SOME CASES OF GENERALIZED FERMAT EQUATION

by

Altan Erdoğan

B.S., Mathematics, Boğaziçi University, 2005

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Mathematics

Boğaziçi University

2008

To Cansu Şipal,

your presence is everything for me...

ACKNOWLEDGEMENTS

It was an honor to have Cem Yalçın Yıldırım as my thesis supervisor. I started to realize the beautiful world hidden in number theory as I tried to follow his way of understanding mathematics during the number theory courses and my thesis study. I am deeply thankful for his guidance, support and endless patience he showed me throughout the years I spent in the department.

I would like to express my sincere gratitude to my advisor Alp Eden not only for his endless support and patience he showed me during my graduate program but also for his guidance which greatly contributed to my future plans in mathematics.

I thank to all other members of mathematics department for their contributions to such a supporting, motivating and encouraging ambient of this department.

I also thank Nihat Sadık Değer and İlhan İkeda for reading my draft and participating in my thesis committee.

I am thankful to all of my officemates for the unforgottable years we spent with frienship, support and efforts for the will of mathematics.

Finally, I am grateful to my parents Saliha and İsmail Erdoğan for their support throughout my education.

ABSTRACT

SOME CASES OF GENERALIZED FERMAT EQUATION

This thesis presents a classification of some cases of generalized Fermat equation and applications of elementary methods to these equations in order to find integer solutions to these equations. Applications of some more recent and advanced methods for some equations where elementary methods do not work are also presented. The classification consists of three cases. The solution sets of equations in the first two cases are completely determined. The third case where Fermat equation is included still contains unsolved problems. Applications of elementary methods to some of the equations in this case and some open problems related to this case are presented in the last chapter of the thesis.

ÖZET

GENELLEŞTİRİLMİŞ FERMAT DENKLEMİNİN BAZI DURUMLARI

Bu tezde genelleştirilmiş Fermat denkleminin belirli durumlarının sınıflandırılması ile bu durumların tamsayılar üzerindeki çözüm kümelerinin bulunması için basit yöntemlerin uygulamaları verilmektedir. Basit yöntemlerin uygulanamadığı durumlar için daha yeni ve gelişmiş yöntemlerin uygulamaları da incelenmektedir. Sınıflandırma üç duruma göre yapılmıştır. İlk iki durumdaki denklemlerin çözüm kümeleri tamamen bulunmuştur. Fakat Fermat denkleminin de dahil olduğu üçüncü durum ise henüz cevaplanmamış sorular içermektedir. Tezin son bölümünde bu duruma ait olan denklemlerin bazıları için basit yöntemlerin uygulamaları ve bu durumla ilişkili cevaplanmamış soruların bir kısmı yer almaktadır.

TABLE OF CONTENTS

1. INTRODUCTION

Fermat's last theorem says that the Diophantine equation

$$x^p + y^p = z^p$$

has no non-zero integer solutions for integer $p \geq 3$. This equation is a special case of the so-called generalized Fermat equation

$$Ax^p + By^q = Cz^r \tag{1.0.1}$$

where A, B and C are non-zero integers and $p, q, r \in \mathbb{Z}_{>1}$. Here, recent works on the last equation will be presented and some special cases of (1.0.1) will be solved. In the case where $A = B = C = 1$, the equation (1.0.1) may have no solution in integers, finitely many solutions or infinitely many solutions for different values of (p, q, r). We need to make a definition to specify which solutions we are looking for. For instance, $(x, y, z) = (2^{4k+1}, 2^{4k+1}, 2^{3k+1})$ gives a solution for the Diophantine equation $x^3 + y^3 = z^4$ for any nonnegative integer k. But such a parametric solution in which x, y and z are not pairwise coprime can be found for many similar equations, and so we omit such solutions. Also we need to omit solutions involving 0. We make the following definition to specify the solution sets for the case $A = B = C = 1$.

Definition 1.1. *Let p, q and r be positive integers greater than or equal to 2. Any solution in integers (x, y, z) to the equation $x^p + y^q = z^r$ is called a trivial solution if one of the following holds:*

1. $\gcd(x, y, z) > 1$
2. $\{x, y, z\} \cap \{0\} \neq \emptyset$

Remark 1.1. *We take $A = B = C = 1$ in this definition. Otherwise solutions in which x, y and z are not pairwise coprime should also be considered.*

We shall classify (1.0.1) with respect to the powers p, q and r as done in [1] by F. Beukers. The classification into three parts will be according to the sum of reciprocals of p, q and r.

1. Hyperbolic Cases

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

2. Euclidean Cases

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1.$$

3. Spherical Cases

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1.$$

The hyperbolic cases are the most challenging ones and there are still open problems related to equations in hyperbolic cases. The solution sets for the equations in euclidean and spherical cases are completely determined. Some of the equations in Euclidean and Spherical cases are shown to have no nontrivial solutions, and the nontrivial solution sets of others are completely characterized, i.e. shown to have finitely many solutions or parametric solutions in two variables. There is a similar situation for some equations belonging to the hyperbolic cases. Some Diophantine equations of small degrees in the hyperbolic case are shown to have no nontrivial solutions. Proofs of these are given in Chapter 5. But one of the most important results for the hyperbolic cases is given by A. Granville and

H. Darmon in [2], where it is proved that only finitely many nontrivial solutions exist for (1.0.1) for any choice of A, B and C with $ABC \neq 0$.

The first chapter is a review of quadratic fields. We will use quadratic fields many times in later sections. The chapters coming after this chapter include some Diophantine equations for the Euclidean, Spherical and Hyperbolic cases. Since A, B and C can take any arbitrary integer values in fact we have an infinite set of Diophantine equations for all three cases and the values of A,B and C determine the number of solutions as well as the existence of solutions. In our thesis we shall be concerned with the case $A = B = C = 1$.

Before going into the chapters, nontrivial solutions for the Pythagorean case should be given. This is well-known, but it will be used in some other Diophantine equations and we include it for sake of completeness. We now find the nontrivial integer solutions of the equation

$$x^2 + y^2 = z^2.$$

Since $\gcd(x, y, z)$=1 we have that exactly two variables among x, y and z must be odd. Since the sum of squares of two odd integers is $\equiv 2 \pmod 4$, we see that z must be odd. Without loss of generality we assume that x is odd and y is even. We can write the above equation as

$$(z - x)(z + x) = y^2.$$

Now $(z - x)$ and $(z + x)$ are both even. But we must have $\gcd(z - x, z + x)$=2, otherwise we would have a contradiction since $\gcd(z, x)$=1. So if we say $y = 2w$, we have that

$$\left(\frac{z - x}{2}\right)\left(\frac{z + x}{2}\right) = w^2.$$

But then each of the two factors in the left-hand side of the last equation must be the square of some integer. So we have

$$z - x = 2a^2,$$
$$z + x = 2b^2$$

for some positive integers a and b with $\gcd(a, b)$=1. Note that since z and x are both odd, exactly one of a and b must be even. Hence we have a solution given by

$$z = a^2 + b^2$$
$$x = b^2 - a^2$$
$$y = 2ab$$

where $\gcd(a, b)$=1.

For the case of $p = q = r = 2$ we have used a very important property of integers, the unique factorization property. In many cases we can not factorize the equation in $\mathbb{Z}$ or factorization over $\mathbb{Z}$ does not help. Then for each equation we work with the integers of number fields, i.e. field extensions of rationals and see whether unique factorization works there. But if unique factorization does not work in that number field, one can apply ideal class theory for such number fields. In the next chapter we introduce basic aspects of quadratic number fields.

2. QUADRATIC FIELDS

We will restrict this section to quadratic fields for our future purposes. We use the notation and definitions of [3]. A *quadratic field* is one of the form $\mathbb{Q}(\xi)$ where ξ is a root of a polynomial of degree two which is irreducible over $\mathbb{Q}$. The elements of such a field are the totality of the numbers of the form $a_0 + a_1\xi$ where a_0 and a_1 are rational numbers. Since ξ is of the form $(a + b\sqrt{m})/c$ where a, b, c and m are integers we see that

$$\mathbb{Q}(\xi) = \mathbb{Q}(a + b\sqrt{m}) = \mathbb{Q}(\sqrt{m}).$$

Here we assume that m is a square-free integer and not equal to 1. So it is reasonable to define a quadratic field by m instead of ξ. Below we state theorems and definitions from [3] to characterize the integers and primes of a quadratic field.

Theorem 2.1. *Let $\mathbb{Q}(\sqrt{m})$ be a quadratic field where m may be a positive or negative square-free integer other than 1. Numbers of the form $a + b\sqrt{m}$ with rational integers a and b are integers of $\mathbb{Q}(\sqrt{m})$. These are the only integers of $\mathbb{Q}(\sqrt{m})$ if $m \equiv 2$ or 3 (mod 4). If $m \equiv 1$ (mod 4), then the numbers $(a + b\sqrt{m})/2$ with odd rational integers a and b are also integers of $\mathbb{Q}(\sqrt{m})$, and there are no further integers.*

Definition 2.1. *The norm $N(\alpha)$ of a number $\alpha = (a + b\sqrt{m})/c$ in $\mathbb{Q}(\sqrt{m})$ is the product of α and its conjugate $\bar{\alpha} = (a - b\sqrt{m})/c$,*

$$N(\alpha) = \alpha\bar{\alpha} = \frac{a^2 - b^2 m}{c^2}$$

Definition 2.2. *Any divisor of the integer 1 is called a unit of the quadratic field $\mathbb{Q}(\sqrt{m})$. Nonzero integers α and β are called associates if α/β is a unit.*

Immediate consequences of the previous definition are that the reciprocal of a unit is

also a unit and the units of a quadratic field form a multiplicative group.

Theorem 2.2. *The norm of a product equals the product of the norms, $N(\alpha\beta) = N(\alpha)N(\beta)$. $N(\alpha) = 0$ if and only if $\alpha = 0$. The norm of an integer of $\mathbb{Q}(\sqrt{m})$ is a rational integer. The norm of an integer in $\mathbb{Q}(\sqrt{m})$ is equal to ± 1 if and only if it is a unit.*

We give a characterization for primes of a quadratic field.

Definition 2.3. *An integer α in a quadratic field $\mathbb{Q}(\sqrt{m})$ is called a prime if it is divisible only by its associates and the units of the field.*

Remark 2.1. *This definition is how primes are defined in [3]. An element satisfying the conditions of the above definition are called as 'irreducible' in many sources. Alternatively the definiton of primes can be given as: 'If whenever π divides $\alpha\beta$, then either π divides α or π divides β, we call π a prime'. So according to such definitions, in general if π is a prime then it is irreducible, but not vice versa always. If the field $\mathbb{Q}(\sqrt{m})$ has the unique factorization property then these are the same concepts. But since we use only the quadratic fields with unique factorization property in later chapters, Definition 2.3 is suitable.*

Now we can use quadratic fields as we used the set of rational integers $\mathbb{Z}$ to find the Pythagorean triples. But there is a great obstacle here. Any number in $\mathbb{Z}$ can be factorized into prime(s) powers in a unique way up to order of the primes. But this is not true for an arbitrary quadratic field.

Definition 2.4. *A quadratic field $\mathbb{Q}(\sqrt{m})$ is said to have unique factorization property if every integer α in $\mathbb{Q}(\sqrt{m})$, not zero or a unit, can be factored into primes uniquely up to multiplications by units and order of the prime factors.*

It is not an easy question to determine whether a quadratic field has unique factorization property or not. The following theorem from [4] provides a way to determine some of them.

Theorem 2.3. *Every Euclidean quadratic field has unique factorization property.*

The above theorem is useful but the disadvantage of it is that there are only a finite number of integers m such that $\mathbb{Q}(\sqrt{m})$ is a norm-Euclidean quadratic field as quoted below from [4].

Theorem 2.4. *The only norm-Euclidean quadratic fields, $\mathbb{Q}(\sqrt{m})$ are of those such that m equals to one of the following:*

$$-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

We should note that this list does not contain all of the quadratic fields possessing unique factorization property. There are quadratic fields which are not Euclidean but which has unique factorization property. For $m < 0$ all of these are known: $m = -19, -43, -67, -163$. The question of determining all real quadratic fields $\mathbb{Q}(\sqrt{m})$, $m > 0$, with unique factorization property is still open. It is conjectured that there are infinitely many such fields. Below is a list of all square-free numbers $2 \leq m \leq 100$ such that $\mathbb{Q}(\sqrt{m})$ has the unique factorization property:

$$2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61,$$
$$62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97.$$

Now if we are 'lucky' enough we can attack the problem by finding an appropriate m such that (1.0.1) with $A = B = C = 1$ can be factorized over the ring of integers of $\mathbb{Q}(\sqrt{m})$ having the unique factorization property. In fact we will see that many of the equations with $\max\{p, q, r\} = 4$ can be worked on by this method.

Below we give further results on integers and primes of a quadratic field $\mathbb{Q}(\sqrt{m})$.

These are simple results which will be used in later sections.

Lemma 2.1. *Let α and β be two integers in $\mathbb{Q}(\sqrt{m})$. If β divides α, then $\bar{\beta}$ divides $\bar{\alpha}$.*

Proof. We write $\alpha = \beta\gamma$ for some integer γ in $\mathbb{Q}(\sqrt{m})$. Then $\bar{\alpha} = \bar{\beta}\bar{\gamma}$. □

Lemma 2.2. *If π is a prime and ϵ is a unit in $\mathbb{Q}(\sqrt{m})$, then $\epsilon\pi$ is also a prime*

Proof. Assume that π is an integer and ϵ is a unit in $\mathbb{Q}(\sqrt{m})$. Also suppose that $\epsilon\pi$ is not a prime. Then there exist non-unit integers β and γ in $\mathbb{Q}(\sqrt{m})$ such that $\epsilon\pi = \beta\gamma$. Since ϵ is a unit, so is $1/\epsilon$. Multiplying both sides by $1/\epsilon$ we get that π is not a prime. □

Lemma 2.3. *An integer α in $\mathbb{Q}(\sqrt{m})$ is a prime if and only if $\bar{\alpha}$ is a prime.*

Proof. First we will show that $\alpha/\bar{\alpha}$ is a unit by cheking its norm. We have

$$N\left(\frac{\alpha}{\bar{\alpha}}\right) = N\left(\frac{\alpha^2}{N(\alpha)}\right) = \frac{N(\alpha)^2}{N(\alpha)^2} = 1.$$

By the previous lemma the proof is completed. □

Now we consider a quadratic field $\mathbb{Q}(\sqrt{m})$ with unique factorization property. Take any integer α in $\mathbb{Q}(\sqrt{m})$. Up to multiplication by units and order, we can factorize α into prime powers as

$$\alpha = \pi_1^{k_1}.....\pi_n^{k_n}$$

where all the π_i are prime for $i = 1, 2, ..., n$. Then by the above lemmas we obtain the factorization of $\bar{\alpha}$ into prime powers as

$$\bar{\alpha} = \bar{\pi_1}^{k_1}.....\bar{\pi_n}^{k_n}.$$

3. EUCLIDEAN CASES

In these cases we can list the possibilities for the set $\{p, q, r\}$. Since the sum of reciprocals of p, q and r is equal to 1, at least one of these powers must be less than 4. Without loss of generality we can say that p is smaller than 4 which results in two cases.

Case 1: $p = 2$. We have that

$$\frac{1}{q} + \frac{1}{r} = \frac{1}{2}$$

So at least one of q and r, say q must be smaller than 5. Since $q = 2$ is impossible, we only have two possibilities that $q = 3$ or $q = 4$. Hence the set $\{p, q, r\}$ must be equal to one of $\{2,3,6\}$ and $\{2,4,4\}$

Case 2: $p = 3$. We have

$$\frac{1}{q} + \frac{1}{r} = \frac{2}{3}$$

By a similar argument we have that at least one of q and r must be smaller than 4. Without loss of generality say $q < 4$. The case of $q = 2$ gives the set $\{3,2,6\}$ where the case $q = 3$ gives the set $\{3,3,3\}$.

Hence the Euclidean case includes only finitely many choices for the set $\{p, q, r\}$ and the corresponding Diophantine equations to such choices are

$$x^3 + y^3 = z^3,$$
$$x^2 + y^4 = z^4,$$
$$x^4 + y^4 = z^2,$$
$$x^2 + y^3 = z^6,$$
$$x^2 + y^6 = z^3.$$

We could also have included the equation $x^3 + y^6 = z^2$. But if there is a nontrivial solution in integers to this equation, say (a, b, c) then we would have a nontrivial solution in integers for $x^2 + y^3 = z^6$ given by $(x, y, z) = (c, -a, b)$. So it will be enough to look for the nontrivial solutions in integers of just one of these two equations.

Now we will look for the solution sets for these equations given the triple (p, q, r).

3.1. Case of (3,3,3)

We will show that the equation

$$x^3 + y^3 = z^3 \tag{3.1.1}$$

has no solutions in integers. The first proof was given by L. Euler. Here we will combine two alternative proofs; one of them uses unique factorization property of $\mathbb{Q}(\sqrt{-3})$ (which can be found in [3]) and the other one uses a very elementary way (which can be found in [5]). But here we give a proof combining these two alternative proofs. First we state a lemma which is necessary in the proof.

Lemma 3.1. *Let a and b be relatively prime nonnegative integers such that $a^2 + 3b^2 = s^3$ for some integer s. Then there are integers u and v such that $s = u^2 + 3v^2$, $a = u^3 - 9uv^2$ and $b = 3u^2v - 3v^3$.*

The proof of this lemma (in fact a more general version) is given by induction on the number of (not necessarily distinct) prime divisors of s in [5]. It uses elementary techniques. But here we will give a shorter proof using unique factorization property of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$.

