2, \cdots, x_N) = (z_1, \cdots, z_k, y_{01}, \cdots, y_{0h}, \cdots, y_{k1}, \cdots, y_{kh}),$$

we construct the linear forms with rational coefficients as given below.

For $i = 1, \cdots, k$, let

$$L_{i,\infty}(x) = z_i + y_{01} + \cdots + y_{0h} - y_{i1} - \cdots - y_{ih},$$

and for $(i,\nu) \notin \{(1,\infty),(2,\infty),\cdots,(k,\infty)\}$, let

$$L_{i,\nu}(x) = x_i.$$

We observe that for each $\nu \in S$, the linear forms $L_{i,\nu}$'s are linearly independent. Also, for a given $a \in \mathcal{B}$, we write

$$\mathbf{x} = d_{a,b} m^{ha} \Big(z_1(a,b), \cdots, z_k(a,b), m^{-b}, \cdots, m^{-ha}, \frac{n^b}{m^a}, \frac{n^b}{m^{2a}}, \cdots, \frac{n^b}{m^{ha}}, \cdots, \frac{n^{kb}}{m^a}, \frac{n^{kb}}{m^{2a}} \cdots, \frac{n^{kb}}{m^{ha}} \Big), \tag{4.4}$$

and note that $\mathbf{x} \in \mathbb{Z}^N$. □

Lemma 4.5. *If the equation* (4.3) *holds, then assuming* $d_{a,b} \leq m^{(1-\varepsilon)a}$ *for all* $a \in \mathcal{B}$, *there exists* $\delta > 0$ *such that*

$$\prod_{\nu \in S} \prod_{i=1}^{N} |L_{i,\nu}(\boldsymbol{x})|_\nu < \|\boldsymbol{x}\|^{-\delta},$$

where $\boldsymbol{x}$ *is given by* (4.4).

Proof. We postpone the proof of this lemma for the next section. □

Proof of Theorem 4.2. By Lemma 4.5, the above $L_{i,\nu}$'s and $\mathbf{x}$ satisfy the conditions of Theorem 4.1, and therefore the solutions $\mathbf{x}$ are contained in finitely many proper subspaces of $\mathbb{Q}^N$. That is, for infinitely many $a \in \mathcal{B}$, $\mathbf{x}$ satisfies an equation

$$\zeta_1 Z_1 + \zeta_2 Z_2 + \cdots + \zeta_k Z_k + \sum_{i,j} \gamma_{i,j} Y_{i,j} = 0$$

with rational coefficients (not all zero), where $0 \leq i \leq k$, $1 \leq j \leq h$. Therefore, by the

definition of $\mathbf{x}$, we have

$$\zeta_1 \frac{n^b-1}{m^a-1} + \zeta_2 \frac{n^{2b}-1}{m^a-1} + \cdots + \zeta_k \frac{n^{kb}-1}{m^a-1} + \sum_{i,j} \gamma_{i,j} \left(\frac{n^{ib}}{m^{ja}} \right) = 0 \tag{4.5}$$

for infinitely many integers a. That is, simplifying (4.5) we have that

$$\sum_{i,j=0}^{M} \beta_{i,j} m^{ja} n^{ib} = 0 \tag{4.6}$$

holds for infinitely many integers $a \in \mathcal{B}$, where $\beta_{i,j}$'s are rational, not all zero. Now since m and n are multiplicatively independent, there are no non-negative integers i and j such that $m^j = n^i$. Therefore, $m^j n^i$ are all distinct, and hence there is a unique greatest term $m^{j_0} n^{i_0}$ with non-zero coefficient β_{i_0,j_0}. Then by (4.6) we conclude that

$$m^{j_0 a} n^{i_0 b} \left(\beta_{i_0,j_0} + \sum_{\substack{i,j=0 \\ i \neq i_0, j \neq j_0}}^{M} \beta_{i,j} \frac{1}{m^{ja} n^{ib}} \right) = 0 \tag{4.7}$$

