# Some Diophantine Problems

by

Tho Nguyen Xuan

A Dissertation Presented in Partial Fulfillment
of the Requirement for the Degree
Doctor of Philosophy

Approved April 2019 by the
Graduate Supervisory Committee:

Andrew Bremner, Chair
Nancy Childress
John Jones
John Quigg
Susanna Fishel

ARIZONA STATE UNIVERSITY

May 2019

ABSTRACT

Diophantine arithmetic is one of the oldest branches of mathematics, the search for integer or rational solutions of algebraic equations. Pythagorean triangles are an early instance. Diophantus of Alexandria wrote the first related treatise in the fourth century; it was an area extensively studied by the great mathematicians of the seventeenth century, including Euler and Fermat. The modern approach is to treat the equations as defining geometric objects, curves, surfaces, etc. The theory of elliptic curves (or curves of genus 1, which are much used in modern cryptography) was developed extensively in the twentieth century, and has had great application to Diophantine equations. This theory is used in application to the problems studied in this thesis. This thesis studies some curves of high genus, and possible solutions in both rationals and in algebraic number fields, generalizes some old results and gives answers to some open problems in the literature. The methods involve known techniques together with some ingenious tricks. For example, the equations $y^2 = x^6 + k$, $k = -39, -47$, the two previously unsolved cases for $|k| < 50$, are solved using algebraic number theory and the elliptic Chabauty method. The thesis also studies the genus three quartic curves $F(x^2, y^2, z^2) = 0$ where F is a homogeneous quadratic form, and extend old results of Cassels, and Bremner. It is a very delicate matter to find such curves that have no rational points, yet which do have points in odd-degree extension fields of the rationals. The principal results of the thesis are related to surfaces where the theory is much less well known. In particular, the thesis studies some specific families of surfaces, and give a negative answer to a question in the literature regarding representation of integers n in the form $n = (x+y+z+w)(1/x+1/y+1/z+1/w)$. Further, an example, the first such known, of a quartic surface $x^4+7y^4 = 14z^4+18w^4$ is given with remarkable properties: it is everywhere locally solvable, yet has no nonzero rational point, despite having a point in (non-trivial) odd-degree extension fields

of the rationals. The ideas here involve manipulation of the Hilbert symbol, together with the theory of elliptic curves.

ACKNOWLEDGEMENTS

I would like to thank my advisor Professor Andrew Bremner for his guidance, his generosity, his encouragement and his kindness during my graduate years. Without his help and support, I will not be able to finish the thesis. I show my most respect to him, both his personality and his mathematical expertise.

I would like to thank Professor Susanna Fishel for some talks we had. These talks did encourage me a lot at the beginning of my graduate years. I would like to thank other members of my Phd committee, Professor John Quigg, Professor John Jones, and Professor Nancy Childress. I would like to thank the school of mathematics and statistical sciences at Arizona State University for all the funding and support.

And finally, I would like to thank the members in my family. My grandmother, my father, my mom, Mr Phuong and his wife Mrs Doi and their son Phi, and to my cousin Mr Tan for all of their constant support and encouragement during my undergraduate and my graduate years.

TABLE OF CONTENTS


Page

LIST OF TABLES . . . . . . . . . . v

CHAPTER

1 INTRODUCTION . . . . . . . . . . 1

2 EQUATION $Y^2 = X^6 + k$ . . . . . . . . . . 4

2.1 Introduction . . . . . . . . . . 4

2.2 Equation $y^2 = x^6 - 39$ . . . . . . . . . . 4

2.3 Equation $y^2 = x^6 - 47$ . . . . . . . . . . 24

3 CUBIC POINTS ON QUARTIC CURVES . . . . . . . . . . 31

3.1 Introduction . . . . . . . . . . 31

3.2 Cubic Points and Their Associated Curves . . . . . . . . . . 31

3.3 Some Applications . . . . . . . . . . 41

3.3.1 Equation $x^4 + y^4 = 4pz^4$ . . . . . . . . . . 41

3.3.2 Equation $x^4 + nx^2y^2 + y^4 = Dz^4$ . . . . . . . . . . 48

4 THE HILBERT SYMBOL AND APPLICATIONS . . . . . . . . . . 54

4.1 Introduction . . . . . . . . . . 54

4.2 Equation $(x + y + z + w)(1/x + 1/y + 1/z + 1/w) = n$ . . . . . . . . . . 55

4.3 Equation $\frac{x}{y} + p\frac{y}{z} + \frac{z}{w} + p\frac{w}{x} = 8pn$ . . . . . . . . . . 84

4.4 Equation $x^4 + 7y^4 = 14z^4 + 18w^4$ . . . . . . . . . . 98

REFERENCES . . . . . . . . . . 107

APPENDIX

A EQUATION $(x + y + z + w)(1/x + 1/y + 1/z + 1/w) = n$ . . . . . . . . . . 110

B EQUATION $x^4 + y^4 = Dz^4$ . . . . . . . . . . 126

## LIST OF TABLES


Table Page

2.1 Possible Values Of $(r, s)$ ... 22

2.2 Solutions Corresponding to the Values Of $(\lambda, r, s)$ ... 23

A.1 Solutions Of $(x+y+z+w)(1/x+1/y+1/z+1/w) = n$ ... 111

A.2 Solutions Of $(x+y+z+w)(1/x+1/y+1/z+1/w) = 4m^2,\ m \equiv 2 \pmod 4$ ... 124

A.3 Solutions Of $(x+y+z+w)(1/x+1/y+1/z+1/w) = 4m^2+4,\ m \equiv 2 \pmod 4$ ... 125

B.1 Solutions Of $x^4 + y^4 = Dz^4,\ z = t^2 + 1$ ... 127

# Chapter 1

# INTRODUCTION

Chapter 2 resolves two unsolved cases of the equation $y^2 = x^6 + k$ in rational numbers, where $k$ is an integer in the range $|k| \leq 50$. The two cases are $k = -39$ and $k = -47$. This type of equation has been studied by Bremner and Tzanakis [6]. The standard technique in this chapter is the elliptic curve Chabauty method. The main results are

**Theorem 1.** *The only rational solutions* $(x, y)$ *to the equation*

$$y^2 = x^6 - 39$$

*are* $(\pm 2, \pm 5)$.

**Theorem 2.** *The only rational solutions* $(x, y)$ *to the equation*

$$y^2 = x^6 - 47$$

*are* $(\pm\frac{63}{10}, \pm\frac{249953}{10^3})$.

Chapter 3 studies the equation $F(x^2, y^2, z^2) = 0$ in odd degree number fields where $F$ is a nonsingular homogeneous irreducible polynomial with rational coefficients. Many examples were given, where $F(x^2, y^2, z^2) = 0$ has solutions in some cubic extensions of $\mathbb{Q}$ but does not have solutions in $\mathbb{Q}$. For example, in Bremner, Lewis and Morton [2], Cassels [11], Bremner [3]. This chapter finds a necessary condition (Theorem 3.2.1) when $F(x^2, y^2, z^2) = 0$ has solutions in rational numbers or odd degree number fields. The main results are

**Theorem 3.** *Let $p$ be an odd prime. Then the equation*

$$x^4 + y^4 = 4pz^4$$

*does not have solutions in any odd degree number field except $xyz = 0$.*

**Theorem 4.** *Let $n, D$ be non zero integers such that $D$ is fourth power free, $2 - n, n^2 - 4, (2+n)D, (4-n^2)D, (n^2-4)D$ and $D$ are not perfect squares. Assume that the rank of the curve $x^2 + nxy^2 + y^4 = Dz^4$ is at most one. Then the equation*

$$x^4 + nx^2y^2 + y^4 = Dz^4$$

*does not have solutions in any odd degree extension of $\mathbb{Q}$ except $xyz = 0$. In particular, the equation $x^4 + nx^2y^2 + y^4 = Dz^4$ does not have rational solutions except $x = y = z = 0$.*

Theorem 3, 4 extend some old results by Cassels [11] and Bremner [3].

Chapter 4 focuses on applications of $p-$adic analysis and elliptic curves to some Diophantine problems. $P-$adic analysis gives us tools to study local information on equations over rationals or integers, while elliptic curves give us tools to transform complicated equations into simple equations. By combining these tools, we can solve some hard problems. The main results are

**Theorem 5.** *Let $n$ be a positive integer such that $n = 4m^2$ or $n = 4m^2 + 4$, where $m \not\equiv 2 \mod 4$. Then the equation*

$$n = (x + y + z + w)(\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{w})$$

*does not have solutions $x, y, w, z \in \mathbb{Z}^+$.*

Theorem 5 gives a negative answer to a conjecture by Bremner, Guy, Nowakowski [4]. Different homogeneous forms in three variables have been studied: $(x+y+z)(\frac{1}{x}+\frac{1}{y}+\frac{1}{z})$

by Bremner, Guy, Nowakowski [4]; $\frac{(x+y+z)^3}{xyz}$, $\frac{x}{y}+\frac{y}{z}+\frac{z}{x}$ by Bremner, Guy [5]; $\frac{(x+y+z)^3}{xyz}$ by Brueggemen [10]; $\frac{x}{y+z}+\frac{y}{z+x}+\frac{z}{x+y}$ by Bremner, Macleod [7]. Theorem 5 is the first example on the four variable case. The proof uses $p-$ adic analysis in a very nontrivial way.

**Theorem 6.** *Let $p=1$ or $p$ be an odd prime such that $p \equiv 1 \mod 8$. Then for every positive integer $n$, the equation*

$$\frac{x}{y}+p\frac{y}{z}+\frac{z}{w}+p\frac{w}{x}=8pn$$

*does not have solutions $x,y,z,w \in \mathbb{Z}^+$.*

Theorem 6 is an application of the techniques used to prove Theorem 5.

**Theorem 7.** *Consider the surface $S\colon x^4+7y^4=14z^4+18w^4$. Then $S$ is everywhere locally solvable, and $S$ has no rational points except $(0,0,0,0)$. For every odd integer $n \geq 3$, there is a number field $K$ of degree $n$ such that $S$ has a nontrivial point in $K$.*

The family of surfaces $ax^4+by^4=cz^4+dw^4$, where $a,b,c,d \in \mathbb{Z}$ and $abcd \in \mathbb{Z}^2$, has been studied extensively by Swinnerton-Dyer and Bright [21] and Bright [8, 9]. A modern approach to show the non existence of rational points is to study the Brauer groups of these surfaces, but we will prove Theorem 7 in a more classical way, only using $p-$ adic analysis and some algebraic curve theory. The proof is motivated by a paper of Swinnerton-Dyer [21]. The surface $x^4+7y^4=14z^4+18w^4$ has three interesting properties: $(i)$ unsolvable in the rational numbers, $(ii)$ everywhere locally solvable, $(iii)$ solvable in a cubic number field. None of the examples by Swinnerton-Dyer and Bright is proved to have all three properties $(i),(ii)$ and $(iii)$. The surface $x^4+7y^4=14z^4+18w^4$ is the first known example with these properties.

# Chapter 2

# EQUATION $Y^2 = X^6 + K$

## 2.1 Introduction

In their paper, Brenner and Tzanakis [6] studied the equation $y^2 = x^6 + k$ in rational numbers, where k is an integer in the range $|k| \leq 50$. They solved all the equations except $k = -39$ and $k = -47$. The main approach used by Bremner and Tzanakis is the elliptic curve Chabauty method. In this paper, we shall solve the equation $y^2 = x^6 + k$ with $k = -39$ or $k = -47$. For $k = -39$, we shall present two approaches which might be applicable to other values of $k$. For $k = -47$, we only present one approach. The main tools are the elliptic curve Chabauty method and algebraic number theory. In summary, we shall prove:

**Theorem 8.** *The only rational solutions $(x, y)$ to the equation*

$$y^2 = x^6 - 39$$

*are* $(\pm 2, \pm 5)$.