Proof. First we note that a and b can not be both odd. Since then s would be even and we have $a^2 + 3b^2 \equiv 4 \pmod 8$ whereas $s^3 \equiv 0 \pmod 8$. So a and b should have different parities. We can factorize $a^2 + 3b^2 = s^3$ as

$$(a + b\sqrt{-3})(a - b\sqrt{-3}) = s^3$$

in the quadratic field $\mathbb{Q}(\sqrt{-3})$. By Theorem 2.4, $\mathbb{Q}(\sqrt{-3})$ has the unique factorization property. Also by Theorem 2.1 we know that the integers of $\mathbb{Q}(\sqrt{-3})$ are of the form $(r + k\sqrt{-3})/2$, where r and k are both even or odd rational integers. By the results we found in Chapter 2, we see that the prime factors of $a + b\sqrt{-3}$ and $a - b\sqrt{-3}$ are in a one-to-one correspondence, i.e. (not necessarily distinct) prime factors of $a + b\sqrt{-3}$ and $a-b\sqrt{-3}$ are conjugates of each other. But if $a+b\sqrt{-3}$ is divisible by a prime $(r+k\sqrt{-3})/2$ then so is s^3. So we deduce that in fact the cube of $(r + k\sqrt{-3})/2$ divides $a + b\sqrt{-3}$ (Here we should consider that $a + b\sqrt{-3}$ and $a - b\sqrt{-3}$ are associates. Thus $(r + k\sqrt{-3})/2$ also divides $a - b\sqrt{-3}$. But since the power of s is odd, the last statement follows). But if r and k are both odd then we have

$$\left(\frac{r + k\sqrt{-3}}{2}\right)^3 = \frac{r^3 - 9rk^2}{8} + \frac{(3r^2k - 3k^3)\sqrt{-3}}{8}$$

But since r and k are both odd, we have that $r^3 - 9rk^2 = 8t$ and $3r^2k - 3k^3 = 8w$ for some rational integers t and w. So we have

$$\left(\frac{r + k\sqrt{-3}}{2}\right)^3 = t + w\sqrt{-3}.$$

Now by collecting (not necessarily distinct) prime divisors of $a + b\sqrt{-3}$ we have that

$$a + b\sqrt{-3} = (u + v\sqrt{-3})^3,$$
$$a - b\sqrt{-3} = (u - v\sqrt{-3})^3,$$
$$s = (u + v\sqrt{-3})(u - v\sqrt{-3})$$

for some rational integers u and v. By equating the real and imaginary parts of the above equations we get the desired result. □

Now we can state and prove our theorem. The proof of the theorem below is given by [5].

Theorem 3.1. *$x^3 + y^3 = z^3$ has no solutions in nonzero integers.*

Proof. Assume that there is a solution in nonzero integers. Among all of the solutions we take a solution (x, y, z) which makes $|xyz|$ as small as possible. Since $\gcd(x, y, z)=1$ only one of them can be even. By rearranging the equation we can stipulate that z is even and the others are odd.

Now let $u = \frac{1}{2}(x + y)$ and $w = \frac{1}{2}(x - y)$. Since $\gcd(x, y)=1$, we have that u and w can not be both odd. Also we have that $2u^3 + 6uw^2 = 2u(u^2 + 3w^2) = z^3$. Now we will solve two cases according to whether 3 divides u or not.

Case I: $3 \nmid u$. Since u and w have different parities, $u^2 + 3w^2$ must be odd. Also we have that $\gcd(2u, u^2 + 3w^2)=1$. So there are integers t and s such that $2u = t^3$ and $u^2 + 3w^2 = s^3$. By the lemma stated above, there exist integers a and b such that $u = a^3 - 9ab^2 = a(a-3b)(a+3b)$ and $w = 3a^2b - 3b^3 = 3b(a-b)(a+b)$. Since $\gcd(u, w)=1$, it follows that $\gcd(a, 3b)=1$ and the parities of a and b are different. So $\gcd(a - 3b, a + 3b)=1$.

Since $t^3 = 2u = 2a(a-3b)(a+3b)$, it follows that there are integers c, d and e such that $2a = c^3$, $a - 3b = d^3$ and $a + 3b = e^3$. Thus $d^3 + e^3 = c^3$ and $|cde| \neq 0$. But then

$$|cde|^3 = |2u| = |x + y| < |z|^3 < |xyz|^3$$

which contradicts the choice of (x, y, z).

Case II: $3 \mid u$. Let $u = 3v$ for some integer v. Now we have $18v(3v^2 + w^2) = z^3$. Since $u = 3v$ and w have different parities, $3v^2 + w^2$ is odd. Also we have that $\gcd(18v, 3v^2 + w^2)$=1. So there are integers t and s such that $18v = t^3$ and $3v^2 + w^2 = s^3$. By the lemma above we conclude that there are integers a and b such that $w = a^3 - 9ab^2 = a(a-3b)(a+3b)$ and $v = 3a^2b - 3b^3 = 3b(a-b)(a+b)$. Since $\gcd(u, w)$=1 we have that a and b have different parities. So $a + b$ and $a - b$ are both. Also we know that $\gcd(a, b)$=1 which implies $\gcd(a - b, a + b)$=1. We write $18v = t^3 = 3^3 2b(a-b)(a+b)$. So there are integers c, d and e such that $2b = c^3$, $a - b = d^3$ and $a + b = e^3$. Thus $e^3 = c^3 + d^3$. But we have $cde \neq 0$ and

$$|cde|^3 = |2v/3| = |2u/9| < |xyz|^3$$

which gives the same contradiction as in the first case. □

3.2. Case of (2,4,4)

We will show that the Diophantine equation

$$x^2 + y^4 = z^4 \tag{3.2.1}$$

has no nontrivial solutions in positive integers.

Since we are looking for nonnegative pairwise coprime integer solutions to (3.2.1), exactly two of x, y and z must be odd. But x and y can not be both odd. This can be seen easily by considering the equation in (mod 4). So we have two cases; x can be odd or x can be even.

Suppose that we have a solution (x, y, z) to (3.2.1) with x being even. By applying the Pythagorean solutions to (3.2.1) we have $x = 2uv$, $y^2 = u^2 - v^2$ and $z^2 = u^2 + v^2$ for some integers u and v having different parities and with $\gcd(u, v)$=1. But then we have $(yz)^2 = u^4 - v^4$. So if we have a solution to (3.2.1) with x being even, then we get a new solution (yz, v, u) to the same equation. But yz is odd, and thus it suffices to prove that (3.2.1) does not have any solutions in integers (x, y, z) where x is an odd integer.

Now we suppose that there is a solution (x, y, z) in which x is odd. Among all of the solutions we choose one of the solutions in which z is as small as possible. Again by applying Pythagorean solutions to (3.2.1) we get $y^2 = 2uv$, $x = u^2 - v^2$ and $z^2 = u^2 + v^2$ for some integers u and v having different parities and with $\gcd(u, v)$=1. Without loss of generality we assume that u is even and v is odd. Since $y^2 = 2uv$, it follows that $u = 2a^2$ and $v = b^2$ for some relatively prime integers a and b. Putting these values of u and v we get

$$z^2 = b^4 + 4a^4$$

Applying Pythagorean solutions to the last equation we get $z = e^2 + f^2$, $2a^2 = 2ef$ and $b^2 = e^2 - f^2$ for some relatively prime integers e and f with different parities. Note that since z is odd, we have that b is odd, and thus e must be odd and f must be even. But since $2a^2 = 2ef$, it follows that $e = t^2$ and $f = s^2$ for some integers t and s. Putting these values for e and f in $b^2 = e^2 - f^2$ we get

$$b^2 + s^4 = t^4$$

where t is an odd integer. But also we have $t < e < z$ which contradicts the way we have chosen z. Hence we get the desired result.

3.3. Case of (4,4,2)

We can also show that the Diophantine equation for which $x^4+y^4 = z^2$ has no solution by a similar descent technique used in the previous section. The nontrivial solutions of

$$x^4 + y^4 = z^2 \tag{3.3.1}$$

must be of the form

$$x^2 = a^2 - b^2$$
$$z = a^2 + b^2$$
$$y^2 = 2ab$$

for some positive integers a and b where a and b have different parities. But it can easily be seen that a must be odd and b must be even by considering the first equation in modulo 4. Here also without loss of generality we assumed that x is odd and y is even. Since any common divisor of a and b would also divide $\gcd(x, y)$=1, we conclude that

$$a = c^2$$
$$b = 2d^2$$

for some positive integers c and d. Then we have

$$x^2 = (c^2)^2 - (2d^2)^2.$$

So

$$c^2 = e^2 + f^2$$
$$2d^2 = 2ef$$
$$x = e^2 - f^2$$

where e and f are positive integers having different parities. So e and f must be perfect squares since they are relatively prime. Let

$$e = k^2$$
$$f = l^2.$$

But then we have

$$c^2 = k^4 + l^4$$

which is also a solution for (3.3.1). Now we assume that there exists some nontrivial solutions to (3.3.1). Then we pick one of the solutions in which z is as small as possible. But then we get the last equation with the relation $c < a < z$ contradicting the choice of z. This proves that (3.3.1) can not have a nontrivial solution in integers (x, y, z).

3.4. Case of (2,3,6)

We will prove that the equation

$$x^2 + y^3 = z^6 \tag{3.4.1}$$

has only $(x, y, z) = (\pm 3, -2, \pm 1)$ as nontrivial solutions in integers. We will use the lemma below in the proof.

Lemma 3.2. *The only nontrivial integer solutions of the equation*

$$x^3 + y^3 = 2z^3 \tag{3.4.2}$$

are those such that $(x, y, z) = (1, 1, 1)$ *and* $(x, y, z) = (-1, -1, -1)$.

Proof. First we observe that x and y must be odd. We assume that there exists a nontrivial solution to (3.4.2). Among these solutions we choose one which makes $|xyz|$ as small as possible and with $(x, y, z) \neq (1, 1, 1)$ or $(x, y, z) \neq (-1, -1, -1)$. So $|xyz| \geq 2$.We put

$$u = \frac{x + y}{2}, \;\; w = \frac{x - y}{2}.$$

We note that u and w have different parities and $\gcd(u, w)$=1. We put $x = u + w$ and $y = u - w$ in (3.4.2) and get

$$z^3 = u(u^2 + 3w^2).$$

Now we have two cases and we treat them seperately.

Case I: $3 \nmid u$. Since u is not divisible by 3, we have that $\gcd(u, u^2 + 3w^2)$=1. Then there exist integers s and t such that $u^2 + 3w^2 = s^3$ and $u = t^3$. By Lemma 3.1 we have that

$$\begin{aligned} u &= A^3 - 9AB^2 \\ w &= 3A^2B - 3B^3 \\ s &= A^2 + 3B^2 \end{aligned}$$

for some integers A and B having different parities and with $\gcd(A, B)$=1. Now we put $u = t^3$ in the first equation above and get

$$t^3 = A(A - 3B)(A + 3B).$$

Since A and B have different parities and 3 can not divide A, the three factors on the right-hand side of the last equation are pairwise coprime. So there are integers K, L and M such that

$$\begin{aligned} A &= K^3 \\ A - 3B &= L^3 \\ A + 3B &= M^3. \end{aligned}$$

So we get $2K^3 = L^3 + M^3$. This equation has the same form with (3.4.2). But if $|x|$ and $|y|$ are not equal to 1, we observe that

$$|KLM|^3 = |u| = \frac{|x + y|}{2} < |xyz|^3,$$

contradicting the choice of the solution (x, y, z).

Case II: $3 \mid u$. We let $u = 3v$. Then we have $z^3 = 9v(3v^2 + w^2)$. Since $\gcd(9v, 3v^2 + w^2) = 1$, there are integers t and s such that

$$\begin{aligned} 9v &= t^3 \\ 3v^2 + w^2 &= s^3. \end{aligned}$$

By Lemma 3.1 there are relatively prime integers A and B such that

$$\begin{aligned} w &= A^3 - 9AB^2 \\ v &= 3A^2B - 3B^3. \end{aligned}$$

Also A and B have different parities. Then we get

$$t^3 = 9v = 27B(A+B)(A-B).$$

So there are integers K, L and M such that

$$\begin{aligned} B &= K^3 \\ A+B &= L^3 \\ A-B &= M^3. \end{aligned}$$

Thus we have the equation $2K^3 = L^3 + M^3$ which has the same form with (3.4.2). But again we have

$$|KLM|^3 = \frac{|t|^3}{27} = \frac{|v|}{3} = \frac{|u|}{9} = \frac{|x+y|}{18} < |xyz|^3,$$

contradicting the way we have chosen (x, y, z). Note that the inequality comes from the fact that $|x+y| \leq 2\max\{|x|, |y|\} < |xyz|^3$ since we have assumed that $|xyz| \geq 2$. □

Now we can prove that (3.4.1) has no nontrivial solutions in integers (x, y, z). First we write (3.4.1) as

$$y^3 = (z^3 - x)(z^3 + x).$$

First we assume that y is even. Then $(z^3 - x)$ and $(z^3 + x)$ have a common factor which is 2. But since gcd(x, z)=1, we have that gcd$(z^3 - x, z^3 + x)$=2. Now we let $2^k||y$. Then we have two possibilities, namely;

$$\left(\frac{y}{2^k}\right)^3 = \left(\frac{z^3 - x}{2^{3k-1}}\right)\left(\frac{z^3 + x}{2}\right)$$

or

$$\left(\frac{y}{2^k}\right)^3 = \left(\frac{z^3 - x}{2}\right)\left(\frac{z^3 + x}{2^{3k-1}}\right)$$

where $k \geq 1$. In both cases the two factors on the right-hand side of each equation are relatively prime. For the first case, we have

$$\begin{aligned} z^3 - x &= 2^{3k-1}a^3 \\ z^3 + x &= 2b^3 \end{aligned}$$

for some integers a and b. Adding up these two equations and dividing by 2, we get

$$z^3 + (-b)^3 = 2(2^{k-1}a)^3.$$

Similarly we get an equation of the same form for the second possibility. But by Lemma (3.2) we know that the last equation has the only solutions $|z| = |b| = 1$. So we have the solutions $(x, y, z) = (\pm 3, -2, \pm 1)$.

Now we assume that y is odd. Then we have gcd$(z^3 + x, z^3 - x)$=1 and so there are

integers c and d such that

$$z^3 - x = c^3$$
$$z^3 + x = d^3.$$

Then adding up these two equations we get $c^3 + d^3 = 2z^3$ which has the only nontrivial solutions as $|c| = |d| = 1$. But this does not give any nontrivial solutions to (3.4.1). This completes the proof.

3.5. Case of (2,6,3)

We will prove that the equation

$$x^2 + y^6 = z^3 \tag{3.5.1}$$

has no nontrivial solutions in integers. In order to complete the proof we will need the following result which is similar to Lemma 3.1.

Lemma 3.3. *Let a and b be relatively prime integers such that $a^2+b^2 = c^3$ for some integer c. Then there are integers u and v such that $c = u^2+v^2$, $a = u^3-3v^2u$ and $b = 3u^2v-v^3$.*

Proof. We factorize the equation $a^2 + b^2 = c^3$ in $\mathbb{Q}(i)$ as

$$(a + ib)(a - ib) = c^3.$$

By Chapter 2 we know that $\mathbb{Q}(i)$ has unique factorization property and the integers of $\mathbb{Q}(i)$ are of the form $g + ih$ where g and h are rational integers. Also we see that a and b have different parities by considering $a^2 + b^2 \equiv c^3 \pmod 4$. The only common divisor of $a + ib$ and $a - ib$ should be a divisor of 2 in $\mathbb{Q}(i)$. But $2 = -i(1 + i)^2$ and $N(1 + i) = 2$ which

implies that $1+i$ is a prime in $\mathbb{Q}(i)$. So the common divisor can only be an associate of $1+i$. But we can easily see that $(a+ib)/(1+i)$ is not an integer in $\mathbb{Q}(i)$. So both of $a+ib$ and $a-ib$ are cubes of some integers in $\mathbb{Q}(i)$. We write

$$a+ib = (u+iv)^3$$
$$a-ib = (u-iv)^3$$

for some rational integers u and v. By equating real and imaginary parts we complete the proof. □

Lemma 3.4. *Let r and s be relatively prime integers of different parities. Then the equation $y^3 = s^3 - 3r^2s$ has no nontrivial solution in integers (y, r, s).*

Proof. Suppose that the equation $y^3 = s^3 - 3r^2s$ has at least one nontrivial solution in integers (y, r, s). Among the solutions we pick one of them which makes $|y|$ as small as possible. We write $y^3 = s(s^2 - 3r^2)$ and deal with two cases.

Case I: $3 \nmid s$. Now we have $\gcd(s, s^2 - 3r^2)$=1, so there are integers t and v such that $s = t^3$ and $s^2 - 3r^2 = v^3$. Factorizing over $\mathbb{Q}(\sqrt{3})$ we have

$$(s - r\sqrt{3})(s + r\sqrt{3}) = v^3.$$

We know that $\mathbb{Q}(\sqrt{3})$ has unique factorization property. Since r and s have different parities, by Chapter 2 we can find integers k and l such that $s \pm r\sqrt{3} = (k \pm l\sqrt{3})^3$. Also we note that k and l have different parities and $\gcd(k, l)$=1. By equating coefficients and putting $s = t^3$, we get

$$t^3 = s = k^3 + 9kl^2 = k(k^2 + 9l^2).$$

But since s is not divisible by 3, we have $\gcd(k, k^2 + 9l^2)$=1. Then we can find integers e and f such that $k = e^3$ and $k^2 + 9l^2 = f^3$. Again e and f have different parities and $\gcd(e, f)$=1. Now we use $\mathbb{Q}(i)$ once more to factorize the last equation and get

$$(k - 3il)(k + 3il) = f^3.$$

But $\gcd(k, 3l)$=1 and so there are integers g and h with $k \pm 3il = (g \pm ih)^3$. Thus we have the equation

$$k = e^3 = g^3 - 3gh^2$$

which has the same form with $y^3 = s^3 - 3r^2s$. But here we have

$$|e|^3 = |k| < |s| = |t|^3 \leq |tv|^3 = |y|^3,$$

and this contradicts the choice of y.