holds for infinitely many integers $a \in \mathcal{B}$. This implies that

$$\left(\beta_{i_0,j_0} + \sum_{\substack{i,j=0 \\ i \neq i_0, j \neq j_0}}^{M} \beta_{i,j} \frac{1}{m^{ja} n^{ib}} \right) = 0,$$

and if we let $a \to \infty$, we get $\beta_{i_0,j_0} = 0$, which is a contradiction (note that since $a \leq b \leq a+\ell$, as $a \to \infty$, then $b \to \infty$). Therefore, the polynomial in the left hand side of (4.5) is identically zero. Thus, if we let $Y = n^b$ and $X = m^a$, then we get the identity

$$\zeta_1 \frac{Y-1}{X-1} + \zeta_2 \frac{Y^2-1}{X-1} + \cdots + \zeta_k \frac{Y^k-1}{X-1} + \sum_{i,j} \gamma_{i,j} \frac{Y^i}{X^j} = 0$$

in $\mathbb{Q}(X,Y)$. From here, we have that

$$\frac{g(Y)}{X-1} + \frac{h(X,Y)}{X^h} = 0, \tag{4.8}$$

where g and h are polynomials. From (4.8), we get

$$(X-1)h(X,Y) = -X^h g(Y).$$

Since $(X-1) \nmid X^h$, then $(X-1)|g(Y)$ and therefore $g = 0$. Hence $h = 0$, which means that all the coefficients of (4.5) are zero and we get a contradiction. Therefore $d_{a,b} > m^{(1-\varepsilon)a}$ and by Lemma 4.3 we deduce the assertion of Theorem 4.2. □

4.2 Proof of Lemma 4.5

In this section, we give a detailed proof of Lemma 4.5.

Proof. For every $i > k$, $|L_{i,\nu}(\mathbf{x})|_\nu = x_i$. Here x_i is of the form $d_{a,b}u_i$ where u_i is of the form $m^e n^f$, where $e, f \in \mathbb{Z}$. Then, by the product formula we have that $\prod_{\nu\in S}|u_i|_\nu = 1$ and $\prod_{\nu\in S}|d_{a,b}|_\nu \leq |d_{a,b}|_\infty = d_{a,b}$. Therefore, for $i > k$, we have

$$\prod_{\nu\in S}|L_{i,\nu}(\mathbf{x})|_\nu = \prod_{\nu\in S}|d_{a,b}|_\nu \prod_{\nu\in S}|u_i|_\nu \leq d_{a,b}\cdot 1 = d_{a,b}. \tag{4.9}$$

Hence, we can write

$$\begin{aligned}\prod_{\nu\in S}\prod_{i=1}^{N}|L_{i,\nu}(\mathbf{x})|_\nu &= \prod_{\nu\in S}\left(\prod_{i=1}^{k}|L_{i,\nu}(\mathbf{x})|_\nu \cdot \prod_{i=k+1}^{N}|L_{i,\nu}(\mathbf{x})|_\nu\right)\\ &= \prod_{\nu\in S}\prod_{i=1}^{k}|L_{i,\nu}(\mathbf{x})|_\nu \cdot \prod_{i=k+1}^{N}\prod_{\nu\in S}|L_{i,\nu}(\mathbf{x})|_\nu.\end{aligned} \tag{4.10}$$

Therefore, we have

$$\prod_{\nu\in S}\prod_{i=1}^{N}|L_{i,\nu}(\mathbf{x})|_\nu \le \prod_{\nu\in S}\prod_{i=1}^{k}|L_{i,\nu}(\mathbf{x})|_\nu \cdot \prod_{k+1}^{N} d_{a,b} = d_{a,b}^{N-k}\prod_{i=1}^{k}\prod_{\nu\in S}|L_{i,\nu}(\mathbf{x})|_\nu$$
$$= d_{a,b}^{N-k}\left(\prod_{i=1}^{k}|L_{i,\infty}(\mathbf{x})|\right)\prod_{p|mn}\prod_{i=1}^{k}|x_i|_p. \quad (4.11)$$