**Theorem 9.** *The only rational solutions $(x, y)$ to the equation*

$$y^2 = x^6 - 47$$

*are* $(\pm\frac{63}{10}, \pm\frac{249953}{10^3})$.

## 2.2 Equation $y^2 = x^6 - 39$

In this section we shall present the proof of Theorem 8.

*Proof.* The equation $y^2 = x^6 - 39$ is equivalent to

$$Y^2 = X^6 - 39Z^6, \tag{2.2.1}$$

where $X, Y, Z$ are coprime integers. We have

$$(X^3 - Y)(X^3 + Y) = 39Y^2.$$

Let $d = \gcd(X^3 - Y, X^3 + Y)$. Then $d | \gcd(2X^3, 2Y) = 2$. We can choose the sign of $Y$ such that $13 | X^3 + Y$.

Case $d = 1$ : we have

$$X^3 + Y = 39V^6, \quad X^3 - Y = U^6, \quad \gcd(U, V) = 1,$$

or

$$X^3 + Y = 13V^6, \quad X^3 - Y = 3U^6, \quad \gcd(U, V) = 1.$$

So

$$2X^3 = 39V^6 + U^6 \quad \text{or} \quad 2X^3 = 13V^6 + 3U^6, \quad \gcd(U, V) = 1.$$

In the former case, we have $3 \nmid U$. So $U^6 \equiv 1 \mod 9$, hence $2X^3 \equiv 3V^6 + 1 \mod 9$. Thus $X^3 \equiv -1 \mod 3$, so $X \equiv -1 \mod 3$. Therefore $X^3 \equiv -1 \mod 9$. So $V^6 + 1 \equiv 0 \mod 3$, impossible.

In the latter case, we have

$$2X^3 = 13V^6 + 3U^6, \quad \gcd(U, V) = 1. \tag{2.2.2}$$

We shall deal with this case later.

Case $d = 2$: we have

$$X^3 + Y = 2 \cdot 39V^6, \quad X^3 - Y = 2^5 \cdot U^6, \quad \gcd(U, V) = 1,$$

$$X^3 + Y = 2^5 \cdot 39V^6, \quad X^3 - Y = 2 \cdot U^6, \quad \gcd(U, V) = 1,$$

$$X^3 + Y = 2 \cdot 13V^6, \quad X^3 - Y = 2^5 \cdot 3U^6, \quad \gcd(U, V) = 1,$$

$$X^3 + Y = 2^5 \cdot 13V^6, \quad X^3 - Y = 2 \cdot 3U^6, \quad \gcd(U, V) = 1.$$

This gives

$$X^3 = 39V^6 + 16U^6,$$

$$X^3 = 624V^6 + U^6,$$

$$X^3 = 13V^6 + 48U^6,$$

$$X^3 = 208V^6 + 3U^6.$$

The first equation: $\pm 1, \pm 5 \equiv 3U^6 \equiv \pm 3 \mod 13$, impossible.

The third equation: $\pm 1, \pm 5 \equiv \pm 4 \mod 13$, impossible.

The fourth equation: $\pm 1, \pm 5 \equiv \pm 3 \mod 13$, impossible.

There remains the second equation:

$$X^3 = 624V^6 + U^6, \quad \gcd(U, V) = 1.$$

This gives

$$(624(X/U^2))^3 = (624(V^3/U^3))^2 + 624^3.$$

The elliptic curve $y^2 = x^3 - 624^3$ has rank 0, so $X^3 = 624V^6 + U^6$ only has trivial solutions.

We only need to deal with the case (2.2.2)

$$2X^3 = 3U^6 + 13V^6, \quad \gcd(U, V) = 1.$$

Observe that $2|X$ and $2 \nmid U, V$.

**Solution 1:** Let $K = \mathbb{Q}(\theta)$, where $\theta = \sqrt[3]{39}$. $K$ has the ring of integers $\mathcal{O}_K = \mathbb{Z}[\theta]$ and a fundamental unit $\epsilon = 2\theta^2 - 23$ of norm 1.

**Lemma 1.** *Consider the elliptic curve*

$$E : v^2 = u^3 - 39,$$

*let* $\phi$ *be a map* $E(\mathbb{Q}) \to K^*/(K^*)^2$ *given by*

$$\begin{aligned} \phi(u,v) &= u - \theta \mod (K^*)^2, \\ \phi(\infty) &= (K^*)^2. \end{aligned}$$

*Then* $\phi$ *is a group homomorphism with the kernel* $2E(\mathbb{Q})$.

*Proof.* This is the standard 2-descent. See Silverman [18]. □

We have

$$E(\mathbb{Q}) = \mathbb{Z}(10,31) \oplus \mathbb{Z}(4,5).$$

Because $(X^2/Z^2, Y/Z^3) \in E(\mathbb{Q})$, Lemma 1 implies

$$(X^2 - \theta Z^2) \equiv \alpha \mod (K^*)^2,$$

where $\alpha \in \{1, 4-\theta, 10-\theta, (4-\theta)(10-\theta)\}$.

Because $10 - \theta = \epsilon(3\theta^2 + 10\theta + 34)^2$, we have the following cases:

**Case 1:** $X^2 - \theta Z^2 \in K^2$.

Because $X^2 - \theta Z^2 \in \mathbb{Z}[\theta] = \mathcal{O}_K$, we have

$$X^2 - \theta Z^2 = (a + b\theta + c\theta^2)^2,$$

where $a, b, c \in \mathbb{Z}$. Comparing coefficients of $\theta^0, \theta, \theta^2$ gives:

$$\begin{cases} X^2 = a^2 + 78bc, \\ Z^2 = -2ab - 39c^2, \\ 0 = 2ac + b^2. \end{cases}$$

From $\gcd(X, Z) = 1$, we have $\gcd(a, b, c) = 1$. Because $2|X$, from the first and the third equations, we have $2|a$, $b$. Thus $2 \nmid c$. Let $a = 2a_1$, $b = 2b_1$. Then

$$\begin{cases} (X/2)^2 = a_1^2 + 39b_1c, \\ Z^2 = -8a_1b_1 - 39c^2, \\ 0 = a_1c + b_1^2. \end{cases}$$

Since $\gcd(a, b, c) = 1$, the third equation implies $\gcd(a_1, c) = 1$. Hence $\exists\, r, s \in \mathbb{Z}$, $r > 0$ such that

$$a_1 = r^2, \quad c = -s^2, \quad b_1 = -rs, \quad \gcd(r, s) = 1, \tag{2.2.3}$$

or

$$a_1 = -r^2, \quad c = s^2, \quad b_1 = -rs, \quad \gcd(r, s) = 1. \tag{2.2.4}$$

Case (2.2.3) gives

$$(X/2)^2 = r(r^3 - 39s^3),$$

$$Z^2 = s(8r^3 - 39s^3).$$

Because $\gcd(X, Z) = 1$, we have $\gcd(r, 39) = \gcd(s, 2) = 1$. Hence $\gcd(r, r^3 - 39s^3) = \gcd(s, 8r^3 - 39s^3) = 1$. Because $r > 0$, we have $8r^3 - 39s^3 > r^3 - 39s^3 > 0$. Thus $s > 0$. It follows that

$$r = A^2, \quad r^3 - 39s^3 = C^2, \quad X = \pm AC,$$

$$s = B^2, \quad 8r^3 - 39s^3 = D^2, \quad Z = \pm BD.$$

Therefore $D^2 = 8A^6 - 39B^6$. So $D^2 + A^6 \equiv 0 \mod 3$. Hence $A \equiv D \equiv 0 \mod 3$. Thus $3|X$, $Z$, a contradiction.

Case (2.2.4) gives

$$(X/2)^2 = r(r^3 - 39s^3),$$

$$Z^2 = -s(8r^3 + 39s^3).$$

We have $\gcd(r,39)=\gcd(s,2)=1$. Because $r>0$, if $s>0$, then $Z^2=-s(8r^3+39s^3)<0$, impossible. Therefore $s<0$. Thus

$$r=A^2,\quad r^3-39s^3=C^2,\quad X=\pm AC,$$

$$s=-B^2,\quad 8r^3+39s^3=D^2,\quad Z=\pm BD.$$

Thus $D^2=8A^6-39B^6$. So $D^2+A^6\equiv 0 \mod 3$. Therefore $A\equiv D\equiv 0 \mod 3$. Hence $3|X,\ Z$, a contradiction.

**Case 2:** $(X^2-\theta Z^2)\in \epsilon K^2$.

Because $\epsilon$ is a unit and $X^2-\theta Z^2\in\mathcal{O}_K$, we have

$$X^2-\theta Z^2=(2\theta^2-23)(a+b\theta+c\theta^2)^2,$$

where $a,b,c\in\mathbb{Z}$. Comparing the coefficients of $\theta^0,\theta,\theta^2$ gives

$$\begin{cases} X^2=-23a^2+156ab-1794bc+3042c^2,\\ Z^2=46ab-156ac-78b^2+897c^2,\\ 0=2a^2-46ac-23b^2+156bc.\end{cases}$$

Because $\gcd(X,Z)=1$, we have $\gcd(a,b,c)=1$. From the third equation, we have $2|b$. $2|X$. Thus the first equation implies $2|a$. Hence $2\nmid c$. The first equation gives

$$X^2\equiv 2c^2\equiv 2 \mod 4,$$

impossible.

Case 3: $X^2-\theta Z^2\in\epsilon(4-\theta)K^2$.

Let

$$X^2-\theta Z^2=\epsilon(4-\theta)(\frac{a+b\theta+c\theta^2}{n})^2,$$

where $n, a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$. Comparing the coefficients of $\theta^0, \theta, \theta^2$ gives

$$\begin{cases} (nX)^2 = -170a^2 + 624ab + 1794ac + 897b^2 - 13260bc + 12168c^2, \\ (nZ)^2 = -23a^2 + 340ab - 624ac - 312b^2 - 1794bc + 6630c^2, \\ 0 = 8a^2 + 46ab - 340ac - 170b^2 + 624bc + 897c^2. \end{cases}$$

From the third equation, we have $2|c$. Because $2|nX$, from the first equation, we have $2|b$. Therefore $2 \nmid a$. Then the first equation gives

$$(nX)^2 \equiv 2a^2 \equiv 2 \mod 4,$$

impossible.

**Case 4:** $(X^2 - \theta Z^2)(4 - \theta) \in K^2$.

We have $x = X/Z$, $y = Y/Z^3$, $y^2 = (x^2 - \theta)(x^4 + \theta x^2 + \theta^2)$, and $(x^2 - \theta)(4 - \theta) \in K^2$. Thus

$$(4 - \theta)(x^4 + \theta x^2 + \theta^2) \in K^2.$$

Let $(4 - \theta)(x^4 + 4\theta x^2 + \theta^2) = \beta^2$. Then $((4 - \theta)x^2, (4 - \theta)\beta)$ is a point on

$$G : v^2 = u(u^2 + \theta(4 - \theta)u + \theta^2(4 - \theta)^2).$$

We have

$$G(K) = \mathbb{Z}/2\mathbb{Z}(0, 0) \oplus \mathbb{Z}(\frac{4\theta^2 - 39}{4}, \frac{20\theta^2 - 195}{8}).$$

The curve $G$ has rank 1 over $K$, and $[K : \mathbb{Q}] = 3$.