Case II: $3 \mid s$. Now r is not divisible by 3, so from $(-y)^3 = s(3r^2 - s^2)$ we get $s = 3^2t^3$ and $3r^2 - s^2 = 3v^3$ for some relatively prime integers t and v. We put $s = 3u$ and get $r^2 - 3u^2 = v^3$. Factorizing over $\mathbb{Q}(\sqrt{3})$ we have

$$(r - u\sqrt{3})(r + u\sqrt{3}) = v^3.$$

Then there are integers k and l such that $r \pm u\sqrt{3} = (k \pm l\sqrt{3})^3$. Also we note that k and l have different parities and $\gcd(k, l)$=1. By equating coefficients and since $u = 3t^3$ we get

$$u = 3t^3 = 3k^2l + 3l^3,$$

or

$$t^3 = k^2 l + l^3 = l(k + il)(k - il).$$

Then there are integers e, g and h such that $l = e^3$ and $k \pm il = (g \pm ih)^3$. Combining these results we get the equation

$$e^3 = 3g^2 h - h^3.$$

Here if e is not divisible by 3, we get an equation with the same form of the previous case (We just need to write the equation as $e^3 = (-h)^3 - 3g^2(-h)$). But if e is divisible by 3, we have the same form with $(-y)^3 = 3r^2 s - s^3$. But then we have

$$|e|^3 = |l| < |u| = 3|t|^3 \leq |3tv|^3 = |y|^3$$

which contradicts the choice of y. Thus the proof is completed. □

Now we apply Lemma 3.3 to (3.5.1), for $x = a$, $y^3 = b$ and $z = t$. Then we get

$$\begin{aligned} x &= r^3 - 3rs^2 \\ y^3 &= 3r^2 s - s^3 \\ z &= r^2 + 3s^2 \end{aligned}$$

for some integers r and s. But by Lemma 3.4 there are no nontrivial solutions to $y^3 = 3r^2 s - s^3$ which shows that there are nontrivial solutions to (3.5.1).

4. SPHERICAL CASES

It can easily be seen that at least one of p, q and r must be smaller than 3. Without loss of generality let this be p. So we have $p < 3$, i.e. $p = 2$. Then we have that

$$\frac{1}{q} + \frac{1}{r} > \frac{1}{2}.$$

So at least one of q and r must be smaller than 4. If we say that $q < 4$, the first case which is $q = 2$ gives that $r \geq 2$. The second case which is $q = 3$ gives that r must be one of 2, 3, 4 and 5.

Hence in the spherical cases the set $\{p, q, r\}$ must be $\{2,2,k\}$ or $\{2,3,m\}$ where $k \geq 2$ and m=3, 4 or 5. If we write the corresponding Diophantine equations, we have the following list:

$$\begin{aligned}
x^2 + y^2 &= z^k, \\
x^2 + y^k &= z^2, \\
x^2 + y^3 &= z^3, \\
x^2 + y^3 &= z^4, \\
x^2 + y^4 &= z^3, \\
x^2 + y^3 &= z^5.
\end{aligned}$$

In fact there are more equations, but the above equations will be enough since solutions of the others can be found by appropriate changes of variables and signs.

4.1. Case of (2,2,k)

The solutions for the case $k = 2$ are the Pythagorean triples given in the introduction. So we omit this case and take $k \geq 3$.

$$x^2 + y^2 = z^k. \tag{4.1.1}$$

A similar argument to finding Pythagorean triples will be used and it will be shown that a parametric family of solutions exists to (4.1.1). First note the following reduction: If k is even, say $k = 2l$, then we have a Pythagorean triple namely (x, y, z^l). So we have

$$\begin{aligned} x &= a^2 - b^2 \\ y &= 2ab \\ z^l &= a^2 + b^2 \end{aligned}$$

for some positive integers a and b. But the last equation gives another version of our question and if l is also even we can repeat the procedure to decrease the power of z until it is odd. Hence we can assume k to be odd in (4.1.1). Here we have also that z must be odd since otherwise the left-hand side of (4.1.1) would be congruent to 2 whereas right-hand side would be congruent to 0 modulo 4. Also note that then x and y must have different parities. If we factorize (4.1.1) in $\mathbb{Q}(i)$, we have

$$(x + iy)(x - iy) = z^k. \tag{4.1.2}$$

If the factors in (4.1.2) have a common divisor different from a unit in $\mathbb{Q}(i)$, say d then it must divide $2x$ and $2iy$. If d does not divide 2, then it divides x, and so $N(d)$ divides $N(x) = x^2$. Since i is a unit in $\mathbb{Q}(i)$, then $N(d)$ would also divide y^2 which implies that

$\gcd(x, y) > 1$. We also have that 2 is an associate of a square of a prime in $\mathbb{Q}(i)$. We can easily see that this prime is in fact $1 + i$. Note that up to multiplication by a unit this prime is unique. So the common divisor of $x + iy$ and $x - iy$ may be $1 + i$. But then we have that 2 divides $x^2 + y^2$ which contradicts the fact that z is odd. So we have

$$\begin{aligned} x + iy &= (a + ib)^k \\ x - iy &= (a - ib)^k \end{aligned} \tag{4.1.3}$$

for some rational integers a and b. By equating the real and imaginary parts we have

$$\begin{aligned} x &= \sum_{j=0}^{(k-1)/2} \binom{k}{2j} (-1)^j a^{k-2j} b^{2j} \\ y &= \sum_{j=0}^{(k-1)/2} \binom{k}{2j+1} (-1)^j a^{k-2j-1} b^{2j+1} \\ z &= a^2 + b^2. \end{aligned}$$

Hence we have a solution to (4.1.1) for any integers a and b. But we need to make the restrictions that $\gcd(a, b)$=1, and if a is odd then b must be even or vice versa to satisfy the condition that $\gcd(x, y, z)$=1.

4.2. Case of (2,k,2)

In this section we consider

$$x^2 + y^k = z^2. \tag{4.2.1}$$

This equation is different from the previous one. Here y can be odd or even and each case gives different solutions to (4.2.1). We can rewrite (4.2.1) as

$$y^k = (z - x)(z + x). \tag{4.2.2}$$

First we will consider the case in which x is odd, y is even and z is odd. Since z and x are both odd, the factors on the right side of (4.2.2) are divisible by 2. But again by the same reason, at least one of the factors can not be divisible by a higher power of 2. First assume that $(z - x)$ is not divisible by a higher power of 2. Let $y = 2u$. Then we have

$$u^k = \left(\frac{z - x}{2}\right)\left(\frac{z + x}{2^{k-1}}\right).$$

So both of the two factors in the last equation must be k-th powers of some integers, say

$$\begin{aligned} z - x &= 2a^k \\ z + x &= 2^{k-1}b^k. \end{aligned}$$

Solving these two equations gives a parametric solution to (4.2.1) with

$$\begin{aligned} x &= 2^{k-2}b^k - a^k \\ y &= 2ab \\ z &= 2^{k-2}b^k + a^k \end{aligned}$$

where a and b are any integers. Again we say that a and b have different parities and $\gcd(a, b)$=1 to omit trivial solutions. If $(z + x)$ is not divisible by a higher power of 2, we

can carry out the same steps and easily see that we have a similar solution set

$$x = b^k - 2^{k-2}a^k$$
$$y = 2ab$$
$$z = b^k + 2^{k-2}a^k.$$

Note that this solution just says that if (x, y, z) is a solution then $(-x, y, z)$ is also solution.

Remark 4.1. We don't search only positive solutions for (4.2.1). If k is odd, the problem differs whether y is positive or negative. Because of such a difference we do not make the restriction that a and b should be positive integers. They can be either positive or negative.

The next case is that in which x is even, and y and z are both odd. But we will consider this case with other one, where x and y are both odd, since they give similar results. In both of these cases we can directly say that $(z - x)$ and $(z + x)$ must be both k-th powers of some integers. Then we have

$$z - x = a^k$$
$$z + x = b^k.$$

So we have a solution set for (4.2.1) as

$$\begin{aligned} x &= \frac{b^k - a^k}{2} \\ y &= ab \\ z &= \frac{b^k + a^k}{2} \end{aligned}$$

for some odd integers a and b. Note that the choices for a and b, in fact congruence classes of a and b modulo 4, determines the parities of x and z. Also whether k is odd or even

restricts the solution set. If k is even, it can easily be seen that z can not be even. But if k is odd, we can have solutions for both of the last two cases, i.e. solutions in which z may be odd or even.

4.3. Case of (2,3,3)

Now, we will look for the solutions for the Diophantine equation

$$z^2 = x^3 + y^3. \tag{4.3.1}$$

We will see that (4.3.1) has infinitely many nontrivial solution. We will also see that the solution set can be completely determined by a finite set of binary quartic forms, i.e. there are finitely many pairs of binary quartic forms $(f(u,v), g(u,v))$ such that any solution (x,y,z) of (4.3.1) can be given by $x = f(u,v)$ and $y = g(u,v)$ for some integers u and v, and for any integers u and v if we put $x = f(u,v)$ and $y = g(u,v)$ we get a solution to (4.3.1). So our aim is to find such quartic forms. In [6] these quartic forms are found by using the invariants of a binary quartic form. This method has been generalized to the cases $\{p,q,r\} = \{2,3,4\}$ and $\{p,q,r\} = \{2,3,5\}$ in [7]. We will see this method later. Here we will find solutions as given in [8]. Unique factorization property of the ring of integers of the quadratic field $\mathbb{Q}(\xi) = \mathbb{Q}(\sqrt{-3})$ where ξ is a primitive cube root of 1 will be used. We denote the ring of integers of $\mathbb{Q}(\xi)$ by $\mathbb{Z}[\xi]$. We write (4.3.1) as

$$x^3 + y^3 = (x+y)(x+\xi y)(x+\xi^2 y) \tag{4.3.2}$$

Case I: $3 \nmid z$. If π is a prime which divides two of the factors in the right-hand side of (4.3.2) then we have that π divides $(1-\xi)y$. But if π divides y, then we would also have that π divides x. But then $N(\pi)$ which is an integer other than 1 divides $\gcd(x,y)$. So we must have that π divides $1-\xi$ (Note that $x+\xi y$ and $x+\xi^2 y$ are conjugates and so either

they are both divisible by π or not). But since $N(1-\xi) = (1-\xi)(1-\xi^2) = 3$ we have that $1-\xi$ is a prime, and so π should be an associate of $1-\xi$ which contradicts the assumption that 3 does not divide z (Since if $1-\xi$ divides $x+\xi y$ or $x+\xi^2 y$, then $N(1-\xi) = 3$ divides $N(x+\xi y) = (x+\xi y)(x+\xi^2 y)$ and so $3|z$). So we may assume that the factors in the right-hand side of (4.3.2) are pairwise coprime. Then each of these three factors must be a unit times a square of some integer in $\mathbb{Z}[\xi]$. Since the binary quadratic form $x^2 - xy + y^2$ is nonnegative and $(x+y)(x^2-xy+y^2) = z^2$, $x+y$ should be nonnegative. The units of $\mathbb{Z}[\xi]$ are $\pm 1, \pm\xi$ and $\pm\xi^2$. So we have $x + \xi y = (-\xi)^k \alpha^2$ for some rational integer k and $\alpha \in \mathbb{Z}[\xi]$, and similarly $x + \xi^2 y = (-\xi^2)^k \bar{\alpha}^2$. But by using the identity $\xi^4 = \xi$, we get $(-\xi)^k \alpha^2 = (-1)^k (\alpha \xi^{2k})^2$. So our problem reduces to solving the following equations.

$$\begin{aligned} x + y &= a^2 \\ x + \xi y &= \epsilon \alpha^2 \\ x + \xi^2 y &= \epsilon \bar{\alpha}^2 \\ z &= \pm a \alpha \bar{\alpha} \end{aligned}$$

where $a \in \mathbb{Z}$, $\alpha \in \mathbb{Z}[\xi]$ and $\epsilon = \pm 1$. Now we will try to reduce the above conditions to a single quadratic equation in $\mathbb{Z}[\xi]$. We put $\beta = \xi^2 \alpha$. Then by using the facts that $\xi^3 = 1$, $\xi^2 + \xi + 1 = 0$ and $\bar{\xi} = \xi^2$ we have

$$\beta^2 + \bar{\beta}^2 = \xi \alpha^2 + \xi^2 \bar{\alpha}^2 = \epsilon(\xi(x+\xi y) + \xi^2(x+\xi^2 y)) = \epsilon(-x-y) = -\epsilon a^2.$$

Thus from any solution (x, y, z) of (4.3.1) we can find a solution to $\beta^2 + \bar{\beta}^2 = -\epsilon a^2$. Now we prove the converse. Assume that $\beta \in \mathbb{Z}[\xi]$ and $a \in \mathbb{Z}$ satisfy $\beta^2 + \bar{\beta}^2 = -\epsilon a^2$. If we let $\alpha = \xi\beta$, we get

$$\frac{\epsilon\bar{\alpha}^2 - a^2}{\epsilon\alpha^2 - a^2} = \frac{\epsilon\xi\bar{\beta}^2 - a^2}{\epsilon\xi^2\beta^2 - a^2} = \frac{\epsilon\xi(-\epsilon a^2 - \beta^2) - a^2}{\epsilon\xi^2\beta^2 - a^2} = \frac{\xi^2 a^2 - \epsilon\xi\beta^2}{\epsilon\xi^2\beta^2 - a^2} = \frac{-\xi^2(\epsilon\xi^2\beta^2 - a^2)}{\epsilon\xi^2\beta^2 - a^2} = -\xi^2 = \frac{\bar{\xi} - 1}{\xi - 1}.$$

So $y = (\epsilon\alpha^2 - a^2)/(\xi - 1)$ is in $\mathbb{Q}$. In fact if we let $\alpha = (c + d\sqrt{-3})/2$ where c and d are both even or odd and $\xi = (-1 \pm \sqrt{-3})/2$, we can easily see that $y \in \mathbb{Z}$. Hence from any solution of the equation $\beta^2 + \bar{\beta}^2 = -\epsilon a^2$ where $\beta \in \mathbb{Z}[\xi]$ and $a \in \mathbb{Z}$ we get a solution to (4.3.1). So the problem of finding the solution set of (4.3.1) is reduced to finding the solutions of $\beta^2 + \bar{\beta}^2 = -\epsilon a^2$ where $\beta \in \mathbb{Z}[\xi]$ and $a \in \mathbb{Z}$. By putting $\beta = u + v\xi$ we get

$$a^2 = \epsilon(v^2 + 2uv - 2u^2).$$

We can make one more reduction. Since $\gcd(x, y)$=1, a and β must be coprime in $\mathbb{Z}[\xi]$. Then we have $\gcd(u, v)$=1. Also since $v^2 + 2uv - 2u^2 = (u + v)^2 - 3u^2$ and 3 does not divide a we have $1 \equiv a^2 \equiv \epsilon((u + v)^2 - 3u^2) \equiv \epsilon(u + v)^2 \equiv \epsilon \pmod 3$ which implies that $\epsilon = 1$. Note that we have $\gcd(u + v, a)$=1. Also from the above equation we see that if a is even, then u and v must be both even which is impossible. So a and v must be odd. In this case we change β into $\bar{\beta}$. So the pair (u, v) changes into $(u - v, -v)$ which can be easily seen by putting $\xi = (-1 \pm \sqrt{-3})/2$. Thus we can assume that $u + v$ and a have different parities. Now it suffices to find the solutions of the equation

$$3u^2 = k^2 - a^2$$

where $k = u + v$, and k and a have different parities. We write the above equation as

$$3u^2 = (k - a)(k + a).$$

We can assume that 3 divides $k - a$ (If necessary we can replace a by $-a$. Note that this replacing does not effect the values of x and y). Also since k and a have different parities

and gcd(k, a)=1, we have that gcd$(k-a, k+a)$=1. Then we have

$$\begin{aligned} k-a &= \delta 3d^2 \\ k+a &= \delta e^2 \\ u &= \delta_1 de \end{aligned}$$

where $\delta, \delta_1 = \pm 1$, d and e are both odd and gcd(d, e)=1 . But again if necessary by replacing u, v and a by $-u$, $-v$ and $-a$ respectively we can assume that $\delta = 1$. Also if necessary replacing d by $-d$ we can assume that $\delta_1 = 1$. Note that since we need β^2, not β, this replacing does not effect x and y. Since $k-a$ and $k+a$ are both odd we have

$$\begin{aligned} k &= \frac{3d^2+e^2}{2} \\ a &= \frac{e^2-3d^2}{2} \\ u &= de. \end{aligned}$$

Now we let $s = d$ and $t = (e-d)/2$. We write all of the variables in the below equations

$$\begin{aligned} u &= de \\ v &= k-u \\ \beta &= u+v\xi \\ \alpha &= \xi\beta \\ y &= \frac{\alpha^2-a^2}{\xi-1} \\ x+y &= a^2 \\ x^3+y^3 &= z^2 \end{aligned}$$

in terms of s and t and get the following parametrization of x and y.

$$\begin{aligned} x &= s(s+2t)(s^2-2st+t^2) \\ y &= -4t(s-t)(s^2+st+t^2) \\ z &= \pm(s^2-2st-2t^2)(s^4+2s^3t+6s^2t^2-4st^3+4t^4). \end{aligned}$$

Here we have some restrictions on s and t; s must be odd, $\gcd(s,t)=1$ and $3 \nmid s-t$ (To see the last restriction we write $s-t=(3d-e)/2$. If $3 \mid s-t$ then $3 \mid e$. Then we have $3 \mid a$ and finally $3 \mid z$ which contradicts the assumption that $3 \nmid z$). Thus we have completed the case 3 does not divide z.