Again, for $i \le k$ we know that $x_i = d_{a,b}m^{ha}z_i(a,b) = c_{i,a,b}m^{ha}$. We have

$$\prod_{p|mn}|x_i|_p = \prod_{p|mn}|c_{i,a,b}|_p \prod_{p|mn}|m^{ha}|_p \le 1\cdot\prod_{p|mn}|m^{ha}|_p,$$

and therefore, we conclude that

$$\prod_{p|mn}|x_i|_p \le m^{-ha}. \quad (4.12)$$

Also, using (4.3) we have

$$|L_{i,\infty}(\mathbf{x})| = O(d_{a,b}m^{ha}n^{ib}m^{-(h+1)a}) = O(d_{a,b}n^{ib}m^{-a}) \quad (4.13)$$

for $i \le k$.

Therefore, plugging (4.12) and (4.13) in (4.11), we get

$$\prod_{\nu\in S}\prod_{i=1}^{N}|L_{i,\nu}(\mathbf{x})|_\nu = O\Big(d_{a,b}^{N-k}d_{a,b}^{k}m^{-ka}n^{-hka}\prod_{i=1}^{k}n^{ib}\Big) = O\big(d_{a,b}^{N}m^{-hka}n^{bk^2}\big). \quad (4.14)$$

Since $d_{a,b} \le m^{(1-\varepsilon)a}$ for all $a \in \mathcal{B}$ and $N = hk+h+k$, we simplify (4.14) to get

$$\prod_{\nu\in S}\prod_{i=1}^{N}|L_{i,\nu}(\mathbf{x})|_\nu = O(m^{aN}m^{-\varepsilon aN}m^{-hka}n^{bk^2}) = O\Big((m^{h+k}m^{-\varepsilon N})^a n^{bk^2}\Big), \quad (4.15)$$

where the constants depend on m,n,h,k.

Now, let us choose the positive integer k such that $\varepsilon k > 2$. Then since $\varepsilon N > 2h+\varepsilon h+2 >$

$2h$, we have that $m^{\varepsilon N-h-k} > m^{h-k}$. Therefore, (4.15) becomes

$$\prod_{\nu\in S}\prod_{i=1}^{N}|L_{i,\nu}(\mathbf{x})|_\nu = O\big(n^{bk^2}m^{-ha}m^{ka}\big) = O(n^{ak^2}m^{-ha}m^{ka}), \tag{4.16}$$

since $b \le a+\ell$, and k,ℓ are fixed. Next, we choose the positive integer h such that $m^h > 2m^k n^{k^2}$. This implies that $n^{ak^2}m^{-ha}m^{ka} < 2^{-a}$. Hence, (4.16) takes the form

$$\prod_{\nu\in S}\prod_{i=1}^{N}|L_{i,\nu}(\mathbf{x})|_\nu = O(2^{-a}). \tag{4.17}$$

Lastly, since $d_{a,b} < m^a$, then from the definition of $\mathbf{x}$, we can conclude that $\max|x_i| < C^a$, where the constant C depends only on m,n,h,k. Therefore, if we take $\delta < \frac{\log 2}{\log C}$, then for $a \in \mathcal{B}$, (4.17) becomes

$$\prod_{\nu\in S}\prod_{i=1}^{N}|L_{i,\nu}(\mathbf{x})|_\nu < \|\mathbf{x}\|^{-\delta} \tag{4.18}$$

Hence, Theorem 4.1 is satisfied.

□

4.3 A more general version of Theorem 3.4

In Chapter 3, we proved Theorem 3.12, which was an effective analogue of Theorem 3.4. In this section, we use Theorem 4.2 to state and prove a more general version of Theorem 3.4. We have the following theorem.