The first approach is to use the elliptic curve Chabauty method. With the search bound of 350 and the assumption of the Generalized Riemann Hypothesis, Pseudo-MordellWeil returns "false". The second approach is to use the formal group technique as in Flynn [15] which will almost guarantee the solution when $\text{rank}(G(K)) < [K : \mathbb{Q}]$. If we follow this approach, then the smallest prime that might work is $p = 7$. The order of the generator $(\frac{4\theta^2-39}{4}, \frac{20\theta^2-195}{8})$ in $\mathbb{F}_7(\theta)$ with $\theta^3 - 39 = 0$ is 86. In $G(K)$, we shall need to compute the set $\{m(0,0)+n(\frac{4\theta^2-39}{4}, \frac{20\theta^2-195}{8}): n=0,1, m=-42,-41,...,m=43\}$ and then compute the corresponding formal power series, see Flynn [15] for more details about this approach. This might work, but it shall take too much computation. We will take another approach which might possibly be applicable in case $\mathrm{rank}(G(K)) \geq [K:\mathbb{Q}]$.

We have

$$X^2 - \theta Z^2 = (4-\theta)(a+b\theta+c\theta^2)^2,$$

where $a,b,c \in \mathbb{Q}$. Thus

$$X^2 = 4a^2 - 78ac - 39b^2 + 312bc, \tag{2.2.5}$$

$$Z^2 = a^2 - 8ab + 78bc - 156c^2, \tag{2.2.6}$$

$$0 = -2ab + 8ac + 4b^2 - 39c^2. \tag{2.2.7}$$

If $4c-b=0$, then from (2.2.7), we have $4b^2-39c^2=0$. So $b=c=0$. Therefore

$$x = \frac{X}{Z} = \pm 2.$$

If $4c-b \neq 0$, then from (2.2.7), we have $a = \frac{39c^2-4b^2}{2(4c-b)}$.

Let $P=5c$ and $Q=4c-b$. Then

$$X^2 = \frac{P^4 - 5P^3Q + 24P^2Q^2 - 20PQ^3 - 23Q^4}{Q^2},$$
$$Z^2 = \frac{P^4 - 24P^2Q^2 + 40PQ^3 - 48Q^4}{4Q^2}.$$

Let $P=dp$, $Q=dq$, $X_1 = \frac{qX}{d}$, $Z_1 = \frac{2qZ}{d}$, where $d = \gcd(P,Q)$. Then

$$\begin{aligned} X_1^2 &= p^4 - 5p^3q + 24p^2q^2 - 20pq^3 - 23q^4, \\ Z_1^2 &= p^4 - 24p^2q^2 + 40pq^3 - 48q^4. \end{aligned} \tag{2.2.8}$$

We have $\gcd(p,q)=1$ and $X_1, Z_1 \in \mathbb{Z}$.

**Lemma 2.** *In (2.2.8), we have*

$$\gcd(X_1, 39) = \gcd(Z_1, 13) = \gcd(Z_1, 2) = 1.$$

*Proof.* First, we show that $2 \nmid Z_1$.

If $q \nmid d$, then $\exists$ a prime $l|q$ such that $l|X_1 = \frac{qX}{d}$. Thus

$$l|p^4 - 5p^3q + 24p^2q^2 - 20pq^3 - 23q^4.$$

Because $l|q$, we have $l|p$. So $l|\gcd(p, q) > 1$, a contradiction. Therefore $q|d$. Thus $X_1|X$ and $Z_1|2Z$. From (2.2.2), we have $\gcd(U, V) = 1$, $2|X$ and $2 \nmid Z$. If $2|Z_1$. Then from

$$Z_1^2 = p^4 - 24p^2q^2 + 40pq^3 - 48q^4,$$

we have $2|p$. Thus $2 \nmid q$. Hence $2 \nmid X_1$. From $2|X = (\frac{d}{q})X_1$, we have $2|\frac{d}{q}$. So $\frac{d}{2q} \in \mathbb{Z}$. Because $2 \nmid Z = (\frac{d}{2q})Z_1$, we have $2 \nmid Z_1$, a contradiction. So $2 \nmid Z_1$.

If $3|X_1$, then

$$3|p^4 - 5p^3q + 24p^2q^2 - 20pq^3 - 23q^4.$$

Thus

$$3|p^4 + q^4 + p^3q + qp^3.$$

Because $\gcd(p, q) = 1$, we have $3 \nmid p, q$. Hence $3|2 + 2pq$. So $pq \equiv -1 \mod 3$, thus $p + q \equiv 0 \mod 3$. Therefore

$$Z_1^2 = p^4 - 24p^2q^2 + 40pq^3 - 48q^4 \equiv -3p^4 \mod 9,$$

which is not possible. So $3 \nmid X_1$.

If $13|X_1$, then

$$13|p^4 - 5p^3q + 24p^2q^2 - 20pq^3 - 23q^4.$$

Thus $13|p + 2q$. So

$$Z_1^2 = p^4 - 24p^2q^2 + 40pq^3 - 48q^4 \equiv -39q^4 \mod 13^2,$$

which is not possible. Hence $13 \nmid X_1$.

If $13|Z_1$, then

$$13|p^4 - 24p^2q^2 + 40pq^3 - 48q^4.$$

Thus

$$13|(p+2q)(p+7q).$$

If $13|p+2q$ or $13|p+7q$, then

$$Z_1^2 = p^4 - 24p^2q^2 + 40pq^3 - 48q^4 \equiv -39q^4 \mod 13^2,$$

which is not possible. So $13 \nmid Z_1$.

$\square$

Let $L = \mathbb{Q}(\phi)$, where $\phi$, $\sim 2.8502$, is the largest real root of $x^4 - 6x^2 - 5x - 3 = 0$. L has class number 1, the ring of integers $\mathcal{O}_L = \mathbb{Z}[\phi]$, and two positve fundamental units $\epsilon_1 = \phi + 2$, $\epsilon_2 = \phi^3 - \phi^2 - \phi - 1$ with $\text{Norm}(\epsilon_1) = \text{Norm}(\epsilon_2) = -1$.

Let

$$F(p,q) = p^4 - 5p^3q + 24p^2q^2 - 20pq^3 - 23q^4,$$
$$G(p,q) = p^4 - 24p^2q^2 + 40pq^3 - 48q^4.$$

Then

$$F(p,q) = (p + (\phi^3 - 7\phi - 5)q)A(p,q),$$
$$G(p,q) = (p + 2\phi q)B(p,q),$$

where

$$A(p,q) = p^3 + (-\phi^3 + 7\phi)p^2q + (4\phi^2 - 5\phi)pq^2 + (4\phi^3 - 5\phi^2 - 12\phi - 5)q^3,$$
$$B(p,q) = p^3 - 2\phi p^2q + (4\phi^2 - 24)pq^2 + (-8\phi^3 + 48\phi + 40)q^3.$$

In $\mathbb{Z}[\phi]$, let

$$p_1 = -2\phi^3 + \phi^2 + 12\phi + 4, \quad p_2 = \phi, \quad p_3 = \phi + 1, \quad q_1 = \phi^3 - 6\phi - 4, \quad q_2 = \phi - 1.$$

Then

$$3 = p_1 p_2 p_3^3, \quad 13 = q_1 q_2^3,$$

$$\mathrm{Norm}(p_1) = 1,\ \mathrm{Norm}(p_2) = \mathrm{Norm}(p_3) = -3,$$

$$\mathrm{Norm}(q_1) = \mathrm{Norm}(q_2) = -13.$$

We also have

$$\mathrm{Res}(p + 2\phi q, B(p,q)) = -8 p_1 p_2^5 q_2^2,$$

$$\mathrm{Res}(p + (\phi^3 - 7\phi - 5)q, A(p,q)) = (4\phi^3 + 6\phi^2 - 31\phi - 53) p_2 p_3^6 q_1 q_2^3.$$

Because $\gcd(X_1, 39) = \gcd(Z_1, 39) = \gcd(Z_1, 2) = 1$ and $\mathrm{Norm}(4\phi^3 + 6\phi^2 - 31\phi - 53) = 1$, we have

$$\begin{cases} p + (\phi^3 - 7\phi - 5)q = (-1)^h \epsilon_1^i \epsilon_2^j S^2, \quad p + 2\phi q = (-1)^{h_1} \epsilon_1^{i_1} \epsilon_2^{j_1} T^2, \\ A(p,q) = (-1)^h \epsilon_1^{-i} \epsilon_2^{-j} S_1^2, \quad B(p,q) = (-1)^{h_1} \epsilon_1^{-i_1} \epsilon_2^{-j_1} T_1^2, \end{cases}$$

where $X_1 = SS_1$ and $Z_1 = TT_1$.

Taking norms gives

$$(X_1)^2 = (-1)^{i+j} \mathrm{Norm}(S)^2, \quad Z_1^2 = (-1)^{i_1 + j_1} \mathrm{Norm}(T)^2.$$

Thus $2 | i + j$ and $2 | i_1 + j_1$. Hence $i = j$ and $i_1 = j_1$.

Let $\beta = \epsilon_1 \epsilon_2 = \phi^3 + 3\phi^2 + 2\phi + 1 > 0$. Then

$$\begin{cases} p + (\phi^3 - 7\phi - 5)q = (-1)^h \beta^i S^2, \quad p + 2\phi q = (-1)^{h_1} \beta^{i_1} T^2, \\ A(p,q) = (-1)^h \beta^{-i} S_1^2, \quad B(p,q) = (-1)^{h_1} \beta^{-i_1} T_1^2. \end{cases} \tag{2.2.9}$$

**Lemma 3.** *We have*

$$(p + (\phi^3 - 7\phi - 5)q)(p + 2\phi q) > 0. \tag{2.2.10}$$

*Proof.* Equation $F(x,1)=0$ has 2 real roots

$$x_1 = -\phi^3 + 7\phi + 5 \sim 1.7976,\ x_2 \sim -0.6206.$$

Equation $G(x,1)=0$ has 2 real roots

$$x_3 = -2\phi \sim -5.7004,\ x_4 \sim 4.1399.$$

We have

$$F(\frac{p}{q},1) > 0 \quad and \quad G(\frac{p}{q},1) > 0.$$

So

$$\frac{p}{q} < x_3 \quad or \quad \frac{p}{q} > x_4.$$

Because $x_3 < x_2 < x_1 < x_4$, we have

$$(p + x_1 q)(p + x_3 q) > 0.$$

□

From Lemma 3 and (2.2.9), we have $h = h_1$. So by mapping $(p,q) \mapsto (-p,-q)$, we can assume that $h = h_1 = 0$.

Case $i \neq i_1$:

Because $\phi - 1 | \phi^3 - 9\phi - 5$, we have

$$(\phi - 1)|(\phi^3 - 9\phi - 5)q = \beta^i S^2 - \beta^{i_1} T^2.$$

Because $i - i_1 = \pm 1$ and $\beta$ is a unit, we have

$$\beta S^2 - T^2 \equiv 0 \mod \phi - 1.$$

If $\phi - 1|S$ or $\phi - 1|T$, then $\phi - 1|S$, $T$. Hence $13 = -\operatorname{Norm}(\phi - 1)|\operatorname{Norm}(S)$, $\operatorname{Norm}(T)$. Thus $13|X$, $Z$, impossible. So $\phi - 1 \nmid S$, $T$. Therefore $S^{12} \equiv T^{12} \equiv 1 \mod \phi - 1$ (because $\operatorname{Norm}(\phi - 1) = -13$). Also $\beta \equiv 7 \mod \phi - 1$, therefore

$$0 \equiv \beta^6 S^{12} - T^{12} \equiv 7^6 - 1 \mod \phi - 1.$$

So $13 = -\operatorname{Norm}(\phi - 1) | (7^6 - 1)^4$. But $13 \nmid 7^6 - 1$, so we have a contradiction.