Case II: $3 \mid z$. Since $\gcd(x,y,z)=1$, we have that $3 \nmid xy$. Now we consider $x+y$ and $x^2-xy+y^2=(x+y)^2-3xy$. Since 3 divides z, we have that 3 divides both $x+y$ and x^2-xy+y^2. But 3^2 can not divide x^2-xy+y^2, otherwise 3 would be a common divisor of x and y. Since $x^2-xy+y^2=(x+\xi y)(x+\xi^2 y)$ and $N(\xi)=(1-\xi)(1-\xi^2)=3$ we have that both $x+\xi y$ and $x+\xi^2 y$ are divisible by $1-\xi$. Thus we have

$$\left(\frac{x+y}{3}\right)\left(\frac{x+\xi y}{1-\xi}\right)\left(\frac{x+\xi^2 y}{1-\xi^2}\right)=\left(\frac{z}{3}\right)^2$$

where all three factors in the left-hand side are pairwise coprime in $\mathbb{Z}[\xi]$. Then by a similar argument of the first case we have

$$\begin{aligned} x+y &= 3a^2 \\ x+\xi y &= \epsilon(1-\xi)\alpha^2 \\ x+\xi^2 y &= \epsilon(1-\xi^2)\bar{\alpha}^2 \\ z &= \pm 3a\alpha\bar{\alpha} \end{aligned}$$

where α is coprime to $1-\xi$ and $\epsilon = \pm 1$. By subtracting the second equation from the first one we get $y = (1-\xi^2)a^2 - \epsilon\alpha^2$. By a similar calculation as we did in Case I we see that $y \in \mathbb{Z}$. So we get $\alpha^2 - \bar{\alpha}^2 = \epsilon a^2(\xi - \xi^2)$. Conversely if α is an integer in $\mathbb{Z}[\xi]$ satisfying $\alpha^2 - \bar{\alpha}^2 = \epsilon a^2(\xi - \xi^2)$, then we can choose $y = (1-\xi^2)a^2 - \epsilon\alpha^2 \in \mathbb{Z}$. Thus it is equivalent to find the solutions of the equation

$$\alpha^2 - \bar{\alpha}^2 = \epsilon a^2(\xi - \xi^2).$$

We put $\alpha = u + v\xi$ and get the equation $a^2 = \epsilon v(2u - v)$. Since α is coprime to a, we see that $\gcd(u, v)=1$. Also if $u + v \equiv 0 \pmod 3$, then we would have $N(\alpha) = u^2 - uv + v^2 \equiv a^2 \equiv 0 \pmod 3$. But this contradicts that α and a are coprime. Now if necessary we can replace α by $\bar{\alpha}$ and so we can assume that $\epsilon = 1$. Now since 3 does not divide $u + v$ and $\gcd(u, v)=1$, we have that $\gcd(v, 2u - v)=1$ or 2 whether v is odd or even respectively. We deal with these subcases seperately.

Case II,I: $2 \nmid v$. Again by replacing α by $\bar{\alpha}$ (if necessary) we can write

$$\begin{aligned} v &= s_1^2 \\ 2u - v &= t_1^2 \\ a &= s_1 t_1 \end{aligned}$$

where s_1 and t_1 are odd rational integers. We put $s = (s_1 + t_1)/2$ and $t = (s_1 - t_1)/2$. Note that s and t have different parities, $\gcd(s, t)=1$ and since $3 \nmid u + v$ we have $s \not\equiv t \pmod 3$.

Thus we have the following equations;

$$\begin{aligned} v &= s_1^2 \\ 2u - v &= t_1^2 \\ a^2 &= v(2u - v) \\ \alpha &= u + v\xi \\ y &= (1 - \xi^2)a^2 - \epsilon\alpha^2 \\ x + y &= 3a^2 \\ x^3 + y^3 &= z^2. \end{aligned}$$

We write each of the above equations in terms of s and t and get

$$\begin{aligned} x &= s^4 - 4ts^3 - 6t^2s^2 - 4st^3 + t^4 \\ y &= 2(s^4 + 2s^3t + 2st^3 + t^4) \\ z &= 3(s - t)(s + t)(s^4 + 2s^3t + 6s^2t^2 + 2st^3 + t^4) \end{aligned} \tag{4.3.3}$$

where s and t have different parities, $\gcd(s, t)$=1 and $s \not\equiv t \pmod 3$.

Case II,II: $2 \mid v$. In this case our calculation is similar to that for the previous case. We only note that in this case we write $v = 2s^2$ and $2u - v = 2t^2$ (we do not need to define extra variables s_1 and t_1). Then we have the following parametrization

$$\begin{aligned} x &= -3s^4 + 6s^2t^2 + t^4 \\ y &= 3s^4 + 6s^2t^2 - t^4 \\ z &= 6st(3s^4 + t^4) \end{aligned} \tag{4.3.4}$$

where s and t have different parities, $\gcd(s,t)$=1 and $3 \nmid t$ (The last condition is equivalent to $3 \nmid u+v$). Thus we have found all of the disjoint parametrizations (up to change of x and y) of the equation $x^3+y^3=z^2$. Note that in [6] in total five parametrizations were given to this equation. Now we can say that two of these five parametrizations must be the same with some of the other three parametrizations. The redundant parametrizations can be found in [7].

4.4. Case of (2,3,4)

Now, we will look for the solutions for the Diophantine equation

$$z^3 = x^2 - y^4. \tag{4.4.1}$$

We will follow the way given in [8]. First we prove two lemmas which are necessary.

Lemma 4.1. *The equation $d^3+e^3=2f^2$ in integers d, e and f with $\gcd(e,f)$=1 can be parametrized by one of the four parametrizations given below, up to exchange of d and e, where s and t denote coprime integers with the indicated congruence conditions modulo 2 and 3. In addition, these parametrizations are disjoint, in that any solution to our equation belongs to a single parametrization (up to exchange of d and e).*
Parametric Solution I:

$$\begin{aligned} d &= -(s^2+4ts-2t^2)(3s^2+4st+2t^2) \\ e &= (s^2+2t^2)(5s^2+8st+2t^2) \\ f &= \pm(s^2-2st-2t^2)(7s^4+20s^3t+24s^2t^2+8st^3+4t^4) \end{aligned}$$

where s is odd and $s \not\equiv t$ (mod 3).

Parametric Solution II:

$$\begin{aligned} d &= (3s^2 - 6st + t^2)(3s^2 + 2st + t^2) \\ e &= (3s^2 - 2st + t^2)(3s^2 + 6st + t^2) \\ f &= \pm(3s^2 - t^2)(9s^4 + 18s^2t^2 + t^4) \end{aligned}$$

where s and t have different parities and $3 \nmid t$.

Parametric Solution III:

$$\begin{aligned} d &= -3s^4 + 12s^2t^2 + 4t^4 \\ e &= 3s^4 + 12s^2t^2 - 4t^4 \\ f &= 6st(3s^4 + 4t^4) \end{aligned}$$

where s is odd and $3 \nmid t$.

Parametric Solution IV:

$$\begin{aligned} d &= -12s^4 + 12s^2t^2 + t^4 \\ e &= 12s^4 + 12s^2t^2 - t^4 \\ f &= 6st(12s^4 + t^4) \end{aligned}$$

where t is odd and $3 \nmid t$.

Proof. First we consider $d^3 + e^3 = (d + e)(d^2 - de + e^2) = 2f^2$. Since d and e can not be both even, we have that $d^2 - de + e^2$ must be odd, and so $d + e$ must be even. We consider two cases as we did in Section 4.3.

Case I: $3 \nmid f$. We again write $(d+e)(d+\xi e)(d+\xi^2 e) = 2z^2$. Note that the three factors

in the left-hand side of this equation are pairwise coprime. There is a rational integer a, and an integer $\alpha \in \mathbb{Z}[\xi]$ such that $d+e = 2a^2$, $d+\xi e = (-\xi)^k \alpha^2$ and $d+\xi^2 e = (-\xi^2)^k \bar{\alpha}^2$. Using the identity $\xi^4 = \xi$ we reduce our problem to below equations;

$$\begin{aligned} d+e &= 2a^2 \\ d+\xi e &= \epsilon\alpha^2 \\ d+\xi^2 e &= \epsilon\bar{\alpha}^2 \end{aligned}$$

where $\epsilon = \pm 1$. Putting $\beta = \xi^2\alpha$, we get $\beta^2 + \bar{\beta}^2 = -2\epsilon a^2$. We put $\beta = u + \xi v$ where $\gcd(u,v)$=1 and get $2a^2 = \epsilon(v^2+2uv-2u^2) = \epsilon((u+v)^2 - 3u^2)$. Now since $3 \nmid f$ we have that $3 \nmid a$, and so $3 \nmid (u+v)$. Thus $2 \equiv \epsilon \pmod 3$ which implies that $\epsilon = -1$. Finally we have a single simplier equation

$$2a^2 = -(v^2+2uv-2u^2).$$

From this equation we see that v must be even. So u must be odd. By considering the last equation in modulo 4 we see that a must be odd. Now after these observations we put $v = 2w$ in this equation and get

$$3w^2 = (u-w)^2 - a^2 = (u-w-a)(u-w+a).$$

We note that $3 \nmid (u-w)$. If necessary we may replace a by $-a$ to assume that $3 \mid (u-w-a)$.

Now if w is odd, we have that $u-w-a = 3s_1^2$ and $u-w+a = t_1^2$ where s_1 and t_1 are odd rational integers and $\gcd(s_1,t_1)$=1 (Otherwise if $\gcd(s_1,t_1) = g > 1$, then we would have $g \mid 2a$. But since g is odd, we would have $g \mid a$, and so $g \mid \gcd(u,v)$ which gives a contradiction). Finally we put $s = s_1$ and $t = (t_1 - s_1)/2$, and write all variables in terms of s and t to get Parametric Solution I.

Now if w is even, we have that $u - w - a = 6s^2$, $u - w + a = 2t^2$ and $w = 2st$ where $3 \nmid t$, s and t have opposite parities and are coprime. From these equations we get $a = t^2 - 3s^2$ and $u = 6s^2 + 4st + t^2$. Writing all variables in terms of s and t we get Parametric Solution II.

Case II: $3 \mid f$. By a similar method of Section 4.3 we can see that all of the three factors in the left-hand side of the equation $(d+e)(d+\xi e)(d+\xi^2 e) = 2z^2$ are divisible by $1-\xi$, and $(d+e)$ is divisible by 3. So we have

$$\left(\frac{d+e}{3}\right)\left(\frac{d+\xi e}{1-\xi}\right)\left(\frac{d+\xi^2 e}{1-\xi^2}\right) = 2\left(\frac{f}{3}\right)^2.$$

From this equation we get

$$\begin{aligned} d+e &= 6a^2 \\ d+\xi e &= (1-\xi)(-\xi)^k\alpha^2 \\ d+\xi^2 e &= (1-\xi^2)(-\xi^2)^k\bar{\alpha}^2 \end{aligned}$$

where a and k are rational integers, and $\alpha \in \mathbb{Z}[\xi]$. Using the identity $\xi = \xi^4$ we can reduce the last two equations to $d+\xi e = (1-\xi)\epsilon\alpha^2$ and $d+\xi^2 e = (1-\xi^2)\epsilon\bar{\alpha}^2$ where $\epsilon = \pm 1$. From these equations we get

$$\begin{aligned} e &= 2(1-\xi^2)a^2 - \epsilon\alpha^2 \\ d &= 2(1-\xi^2)a^2 + \epsilon\bar{\alpha}^2. \end{aligned}$$

From the equation $e = 2(1-\xi^2)a^2 - \epsilon\alpha^2$ we can easily see that α and $1-\xi$ are coprime, otherwise $N(1-\xi) = 3$ would divide e^2 contradicting our assumption that $3 \mid f$. If necessary we may replace d and e, which means replacing α by $\bar{\alpha}$ and ϵ by $-\epsilon$, and so assume that $\epsilon = 1$. Also we have that $\alpha^2 - \bar{\alpha}^2 = 2a^2(\xi - \xi^2)$. Now we put $\alpha = u + \xi v$ in

this equation where u and v are coprime rational integers, and get a single equation

$$2a^2 = v(2u - v).$$

From this equation we see that v and a must be even, and so u must be odd. We put $v = 2w$ and get

$$a^2 = 2w(u - w).$$

Before we go into much details we make a simple remark; $3 \nmid (u - w)$. Otherwise if $u \equiv w \pmod 3$, then we would have $2u \equiv v \pmod 3$, and so $N(\alpha) = u^2 - uv + v^2 \equiv 0 \pmod 3$. But also we have $d^2 - de + e^2 = 3.N(\alpha)^2$. So 3^2 would divide both $(d + e)$ and $(d^2 - de + e^2) = (d + e)^2 - 3de$ which implies that $3 \mid de$. But this contradicts the assumption that $\gcd(d, e, f)$=1.

Now we consider the case where w is odd. Then there are rational integers s and t such that $w = s^2$, $u - w = 2t^2$ and $a = 2st$. Writing all variables in terms of s and t we get Parametric Solution III.

Now if w is even, we put $w = 2s^2$, $u - w = t^2$ and $a = 2st$. This change of variables gives Parametric Solution IV. □

Lemma 4.2. *The equation $d^3 - 2e^3 = f^2$ in integers d, e and f with $\gcd(d, e)$=1 can be parametrized by one of the three parametrizations given below, where s and t denote coprime integers with the indicated congruence conditions modulo 2 and 3. In addition, these parametrizations are disjoint, in that any solution to our equation belongs to a single parametrization.*

Parametric Solution I:

$$\begin{aligned} d &= s(s^3 - 16t^3) \\ e &= -4t(s^3 + 2t^3) \\ f &= \pm(s^6 + 40s^3t^3 - 32t^6) \end{aligned}$$

where s is odd and $s \not\equiv t$ (mod 3).

Parametric Solution II:

$$\begin{aligned} d &= 3s^4 + 12s^3t + 6s^2t^2 + 4st^3 + 3t^4 \\ e &= -3s^4 + 6s^2t^2 + 8st^3 + t^4 \\ f &= \pm(9s^6 + 18s^5t + 45s^4t^2 + 60s^3t^3 + 15s^2t^4 - 6st^5 - 5t^6) \end{aligned}$$

where s and t have different parities and $3 \nmid t$.

Parametric Solution III:

$$\begin{aligned} d &= 7s^4 + 4s^3t + 6s^2t^2 - 4st^3 - t^4 \\ e &= 3s^4 - 8s^3t - 6s^2t^2 - t^4 \\ f &= \pm(17s^6 + 30s^5t - 15s^4t^2 + 20s^3t^3 + 15s^2t^4 + 6st^5 - t^6) \end{aligned}$$

where s and t have different parities and $s \not\equiv t$ (mod 3).

Proof. First we make the simple observations that f must be odd and $3 \nmid f$ (which can be seen by considering the equation modulo 9). But now we are in a different situation. In the previous sections we could factorize the related equation in some quadratic field. But the equation $d^3 - 2e^3 = f^2$ can not be factorized in a way that can help us in any quadratic field. We need to generalize the notions of Section 2 to arbitrary number fields. The

general theory of number fields can be found in Chapter 2 of [9]. We will only summarize the results of the general theory of number fields in this problem. Now we let $\mathbb{K} := \mathbb{Q}(\theta)$ where $\theta^3 = 2$ and $\theta \in \mathbb{R}$. The ring of integers of $\mathbb{K}$ which we denote by $\mathbb{Z}[\theta]$ is a principal ideal domain, and therefore a unique factorization domain. If we let $\alpha = d - e\theta$, we see that our equation is a norm equation, $N(\alpha) = f^2$. So our problem reduces to finding all integers $\alpha = d - e\theta$ in $\mathbb{Z}[\theta]$ whose norm is equal to f^2.

In the previous lemma we had worked with the quadratic field $\mathbb{Q}(\xi)$ and its ring of integers $\mathbb{Z}[\xi]$ where ξ is a primitive cube root of 1. In $\mathbb{Z}[\xi]$ any unit is in fact some root of 1 contained in $\mathbb{Z}[\xi]$. But in $\mathbb{Z}[\theta]$, which is a cubic field we have a different situation. The only roots of 1 contained in $\mathbb{Z}[\theta]$ are ± 1, but these are not the only units. If we let $\epsilon = \theta - 1$, we see that $N(\epsilon) = (\theta - 1)(\theta\xi - 1)(\theta\xi^2 - 1) = 1$ which implies that $\theta - 1$ is also a unit. The unit ϵ is the fundamental unit of $\mathbb{Z}[\theta]$, i.e. any unit $\gamma \in \mathbb{Z}[\theta]$ is of the form $\gamma = \pm\epsilon^k$ for some integer k (Note that fundamental unit is not unique. We could also choose $1/(\theta - 1)$ as the fundamental unit).