Theorem 4.6. *Let $\ell \in \mathbb{N}\cup\{0\}$ be fixed. If m and n are coprime integers ≥ 2 with n prime, then there are only finitely many pairs $(a,b) \in \mathbb{N}^2$ with $a > b$ such that $m^a - m^b \big| n^{a+\ell} - n^b$.*

Proof. Let $c = a-b$. Then, since $m^b(m^c-1)\big|n^b(n^{c+\ell}-1)$, we can say that $m^c - 1 = AB$, where $A|n^b$, $\gcd(B,n) = 1$ and $B|(n^{c+\ell}-1)$. We have that $A = n^i$ for some $i \le b$, since n is prime. Since m and n are coprime, they are multiplicatively independent. By Theorem 4.2, we have that

$$\gcd(m^c-1, n^{c+\ell}-1) \ll m^{\varepsilon c},$$

for some $\varepsilon > 0$. Therefore, $B \ll m^{\varepsilon c}$. Hence, we have that

$$\frac{m^c - 1}{m^{\varepsilon c}} \ll n^i. \tag{4.19}$$

Also, since $m^c \equiv 1 \pmod{n^i}$, this implies that $\mathrm{ord}_{n^i}(m) \big| c$. By Lemma 3.11, we know that $n^{i-s} \big| \mathrm{ord}_{n^i}(m)$, where s is defined before Lemma 3.11. Then we can say that $n^i \leq cn^s$. Then (4.19) becomes

$$\frac{m^c - 1}{m^{\varepsilon c}} \ll c, \tag{4.20}$$

since s is fixed. This shows that c is bounded. Again, since $m^b \big| (n^{c+\ell} - 1)$, we conclude that b is bounded, and therefore, a is also bounded. □

We observe that the above proof of Theorem 4.6 is not effective since we have used Theorem 4.2. Nevertheless, we turn to some computational experiments to get a flavor of the number of solutions (a,b) to $m^a - m^b \big| n^{a+\ell} - n^b$ for specific values of m, n, ℓ. In Table A.3, we consider some values of (m,n) and ℓ and record the solutions (a,b) in each case for $1 \leq b < a \leq 10000$.

Bibliography

[1] Alan Baker. Experiments on the *abc*-conjecture. *Publ. Math. Debrecen*, 65(3-4):253–260, 2004.

[2] Yann Bugeaud, Pietro Corvaja, and Umberto Zannier. An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$. *Math. Z.*, 243(1):79–84, 2003.

[3] Geumlan Choi and Alexandru Zaharescu. A class of exponential congruences in several variables. *J. Korean Math. Soc.*, 41(4):717–735, 2004.

[4] Richard K. Guy. *Unsolved problems in number theory*, volume 1 of *Unsolved Problems in Intuitive Mathematics*. Springer-Verlag, New York-Berlin, 1981. Problem Books in Mathematics.

[5] Shanta Laishram and T. N. Shorey. Baker's explicit *abc*-conjecture and applications. *Acta Arith.*, 155(4):419–429, 2012.

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

[7] J.-L. Nicolas and G. Robin. Majorations explicites pour le nombre de diviseurs de N. *Canad. Math. Bull.*, 26(4):485–492, 1983.

[8] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[9] Harry Ruderman and Carl Pomerance. Problems and Solutions: Solutions of Elementary Problems: E2468. *Amer. Math. Monthly*, 84(1):59–60, 1977.

[10] Harry Ruderman and W. Y. Velez. Problems and Solutions: Solutions of Elementary Problems: E2468. *Amer. Math. Monthly*, 83(4):288–289, 1976.

[11] Robert John Rundle. *Generalization of Ruderman's Problem to Imaginary Quadratic Fields*. ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.)–Queen's University (Canada).

[12] A. Schinzel. On primitive prime factors of $a^n - b^n$. *Proc. Cambridge Philos. Soc.*, 58:555–562, 1962.

[13] Wolfgang M. Schmidt. *Diophantine approximations and Diophantine equations*, volume 1467 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1991.

[14] Cameron L. Stewart. On divisors of Lucas and Lehmer numbers. *Acta Math.*, 211(2):291–314, 2013.

[15] Qi Sun and Ming Zhi Zhang. Pairs where $2^a - 2^b$ divides $n^a - n^b$ for all n. *Proc. Amer. Math. Soc.*, 93(2):218–220, 1985.