Case $i = i_1$:

If $q \neq 0$, then

$$(p + (\phi^3 - 7\phi - 5)q)(p^3 - 2\phi p^2 q + 4(\phi^2 - 6)pq^2 + 8(-\phi^3 + 6\phi + 5)q^3) = (ST_1)^2,$$

which represents an elliptic curve

$$C\colon v^2 = (u + \gamma)(u^3 - 2\phi u^2 + 4(\phi^2 - 6)u + 8(-\phi^3 + 6\phi + 5)),$$

where $v = (ST_1)/q^2$, $u = p/q$. The minimal cubic model at $(-\gamma, 0)$ is

$$y^2 = x^3 + (-2s^3 + 2s^2 + 10s + 6)x^2 + (-4s^3 + 8s^2 + 12s)x + (1488s^3 + 1776s^2 - 11128s - 17160).$$

The elliptic Chabauty routine in Magma [1] works and returns $u = 69/26$. Hence $(p, q) = (69, 26)$, $(-69, -26)$. This gives no solutions $(X_1, Z_1)$.

Therefore $q = 0$, so $X_1 = \pm 2$ and $Z_1 = \pm 1$. Thus

$$x = \frac{X_1}{Z_1} = \pm 2.$$

So the only rational solutions to $y^2 = x^6 - 39$ are $(x, y) = (\pm 2, \pm 5)$.

**Remark 1.** $(i)$ *From the system* (2.2.8)*, we have a curve*

$$F\colon \omega^2 = (\lambda^4 - 5\lambda^3 + 24\lambda^2 - 20\lambda - 23)(\lambda^4 - 24\lambda^2 + 40\lambda - 48), \qquad (2.2.11)$$

*where* $\omega = \frac{X_1 Z_1}{q^4}$ *and* $\lambda = \frac{p}{q}$*. This curve has genus 3 and the Jacobian rank at most 3. We are unable to compute the Jacobian rank. Computer search reveals no rational points on* (2.2.11)*. It might be possible to show* $F$ *has no rational points using the partial descent on hyperelliptic curves as in Siksek and Stoll [19] but we have not proceeded in this way.*

$(ii)$ *More generally, **Solution 1** gives us an approach to the equation* $y^2 = x^6 + k$ *in* *principle. We write* $y^2 = x^6 + k$ *as* $Y^2 = X^6 + kZ^6$*, then compute the generators of the MordellWeil group of the elliptic curve* $E_k\colon v^2 = x^3 + k$*. Using 2-descent as in Lemma 1, we shall need to solve a finite number of equations*

$$X^2 - \theta Z^2 = (x_i - \theta)(a_i + b_i\theta + c_i\theta^2)^2,$$

*where* $\theta = k^{1/3}$ *and the set* $\{(x_i, y_i)\}_i$ *is a finite set* $a_i, b_i, c_i \in \mathbb{Q}$*.*
*Thus for each* $i$*, we have a system of equations:*

$$\begin{cases} X^2 = S_0(a_i, b_i, c_i), \\ Z^2 = S_1(a_i, b_i, c_i), \\ 0 = S_3(a_i, b_i, c_i), \end{cases}$$

*where* $S_0, S_1, S_2$ *are homogenous rational polynomials of degree 2 in* $a_i, b_i, c_i$*.*
*Assume from* $S_3(a_i, b_i, c_i) = 0$ *that we can solve for one of* $a_i, b_i, c_i$ *in term of the two other variables. Then from* $(XZ)^2 = S_0(a_i, b_i, c_i)S_1(a_i, b_i, c_i)$*, we have a genus 3 curve*

$$F_i\colon \omega^2 = p_i(\lambda)q_i(\lambda),$$

*where* $p_i(\lambda), q_i(\lambda)$ *are rational polynomials of degree 4. The partial descent method and the Chabauty method might help to find rational points on* $F_i$*.*

**Solution 2:** In this section, we shall present another solution to $y^2 = x^6 - 39$. The approach taken here is classical and is applied to the case $k = -47$. We shall start from (2.2.2)

$$2X^3 = 3U^6 + 13V^6, \quad Z = UV, \quad \gcd(U, V) = 1. \tag{2.2.12}$$

Observe that $U, V$ are odd and $X$ is even. Let $K = \mathbb{Q}(\theta)$, where $\theta^2 = -39$. The ring of integers is $\mathcal{O}_K = \mathbb{Z}[\frac{1+\theta}{2}]$. The class number is 4. The ideal $(2) = p_{21}p_{22}$, where

$p_{21} = (2, \frac{1+\theta}{2})$ and $p_{21}^4 = (\frac{5+\theta}{2})$; the ideal $(3) = p_3^2$, where $p_3 = (3, \theta)$; and $(\theta) = p_3 p_{13}$. We write (2.2.12) as

$$\frac{(3U^3 + \theta V^3)}{2} \frac{(3U^3 - \theta V^3)}{2} = 12(\frac{X}{2})^3.$$

A common ideal divisor J of the factors on the left divides $(3U^3) = p_3^2(U)^3$ and $p_3 p_{13}(V)^3$. $J^2$ divides $(12(\frac{X}{2})^3) = p_{21}^2 p_{22}^2 p_3^2 (\frac{X}{2})^3$. Certainly, $p_3$ divides J. Since $J | p_3 p_{13}(V)^3$ and $3 \nmid V$, we have $p_3^2 \nmid J$. Further $p_{13} \nmid J$, otherwise $13|X$, impossible. So $J = p_3$.

Since $p_{22}^2 | (\frac{3U^3+\theta V^3}{2})$, we have

$$\begin{aligned}(\frac{3U^3 + \theta V^3}{2}) &= p_3 p_{22}^2 \mathcal{A}^3 \\ &= (\frac{3+\theta}{2}) \mathcal{A}^3.\end{aligned}$$

It follows that $\mathcal{A}$ is principal. Hence $\mathcal{A} = (A)$ for some element $A \in \mathcal{O}_K$. Further, any unit in $\mathbb{Q}(\theta)$ is $\pm 1$, so it can be absorbed into A. Let $A = a + b\frac{\theta+1}{2}$, where $a, b \in \mathbb{Z}$. Then

$$\begin{aligned}\frac{3U^3 + \theta V^3}{2} &= \frac{3+\theta}{2} A^3 \\ &= \frac{3+\theta}{2}(a + b\frac{1+\theta}{2})^3 \\ &= \frac{3(a^3 - 18a^2 b - 48ab^2 + 44b^3)}{2} + \frac{\theta(a^3 + 6a^2 b - 24ab^2 - 28b^3)}{2}.\end{aligned}$$

Thus

$$U^3 = a^3 - 18a^2 b - 48ab^2 + 44b^3, \quad V^3 = a^3 + 6a^2 b - 24ab^2 - 28b^3. \qquad (2.2.13)$$

If $3|U$, then $a \equiv b \mod 3$. Hence $a^3 \equiv b^3 \mod 9$. So $0 \equiv 3ab^2 \mod 9$, leading to $a \equiv b \equiv 0 \mod 9$, and hence $\gcd(U, V) > 1$, impossible. Therefore $3 \nmid U$. If $3|V$, then $a \equiv b \mod 3$, implying $3|U$, impossible. So $3 \nmid U, V$.

Let $L = \mathbb{Q}(\phi)$, where $\phi^3 - 12\phi - 10 = 0$. Then $L$ has class number 3 and two fundamental units

$$\epsilon_1 = 1 + \phi, \quad \epsilon_2 = 3 + \phi, \quad \text{Norm}(\epsilon_1) = -1, \quad \text{Norm}(\epsilon_2) = 1.$$

Let $q_{13} = (13, \phi - 2)$ and $p_7 = (7, \phi)$. Then

$$(2) = p_2^3; \quad (3) = p_3^3; \quad (13) = p_{13} q_{13}^2,$$

where

$$\begin{aligned}
(2+\phi) =& p_2 p_3, \\
(4+\phi) =& p_2 p_{13}, \\
(-2+\phi) =& p_2 q_{13}, \\
(-\phi^2 - 2\phi + 2) =& p_2^2 p_{11}, \\
(\phi^2 - 2\phi - 6) =& p_2^2 p_7.
\end{aligned}$$

We have

$$\phi \equiv 9 \mod p_{13}, \quad \phi \equiv 2 \mod q_{13},$$

and

$$\begin{aligned}
U^3 =& (a + (-\phi^2 - 2\phi + 2)b)(a^2 + (\phi^2 + 2\phi - 20)ab + (-6\phi^2 + 14\phi + 32)b^2), \\
V^3 =& (a + (\phi^2 - 2\phi - 6)b)(a^2 + (-\phi^2 + 2\phi + 12)ab + (-2\phi^2 - 2\phi + 8)b^2).
\end{aligned}$$

The gcd of $(a+(-\phi^2-2\phi+2)b)$ and $(a^2+(\phi^2+2\phi-20)ab+(-6\phi^2+14\phi+32)b^2)$ divides $78(2+\phi)$. The gcd of $(a+(\phi^2-2\phi-6)b)$ and $(a^2+(-\phi^2+2\phi+12)ab+(-2\phi^2-2\phi+8)b^2)$ divides $18(2-\phi)$.

Let

$$(a + (-\phi^2 - 2\phi + 2)b) = p_2^{i_1} p_3^{i_2} p_{13}^{i_3} q_{13}^{i_4} \mathcal{X}^3,$$

where $\mathcal{X}$ is an ideal in $\mathcal{O}_L$. Taking norms gives

$$U^3 = 2^{i_1} 3^{i_2} 13^{i_3+i_4} X_1^3,$$

where $X_1 = \text{Norm}(\mathcal{X})$. So

$$i_1 = i_2 = 0, \quad i_3 + i_4 \equiv 0 \mod 3.$$

Thus

$$(a+(-\phi^2-2\phi+2)b)=\mathcal{X}^3,$$

or

$$(a+(-\phi^2-2\phi+2)b)=(13)\mathcal{X}^3,$$

or

$$(a+(-\phi^2-2\phi+2)b)=(2\phi^2-9\phi-3)\mathcal{X}^3.$$

The later two cases cannot occur. Otherwise, $a-6b\equiv 0 \mod 13$. Setting $a=6b+13c$ gives

$$U^3=13^2(4b^4+12b^2c-13c^3),\quad V^3=13(20b^3+156b^2c+312bc^2+169c^3).$$

Then $13|U,V$, contradicting $\gcd(U,V)=1$. Thus

$$\begin{aligned}(a+(-\phi^2-2\phi+2)b)=&\mathcal{X}^3,\\(a^2+(\phi^2+2\phi-20)ab+(-6\phi^2+14\phi+32)b^2)=&\bar{\mathcal{X}}^3,\end{aligned}\tag{2.2.14}$$

where $\mathcal{X}\bar{\mathcal{X}}=(U)$.

Similarly

$$\begin{aligned}(a+(\phi^2-2\phi-6)b)=&\mathcal{Y}^3,\\(a^2+(-\phi^2+2\phi+12)ab+(-2\phi^2-2\phi+8)b^2)=&\bar{\mathcal{Y}}^3,\end{aligned}\tag{2.2.15}$$

where $\mathcal{Y}\bar{\mathcal{Y}}=(V)$.