Now we write our equation as $(d - e\theta)(d^2 + de\theta + e^2\theta^2) = f^2$. Since $3 \nmid f$ and $d^2 + de\theta + e^2\theta^2 = (d - e\theta)^2 + 3de\theta$, we see that the two factors $d^2 + de\theta + e^2\theta^2$ and $d - e\theta$ are coprime in $\mathbb{Z}[\theta]$. So $d - e\theta = \pm\epsilon^k\beta^2$ for some rational integer k and $\beta \in \mathbb{Z}[\theta]$. We can assume that $k = 0$ or 1. Otherwise the higher powers can be counted in β. Also note that since $N(d - e\theta) = z^2 = \pm N(\beta)^2$, the sign can not be negative. Thus our problem now reduces to finding $\beta \in \mathbb{Z}[\theta]$ such that $d - e\theta = \epsilon^k\beta^2$. If we let $\beta = u + v\theta + w\theta^2$ the only condition is that the coefficient of θ^2 in $\epsilon^k\beta^2$ must be zero. We can deal with two cases whether $k = 0$ or 1.

If $k = 0$, we get $v^2 + 2uw = 0$, $d = u^2 + 4vw$, $e = -2(w^2 + uv)$ and $f = \pm(u^3 + 2v^3 + 4w^3 - 6uvw)$. Since $\gcd(d, e) = 1$, then $\gcd(u, w) = 1$. Also $v = 2v_1$ is even, so u must be odd. From $uw = -2v_1^2$, we have $u = \epsilon_1 s^2$, $w = -\epsilon_1 2t^2$ and $v = \epsilon_2 2st$ where $\epsilon_1, \epsilon_2 = \pm 1$. Note that we also have $\gcd(s, t) = 1$ since $\gcd(u, w) = 1$. If necessary by replacing β with

$-\beta$ and s by $-s$ we can assume that $\epsilon_1 = \epsilon_2 = 1$. So we have Parametric Solution I.

If $k = 1$, then we obtain the following equations:

$$\begin{aligned} 0 &= u(2v - 2w) - v^2 + 2w^2 \\ d &= -u^2 + 4wu + 2v^2 - 4wv \\ e &= -u^2 + 2vu - 4wu + 2w^2. \end{aligned}$$

We can write the first equation as $(u-w)^2 + w^2 = (v-u)^2$. Since $\gcd(u, v, w) = 1$, we have that $\gcd((u-w), w, (u-v)) = 1$. The solution of the last equation is just the Pythagorean triple, i.e. $u - w = 2st$, $w = s^2 - t^2$ and $v - u = \epsilon_1 s^2 + t^2$, or $w = 2st$, $u - w = s^2 - t^2$ and $v - u = \epsilon_1 s^2 + t^2$ where s and t are coprime rational integers of opposite parity and $\epsilon_1 = \pm 1$. Since we can change β by $-\beta$, we can assume that $\epsilon_1 = 1$. Thus in the first case for u, w and v we have the following parametrization;

$$\begin{aligned} w &= s^2 - t^2 \\ u &= s^2 - t^2 + 2st \\ v &= 2s^2 + 2st. \end{aligned}$$

Note that if $3 \mid t$, then we have $v \equiv 2w \equiv 2u \pmod 3$. But then $\beta^2 = u^2 + v^2\theta^2 + 2w^2\theta + 2uv\theta + 2wu\theta^2 + 4vw \equiv 9u^2 + 6u^2\theta + 3u^2\theta^2 \equiv 0 \pmod 3$ which contradicts that $3 \nmid f$. Replacing gives us Parametric Solution II. In the second case of the Pythagorean solution we have

$$\begin{aligned} w &= 2st \\ u &= s^2 - t^2 + 2st \\ v &= 2s^2 + 2st. \end{aligned}$$

If $s \equiv t \pmod 3$, then we have $2v \equiv u \equiv w \pmod 3$. But then we have $\beta^2 \equiv 3v^2(1+\theta+\theta^2) \equiv 0 \pmod 3$ which contradicts that $3 \nmid f$. Replacing gives us Parametric Solution III. The proof is thus complete. □

Now we return to the equation (4.4.1). We write this equation as

$$(x - y^2)(x + y^2) = z^3.$$

Since $\gcd(x, y, z) = 1$, we have two possibilities; either $x - y^2$ and $x + y^2$ are coprime ($2 \nmid z$), or x and y are both odd and $(x - y^2)/2$ and $(x + y^2)/2$ are coprime ($2 \mid z$).

Case I: $2 \nmid z$. Here there are rational integers a and b with $\gcd(a, b) = 1$ such that $x - y^2 = a^3$, $x + y^2 = b^3$ and $z = ab$. Then we have $2y^2 = b^3 - a^3$, $x = y^2 + a^3$ and $z = ab$. Now we apply Lemma 4.1 with $b = d$, $-a = e$ and $y = f$ (Note that trying $b = e$ and $-a = d$ is just replacing x by $-x$ in (4.4.1). Thus we do not need to consider this possibility). So we have the following four parametrizations for this case:

$$\begin{aligned} x &= \pm 4s(s+2t)(s^2+st+t^2)(s^4+4s^3t+16s^2t^2+24st^3+12t^4) \\ &\times (19s^4-4s^3t+8st^3+4t^4) \\ y &= \pm(s^2-2st-2t^2)(7s^4+20s^3t+24s^2t^2+8st^3+4t^4) \\ z &= (s^2+2t^2)(s^2+4st-2t^2)(3s^2+4st+2t^2)(5s^2+8st+2t^2) \end{aligned}$$

where s is odd and $s \not\equiv t \pmod 3$;

$$\begin{aligned} x &= \pm 4st(3s^2+t^2)(3s^4-2s^2t^2+3t^4)(81s^4-6s^2t^2+t^4) \\ y &= \pm(3s^2-t^2)(9s^4+18s^2t^2+t^4) \\ z &= -(3s^4-12s^2t^2-4t^4)(3s^2-2st+t^2)(3s^2+2st+t^2)(3s^2+6st+t^2) \end{aligned}$$

where s and t have different parities and $3 \nmid t$;

$$\begin{aligned} x &= \pm(3s^4 - 4t^4)(9s^8 + 408s^4t^4 + 16t^8) \\ y &= \pm 6st(3s^4 + 4t^4) \\ z &= (3s^4 - 12s^2t^2 - 4t^4)(3s^4 + 12s^2t^2 - 4t^4) \end{aligned}$$

where s is odd and $3 \nmid t$.

$$\begin{aligned} x &= \pm(12s^4 - t^4)(144s^8 + 408s^4t^4 + t^8) \\ y &= \pm 6st(3s^4 + t^4) \\ z &= (12s^4 - 12s^2t^2 - t^4)(12s^4 + 12s^2t^2 - t^4) \end{aligned}$$

where t is odd and $3 \nmid t$.

Case II: $2 \mid z$. Here we have $8 \mid (x - y^2)(x + y^2)$. If necessary we may replace x by $-x$ and so we can assume that $4 \mid (x - y^2)$ and $2 \mid\mid (x + y^2)$. So there are rational integers a and b with $\gcd(a, b) = 1$ such that $x - y^2 = 4a^3$, $x + y^2 = 2b^3$ and $z = 2ab$. Then we have $b^3 - 2a^3 = y^2$, $x = 4a^3 + y^2$ and $z = 2ab$. Now we apply Lemma 4.2 with $d = b$, $e = a$ and $f = y$, and get the following three parametrization:

$$\begin{aligned} x &= \pm(s^6 - 176s^3t^3 - 32t^6)(s^6 + 32t^6) \\ y &= \pm(s^6 + 40s^3t^3 - 32t^6) \\ z &= -8st(s^3 - 16t^3)(s^3 + 2t^3) \end{aligned}$$

where s is odd and $s \not\equiv t \pmod 3$;

$$\begin{aligned} x &= \pm(-27s^{12} + 324s^{11}t + 1728s^{10}t^2 + 3564s^9t^3 + 3267s^8t^4 \\ &+ 2376s^7t^5 + 2772s^6t^6 + 3960s^5t^7 + 4059s^4t^8 \\ &+ 2420s^3y^9 + 726s^2t^{10} + 156st^{11} + 29t^{12}) \\ y &= \pm(9s^6 + 18s^5t + 45s^4t^2 + 60s^3t^3 + 15s^2t^4 - 6st^5 - 5t^6) \\ z &= -2(3s^4 - 6s^2t^2 - 8s^3t - t^4)(3s^4 + 12s^3t + 6s^2t^2 + 4st^3 + 3t^4) \end{aligned}$$

where s and t have different parities and $3 \nmid t$;

$$\begin{aligned} x &= \pm(397s^{12} + 156s^{11}t + 2046s^{10}t^2 + 1188s^9t^3 - 1485s^8t^4 - 2376s^7t^5 \\ &- 924s^6t^6 - 792s^5t^7 + 99s^4t^8 + 44s^3t^9 - 66s^2t^{10} - 12st^{11} - 3t^{12}) \\ y &= \pm(17s^6 + 30s^5t - 15s^4t^2 + 20s^3t^3 + 15s^2t^4 + 6st^5 - t^6) \\ z &= 2(3s^4 - 8s^3t - 6s^2t^2 - t^4)(7s^4 + 4s^3t + 6s^2t^2 - 4st^3 - t^4) \end{aligned}$$

where s and t have different parities and $s \not\equiv t \pmod 3$.

4.5. Case of (2,4,3)

Now, we will look for the solutions of the Diophantine equation

$$z^3 = x^2 + y^4. \tag{4.5.1}$$

Again we will follow the way given in [8]. Note that if we consider the above equation in modulo 8, we see that x and y can not be both odd. We can write the above equation as

$$(x - iy^2)(x + iy^2) = z^3$$

over $\mathbb{Z}[i]$. The only possible divisor of the factors in the left-hand side of the above equation is an associate of $1+i$. But since $N(1+i)=2$ and these factors are both odd, we can conclude that these factors are coprime in $\mathbb{Z}[i]$. So there exists $\alpha \in \mathbb{Z}[i]$ such that $x+iy^2=\alpha^3$, $x-iy^2=\bar{\alpha}^3$ and $z=\alpha\bar{\alpha}$. If we put $\alpha=u+iv$ we get $z=u^2+v^2$, $x=u^3-3uv^2$ and $y^2=3u^2v-v^3$. Also we can deduce that u and v have opposite parities since $\gcd(x,y)=1$. So it will suffice to find the solutions of the last equation with $\gcd(u,v)=1$. We deal with two cases; 3 divides v or 3 does not divide v.

Case I: $3 \nmid v$. From $y^2=v(3u^2-v^2)$ we have that $v=\epsilon a^2$, $3u^2-v^2=\epsilon b^2$ and $y=\pm ab$ where a and b are coprime rational integers with b being odd and $3 \nmid ab$, and $\epsilon=\pm 1$. By considering $3u^2-v^2=\epsilon b^2$ in modulo 3 and using the assumption that $3 \nmid v$ we deduce that $\epsilon=-1$. Then we have $3u^2=(v-b)(v+b)$. If necessary we replace b by $-b$ to assume that 3 divides $v-b$. Also note that if v is even, then u, a and b must be odd, even and odd respectively, and we must have that $4 \mid v$. But then we have $3u^2=v^2-b^2 \equiv 7 \pmod 8$ which is impossible. Thus v, u, a and b must be odd, even, odd and odd respectively. So we can write $v-b=6\epsilon_1 c^2$ and $v+b=2\epsilon_1 d^2$ where c and d are coprime rational integers with $3 \nmid d$ and $\epsilon_1=\pm 1$. Then we have $v=-a^2=\epsilon_1(3c^2+d^2)$. Thus we easily see that $\epsilon_1=-1$ and we get the equation $d^2+3c^2=a^2$. Since a is odd we have that c is even and d is odd. We write the last equation as $3c^2=(a-d)(a+d)$. Since $\gcd((a-d)/2,(a+d)/2)=1$, there are rational integers s and t of opposite parity with $\gcd(s,t)=1$ such that $a-d=\pm 6t^2$, $a+d=\pm 2s^2$ and $c=2st$. So we have that $a=\pm(s^2+3t^2)$ and $d=\pm(s^2-3t^2)$. Since $3 \nmid a$ we have that $3 \nmid s$. Writing all variables in terms of s and t we have the following parametrization for (4.5.1).
Parametric Solution I:

$$\begin{aligned} x &= 4st(s^2-3t^2)(s^4+6s^2t^2+81t^4)(3s^4+2s^2t^2+3t^4) \\ y &= \pm(s^2+3t^2)(s^4-18s^2t^2+9t^4) \\ z &= (s^4-2s^2t^2+9t^4)(s^4+30s^2t^2+9t^4) \end{aligned}$$

where s and t have different parities, $\gcd(s,t)$ =1 and $3 \nmid s$.

Case II: $3 \mid v$. We put $v = 3w$ in $y^2 = v(3u^2 - v^2)$ and get $(y/3)^2 = w(u^2 - 3w^2)$. So $\gcd(w, u^2 - 3w^2)$=1 since $\gcd(u, v) = 1$. Then there exist rational integers a and b such that $w = \epsilon a^2$ and $u^2 - 3w^2 = \epsilon b^2$ where b is odd (since u and v have opposite parities), a and b have different parities (since $\gcd(a, b) = 1$ and b is odd) and $\epsilon = \pm 1$ Also note that u and w must have different parities which implies that $\epsilon = 1$ (by considering the equation $u^2 - 3w^2 = \epsilon b^2$ in modulo 4). Thus we have to deal with the equations $u^2 - 3w^2 = b^2$ and $w = a^2$. We write the first one as $3w^2 = (u - b)(u + b)$. We may replace b by $-b$ in order to assume that $3 \mid (u - b)$ and $3 \nmid (u + b)$. We only know that b is odd. u may be odd or even. First we take u odd. Then there are coprime integers of opposite parity c and d such that $u - b = \pm 6d^2$, $u + b = \pm 2c^2$ and $w = 2cd$. From $w = a^2 = 2cd$, we see that there are coprime integers s and t with $3 \nmid s$ such that $c = 2s^2$, $d = 2t^2$ and $a = \pm 2st$ where t is odd, or $c = s^2$, $d = 2t^2$ and $a = \pm 2st$ where s is odd. These two possibilities give us two more parametrizations of (4.5.1). Parametric Solution II:

$$\begin{aligned} x &= \pm(4s^4 + 3t^4)(16s^8 - 408s^4t^4 + 9t^8) \\ y &= 6st(4s^4 - 3t^2) \\ z &= 16s^8 + 168s^4t^4 + 9t^8 \end{aligned}$$

where t is odd and $3 \nmid s$. Parametric Solution III:

$$\begin{aligned} x &= \pm(s^4 + 12t^4)(s^8 - 408s^4t^4 + 144t^8) \\ y &= 6st(s^4 - 12t^4) \\ z &= s^8 + 168s^4t^4 + 144t^8 \end{aligned}$$

where s is odd and $3 \nmid s$.

We return to $u^2 - 3w^2 = b^2$. We had assumed u to be odd and found the above two parametrizations. Now we assume that u is even. This is the same case as we did in Case I of Section 4.3. There are odd integers c_1 and d_1 such that

$$\begin{aligned} u &= \pm\frac{c_1 + 3d_1^2}{2} \\ b &= \pm\frac{c_1 - 3d_1^2}{2} \\ w &= \pm c_1 d_1. \end{aligned}$$

We set $c_1 = c + d$ and $d_1 = c - d$ for some integers c and d which are odd and even respectively. Then we have $w = a^2 = c^2 - d^2$. So we have reduced the problem to finding the Pythagorean triples. There are integers s and t which are coprime and have different parities such that $c = s^2 + t^2$, $d = 2st$ and $a = s^2 - t^2$. Note that if $s \equiv t \pmod 3$ then we have that $c \equiv d \pmod 3$. But then we have $u = 2(c^2 + cd + d^2) \equiv 0 \pmod 3$ which contradicts that $3 \nmid u$. Replacing gives us Parametric Solution IV;

$$\begin{aligned} x &= \pm 2(s^4 + 2s^3t + 6s^2t^2 + t^4)(23s^8 - 16s^7t - 172s^6t^2 - 112s^5t^3 \\ &- 22s^4t^4 - 112s^3t^5 - 172s^2t^6 - 16st^7 + 23t^8) \\ y &= \pm 3(s - t)(s + t)(s^4 + 8s^3t + 6s^2t^2 8st^3 + t^4) \\ z &= 13s^8 + 16s^7t + 28s^6t^2 + 112s^5t^3 + 238s^4t^4 + 112s^3t^5 + 28s^2t^6 + 16st^7 + 13t^8 \end{aligned}$$

where s and t have different parities and $s \not\equiv t \pmod 3$.

4.6. Case of (2,3,5)

Now the equation is

$$x^2 + y^3 = z^5. \tag{4.6.1}$$

Note that the left-hand side of this equation can not be factorized in any field in a way that can help us, and so the methods we used in the previous sections do not work here. We apply a totally different approach given in [7]. A more general and detailed version of this idea is given in [10]. In fact the method is applied for also $\{p,q,r\} = \{2,3,3\}$ and $\{p,q,r\} = \{2,3,4\}$ cases, and gives a way to find nontrivial integer solutions to the equations of the form $x^2 + y^3 + dz^r = 0$ where d is a nonzero integer and $r \in \{3,4,5\}$. It is a generalization of Mordell's method [6].