[16] Marian Vâjâitu and Alexandru Zaharescu. A finiteness theorem for a class of exponential congruences. *Proc. Amer. Math. Soc.*, 127(8):2225–2232, 1999.

Appendix A

Tables

Table A.1: Values of $q_3(k)$ for $1 \leq k \leq 40$

k	$q_3(k)$	k	$q_3(k)$	k	$q_3(k)$	k	$q_3(k)$
1	0.59873	11	0.08153	21	0.00002	31	1.24×10^{-7}
2	0.35848	12	0.96575	22	0.00028	32	0.000006
3	0.21464	13	0.00127	23	0.00035	33	0.000001
4	0.64257	14	0.00076	24	0.00204	34	2.66×10^{-8}
5	0.07694	15	0.00045	25	0.000002	35	0.000001
6	0.32249	16	0.02318	26	0.000001	36	0.22328
7	0.02758	17	0.00016	27	9.66×10^{-7}	37	5.72×10^{-9}
8	0.08257	18	0.013	28	0.00008	38	3.42×10^{-9}
9	0.00988	19	0.00005	29	3.46×10^{-7}	39	2.05×10^{-9}
10	0.06512	20	0.00964	30	0.00049	40	0.00001

Table A.2: Values of $q_{m+1}(k)$ for $3 \leq m \leq 7$ and $1 \leq k \leq 20$

k	$m=3$	$m=4$	$m=5$	$m=6$	$m=7$
1	0.44353	0.35848	0.30392	0.26556	0.23693
2	0.19672	0.38554	0.09236	0.07052	0.16841
3	0.08725	0.04607	0.02807	0.01872	0.0133
4	0.1935	0.04954	0.00853	0.02486	0.04727
5	0.18881	0.06512	0.00259	0.00132	0.00074
6	0.69282	0.13371	0.17101	0.01508	0.03025
7	0.00337	0.00076	0.00023	0.00009	0.00004
8	0.00748	0.00081	0.00007	0.00012	0.00014
9	0.00066	0.00185	0.00042	0.00012	0.000002
10	0.00324	0.00115	0.00007	0.00001	0.00001
11	0.003	0.0000125	0.000002	4.63×10^{-7}	1.32×10^{-7}
12	0.02637	0.00368	0.001752	0.00034	0.00034
13	0.00002	0.000001	1.88×10^{-7}	3.26×10^{-8}	7.41×10^{-9}
14	0.00001	0.00005	0.000001	2.51×10^{-7}	5.27×10^{-9}
15	0.00005	0.00007	1.74×10^{-8}	2.3×10^{-9}	1.29×10^{-8}
16	0.00019	0.000003	9×10^{-8}	5.2×10^{-8}	2.51×10^{-8}
17	9.94×10^{-7}	2.66×10^{-8}	6.58×10^{-7}	1.62×10^{-10}	2.33×10^{-11}
18	0.02823	0.00003	0.000002	3.52×10^{-8}	2.84×10^{-9}
19	1.95×10^{-7}	3.42×10^{-9}	2.84×10^{-8}	1.14×10^{-11}	1.31×10^{-12}
20	0.00002	0.000001	4.97×10^{-10}	8.36×10^{-10}	2.56×10^{-10}

Table A.3: Number of solutions (a,b) for some values of (m,n) and ℓ

(m,n)	$\ell=1$	$\ell=2$	$\ell=5$	$\ell=10$	$\ell=20$	$\ell=100$
$(4,5)$	1	2	1	2	1	1
$(6,7)$	0	1	0	2	0	0
$(10,11)$	0	0	1	1	1	1
$(12,14)$	0	0	0	0	0	0
$(13,16)$	1	2	1	1	2	1
$(14,19)$	0	0	0	3	0	0
$(15,22)$	0	0	0	0	0	0
$(17,25)$	0	0	0	0	0	0
$(19,29)$	0	0	0	0	0	0
$(20,31)$	0	0	1	1	0	1