If $\mathcal{X}\sim 1$, then from (2.2.14)

$$\begin{aligned}a+(-\phi^2-2\phi+2)b=&\epsilon_1^{i_1}\epsilon_2^{i_2}X_1^3,\quad X_1\in\mathcal{O}_L,\\a^2+(\phi^2+2\phi-20)ab+(-6\phi^2+14\phi+32)b^2=&\epsilon_1^{-i_1}\epsilon_2^{-i_2}\bar{X_1}^3,\quad X_1\bar{X}_1=U.\end{aligned}\tag{2.2.16}$$

If $\mathcal{X}\sim p_2$, then from (2.2.14)

$$\begin{aligned}a+(-\phi^2-2\phi+2)b=&\frac{1}{4}\epsilon_1^{i_1}\epsilon_2^{i_2}X_2^3,\quad X_2\in\mathcal{O}_L,\\a^2+(\phi^2+2\phi-20)ab+(-6\phi^2+14\phi+32)b^2=&\frac{1}{2}\epsilon_1^{-i_1}\epsilon_2^{-i_2}\bar{X_2}^3,\quad X_2\bar{X}_2=2U.\end{aligned}\tag{2.2.17}$$

If $\mathcal{X} \sim p_2^2$, then from (2.2.14)

$$\begin{aligned} a+(-\phi^2-2\phi+2)b =& \frac{1}{2}\epsilon_1^{i_1}\epsilon_2^{i_2}X_3^3, \quad X_3 \in \mathcal{O}_L, \\ a^2+(\phi^2+2\phi-20)ab+(-6\phi^2+14\phi+32)b^2 =& \frac{1}{4}\epsilon_1^{-i_1}\epsilon_2^{-i_2}\bar{X_2}^3, \quad X_3\bar{X}_3 = 2U. \end{aligned} \tag{2.2.18}$$

Similarly:

If $\mathcal{Y} \sim 1$, then from (2.2.15)

$$\begin{aligned} a+(\phi^2-2\phi-6)b =& \epsilon_1^{j_1}\epsilon_2^{j_2}Y_1^3, \quad Y_1 \in \mathcal{O}_L, \\ a^2+(-\phi^2+2\phi+12)ab+(-2\phi^2-2\phi+8)b^2 =& \epsilon_1^{-j_1}\epsilon_2^{-j_2}\bar{Y_1}^3, \quad Y_1\bar{Y}_1 = V. \end{aligned} \tag{2.2.19}$$

If $\mathcal{Y} \sim p_2$, then from (2.2.15)

$$\begin{aligned} a+(\phi^2-2\phi-6)b =& \frac{1}{4}\epsilon_1^{j_1}\epsilon_2^{j_2}Y_2^3, \quad Y_2 \in \mathcal{O}_L, \\ a^2+(-\phi^2+2\phi+12)ab+(-2\phi^2-2\phi+8)b^2 =& \frac{1}{2}\epsilon_1^{-j_1}\epsilon_2^{-j_2}\bar{Y_2}^3, \quad Y_2\bar{Y}_2 = 2V. \end{aligned} \tag{2.2.20}$$

If $\mathcal{Y} \sim p_2^2$, then from (2.2.15)

$$\begin{aligned} a+(\phi^2-2\phi-6)b =& \frac{1}{2}\epsilon_1^{j_1}\epsilon_2^{j_2}Y_3^3, \quad Y_3 \in \mathcal{O}_L, \\ a^2+(-\phi^2+2\phi+12)ab+(-2\phi^2-2\phi+8)b^2 =& \frac{1}{4}\epsilon_1^{-j_1}\epsilon_2^{-j_2}\bar{Y_3}^3, \quad Y_3\bar{Y}_3 = 2V. \end{aligned} \tag{2.2.21}$$

The equations (2.2.16) – (2.2.18) and (2.2.19) – (2.2.21) give the following equations respectively in $\mathcal{O}_L$:

$$\begin{aligned} a+(-\phi^2-2\phi+2)b =& \frac{1}{\mu}\epsilon_1^{i_1}\epsilon_2^{i_2}X_i^3, \\ a^2+(\phi^2+2\phi-20)ab+(-6\phi^2+14\phi+32)b^2 =& \frac{1}{\mu'}\epsilon_1^{-i_1}\epsilon_2^{-i_2}\bar{X_i}^3, \end{aligned}$$

where $(\mu, \mu') = (1,1), (4,2), (2,4)$; and

$$\begin{aligned} a+(\phi^2-2\phi-6)b =& \frac{1}{\upsilon}\epsilon_1^{j_1}\epsilon_2^{j_2}Y_3^3, \quad Y_j \in \mathcal{O}_L, \\ a^2+(-\phi^2+2\phi+12)ab+(-2\phi^2-2\phi+8)b^2 =& \frac{1}{\upsilon'}\epsilon_1^{-j_1}\epsilon_2^{-j_2}\bar{Y_3}^3, \quad Y_j\bar{Y}_j = V, \end{aligned}$$

where $(\upsilon, \upsilon^{'}) = (1,1),(4,2),(2,4)$.

We accordingly have equations in $\mathcal{O}_L$ :

$$(a+(-\phi^2-2\phi+2)b)(a^2+(-\phi^2+2\phi+12)ab+(-2\phi^2-2\phi+8)b^2) = \frac{1}{\mu\upsilon^{'}}\epsilon_1^r\epsilon_2^s X_i^3\bar{Y_j}^3, \tag{2.2.22}$$

$$(a+(\phi^2-2\phi-6)b)(a^2+(\phi^2+2\phi-20)ab+(-6\phi^2+14\phi+32)b^2) = \frac{1}{\mu^{'}\upsilon}\epsilon_1^{-r}\epsilon_2^{-s}\bar{X_i}^3 Y_j^3, \tag{2.2.23}$$

where $r(=i_1-j_1)=0,\pm1,\ s(=i_2-j_2)=0,\pm1$.

Now $3\nmid UV$, so $(X_i),(\bar{X}_i),(Y_j),(\bar{Y}_j)$ are coprime to $p_3$. Then for $\alpha\in\mathcal{O}_L$ and $p_3\nmid(\alpha)$, we have $p_3|(\alpha^2-1)$. Therefore $3=p_2^3|(\alpha^2-1)^3\equiv\alpha^6-1 \mod 3$. Hence $\alpha^3\equiv\pm1 \mod 3$. It follows that $X_i^3\bar{Y_j}^3\equiv\pm1 \mod 3$. Since $\mu,\mu^{'},\upsilon,\upsilon^{'}\equiv\pm1 \mod 3$, equation (2.2.22) gives

$$(a+b)(a^2+ab+b^2)+b(a^2+ab+b^2)\phi^2\equiv\pm\epsilon_1^r\epsilon_2^s \mod 3, \tag{2.2.24}$$

and equation (2.2.23) gives

$$(a+b)(a^2-b^2)+b^2(a-b)\phi-b(a^2-b^2)\phi^2\equiv\pm\epsilon_1^{-r}\epsilon_2^{-s} \mod 3. \tag{2.2.25}$$

We have

Table 2.1: Possible Values Of $(r,s)$

| (r,s) | $\epsilon_1^r\epsilon_2^s$ | $\epsilon_1^{-r}\epsilon_2^{-s}$ |
|---|---|---|
| (-1,-1) | $-\phi^2+2\phi+7$ | $\phi^2+4\phi+3$ |
| (-1,0) | $-\phi^2+\phi+11$ | $\phi+1$ |
| (-1,1) | $-2\phi^2+2\phi+23$ | $-2\phi^2+6\phi+7$ |
| (0,-1) | $\phi^2-3\phi-3$ | $\phi+3$ |
| (0,0) | 1 | 1 |
| (0,1) | $\phi+3$ | $\phi^3-3\phi-3$ |

| | | |
|---|---|---|
| (1,-1) | $-2\phi^2+6\phi+7$ | -$2\phi^2+2\phi+23$ |
| (1,0) | $\phi+1$ | $-\phi^2+\phi+11$ |
| (1,1) | $\phi^2+4\phi+3$ | $-\phi^2+2\phi+7$ |

Comparing coefficients of $\phi$, equation (2.2.24) eliminates all but $(r,s)=(0,-1),(0,0),(1,-1)$, with corresponding units $\zeta=\epsilon_1^r\epsilon_2^s=\phi^2-3\phi-3, 1, -2\phi^2+6\phi+7$. It remains to treat the nine pairs of equations at (2.2.22), (2.2.23):

$$C_1\colon (a+(-\phi^2-2\phi+2)b)(a^2+(-\phi^2+2\phi+12)ab+(-2\phi^2-2\phi+8)b^2)=\frac{1}{\lambda}\cdot\zeta\cdot cube,$$
$$C_2\colon (a+(\phi^2-2\phi-6)b)(a^2+(\phi^2+2\phi-20)ab+(-6\phi^2+14\phi+32)b^2)=\frac{1}{\lambda'}\cdot\zeta\cdot cube, \quad (2.2.26)$$

where $(\lambda,\lambda')=(1,1),(4,2),(2,4)$ and $\zeta\in\{\phi^2-3\phi-3,1,-2\phi^2+6\phi+7\}$.
For each pairs of equations in (2.2.26), the elliptic curve Chabauty routine in Magma [1] works on either $C_1$ or $C_2$. The result is recorded in the following table, where $\emptyset$ means there are no solutions.

Table 2.2: Solutions Corresponding to the Values Of $(\lambda,r,s)$

| $\lambda$ | (r,s) | Curve | Rank | Cubic model | $(a,b)$ |
|---|---|---|---|---|---|
| 1 | (0,-1) | $C_2$ | 1 | $y^2=x^3+9(-17\phi^2+16\phi+193)$ | $\emptyset$ |
| 1 | (0,0) | $C_2$ | 1 | $y^2=x^3+(360802\phi^2-6430320\phi-7101783)$ | $(\pm1,0)$ |
| 1 | (-1,1) | $C_1$ | 0 | $y^2=x^3+(2168127\phi^2-6430320\phi-7101783)$ | $\emptyset$ |
| 4 | (0,-1) | $C_1$ | 0 | $y^2=x^3+(9204\phi^2-27144\phi-30732)$ | $\emptyset$ |
| 4 | (0,0) | $C_1$ | 0 | $y^2=x^3+(-312\phi^2+312\phi+4212)$ | $\emptyset$ |
| 4 | (1,-1) | $C_1$ | 1 | $y^2=x^3+(28\phi^2-68\phi-83)$ | $\emptyset$ |

| | | | | | |
|---|---|---|---|---|---|
| 2 | (0,-1) | $C_2$ | 1 | $y^2 = x^3 + (28\phi^2 - 68\phi - 83)$ | $\emptyset$ |
| 2 | (0,0) | $C_1$ | 0 | $y^2 = x^3 + (64584\phi^2 + 247104\phi + 169533)$ | $\emptyset$ |
| 2 | (1,-1) | $C_2$ | 1 | $y^2 = x^3 + (7\phi^2 - 20\phi - 23)$ | $\emptyset$ |

So $(a,b) = (\pm 1, 0)$. Hence $|U| = |V| = 1$. Thus $X = 2$ and $(x,y) = (\pm 2, \pm 5)$. □

## 2.3 Equation $y^2 = x^6 - 47$

In this section, we will prove Theorem 9.

*Proof.* Equation $y^2 = x^6 - 47$ is equivalent to

$$Y^2 = X^6 - 47Z^6,$$

where $X, Y, Z$ are coprime. We have

$$(X^3 - Y)(X^3 + Y) = 47Z^6.$$

The $\gcd(X^3 - Y, X^3 + Y)$ divides $\gcd(2X^3, 2Y)$, so divides 2. We can choose the sign of $Y$ such that $47 | X^3 + Y$.

Case gcd is 1:

$$X^3 + Y = 47V^6, \quad X^3 - Y = U^6, \quad \gcd(U,V) = 1.$$

So

$$2X^3 = 47V^6 + U^6, \quad \gcd(U,V) = 1.$$

If $13 \nmid UV$, then $2X^3 \equiv \pm 1 \pm 47 \mod 13$. Thus $4X^6 \equiv (1 \pm 5)^2 \mod 13$. So $\pm 4 \equiv \pm 3 \mod 13$, impossible. Therefore $13 | UV$. If $13 | U$, then $2X^3 \equiv 47V^6 \equiv \pm 5 \mod 13$. Thus $4X^6 \equiv 25 \equiv -1 \mod 13$. So $\pm 4 \equiv -1 \mod 13$, impossible. If $13 | V$, then $2X^3 \equiv U^6 \mod 13$. Thus $4X^6 \equiv U^{12} \equiv 1 \mod 13$. So $\pm 4 \equiv \pm 1 \mod 13$, impossible.