We take a generic (or base) form of order k given by

$$f = \sum_{i=0}^{k} \binom{k}{i} a_i x_1^{k-i} x_2^i.$$

Let $g = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \in GL(2,\mathbb{C})$ act on $\mathbb{C}^2$ as

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \longmapsto g \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} g_{11}x_1 + g_{12}x_2 \\ g_{21}x_1 + g_{22}x_2 \end{bmatrix}$$

and define a' by $f(a', x_1, x_2) := f(a, g(x_1, x_2))$ where a and a' are coefficient vectors.

Definition 4.1. *A form $C \in \mathbb{C}[a_0, ..., a_k, x_1, x_2] = \mathbb{C}[a, x_1, x_2]$ is called a covariant if there is a $p \in \mathbb{Z}$ such that:*

$$C(a', x_1, x_2) = \det(g)^p C(a, g(x_1, x_2))$$

for all $g \in GL(2,\mathbb{C})$ where a' is defined above for fixed f and given g. The number p is called the weight of the covariant.

We may also write $C = C(f)$ to emphasize the dependence on the coefficients of f.

This definition and much of the later things in this section can be generalized to arbitrary fields and ring of integers [10]. But for our further purposes we work with $\mathbb{C}$ and $\mathbb{Z}$.

Example 4.1. *Let*

$$H(f) = \left(\frac{1}{k(k-1)}\right)^2 \begin{vmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{vmatrix}$$

and

$$t(f) = \frac{1}{k(k-2)} \begin{vmatrix} f_x & f_y \\ H_x & H_y \end{vmatrix}.$$

These are covariants of weight 2 and 3 respectively. Written explicitly

$$\begin{aligned} f &= a_0 x_1^k + ... \\ H(f) &= (a_0 a_2 - a_1^2) x_1^{2k-4} + ... \\ t(f) &= (a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3) x_1^{3k-6} + ... \end{aligned}$$

Later we will see a way to generate covariants. These covariants play a central role in two ways. First one is that the relation of the covariants $H(f)$ and $t(f)$ with f gives an idea to attack the equation (4.6.1). Next we will use these covariants to characterize the forms (in terms of coefficients) satisfying this relation.

Definition 4.2. *We define*

$$\begin{aligned} f_3 &:= x_2^4 - 2\sqrt{-3}x_1^2x_2^2 - x_1^4 \\ f_4 &:= x_1x_2(x_1^4 - x_2^4) \\ f_4^* &:= x_1x_2(x_1^4 + x_2^4) \\ f_5 &:= x_1x_2(x_2^{10} - 11x_1^5x_2^5 - x_1^{10}). \end{aligned}$$

We quote the following passage from [7] to summarize the derivation of these forms: "...Felix Klein embeds tetrahedron, octahedron and icosahedron on the 2-sphere which he then projects onto the extended complex plane. After a suitable rotation of the sphere, forms whose roots correspond to the vertices of the solid are" the forms we just defined above. We identify the exponent of z, r=3, 4 or 5 in $x^2 + y^3 + dz^r = 0$ with the order of the base forms k=4, 6 or 12 respectively. Here k and r denote the number of vertices and edges meeting at each vertex of the solid. Whenever we use r and k without explanation this identification should be understood. We let $(\beta_3, \beta_4, \beta_5) = (3\sqrt{3}, 432, 1728)$ to get the relations

$$\left(\frac{1}{2}t(f_r)\right)^2 + H(f_r)^3 + \frac{1}{\beta_r}f_r^r = 0$$

and

$$\left(\frac{1}{2}t(f_4^*)\right)^2 + H(f_4^*)^3 - \frac{1}{\beta_4}f_4^{*4} = 0.$$

As it is seen these equations provide a way to deal with the cases $\{p, q, r\} = \{2, 3, r\}$ for $r = 3, 4$ or 5. These equations can be verified by direct calculations.

Definition 4.3. *For $r \in \{3,4,5\}$ and for $d \in \mathbb{C}^*$ define:*

$$\begin{aligned} C(r) &:= \{f_r \circ g | g \in GL(2,\mathbb{C})\} \\ C(r,d) &:= \{f \in C(r) | \left(\frac{1}{2}t(f)\right)^2 + H(f)^3 + df^r = 0\}. \end{aligned}$$

Lemma 4.3. *We have $f_r \in C(r, \beta_r^{-1})$. Suppose $f \in C(r,d)$. If $g \in GL(2,\mathbb{C})$, then $f \circ g \in C(r, \det(g)^6 d)$ and if $\lambda \in \mathbb{C}^*$ then $\lambda f \in C(r, \lambda^{6-r} d)$.*

Proof. The first claim comes from the definition of β_r. For the second we observe that $t(f)^2, H(f)^3$ and f^r are covariants of weights 6, 6 and 0 respectively. The third one follws since

$$\begin{aligned} H(\lambda f) &= \lambda^2 H(f) \\ t(\lambda f) &= \lambda^3 t(f) \end{aligned}$$

and so

$$\left(\frac{1}{2}t(\lambda f)\right)^2 + H(\lambda f)^3 + d\lambda^{6-r}(\lambda f)^r = 0.$$

□

Proposition 4.1. *We have*

$$C(r,d) = \{f = f_r \circ g | \det(g)^6 = \beta_r d\}$$
$$C(r) = \bigcup_{d \in \mathbb{C}^*} C(r,d).$$

Proof. Proof follows by the previous lemma. □

$C(3)$ are the tetrahedral Klein forms, $C(4)$ are the octahedral Klein forms and $C(5)$ are the icosahedral Klein forms.

Definition 4.4 (Parametrizations)**.** *Given $f \in C(r,d)$ then:*

$$\Psi(f) := (\frac{1}{2}t(f), H(f), f)$$

is a parametrized solution to the equation $X^2 + Y^3 + dZ^r = 0$.

Below we define what we mean for $f \in C(r,d)$ to be integral.

Definition 4.5 (Integrality)**.** *Give $r \in \{3,4,5\}$ we consider $k = 4,6,12$ respectively. We define:*

$$\begin{aligned} \vartheta_3 &:= \{a_0, ..., a_4\} \\ \vartheta_4 &:= \{a_0, ..., a_6\} \\ \vartheta_5 &:= \{a_0, ...a_5, 7a_6, a_7, ..., a_{12}\}. \end{aligned}$$

Furthermore if f is a form of order k we write $\vartheta_r(f)$ to denote the specialization of ϑ_r to the coefficients of f. Let $R \subseteq \mathbb{C}$ be a ring (in practice $\mathbb{Z}$ or $\mathbb{R}$). We define:

$$C(r,d)(R) := \{f \in C(r,d) | \vartheta_r(f) \subseteq R\}$$

which we will consider as the subset of R-integral forms.

By these definitions the aim of studying binary forms become clear. We can divide the proof given in [7] into the following steps.

Step 1: We derive some equations for covariants of a form $f \in C(r,d)(\mathbb{Z})$ which allow us to determine the coefficients of f explicitly.

Step 2: We see that if (X, Y, Z) is a coprime solution to (4.6.1) then it is the integer specialization of a parametrization of the form $\Psi(f)$ with $f \in C(r, d)(\mathbb{Z})$ where $\Psi(f)$ is defined as in Definition 4.4.

Step 3: We see that any other $f' \in C(r, d)(\mathbb{Z})$ for which $\Psi(f')$ has (X, Y, Z) as an integer specialization is SL(2,$\mathbb{Z}$) equivalent to f.

Before going into the details of these steps we write basic results for integral forms.

Proposition 4.2. *Given $r \in \{3, 4, 5\}$ set $k = 4, 6, 12$ respectively. The set of order k forms such that $\vartheta_r(f) \subset \mathbb{Z}$ is closed under the action of $GL(2, \mathbb{Z})$. In particular $C(r, d)(\mathbb{Z})$ is closed under the action of $GL(2, \mathbb{Z})$.*

Proof. $\mathrm{GL}(2, \mathbb{Z})$ is generated by

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

So it is enough to show that the set of order k forms with $\vartheta_r(f) \subseteq \mathbb{Z}$ is closed under S, T and U. First we show it for S. We have that $S(x_1, x_2) = (x_2, -x_1)$. Let

$$f(x_1, x_2) = \sum_{i=0}^{k} \binom{k}{i} a_i x_1^{k-i} x_2^i$$

with $\vartheta_r(f) \subseteq \mathbb{Z}$. Then

$$f'(x_1, x_2) := f(S(x_1, x_2)) = \sum_{i=0}^{k} \binom{k}{i} a_i x_2^{k-i} (-x_1)^i = \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} a_{k-i} x_1^{k-i} x_2^i.$$

So we have that $\vartheta_r(f') \subseteq \mathbb{Z}$ (We may have that $a_6 \notin \mathbb{Z}$ in $k = 5$ case. But if we denote the coefficients of f' by a'_i, we see that $7a'_i = 7(-1)^6 a_6 \in \mathbb{Z}$). Thus we showed that the

set of order k forms with $\vartheta_r(f) \subseteq \mathbb{Z}$ is closed under S. It is easier to show that this set is also closed under U; we just replace x_2 by $-x_2$. Now the transformation T acts on $\mathbb{Z}$ as $T(x_1, x_2) = (x_1 + x_2, x_2)$. Let $f'(x_1, x_2) = f(x_1 + x_2, x_2)$. Then

$$\begin{aligned} f'(x_1,x_2) &= \sum_{i=0}^{k} \binom{k}{i} a_i \left(\sum_{j=0}^{k-i} \binom{k-i}{j} x_1^{k-i-j} x_2^{i+j} \right) \\ &= \sum_{i=0}^{k} a_i \left(\sum_{j=0}^{k-i} \binom{k}{k-i} \binom{k-i}{j} x_1^{k-(i+j)} x_2^{i+j} \right) \\ &= \sum_{i=0}^{k} a_i \left(\sum_{j=0}^{k-i} \binom{k}{i+j} \binom{i+j}{i} x_1^{k-(i+j)} x_2^{i+j} \right) \\ &= \sum_{i=0}^{k} a_i \left(\sum_{t=i}^{k} \binom{k}{t} \binom{t}{i} x_1^{k-t} x_2^{t} \right) \\ &= \sum_{t=0}^{k} \binom{k}{i} \left(\sum_{i=0}^{t} a_i \binom{t}{i} \right) x_1^{k-t} x_2^{t} \end{aligned}$$

which shows that

$$a'_t = \sum_{i=0}^{t} a_i \binom{t}{i} = a_t + \sum_{i=0}^{t-1} a_i \binom{t}{i}$$

where a'_t denotes the coefficient of the term containing x_1^{k-t} in f'. So for $r = 3, 4$ case the result follows. For the $r = 5$ case we only note that 7 divides $\binom{t}{6}$ for $6 < t \leq 12$, and so a'_t is an integer for $6 < t \leq 12$. Hence the proof is complete. □

Proposition 4.3. *Fix $r \in \{3, 4, 5\}$ and $k \in \{4, 6, 12\}$ respectively for the order of the base form. Let*

$$C = \sum_{i=0}^{m} C_i x_1^{m-i} x_2^i$$

be a covariant. Suppose $C_0 \in \mathbb{Z}[a_0, ..., a_k]$ and if $r = 5$ that the covariant has weight ≤ 5. Then $C(f) \in \mathbb{Z}[\vartheta_r, x_1, x_2]$. In particular, if $\vartheta_r(f) \subset \mathbb{Z}$ then $C(f) \in \mathbb{Z}[x_1, x_2]$.

Now we can deal with the three steps given above. First we give some properties of covariants. There are various operations on covariants. We define the Omega operator as

$$\Omega := \frac{\partial^2}{\partial x \partial y'} - \frac{\partial^2}{\partial y \partial x'}.$$

Given two forms C_1 and C_2, the i-th transvectant process is defined as

$$(C_1, C_2)_i := \left(\frac{(k-i)!}{k!}\right)^2 \Omega^i C_1(x, y) C_2(x', y')$$

where the partial derivatives are evaluated at $x, x' = x_1$ and $y, y' = x_2$. The transvectant process creates another form from given forms C_1 and C_2. If C_1 and C_2 are covariants of a base form then $(C_1, C_2)_i$ is also a covariant of that form. For example H and t defined above are $\tau_2(f)$ and $\tau_3(f)$ in the series

$$\tau_{2m}(f) := \frac{1}{2}(f, f)_{2m}, \qquad \tau_{2m+1}(f) := \frac{1}{2}(f, \tau_{2m}(f))_1.$$

For $k = 4$ we define the invariant j as

$$j(f) = \begin{vmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{vmatrix}$$

which has weight 6. In Lecture XII of [11] shows that we can identify covariants with their

leading terms. So we have:

$$\begin{aligned} f &= a_0x_1^k + ... \\ H(f) &= (a_0a_2 - a_1^2)x_1^{2k-4} + ... \\ t(f) &= (a_0^2a_3 - 3a_0a_1a_2 + 2a_1^3)x_1^{3k-6} + ... \\ \tau_4(f) &= (a_0a_4 - 4a_1a_3 + 3a_2^2)x_1^{2k-8} + ... \\ \tau_6(f) &= (a_0a_6 - 6a_1a_5 + 15a_2a_4 - 10a_3^2)x_1^{2k-12} + ... \\ j(f) &= a_0a_2a_4 + 2a_1a_2a_3 - a_2^3 - a_0a_3^2 - a_1^2a_4. \end{aligned}$$

The above forms play a crucial role in the proof. In [7] it is also proved that

$$\begin{aligned} C(3,d) &= \{f \in \mathbb{C}[x_1,x_2]_4 : \tau_4(f) = 0, j(f) = 4d\} \\ C(4,d) &= \{f \in \mathbb{C}[x_1,x_2]_6 : \tau_4(f) = 0, \tau_6(f) = 72d\} \\ C(5,d) &= \{f \in \mathbb{C}[x_1,x_2]_{12} : \tau_4(f) = 0, \tau_6(f) = (360/7)df\} \end{aligned} \tag{4.6.2}$$

where $\mathbb{C}[x_1,x_2]_k$ denotes the set of binary forms in x_1 and x_2 with complex coefficients and degree k. By the last result we complete the statement given in the Step I above. These characterizations with David Hilbert's important result given above allow us to determine the Klein forms. Now we pass to step 2; we show that any solution to $X^2 + Y^3 = dZ^r$ is the integer specialization of the form $\psi(f)$ with $f \in C(r,d)(\mathbb{Z})$.

Lemma 4.4. *Suppose $f \in C(r,d)$ and $X,Y,Z \in \mathbb{C}$ satisfy $X^2 + Y^3 + dZ^r = 0$, then there exist $s_1, s_2 \in \mathbb{C}$ such that $\psi(f)(s_1,s_2) = (X,Y,Z)$.*

Proof. First we consider $f' = f_3, f_4^*, f_5$ along with

$$m' = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$$

respectively. We see that $\det(m^{'})$=-1 and $f^{'} \circ m^{'} = f^{'}$ in all cases. Also $f = f' \circ h$ for some $h \in GL(2, \mathbb{C})$. So if we let $m = h^{-1} m^{'} h$, we have $f \circ m = f' \circ h \circ h^{-1} \circ m^{'} \circ h = f^{'} \circ h = f$, i.e. m fixes f. We note that $\det(m)$=-1. We put

$$\begin{aligned} H(f)(s_1, s_2) &= Y, \\ f(s_1, s_2) &= Z. \end{aligned}$$

From these two equations in two unknowns s_1 and s_2 we find s_1 and s_2. Since $f \in C(r, d)$ we must have $t(f)(s_1, s_2) = \pm 2X$. If it is $+2X$ then we are done. If it is $-2X$ we replace $(s_1, s_2)^T$ with $m(s_1, s_2)^T$ where m is defined above. Note that $H(f)$ and f have even weight (0 and 2 respectively) and $\det(m) = -1$. So the values of $H(f)$ and f do not change. But since $t(f)$ has weight 3 we have the desired result. □

Theorem 4.1 (Lifting Theorem)**.** *Fix d a non-zero integer and $r \in \{3, 4, 5\}$. Suppose that $X, Y, Z \in \mathbb{Z}$ satisfy $X^2 + Y^3 + dZ^r = 0$ with* $\gcd(X, Y, Z)$=*1. Then there exists a binary form $f \in C(r, d)$ and $s_1, s_2 \in \mathbb{Z}$ such that*

$$\Psi(f)(s_1, s_2) = (X, Y, Z).$$

Proof. We take an arbitrary $f \in C(r, d)$ and find s_1, s_2 by Lemma 4.4 such that $\Psi(f)(s_1, s_2) = (X, Y, Z)$. From Proposition 4.1 we know that $C(r, d)$ is closed under $SL(2, \mathbb{C})$ transformations. We apply suitable transformations and get

$$\begin{aligned} f(1, 0) &= a_0 = Z \\ H(1, 0) &= (a_0 a_2 - a_1^2) = Y \\ t(1, 0) &= (a_0^2 a_3 - 3 a_0 a_1 a_2 + 2 a_1^3) = 2X. \end{aligned}$$

Now we want to find an appropriate $\lambda \in \mathbb{C}$ and apply the transformation $(x, y) \longmapsto (x + \lambda y, y)$. This substitution does not change the value of f at $(1, 0)$.

If $Z = a_0 = 0$, then $a_1 \neq 0$. Otherwise we would have $f(1,0) = H(1,0) = 0$ and this would imply that f has a multiple root. But Klein forms do not have any multiple roots. Since gcd(X,Y)=1, we have $X, Y, Z = \pm 1, -1, 0$ which means that $a_0, a_1, a_2 = 0, \pm 1, 0$.