Case gcd is 2:

Then

$$X^3 + Y = 47 \cdot 2 \cdot V^6, \quad X^3 - Y = 2^5 \cdot U^6, \quad \gcd(U, V) = 1,$$

or

$$X^3 + Y = 47 \cdot 2^5 \cdot V^6, \quad X^3 - Y = 2 \cdot U^6, \quad \gcd(U, V) = 1;$$

So

$$X^3 = 47V^6 + 16U^6, \quad \gcd(U, V) = 1,$$

or

$$X^3 = 47 \cdot 2^4 \cdot V^6 + U^6, \quad \gcd(U, V) = 1.$$

The latter case gives $(X/V^2)^3 = 752 + (U^3/V^3)^2$. The elliptic curve $y^2 = x^3 - 752$ has rank 0, and the trivial torsion subgroup, implying $V = 0$. So we only need to consider the case

$$X^3 = 16U^6 + 47V^6. \tag{2.3.1}$$

From $63^3 = 16 \cdot 5^3 + 47$, we would like to show that $X = 63$, $|U| = |V| = 1$.

If $3|U$, then from (2.3.1), we have $X^3 \equiv 47V^6 \equiv 2 \mod 9$. Thus $X^6 \equiv 4 \mod 9$, so $1 \equiv 4 \mod 9$, impossible. So $3 \nmid U$. If $3|V$, then $X^3 \equiv 16U^6 \equiv -2 \mod 9$. Thus $X^6 \equiv 4 \mod 9$, impossible. So $3 \nmid V$. Therefore $X^3 \equiv 0 \mod 9$, giving $3|X$.

From (2.3.1), we also have $2 \nmid X$, $V$.

Let $K = \mathbb{Q}(\theta)$, where $\theta = \sqrt{-47}$. K has the class number 5, the trivial fundamental unit group, and the ring of integers $\mathcal{O}_K = \mathbb{Z}[\frac{1+\theta}{2}]$. The class group of $K$ is generated by the ideal $I = (2, \frac{1+\theta}{2})$. Now

$$(X)^3 = (4U^3 + \theta V^3)(4U^3 - \theta V^3). \tag{2.3.2}$$

Let $J$ be a common ideal dividing both factors on the right side. Then

$$J|(8U^3), \quad J|(2\theta V^3), \quad J^2|(X)^3.$$

Taking norms gives

$$\mathrm{Norm}(J)|64U^6, \quad \mathrm{Norm}(J)|4\cdot 47\cdot V^6, \quad \mathrm{Norm}(J)|X^3.$$

But $2\nmid X$, so $\mathrm{Norm}(J)|\gcd(X^3, U^6, 47V^6) = 1$. Therefore $(4U^3+\theta V^3)$ and $(4U^3 - \theta V^3)$ are coprime ideals. Thus

$$(4U^3+\theta V^3) = \mathcal{A}^3,$$

where $\mathcal{A}$ is an ideal in $\mathcal{O}_K$. K has class number 5 with the trivial unit group, hence

$$4U^3+\theta V^3 = A^3 \tag{2.3.3}$$

with $A\in\mathcal{O}_K$. Let $A = u+v\frac{(1+\theta)}{2}$, where $u,v\in\mathbb{Z}$. Then

$$A^3 = (3/2u^2v+3/2uv^2-11/2v^3)\theta+u^3+3/2u^2v-69/2uv^2-35/2v^3.$$

$A^3\in\mathbb{Z}[\theta]$ implies $u^3+3/2u^2v-69/2uv^2-35/2v^3\in\mathbb{Z}$, hence $\frac{u^2v-uv^2-v^3}{2}\in\mathbb{Z}$. If $2\nmid v$, then $\frac{u^2-u-1}{2}\in\mathbb{Z}$, impossible. So $2|v$. Therefore $A\in\mathbb{Z}[\theta]$. Let

$$4U^3+\theta V^3 = (a+b\theta)^3,$$

where $a,b\in\mathbb{Z}$. Taking norms gives

$$X = a^2+47b^2.$$

$2|X$ implies $2\nmid a,\ b$; $3|X$ implies $3\nmid a,\ b$. Expanding $(a+b\theta)^3$ gives

$$\begin{aligned} 4U^3 &= a(a^2-141b^2),\\ V^3 &= b(3a^2-47b^2). \end{aligned} \tag{2.3.4}$$

In the second equation, we have

$$\gcd(b, 3a^2 - 47b^2) = \gcd(b, 3a^2) = \gcd(b, 3) = 1.$$

Further, $V$ is odd so $b$ is odd. $3a^2 - 47b^2 | V^3$ so $3a^2 - 47b^2$ is odd, hence $a$ is even. Thus $a^2 - 141b^2$ is odd, so $4|a$. If $47|a$, then $47|v^3$ and $47|U^3$. So $47|\gcd(U, V)$, contradicting $\gcd(U, V) = 1$. Hence $47 \nmid a$, so $\gcd(a, a^2 - 141b^2) = 1$. Therefore from (2.3.4), we have

$$a = 4A^3, \quad b = B^3, \quad 3a^2 - 47b^2 = C^3, \quad a^2 - 141b^2 = D^3,$$

where $A, B, C, D \in \mathbb{Z}$, $AD = U$, $CB = V$.

Because $\gcd(U, V) = \gcd(a, b) = \gcd(a, 141) = \gcd(b, 3) = 1$, we have $A, B, C, D$ are coprime. Further, $3, 47 \nmid a$, so $3, 47 \nmid A, D$; $2, 3 \nmid b$ so $2, 3 \nmid B, C$. Now

$$48A^6 - 47B^6 = C^3,$$

$$16A^6 - 141B^6 = D^3.$$

We will show $|A| = |B| = 1$ and $C = 1$, $D = -5$. Indeed, we have

$$3C^3 - D^3 = 128A^6,$$

$$C^3 - 3D^3 = 376B^6.$$

Note that $C^3 \equiv 3D^3 \mod 8$ and $2 \nmid C$, so

$$C \equiv 3D \mod 8.$$

Also $C^3 \equiv 3D^3 \mod 47$ and $47 \nmid D$, so

$$D \equiv -5C \mod 47.$$

Let $L = \mathbb{Q}(\phi)$, where $\phi = \sqrt[3]{3}$. L has class number 1, the ring of integers $\mathcal{O}_L = \mathbb{Z}[\phi]$, and a fundamental unit $\epsilon = \phi^2 - 2$ of norm 1. The ideal $(2) = p_2 q_2$, where $p_2 = (-1 + \phi)$

and $q_2 = (1+\phi+\phi^2)$. The ideal $(47) = p_{47}q_{47}$, where $p_{47} = (2+\phi+2\phi^2)$ and $q_{47} = (2-10\phi+3\phi^2)$. Now

$$(C - D\phi)(C^2 + CD\phi + D^2\phi^2) = 2^3 \cdot 47 \cdot B^6.$$

Because

$$\gcd(C - D\phi, C^2 + CD\phi + D^2\phi^2) = \gcd(C - D\phi, 3D^2\phi^2) = \gcd(C - D\phi, \phi^5) = 1,$$

the two factors on the left are coprime.

We note that

$$C - D\phi \equiv C(1+5\phi) \equiv 0 \mod p_{47},$$

$$C - D\phi \equiv D(3-\phi) \equiv 0 \mod p_2^3.$$

Thus

$$C - D\phi = (-1)^h \epsilon^i p_2^j p_{47}^k G^6,$$

where $G \in \mathcal{O}_L$, and $0 \le h \le 1$, $0 \le i, j, k \le 5$. Taking norms gives

$$2^3 \cdot 47 \cdot B^6 = (-1)^h 2^j 47^k \mathrm{Norm}(G)^6.$$

So $h$ is even, $j \equiv 3 \mod 6$, $k \equiv 1 \mod 6$. Thus $(h, j, k) = (0, 3, 1)$. Then

$$C - D\phi = \epsilon^i (13 - 10\phi + \phi^2) G^6.$$

We claim that $i = 5$.

If $i \equiv 0 \mod 2$, then

$$C - D\phi = (13 - 10\phi + \phi^2)(M + N\phi + P\phi^2)^2, \quad M, N, P \in \mathbb{Z}.$$

Comparing coefficients of $\phi^2$ gives

$$M^2 - 20MN + 13N^2 + 26MP + 6NP - 30P^2 = 0,$$

which is locally unsolvable at 2. Thus $i$ is odd.

If $i = 3$, then

$$C - D\phi = (13 - 10\phi + \phi^2)(M + N\phi + P\phi^2)^3, \quad M, N, P \in \mathbb{Z}.$$

Comparing coefficients of $\phi^2$ gives

$$M^3 - 30M^2N + 39MN^2 + 3N^3 + 39M^2P + 18MNP - 90N^2P - 90MP^2 + 117NP^2 + 9P^3 = 0,$$

which is locally unsolvable at 3.

If $i = 1$, then

$$C - D\phi = (-56 + 23\phi + 11\phi^2)(M + N\phi + P\phi^2)^3, \quad M, N, P \in \mathbb{Z}.$$

Comparing coefficients of $\phi^2$ gives

$$11M^3 + 69M^2N - 168MN^2 + 33N^3 - 168M^2P + 198MNP + 207N^2P + 207MP^2 - 504NP^2 + 99P^3 = 0,$$

which is locally unsolvable at 3. Therefore $i = 5$, equivalently, on taking $i = -1$, we have

$$C - D\phi = (1 + 5\phi)G^6.$$

It follows that

$$(C - D\phi)(3C^3 - D^3) = 2(1 + 5\phi)(2AG)^6,$$

or

$$2(1 + 5\phi)(x - \phi)(3x^3 - 1) = y^2,$$

where $x = \frac{C}{D}$ and $y = 2(1 + 5\phi)(2AG)^3/D^2$, representing an elliptic curve over $L$. The cubic model is

$$y^2 = x^3 + (-30\phi^2 + 174\phi + 36)x^2 + (9012\phi^2 + 5040\phi - 12708)x + (207576\phi^2 - 409536\phi + 449064).$$

This curve has rank 2. The Chabauty routine in Magma [1] shows $\frac{C}{D} = \frac{-1}{5}$. Hence $C = 1$, $D = -5$, and $|A| = |B| = 1$. Therefore the only solutions to $y^2 = x^6 - 47$ are

$x = \pm\frac{63}{10}$ and $y = \pm\frac{249953}{10^3}$.

$\square$

# Chapter 3

# CUBIC POINTS ON QUARTIC CURVES

## 3.1 Introduction

This chapter studies the equation $F(x^2, y^2, z^2) = 0$, where $F(X, Y, Z)$ is a non-singular, irreducible, rational homogeneous quadratic polynomial in three variables. This equation defines a curve $\mathcal{C}$ of genus 3. The question of finding all rational points on genus 3 curves is interesting, but currently there are no known algorithms to find all rational points on such curves. We can ask if $\mathcal{C}$ has a point in an odd degree extension of $\mathbb{Q}$. Coray [13] showed that if $\mathcal{C}$ has a point in an odd degree extension of $\mathbb{Q}$, then $\mathcal{C}$ also has a point in $\mathbb{Q}$ or a cubic extension of $\mathbb{Q}$ ( which we shall call a cubic point). Using algebraic number theory, Bremner, Lewis and Morton [2] gave some examples of the form $ax^4 + by^4 = cz^4$ which have no rational solutions but have cubic points where $a, b, c$ are positive integers. Cassels [11] gave an algorithm to find cubic points in $\mathcal{C}$ and some examples where $\mathcal{C}$ has no cubic points. Using a different approach, Bremner [3] studied the equation $x^4 + y^4 = Dz^4$. Based on the techniques of Cassels [11] and Bremner [3], I will prove a necessary condition for $\mathcal{C}$ to have a cubic point, and then apply it to extend some old results on the equation $x^4 + nx^2y^2 + y^4 = Dz^4$.

## 3.2 Cubic Points and Their Associated Curves

We are interested in the genus 3 curve

$$\mathcal{C} \colon F(x^2, y^2, z^2) = 0.$$

We make the following assumption:

$$\text{if } X, Y, Z \in \mathbb{Q} \text{ such that } F(X,Y,Z) = 0 \text{ and } XYZ = 0 \text{ then } X = Y = Z = 0. \tag{3.2.1}$$

Consider three associated curves

$$\begin{cases} E_1\colon F(X, y^2, z^2) = 0, \\ E_2\colon F(x^2, Y, z^2) = 0, \\ E_3\colon F(x^2, y^2, Z) = 0. \end{cases}$$

By definition, a point $(x_0 : y_0 : z_0) \in \mathbb{P}^2(\bar{\mathbb{Q}})$ is a cubic point if $\mathbb{Q}(x_0 : y_0 : z_0)$ is a cubic number field. We need the following.

**Lemma 3.2.1.** *If $\mathcal{C}$ has a point in $\mathbb{P}_2(\mathbb{Q})$ then $\mathcal{C}$ also has a cubic point.*

*Proof.* See Cassels [11]. □

Let $P = (\alpha, \beta, \gamma)$ be a cubic point on $\mathcal{C}$, and $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. $G$ acts on $P$ by

$$g(P) = (g(\alpha) : g(\beta) : g(\gamma)) \ \forall g \in G.$$

If $\gamma \neq 0$ then we can take $\gamma = 1$ and $P = (\alpha, \beta, 1)$. Without loss of generality, we can assume $\alpha \notin \mathbb{Q}$. Then $\beta = p(\alpha)$, where $p(x)$ is a polynomial of degree at most 2 with rational coefficients. The set of orbits of $P$ is $\{(\alpha_i, p(\alpha_i), 1), i = 1, 2, 3\}$, where $\alpha_i, i = 1, 2, 3$ are all Galois conjugates of $\alpha$. Each set of orbits of a cubic point on $\mathcal{C}$ is called a rational triplet.

Let $T$ be a triplet $\{(\alpha_i, \beta_i, \gamma_i), i = 1, 2, 3\}$ on $\mathcal{C}$. Then we have a triple of points $\{(\alpha_i^2, \beta_i, \gamma_i), i = 1, 2, 3\}$ on $E_1$. Because $\alpha_i^2, \beta_i^2, \gamma_i^2, \beta_i\gamma_i$ are linearly dependent over $\mathbb{Q}$, there are $r, s, t \in \mathbb{Q}$ such that

$$\alpha_i^2 = r\beta_i^2 + s\beta_i\gamma_i + t\gamma_i^2$$

for $i = 1, 2, 3$. This holds for $i = 1, 2, 3$ because the triple $\{(\alpha_i^2, \beta_i, \gamma_i), i = 1, 2, 3\}$ is invariant under $G$. The curve

$$X = ry^2 + syz + tz^2$$

intersects $E_1$ at the triplet $\{(\alpha_i^2, \beta_i, \gamma_i), i = 1, 2, 3\}$ and a fourth point which is necessarily a rational point. Denote this point by $v_1(T)$. So $v_1$ maps each rational triplet $T$ on $\mathcal{C}$ to a rational point $v_1(T)$ on $E_1$. See Cassels [11].

Similarly, we have maps $v_2, v_3$ from the set of rational triplets on $\mathcal{C}$ to the set of rational points on $E_2, E_3$ respectively. Thus for each rational triplet $T$ on $\mathcal{C}$ we have a triple $(v_1(T), v_2(T), v_3(T)) \in E_1(\mathbb{Q}) \times E_2(\mathbb{Q}) \times E_3(\mathbb{Q})$.

Denote the groups of rational points on $E_1, E_2, E_3$ by $G_1, G_2,$ and $G_3$ respectively. Let $(P_1, P_2, P_3) \in G_1 \times G_2 \times G_3$. We want to find a rational triplet $T$ such that

$$v_1(T) = P_1,\ \ v_2(T) = P_2\ , v_3(T) = P_3.$$

Cassels [11] and Bremner [3] showed that it is enough to find triplets $T$ such that $v_i(T)$ is in the coset reprentatives of $G_i/2G_i$ for $i = 1, 2, 3$.

The map $v_1$ sends a rational triplet to a rational point on $E_1$; thus there is a non trivial rational point on $E_1$. So $F(X, Y, Z) = 0$ has non trivial solutions. Let

$$X : Y : Z = X(l, m) : Y(l, m) : Z(l, m) \tag{3.2.2}$$

be a parameterization of $F(X, Y, Z) = 0$, where $X(l, m), Y(l, m), Z(l, m)$ are degree 2 homogeneous polynomials in $l, m$ with rational coefficients.

Because $P = (\alpha : \beta : \gamma)$ is a cubic point on $\mathcal{C}$, we have $(\alpha^2 : \beta^2 : \gamma^2)$ is a point on $F(X, Y, Z) = 0$. Let $(\alpha^2 : \beta^2 : \gamma^2)$ be parameterized by $\lambda : \mu$.

Let $f(x) = Ax^3 + Bx^2 + Cx + D$ be the defining polynomial of $\frac{\lambda}{\mu}$, where $A, B, C, D \in \mathbb{Z}$ and $\gcd(A, B, C, D) = 1$.

Let $\frac{\lambda_1}{\mu_1}, \frac{\lambda_2}{\mu_2}, \frac{\lambda_3}{\mu_3}$ be all conjugates of $\frac{\lambda}{\mu}$. Then $f(x)$ has the factorization

$$f(x) = A(x - \frac{\lambda_1}{\mu_1})(x - \frac{\lambda_2}{\mu_2})(x - \frac{\lambda_3}{\mu_3}).$$

Assume that $v_1(T) = (X_1, y_1, z_1)$ and let $(X_1 : y_1^2 : z_1^2)$ be parameterized by

$$X_1 : y_1^2 : z_1^2 = X(l_1, m_1) : Y(l_1, m_1) : Z(l_1, m_1), \tag{3.2.3}$$

where $l_1, m_1 \in \mathbb{Q}$.

Assume that in (3.2.2)

$$Z(l, m) = al^2 + blm + cm^2, \tag{3.2.4}$$

where $a, b, c \in \mathbb{Q}$.

The following lemma is due to Cassels [11]

**Lemma 3.2.2.** *Let $d = y_1$ then there are $u, v, w, q \in \mathbb{Q}$ and $q \neq 0$ such that*

$$\begin{cases} qA = m_1u^2 + 2aduw + gaw^2, \\ qB = -l_1u^2 + 2m_1uv + 2bduw + 2advw + (gb + ha)w^2, \\ qC = -2l_1uv + m_1v^2 + 2cduw + 2bdvw + (gc + hb)w^2, \\ qD = -l_1v^2 + 2cdvw + hcw^2, \end{cases} \tag{3.2.5}$$

*where $y_1^2 Z(l, m) - z_1^2 Y(l, m) = (m_1 l - l_1 m)(gl + hm)$.*

*Proof.* Lemma 2.1, Cassels [11]. □

**Lemma 3.2.3.** *If $Z(l, m) = al^2 + cm^2$ in (3.2.4), then*

$$Z(l_1, m_1)((a(cB - aD)^2 + c(cA - aC)^2) \in (\mathbb{Q}^*)^2.$$

*Proof.* Substituting $b = 0$ in (3.2.5), we have

$$\begin{cases} qA = m_1u^2 + 2aduw + gaw^2, \\ qB = -l_1u^2 + 2m_1uv + 2advw + haw^2, \\ qC = -2l_1uv + m_1v^2 + 2cduw + gcw^2, \\ qD = -l_1v^2 + 2cdvw + hcw^2. \end{cases}$$

From the first and the third equations, we have

$$q(cA - aC) = m_1(cu^2 - av^2) + 2l_1auv.$$

From the second and the fourth equations, we have

$$q(cB - aD) = l_1(av^2 - cu^2) + 2m_1cuv.$$

Combining the above two equations, we have

$$\begin{aligned} q^2(c(cA - aC)^2 + a(cB - aD)^2) &= (cm_1^2 + al_1^2)(av^2 - cu^2)^2 + 4l_1^2a^2cu^2v^2 + 4m_1^2ac^2u^2v^2 \\ &= (cm_1^2 + al_1^2)((av^2 - cu^2)^2 + 4acu^2v^2) \\ &= (al_1^2 + cm_1^2)(av^2 + cu^2)^2. \end{aligned} \tag{3.2.6}$$

If $c(cA - aC)^2 + a(cB - aD)^2 = 0$, then $Z(cB - aD, cA - aC) = 0$. Let $q = cA - aC$ and $p = cB - aD$. Then $((X(p, q), Y(p, q), Z(p, q))$ is a solution of $F(X, Y, Z) = 0$ with $Z(p, q) = 0$. By (3.2.1), we have

$$X(p, q) = Y(p, q) = Z(p, q) = 0. \tag{3.2.7}$$

If $p \neq 0$ or $q \neq 0$, then from (3.2.7), $X(l, m), Y(l, m), Z(l, m)$ has a common factor $lq - mp$, thus $F(X, Y, Z) = 0$ has a parameterization $(X_1(l, m) : Y_1(l, m) : Z_1(l, m))$, where $X_1(l, m), Y_1(l, m), Z_1(l, m)$ are linear polynomials in $l, m$. Therefore every point in $F(X,Y,Z)=0$ is a rational point, which contradicts the existence of a cubic point, for example the point $(\alpha^2,\beta^2,\gamma^2)$.

Therefore

$$p=q=0.$$

So

$$cA-aC=cB-aD=0.$$

The polynomial $f(x)$ is now reducible with a factorization

$$f(x)=(Cx+D)(\frac{B}{D}x^2+1).$$

So

$$c(cA-aC)^2+a(cB-aD)^2\neq 0.$$

From (3.2.6), we have

$$Z(l_1,m_1)((a(cB-aD)^2+c(cA-aC)^2)\in(\mathbb{Q}^*)^2.$$

□

We consider the case where

$$Z(l,m)=al^2+blm+cm^2 \quad \text{where} \quad a\neq 0 \quad \text{or} \quad c\neq 0. \tag{3.2.8}$$

By homogeneity, we assume that $a=1$. Then

$$Z(l,m)=l^2+blm+cm^2. \tag{3.2.9}$$

Let

$$\begin{cases} X_1(l,m)=X(l-\frac{b}{2}m,m),\\ Y_1(l,m)=Y(l-\frac{b}{2}m,m),\\ Z_1(l,m)=Z(l-\frac{b}{2}m,m).\end{cases}$$

Then

$$\begin{cases} X_1(l+\frac{b}{2}m,m)=X(l,m), \\ Y_1(l+\frac{b}{2}m,m)=Y(l,m), \\ Z_1(l+\frac{b}{2}m,m)=Z(l,m). \end{cases}$$

For example, because $Z(l,m)=l^2+blm+cm^2$, we have $Z_1(l,m)=l^2+(c-\frac{b^2}{4})m^2$.