Now if $Z = a_0 \neq 0$ we choose λ such that a_1 takes any integer value. Since gcd(Y,Z)=1, Y is invertible modulo Z^r. We choose λ so that a_1 is an integer which satisfies $a_1 \equiv -X/Y \pmod{Z^r}$. From $H(1,0) = Y$ and $t(1,0) = 2X$ we have

$$\begin{aligned} a_0 a_2 &\equiv Y + \left(\frac{X}{Y}\right)^2 = -\frac{dZ^r}{Y^2} \\ a_0^2 a_3 &\equiv -X\frac{X^2+Y^2}{Y^3} = -\frac{dXZ^r}{Y^3} \end{aligned}$$

in modulo Z^r. This shows that a_0, a_1, a_2, a_3 are all in $\mathbb{Z}$. The rest of the proof is done by using the defining equations of $C(r,d)$ which are given in (4.6.2).

By equating the coefficients all of the other constants can be determined and seen to have the property that $\vartheta_r(f) \subset \mathbb{Z}$. By Proposition 4.3 we complete the proof. □

This theorem completes Step 2. The next theorem finishes step 3.

Theorem 4.2 (Uniqueness Theorem)**.** *Suppose $f_1, f_2 \in C(r,d)(\mathbb{Z})$. Let $\Gamma(f_i) \subset \mathbb{Z}^3$ be the set of relatively prime integers X, Y, Z which occur by specializing the parametrization $\Psi(f_i)$ to integers. Suppose $(X,Y,Z) \in \Gamma(f_i)$. Then*

- *If $(X,Y,Z) \in \Gamma(f_2)$, then f_1 is $SL(2,\mathbb{Z})$ equivalent to f_2.*
- *If $(-X,Y,Z) \in \Gamma(f_2)$, then f_1 is $GL(2,\mathbb{Z})$ equivalent to f_2.*

In particular $\Gamma(f_i)$ are either equal or disjoint.

Proof. Suppose that $(X, Y, Z) \in \Gamma(f_1)$. First we will prove that f_1 is $SL(2, \mathbb{Z})$ to an f whose coefficients are determined only by (X, Y, Z). So if we also have $(X, Y, Z) \in \Gamma(f_2)$, this means that f_2 will also be $SL(2, \mathbb{Z})$ equivalent to f, and so will be $SL(2, \mathbb{Z})$ equivalent to f_1. Since $\vartheta_r(f_1) \subseteq \mathbb{Z}$ we have $f_1, H(f_1) \in \mathbb{Z}[x_1, x_2]$. So we can find relatively prime integers s_1 and s_2 by using the Lifting Theorem such that $f_1(s_1, s_2) = Z$, $H(f_1)(s_1, s_2) = Y$ and $t(f_1)(s_1, s_2) = 2X$. Since $\gcd(s_1, s_2) = 1$, there are integers t_1 and t_2 such that $s_1t_1 + s_2t_2 = 1$. Now we consider the matrix

$$g = \begin{pmatrix} s_1 & -t_2 \\ s_2 & t_1. \end{pmatrix}$$

We see that $g \in SL(2, \mathbb{Z})$ and $g(1, 0)^T = (s_1, s_2)^T$. Thus replacing f_1 by $f = f_1 \circ g$ we can assume that the specialization is at $(1, 0)$. We now show that f is uniquely determined up to $(x_1, x_2) \longmapsto (x_1 + nx_2, x_2)$ where $n \in \mathbb{Z}$.

First we consider the case where $Z = 0$. Then we must have $(X, Y, Z) = (\pm 1, 1, 0)$. So $a_0 = 0$ and $a_1 = \pm 1$. If necessary we replace (x_1, x_2) by $(x_1 + nx_2, x_2)$ for a suitable n and assume that $a_2 = 0$ or 1. But one of the defining equaitons of $C(r, d)$ is that $\tau_4(f) = 0$. The leading term of $\tau_4(f)$ is $a_0a_4 - 4a_1a_3 + 3a_2^2$ and we know that $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}$. So we must have $a_2 = a_3 = 0$. The remaining a_i can be now completely determined by using the defining equations of $C(r, d)$.

Next we consider the case where $Z \neq 0$. Then we have $a_0 = Z$. Again we use the leading term of $\tau_4(f)$ which is $a_0a_4 - 4a_1a_3 + 3a_2^2$. If $Z = a_0$ is even then since $a_0a_4 - 4a_1a_3 + 3a_2^2 = 0$ we must have that a_2 is even. We look at $H(f)(1, 0) = a_0a_2 - a_1^2 = Y$ and $t(f)(1, 0) = a_0^2a_3 - 3a_0a_1a_2 + 2a_1^3 = 2X$. From the first one we get $-a_1^2 \equiv Y \pmod{Z}$. If we let $2^t \mid\mid Z$, then from the second equation we get $a_1^3 \equiv X \pmod{2^t}$ and $a_1^3 \equiv X \pmod{Z/2^t}$. Combining these results and using the fact $\gcd(X, Y, Z)=1$ we have that $a_1 \equiv -X/Y \pmod{Z}$. By replacing $f(x_1, x_2)$ by $f(x_1 + nx_2, x_2)$ for a suitable integer n we

may assume $0 \leq a_1 < |Z|$. So we determined a_1. Now by using $H(f)(1,0) = a_0a_2 - a_1^2 = Y$ and $t(f)(1,0) = a_0^2a_3 - 3a_0a_1a_2 + 2a_1^3 = 2X$ once more we find a_2 and a_3. The remaining a_i can be completely determined by defining equations of $C(r,d)$. Thus we have proved that f_1 is $SL(2,\mathbb{Z})$ equivalent to f whose coefficients can be determined by (X,Y,Z), and so the first claim of the theorem.

For the second claim we take any $g \in GL(2,\mathbb{Z})$ such that det(g)=-1. Let $f' = f_2 \circ g$. Since f_2, H, t has even, odd and even weights respectively we get

$$\left(\frac{1}{2}t(f'), H(f'), f'\right) = \left(-\frac{1}{2}t(f_2 \circ g), H(f_2 \circ g), f_2 \circ g\right).$$

So (X,Y,Z) occurs by specializing the parametrization $\Psi(f')$ to integers. Now we use the first claim and conclude that f' is $SL(2,\mathbb{Z})$ equivalent to f_1. Thus f_2 is $GL(2,\mathbb{Z})$ equivalent to f_1. □

The Lifting theorem gives the existence of the desired binary form and the Uniqueness theorem seperates those binary forms into disjoint classes. Every form in a fixed class is equivalent to other forms in that class. Now we recall the reduction theory of positive definite real binary quadratic forms and generalize it to higher order forms. In that theory we say that a form is reduced if the unique root z_0 in $\mathbb{H}$, i.e. in the upper half-plane is in the fundamental domain for $SL(2,\mathbb{Z})$ given by

$$D := \{z = x + iy : |z| > 1, -\frac{1}{2} \leq x \leq \frac{1}{2}\}$$

Every form is $SL(2,\mathbb{Z})$ equivalent to a reduced form and there is bound on the coefficients of reduced forms in terms of the discriminant, i.e. reduced forms of a given discriminant is finite. In [7] Hermite reduction theory takes place of the reduction theory of positive definite real binary quadratic forms. The Hermite determinant takes the place of the

discriminant. There is an associated representative point z_0 in $\mathbb{H}$ - usually unique. A form is reduced if z_0 in $\mathbb{H}$ is in the fundamental domain for $SL(2,\mathbb{Z})$. Every form is $SL(2,\mathbb{Z})$ equivalent to some reduced form, and there is a bound on the coefficients of reduced forms in terms of the Hermite determinant.

Now the way to find the solutions of Diophantine equations of the form $X^2 + Y^3 + dZ^r = 0$ reduces to finding Hermite reduced forms $f \in C(r,d)(\mathbb{Z})$, classifying them into $GL(2,\mathbb{Z})$ inequivalent forms and deleting the forms not specializing to coprime integers. These steps are given in details in Sections 4 and 5 of [7] and the 27 parametrizations are found for (4.6.1). Since this theory is beyond the scope of this thesis we do not give these steps here.

5. HYPERBOLIC CASES

Many of the special cases of generalized Fermat equation falls into this category. It is proved in [2] that for any fixed A, B, C and fixed p, q and r with $1/p+1/q+1/z < 1$, (1.0.1) can have at most finitely many nontrivial solutions. To prove this Darmon and Granville reduced the problem to Faltings' theorem on the finiteness of the number of rational points on a curve of genus greater than 1. The difficulty of this problem is due to the fact that saying whether the equation $Ax^p + By^q + Cz^r$ represents a curve or not is itself a very difficult problem. It is conjectured that for $A = B = C = 1$, the equations of this category with fixed $p, q, r \geq 3$ has no nontrivial solutions in integers. Fermat equation, $x^p + y^p = z^p$ for $p \geq 4$ which has been proven to have no nontrivial solutions in integers in [12] is an example of such equations.

We know that the above conjecture is not correct if we allow one of the exponents be equal to 2. Below we give the known results about such cases [8].

$$\begin{aligned}
1^r + 2^3 &= (\pm 3)^2 \quad (for \quad r \geq 7), \\
(\pm 3)^4 + (-2)^5 &= (\pm 7)^2, \\
2^9 + (-7)^3 &= (\pm 13)^2, \\
2^7 + 17^3 &= (\pm 71)^2, \\
3^5 + (\pm 11)^4 &= (\pm 122)^2, \\
15613^3 - (\pm 33)^8 &= (\pm 1549034)^2, \\
65^7 + (-1414)^3 &= (\pm 2213459)^2, \\
113^7 + (-9262)^3 &= (\pm 15312283)^2, \\
17^7 + 76271^3 &= (\pm 21063928)^2, \\
(\pm 43)^8 + 96222^3 &= (30042907)^2.
\end{aligned}$$

It is not known whether the list is complete or not. This is another unsolved problem related to Diophantine equations. We can summarize what we said above in the following conjecture from [1]:

Conjecture 1. *The diophantine equation*

$$x^p + y^q = z^r$$

in $x, y, z \in \mathbb{Z}$ *with* $gcd(x, y, z)$*=1,* $xyz \neq 0$ *and* $p, q, r \in \mathbb{Z}_{\geq 3}$ *has no solutions.*

We should also mention the *abc-conjecture* since it has close connections with Diophantine equations. But first we make a definition from [8].

Definition 5.1. *For a nonzero natural number* N *we define the* radical rad(N) *of* N *as the product of distinct prime numbers dividing* N*, i.e.*

$$\mathrm{rad}(N) = \prod_{p|N} p.$$

For example rad(600)=rad$(2^3 \cdot 3 \cdot 5) = 2 \cdot 3 \cdot 5 = 30$. The *abc-conjecture* is as follows.

Conjecture 2. *Let* $\epsilon > 0$*. If* a*,* b *and* c *are three nonzero pairwise coprime integers such that* $a + b + c = 0$ *then*

$$\max\{|a|, |b|, |c|\} = O_\epsilon(\mathrm{rad}(abc)^{1+\epsilon})$$

where $y = O_\epsilon(x)$ *means that* $|y| < K_\epsilon x$ *for some positive constant* K_ϵ *depending only on* ϵ*.*

The *abc-conjecture* leads to the following result.

Proposition 5.1. *The abc-conjecture implies that the total number of nonzero coprime solutions to* $x^p \pm y^q \pm z^r = 0$ *with* $1/p + 1/q + 1/z < 1$ *is finite, even allowing* p, q *and* r *to vary. Here, if* $x = \pm 1$ *(respectively* $y = \pm 1$, *respectively* $z = \pm 1$*) we identify solutions having the same value of* x^p *(respectively* y^q, *respectively* z^r*).*

Proof. Without loss of generality we can assume that $p \leq q \leq r$. We start listing the possible values of p, q and r according to the constraint $1/p + 1/q + 1/z < 1$ starting from $p = 2$. For $p = 2$ we can only have one of the triples $(2, 3, r)$ for $r \geq 7$, $(2, 4, r)$ for $r \geq 5$ and $(2, q, r)$ for $r \geq q \geq 5$. For $p = 3$ our triples may be one of $(3, 3, r)$ for $r \geq 4$ and $(3, q, r)$ for $r \geq q \geq 4$. For $p \geq 4$ any triple (p, q, r) satisfies our condition. In all of these possibilities we have that $1/p + 1/q + 1/z \leq 41/42$ which is attained at $(p, q, r) = (2, 3, 7)$. We let $\epsilon = 41/42$ and apply the *abc-conjecture* to $a = x^p$, $b = \pm y^q$ and $c = \pm z^r$. We have that rad(abc)=rad$(xyz) \leq |xyz|$. We put $M = \max\{|x^p|, |y^q|, |z^r|\}$. Then we have $|xyz| \leq M^{1/p+1/q+1/r}$. So by the *abc-conjecture* we have

$$\begin{aligned} M &= O((xyz)^{1+\epsilon}) = O(M^{(1/p+1/q+1/z)(1+\epsilon)}) \\ &= O(M^{(41/42)(43/42)}) = O(M^{1763/1764}) \end{aligned}$$

which is impossible for sufficiently large M. Thus M must be bounded, and so are x, y, z, p, q and r (except in the special case $\min\{|x|, |y|, |z|\} = 1$). This special case is already known as Catalan's conjecture, i.e. $x^p \pm y^q = 1$ is possible only if $x^p = 9$ and $y^q = 8$. But this conjecture has been proved by P. Mihailescu in [13]. □

In the remaining sections we work on some nonhomogeneous equations of 4^{th} degree.

5.1. Case of (4,4,3)

It will be proved that the following nonhomogeneous Diophantine equation of fourth degree has no nontrivial solutions in integers (x, y, z),

$$x^4 + y^4 = z^3. \tag{5.1.1}$$

To prove that (5.1.1) has no solutions in positive integers x, y and z, we need to prove the following lemma.

Lemma 5.1. *The Diophantine equation*

$$x^4 - 3y^4 = z^2 \tag{5.1.2}$$

has no solution in positive integers x, y and z.

Proof. First note that we can assume $\gcd(x, y, z)$=1. Otherwise if a rational integer, c divides all of x, y and z then we have

$$c^4 \left(\frac{x}{c}\right)^4 - 3c^4 \left(\frac{y}{c}\right)^4 = c^4 \left(\frac{z}{c^2}\right)^2.$$

So we can cancel all of the common factors of x, y and z until $\gcd(x, y, z)$=1. Only the case in which 3 divides both of x and z needs more steps. But in this case it can easily be seen that 3 must also divide y and the same argument follows. We also note that x and y should have different parities. Otherwise left-hand side of (5.1.2) would be congruent to 2 modulo 4. But $z^2 \equiv 2 \pmod 4$ is impossible. Powers of x, y and z are even, thus it is a

matter of choice to assume x, y and z to be positive or negative. We write (5.1.2) as

$$(x^2 - z)(x^2 + z) = 3y^4.$$

Since $\gcd(x, y, z) = 1$ we know that only one of the factors in the left-hand side of the above equation is divisible by 3. If necessary we may replace z by $-z$ and assume that $3 \mid (x^2 - z)$. First we deal with the case where y is odd and x is even. Then z must be necessarily odd. But then $x^4 \equiv 0 \pmod 8$, and $3y^4 + z^2 \equiv 4 \pmod 8$ which gives a contradiction.

So we must only consider the case where y is even, x and z are both odd. Then we have $2 \mid (x^2 - z)$ and $2 \mid (x^2 + z)$. Since x and z are odd, then we must have $2 \mid\mid (x^2 - z)$ or $2 \mid\mid (x^2 + z)$, but not both. First we assume that $2 \mid\mid (x^2 - z)$. Then by using the above equation we get

$$\begin{aligned} x^2 - z &= 6u^4 \\ x^2 + z &= 8v^4 \end{aligned}$$

for some rational integers u and v such that u is odd. Then we have $x^2 = 3u^4 + 4v^4$ with x and u being odd. But this equation can not have any solutions in modulo 4.

Now we assume that $2 \mid\mid (x^2 + z)$. Let S be the set of nonzero pairwise coprime solutions to (5.1.2) with y being even. If S is nonempty, we can take a solution (x, y, z) which makes $|y|$ as small as possible. Then we have

$$\begin{aligned} x^2 - z &= 24u^4 \\ x^2 + z &= 2v^4 \end{aligned}$$

for some rational integers u and v such that v is odd. Then we get $x^2 = 12u^4 + v^4$, $z = v^4 - 12u^4$ and $|y| = 2|uv|$. We write the first of these two equations as

$$(x - v^2)(x + v^2) = 12u^4.$$

We may replace v by $-v$ to assume that $3 \mid (x - v^2)$. Then we have

$$\begin{aligned} x - v^2 &= 6u_1^4 \\ x + v^2 &= 2v_1^4 \end{aligned}$$

for some rational integers u_1 and v_1. From these two equations we get $v^2 = v_1^4 - 3u_1^4$ and $|u| = |u_1 v_1|$. We know that the first one of these two equations have no solutions in integers if u_1 is odd. But if it is even then we have that $|u_1| \leq |u| < |y|$ which contradicts the way we have chosen y. Thus the proof is complete. □

Now we can state and prove our main theorem.

Theorem 5.1. *The Diophantine equation,*

$$x^4 + y^4 = z^3$$

has no nontrivial solution in positive integers (x, y, z).

Proof. Assume that (x, y, z) is a nontirivial solution to (5.1.1). First we will factorize (5.1.1) in $\mathbb{Z}[i]$ as

$$(x^2 + iy^2)(x^2 - iy^2) = z^3. \tag{5.1.3}$$

Now if x and y were both odd, then we would have $x^4 \equiv y^4 \equiv 1$ in (mod 4) and then

$z^3 \equiv 2 \pmod 4$, which is impossible. So we can assume that x is odd, y is even and z is odd. Because of the unique factorization property of $\mathbb{Z}[i]$, the factors in the left hand side of (5.1.3) must be cubes in $\mathbb{Z}[i]$. Let

$$x^2 \pm iy^2 = (k \pm li)^3$$

where gcd(k,l)=1. Then we have

$$x^2 = k(k^2 - 3l^2)$$
$$y^2 = l(3k^2 - l^2).$$

Now we will work on three cases.

Case I: $3 \mid k$, $3 \nmid l$. Let $k = 3m$. Then we have

$$\left(\frac{x}{3}\right)^2 = m(3m^2 - l^2).$$

Then we have $m = a^2$ and $3m^2 - l^2 = b^2$ for some positive rational integers a and b. But from $y^2 = l(3k^2 - l^2)$ we deduce that $l = g^2$ for some positive rational integer g and so we have

$$3a^4 - g^4 = b^2.$$

But this equation has no solution in modulo 4.

Case II: $3 \mid l$, $3 \nmid k$. Let $l = 3n$. Then we have

$$\left(\frac{y}{3}\right)^2 = n(k^2 - 3n^2).$$

Then by a similar argument to Case I, we have an equation as

$$a^4 - 3g^4 = b^2$$

where $a^2 = k$, $g^2 = n$ and $b^2 = k^2 - 3n^2$. But by Lemma 5.1, the last equation has no solution in positive integers.

Case III: $3 \nmid kl$. In this case $k = m^2$, $l = n^2$ and $k^2 - 3l^2 = a^2$ for some positive integers m, n and a. Thus we obtain

$$m^4 - 3n^4 = a^2$$

which again does not have solutions in positive integers by Lemma 5.1. □

5.2. Case of (3,4,4)

We will show that the following Diophantine equation has no nontrival solution in integers x, y and z.

$$x^3 + y^4 = z^4. \tag{5.2.1}$$

We first see that exactly two of the variables x, y and z must be odd. This observation naturally results in three distinct cases which will be proved separately. But before we continue we write (5.2.1) as

$$x^3 = (z^2 + y^2)(z^2 - y^2) = (z^2 + y^2)(z - y)(z + y).$$

The method is to show that each of the three factors in the last equation in must be a perfect cube or some multiple of a perfect cube. To do this we will try to determine the (possible) common divisors of these three factors.

Case I: $2 \nmid xz$, $2 \mid y$. If an integer k divides both of $z^2 + y^2$ and $z^2 - y^2$, then k divides $2z^2$. But since both of $z^2 + y^2$ and $z^2 - y^2$ are odd, we have that k divides both z^2 and y^2. So $k = 1$. A similar argument gives that if k is a common divisor of $z - y$ and $z + y$, then k must be equal to 1. Hence all of the three factors in the right-hand side of the above equation are pairwise coprime and so must be perfect cubes. Let

$$z - y = a^3$$
$$z + y = b^3$$
$$z^2 + y^2 = c^3$$

for some integers a, b and c. Then we have

$$2z = a^3 + b^3$$
$$2y = b^3 - a^3.$$

By taking squares of both sides in the last two equations and adding them, we have

$$a^6 + b^6 = 2c^3.$$

But by Lemma 3.2 the only solutions of the above equation are $a^2 = b^2 = 1$ which implies that $y = 0$.

Case II: $2 \nmid xy$, $2 \mid z$. In fact the proof of case I also includes this case since changing the parity of y and z does not make any difference in the proof of case I.

Case III: $2 \mid x$, $2 \nmid yz$. Since y and z are both odd we have that $z^2 + y^2 \equiv 2 \pmod 4$, i.e. the highest power of 2 dividing $z^2 + y^2$ is 1. Also we have that $z - y$ and $z + y$ are both divisible by 2 and exactly one of them is divisible by 4. Then $16 \mid x^3$ and so $2^6 \mid x^3$. Then 2^k with $k \geq 2$ either divides $z - y$ or $z + y$. But if necessary we may replace y by $-y$ to assume that $2^k \mid (z - y)$, i.e. $2 \mid\mid (z + y)$. Then we write

$$2^3 \left(\frac{x}{2}\right)^3 = 2 \left(\frac{z^2 + y^2}{2}\right) 2 \left(\frac{z + y}{2}\right) (z - y).$$

After cancelling the factor 2 in both sides, we get

$$2 \left(\frac{x}{2}\right)^3 = \left(\frac{z^2 + y^2}{2}\right) \left(\frac{z + y}{2}\right) (z - y).$$

Now the factors in the right-hand side of this equation are pairwise coprime. Then since $(z^2 + y^2)/2$ and $(z + y)/2$ are odd, there are pairwise coprime rational integers a, b and c such that

$$\begin{aligned} z - y &= 2a^3 \\ z + y &= 2b^3 \\ z^2 + y^2 &= 2c^3. \end{aligned}$$

But from these equations we get $a^6 + b^6 = c^3$ which does not have any nontrivial solutions in integers by Theorem 3.1.

5.3. Case of (3,3,4)

We will prove the following theorem.

Theorem 5.2. *The Diophantine equation*

$$x^3 - y^3 = z^4 \tag{5.3.1}$$

has no nontrivial solution in integers x, y and z.

Note that it does not make any difference changing the sign of y^3. Without loss of generality we may assume that $x > 0$. We write (5.3.1) as $(x-y)(x^2+xy+y^2) = z^4$. Then we have $\gcd(x-y, x^2+xy+y^2)$=$\gcd(x-y, 3xy)$=1 or 3. First we deal with the case where the greatest common divisor is 3. Now we recall the results of Section 4.3. In Section 4.3 we have found the parametric solutions of the equation $z^2 = x^3 + y^3$. We are in the second case of that section where $3 \mid z$. Here we only put z^2 instead of z in (4.3.3) and (4.3.4). Then we have one of the following equalities;

$$z^2 = 3(s-t)(s+t)(s^4 + 2s^3t + 6s^2t^2 + 2st^3 + t^4)$$

with s and t having different parities, $\gcd(s,t)$=1 and $s - t \not\equiv 0 \pmod 3$, or

$$z^2 = 6st(3s^4 + t^4)$$

with s and t having different parities, $\gcd(s,t)$=1 and $3 \nmid t$.

Now we consider the equality $z^2 = 3(s-t)(s+t)(s^4 + 2s^3t + 6s^2t^2 + 2st^3 + t^4)$ with $s - t \not\equiv 0 \pmod 3$. By trying all possibilities for s and t in modulo 3, we see that the last factor is not divisible by 3. Also if any prime number c divides two of these three factors we get a contradiction; for example if c divides both $(s+t)$ and $(s^4 + 2s^3t + 6s^2t^2 + 2st^3 + t^4)$, we have $s \equiv -t \pmod c$. Putting this in the other factor we have $t^4 - 2t^4 + 6t^4 - 2t^4 + t^4 \equiv 4t^4 \equiv 0 \pmod c$. Then we must have c =2 or c divides t. But s and t have different

parities, so c must divide t. But this contradicts that gcd(s,t)=1. The other cases can be considered in a similar way. Then we must have

$$\begin{aligned} s-t &= b^2 \\ s+t &= 3c^2 \\ s^4+2s^3t+6s^2t^2+2st^3+t^4 &= u^2 \\ z &= 3bcu. \end{aligned}$$

for some positive integers b, c and u. Then we have

$$\begin{aligned} (s-t)^4 &= b^8 = s^4-4s^3t+6s^2t^2-4st^3+t^4 \\ (s+t)^4 &= 3^4c^8 = s^4+4s^3t+6s^2t^2+4st^3+t^4. \end{aligned}$$

So we see that

$$\begin{aligned} s^4+6s^2t^2+t^4 &= (b^8+3^4c^8)/2 \\ 2s^3t+2st^3 &= (3^4c^8-b^8)/4. \end{aligned}$$

Adding these two equalities we get

$$4u^2 = 3^5c^8+b^8.$$

Since s and t have different parities b and c must be odd. But for any odd number v, $v^8 \equiv 1 \pmod{32}$. So the right side of the last equation is equivalent to 20 in modulo 32. But we also have that u is odd and so $4u^2 \equiv 4$ or $28 \pmod{32}$. So we do not have any solution in this form. Now in the other case we have

$$z^2 = 6st(3s^4+t^4)$$

along with $s \not\equiv t \pmod 2$ and $3 \nmid t$. Then we have that $3s^4 + t^4$ is odd and not divisible by 3. So it must be a perfect square, i.e. $3s^4 + t^4 = u^2$ for some positive odd integer c. We can easily see that s can not be odd by considering in modulo 4. So s must be even and t must be odd. So we put

$$\begin{aligned} s &= 6s_1^2 \\ t &= t_1^2 \\ 3s^4 + t^4 &= u^2. \end{aligned}$$

We write the last equation as

$$(u - t_1^4)(u + t_1^4) = 3^5 2^4 s_1^4$$

where u and t_1 are odd. Now we will apply a descent to this equation. The variables s_i below denote nonzero integers. We pick a solution which makes $|u|$ smallest. We may replace u by $-u$, so we we may assume that 3 divides $(u - t_1^4)$. We have two cases. The first one is that $2 || (u + t_1^4)$. Then we have

$$\begin{aligned} u + t_1^4 &= 2s_2^8 \\ u - t_1^4 &= 3^5 2^3 s_3^8 \end{aligned}$$

where s_2 is odd. Then we have

$$t_1^4 = s_2^8 - 3^5 2^2 s_3^8.$$

We write the last equation as

$$(s_2^4 - t_1^2)(s_2^4 + t_1^2) = 3^5 2^2 s_3^8.$$

The first factor above is divisible by 3, but the second one is not. So we have

$$\begin{aligned} s_2^4 - t_1^2 &= 3^5 2 s_4^8 \\ s_2^4 + t_1^2 &= 2 s_5^8 \end{aligned}$$

where s_5 is odd. From here we get

$$s_2^4 = s_5^8 + 3^5 s_4^8.$$

We write the last equation as

$$(s_2^2 - s_5^4)(s_2^2 + s_5^4) = 3^5 s_4^8.$$

Here we note that the second factor is $\equiv 2 \pmod 8$ and is not divisible by 3. So we can write

$$\begin{aligned} s_2^2 - s_5^4 &= 2^7 3^5 s_6^8 \\ s_2^2 + s_5^4 &= 2 s_7^8 \end{aligned}$$

where s_7 is odd. From here we have

$$s_5^4 = s_7^8 - 2^6 3^5 s_6^8.$$

We write the last equation as

$$(s_7^4 - s_5^2)(s_7^4 + s_5^2) = 2^6 3^5 s_6^8.$$

Then we have

$$\begin{aligned} s_7^4 - s_5^2 &= 2^5 3^5 s_8^8 \\ s_7^4 + s_5^2 &= 2s_9^8 \end{aligned}$$

where s_9 is odd. Then we have

$$s_7^4 = 3^5 2^4 s_8^8 + s_9^8.$$

But we have that $|u| > s_3^8 = |s_4 s_5|^8 \geq |s_4|^8 = |s_6 s_7|^8 \geq |s_7|^2$ which gives the contradiction.

Now we deal with the case where 2 divides $(u - t_1^4)$ but 4 does not divide. Then we have

$$\begin{aligned} u - t_1^4 &= 3^5 2 s_2^8 \\ u + t_1^4 &= 2^3 s_3^8 \end{aligned}$$

where s_2 is odd. Then we have

$$t_1^4 = 2^2 s_3^8 - 3^5 s_2^8.$$

We write this equation as

$$(2s_3^4 - t_1^2)(2s_3^4 + t_1^2) = 3^5 s_2^8.$$

Since the first factor is not divisible by 3 we have

$$\begin{aligned} 2s_3^4 + t_1^4 &= 3^5 s_4^8 \\ 2s_3^4 + t_1^4 &= s_5^8 \end{aligned}$$

where both s_4 and s_5 are odd. Then we have

$$4s_3^4 = 3^5 s_4^8 + s_5^8.$$

But we showed that this equation has no solution in modulo 32. Hence we have completed the case where $\gcd(x-y, x^2+xy+y^2)$=3.

Now we deal with the case where $\gcd(x-y, x^2+xy+y^2)$=1. We can use the solution set of the equation $x^3+y^3=z^2$ as we did above. But here we will give the method in [14]. In this case z is not divisible by 3. Then we have

$$\begin{aligned} x - y &= u^4 \\ x^2 + xy + y^2 &= v^4 \\ z &= uv \end{aligned}$$

for some rational integers u and v such that $\gcd(u,v) = 1$, $3 \nmid uv$ and v is odd. If we put $x = u^4 + y$ in the second equation and solve for y, we get

$$y = \frac{-3u^4 \pm \sqrt{12v^4 - 3u^8}}{6}.$$

Hence $12v^4 - 3u^8$ must be a perfect square. So there is an integer c such that $4v^4 = u^8 + 3c^2$. Note that $(u^8, v^4, c^2) = (1,1,1)$ is a solution of this equation, but all possibilities give trivial

solutions to $x^3 - y^3 = z^4$. We write

$$(2v^4 - u^4)(2v^4 + u^4) = 3c^2.$$

The first factor is not divisible by 3. Since gcd(u, v)=1, we have $d :=$gcd$(2v^4 - u^4, 2v^4 + u^4)$ divides 4. But d can not be 4, since 4 can not divide $2v^4 - u^4$. If $d = 2$, then u must be even and so we have

$$\begin{aligned} 2v^4 - u^4 &= 2s^2 \\ 2v^4 + u^4 &= 6t^2. \end{aligned}$$

Putting $u = 2w$, we get the equations

$$\begin{aligned} v^2 - 8w^4 &= s^2 \\ v^2 + 8w^4 &= 3t^2. \end{aligned}$$

From these two equations we get

$$16w^4 = 3t^2 - s^2$$

which is impossible in modulo 16 since s and t are odd. Hence we have $d = 1$. Then we have

$$\begin{aligned} 2v^4 - u^4 &= s^2 \\ 2v^4 + u^4 &= 3t^2 \end{aligned}$$

where s and t are odd. Then we have

$$\begin{aligned} 4v^4 &= s^2 + 3t^2, \qquad (*) \\ 2u^4 &= 3t^2 - s^2. \qquad (**) \end{aligned}$$

Note that $3 \nmid s$. We write the first equation above as $(2v - s)(2v + s) = 3t^2$. Here exactly one of the factors of $2v - s$ and $2v + s$ is divisible by 3. But since we may change s by $-s$, we can assume that $2v + s$ is divisible by 3. Since v and s are odd and coprime, we have

$$\begin{aligned} 2v - s &= k^2 \\ 2v + s &= 3l^2 \end{aligned}$$

where $\gcd(k, l)$=1. Then we have $4v = k^2 + 3l^2$, $2s = 3l^2 - k^2$ and $t = kl$. We put these into (*) and (**) and get

$$8u^4 + 9l^4 + k^4 = 18k^2l^2.$$

Here $k = u = l$ is a solution but using $\gcd(k, ul) = 1$ forces $u = k = l = 1$, and this again it gives trivial solutions. We solve the last equation in $3l^2$ and get

$$3l^2 = 3k^2 \pm 2\sqrt{2(k^4 - u^4)}.$$

where $\gcd(k, u)$=1, k and u are both odd and not divisible by 3. Then we must have

$$\frac{(k-u)}{2}\frac{(k+u)}{2}\frac{(k^2+u^2)}{2} = b^2$$

for some integer b. But then there are integers g, h and f such that

$$\begin{aligned} \frac{k-u}{2} &= g^2 \\ \frac{k+u}{2} &= h^2 \\ \frac{k^2+u^2}{2} &= f^2. \end{aligned}$$

But then we have $g^4 + h^4 = f^2$ which does not have any nontrivial solutions in integers. Hence we have completed the case where $\gcd(x-y, x^2+xy+y^2)$=1.

REFERENCES

1. Beukers, F., "The Diophantine equation $Ax^p + By^q = Cz^r$", *Lectures held at Institut Henri Poincare*, 2004

2. Darmon, H. and A. Granville, "On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$", *Bulletin on the London Mathematical Society* **27**, pp. 515-543, 1995

3. Montgomery, H. L., I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley & Sons, Inc., 5^{th} Edition, 1991

4. Hardy, G. H. and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publications, 1979

5. Anglin, W. S., *The Queen of Mathematics, An Introduction to Theory of Numbers*, Kluwer Academic Publishers, 1995

6. Mordell, L. J., *Diophantine Equations*, Academic Press, 1969

7. Edwards, J., "A Complete Solution to $X^2 + Y^3 + Z^5 = 0$", *J. Reine Angew. Math.* **571**, pp. 213-236, 2004

8. Cohen, H., *Number Theory: Volume I: Tools and Diophantine Equations*, Springer, 2007

9. Borevich, Z. I. and I. R. Shafarevich, *Number Theory*, Academic Press, 1973

10. Edwards, J., *Platonic solids and solutions to* $x^2 + y^3 = dz^r$, Ph.D. Thesis, Univ. Utrecht, 2005

11. Hilbert, D., *Theory of Algebraic Invariants*, Cambridge University Press, 1993

12. Wiles, A., "Modular elliptic curves and Fermat's Last Theorem", *Annals of Mathematics* **141**, pp. 443-551, 1995

13. Mihailescu, P., "Primary Cyclotomic Units and a Proof of Catalan's Conjecture", *J. Reine Angew. Math.* **572**, pp. 167-195, 2004

14. Yıldırım, C. Y., Unpublished notes obtained through private communication