We have

$$F(X_1(l+\frac{b}{2}m,m),Y_1(l+\frac{b}{2}m,m),Z_1(l+\frac{b}{2}m,m))=F(X(l,m),Y(l,m),Z(l,m))=0.$$

In other words, if $F(X,Y,Z)=0$ has a parameterization $X(l,m):Y(l,m):Z(l,m)$, then it has a parametrization

$$X_1(l,m):Y_1(l,m):Z_1(l,m)=X(l-\frac{b}{2}m,m):Y(l-\frac{b}{2}m,m):Z(l-\frac{b}{2}m,m).$$

Conversely if $F(X,Y,Z)=0$ has a parametrization $(X_1(l,m):Y_1(l,m):Z_1(l,m))$, then it also has a parametrization

$$X(l,m):Y(l,m):Z(l,m)=X_1(l+\frac{b}{2}m,m):Y_1(l+\frac{b}{2}m,m):Z_1(l+\frac{b}{2}m,m).$$

Because $(\alpha^2:\beta^2:\gamma^2)$ is a solution of $F(X,Y,Z)=0$, $(\alpha^2:\beta^2:\gamma^2)$ has a parameterization

$$\alpha^2:\beta^2:\gamma^2=X_1(L_1,M_1):Y_1(L_1,M_1):Z_1(L_1,M_1),$$

where

$$\frac{L_1}{M_1}=\frac{\lambda+\frac{b}{2}\mu}{\mu}=\frac{\lambda}{\mu}+\frac{b}{2}.$$

$\frac{\lambda}{\mu}$ is a root of $f(x)=Ax^3+Bx^2+Cx+D$, so $\frac{L_1}{M_1}$ is a root of

$$f(x-\frac{b}{2})=Ax^3+(-\frac{3}{2}Ab+B)x^2+(\frac{3}{4}Ab^2-Bb+C)x-\frac{1}{8}Ab^3+\frac{1}{8}Bb^2-\frac{1}{2}Cb+D.$$

Let

$$\begin{cases} A_1 &= A, \\ B_1 &= -\frac{3}{2}Ab + B, \\ C_1 &= \frac{3}{4}Ab^2 - Bb + C, \\ D_1 &= -\frac{1}{8}Ab^3 + \frac{1}{4}Bb^2 - \frac{1}{2}Cb + D. \end{cases}$$

The intersection of the curve $E_1$ and the curve $X = ry^2 + syz + tz^2$ contains a rational point $(X_1, y_1^2, z_1^2)$ satisfying

$$\begin{aligned} X_1 : y_1^2 : z_1^2 &= X(l_1, m_1) : Y(l_1, m_1) : Z(l_1, m_1) \\ &= X_1(l_1 + \frac{b}{2}m_1, m_1) : Y_1(l_1 + \frac{b}{2}m_1, m_1) : Z_1(l_1 + \frac{b}{2}m_1) \\ &= X_1(L, M) : Y_1(L, M) : Z_1(L, M), \end{aligned}$$

where $L = l_1 + \frac{b}{2}m_1,$ and $M = m_1$.

Let $H_1(A, B, C, D) = (c_1B_1 - D_1)^2 + c_1(c_1A_1 - C_1)^2$, where $a_1 = 1$ and $c_1 = c - \frac{b^2}{4}$. Then

$$\begin{aligned} H_1(A, B, C, D) = &-b^3AD + b^2cAC + b^2BD - bc^2AB + 3bcAD - bcBC - bCD \\ &+ c^3A^2 - 2c^2AC + c^2B^2 - 2cBD + cC^2 + D^2. \end{aligned} \tag{3.2.10}$$

By applying Lemma 3.2.3 to $Z_1(l, m) = l^2 + (c - \frac{b^2}{4})m^2 = a_1l^2 + c_1m^2$, where $a_1 = 1,$ and $c_1 = c - \frac{b^2}{4}$, we have

$$Z_1(L, M)H_1(A, B, C, D) \in (\mathbb{Q}^*)^2.$$

Because $Z_1(L, M) = Z(l_1, m_1)$, we have

$$Z(l_1, m_1)H_1(A, B, C, D) \in (\mathbb{Q}^*)^2. \tag{3.2.11}$$

**Lemma 3.2.4.** *Assume that in* (3.2.2) $Z(l,m) = al^2 + blm + cm^2$. *Let*

$$H(A,B,C,D) = -b^3AD + b^2cAC + ab^2BD - bc^2AB + 3abcAD - abcBC - a^2bCD$$
$$+ c^3A^2 - 2ac^2AC + ac^2B^2 - 2a^2cBD + a^2cC^2 + a^3D^2.$$

*Then*

$$Z(l_1,m_1)H(A,B,C,D) \in (\mathbb{Q}^*)^2,$$

*where* $(l_1,m_1)$ *is in* (3.2.3).

*Proof.* If $a \neq 0$ or $c \neq 0$, then we can assume that $a \neq 0$. By replacing $b$ by $\frac{b}{a}$ and $c$ by $\frac{c}{a}$ in (3.2.9) , (3.2.10) and (3.2.11), we have

$$Z(l_1,m_1)H(A,B,C,D) \in (\mathbb{Q}^*)^2.$$

If $a = c = 0$, then from the first and the fourth equations in (3.2.5), we have

$$\begin{cases} qA = m_1u^2, \\ qD = -l_1v^2. \end{cases} \tag{3.2.12}$$

So

$$q^2AD = -m_1l_1(uv)^2.$$

Moreover, because $H(A,B,C,D) = -b^3AD$ and $Z(l_1,m_1) = bl_1m_1$, we have

$$q^2Z(l_1,m_1)H(A,B,C,D) = b^4(l_1m_1uv)^2. \tag{3.2.13}$$

From $a = c = 0$, we have $b \neq 0$. Because $f(x) = Ax^3 + Bx^2 + Cx + D$ has no linear factor over $\mathbb{Q}$, we have $A \neq 0$ and $D \neq 0$. In addition $q \neq 0$. So from (3.2.12), we have

$$m_1, l_1, u, v \neq 0.$$

Therefore

$$q, u, v, l_1, m_1 \neq 0. \tag{3.2.14}$$

From (3.2.13) and (3.2.14), we have

$$Z(l_1, m_1)H(A, B, C, D) \in (\mathbb{Q}^*)^2.$$

$\square$

On $E_2$, let $v_2(T) = (x_2, Y_2, z_2)$ be parameterized by

$$x_2^2 : Y_2 : z_2^2 = X(l_2, m_2) : Y(l_2, m_2) : Z(l_2, m_2),$$

where $l_2, m_2 \in \mathbb{Q}$.

On $E_3$, let $v_3(T) = (x_3, y_3, Z_3)$ be parameterized by

$$x_3^2 : y_3^2 : Z_3 = X(l_3, m_3) : Y(l_3, m_3) : Z(l_3, m_3),$$

where $l_3, m_2 \in \mathbb{Q}$.

From Lemma 3.2.4,

$$Z(l_1, m_1)H(A, B, C, D) \in (\mathbb{Q}^*)^2.$$

Hence $H(A, B, C, D) \in \mathbb{Q}^*$.

Similarly, we have

$$Z(l_2, m_2)H(A, B, C, D) \in (\mathbb{Q}^*)^2.$$

Therefore

$$Z(l_1, m_1)Z(l_2, m_2) \in (\mathbb{Q}^*)^2.$$

By symmetry, we have

$$X(l_2, m_2)X(l_3, m_3), \quad Y(l_1, m_1)Y(l_3, m_3) \in (\mathbb{Q}^*)^2.$$

Thus we have the following theorem

**Theorem 3.2.1.** *Let $(X(l_i, m_i) : Y(l_i, m_i) : Z(l_i, m_i))$ be a parameterization of $v_i(T)$ for $i = 1, 2, 3$ respectively. Then*

$$X(l_2, m_2)X(l_3, m_3),\ Y(l_1, m_1)Y(l_3, m_3), Z(l_1, m_1)Z(l_2, m_2) \in (\mathbb{Q}^*)^2.$$

**Remark 3.2.1.** *Bremner [3] proved Theorem 3.2.1 for the family of curves*

$$x^4 + y^4 = Dz^4.$$

*The approach in the paper is computational. The above proof of Theorem 3.2.1 takes a different approach and works for the general equation $F(x^2, y^2, z^2) = 0$.*

## 3.3 Some Applications

### 3.3.1 Equation $x^4 + y^4 = 4pz^4$

**Theorem 3.3.1.** *Let $p$ be an odd prime then the equation*

$$x^4 + y^4 = 4pz^4$$

*does not have solutions in any odd degree number field except $xyz = 0$.*

*Proof.* Consider the genus 3 curve

$$x^4 + y^4 = 4pz^4. \tag{3.3.1}$$

By Corollary 6.6, Coray [13], we only need to show (3.3.1) has no rational points or cubic points.

Because $p$ is an odd prime, (3.3.1) has no nontrivial rational points by considering mod 2. So we only need to show (3.3.1) has no cubic points.

We consider the curve

$$D_1 \colon x^2 + y^4 = 4pz^4.$$

Assume (3.3.1) has a non-trivial cubic point then $D_1$ has a non-trivial rational point. Let $(x_0, y_0, 1)$ be a rational point on the curve $D_1$. Then the corresponding elliptic curve is

$$E_1 \colon y^2 = x(x^2 + 16p). \tag{3.3.2}$$

Let $r$ be the rank of $E_1$ over $\mathbb{Q}$.

If $r \leq 1$, then by Theorem 4, Bremner [3], $C$ has no cubic points.

If $r \geq 2$, then by Proposition 6.2, Chapter X, Silverman [18], we have

$$r = 2 \text{ and } p \equiv 1 \mod 8.$$

A point on $x^2 + y^4 = 4pz^4$ gives a point on $u^2 + 1 = 4pv^4$. By Proposition 6.5, Chapter X, Silverman [18], we have

$$(\frac{2}{p})_4 = 1,$$

where $\left(\text{-}\right)_4$ denotes the bi-quadratic residue symbol.

Because $p \equiv 1 \mod 8$, there are A,B in $\mathbb{Z}^+$ such that

$$p = A^2 + B^2,$$

where $2 \nmid A$ and $2|B$.

In addition, because $(\frac{2}{p})_4 = 1$, from Proposition 6.6, Chap X, Silverman [18], we have

$$AB \equiv 0 \mod 8.$$

Therefore $8|B$.

Now, let $(x, y, z)$ be a non trivial rational point in $D_1$. We can assume that $x, y, z \in \mathbb{Z}^+$ and $\gcd(x, y, z) = 1$. We have

$$x^2 + y^4 = 4pz^4.$$

Thus $2|x, y$. Let $x = 2s$, $y = 2t$. Then

$$s^2 + 4t^4 = pz^4.$$

Because $4p = A^2 + B^2$, we have

$$(pz^2 + 2Bt^2)^2 = p(Bz^2 + 2t^2)^2 + A^2 s^2.$$

Thus

$$(pz^2 + 2Bt^2 + As)(pz^2 + 2Bt^2 - As) = p(Bz^2 + 2t^2)^2.$$

We need the following lemma

**Lemma 3.3.1.** *(Silverman [18]) With the above notations, we have the following cases*

*Case 1:*

$$\begin{cases} pz^2 + 2Bt^2 + As = pu^2, \\ pz^2 + 2Bt^2 - As = v^2, \end{cases}$$

*Case 2:*

$$\begin{cases} pz^2 + 2Bt^2 + As = u^2, \\ pz^2 + 2Bt^2 - As = pv^2, \end{cases}$$

*Case 3:*

$$\begin{cases} pz^2 + 2Bt^2 + As = 2pu^2, \\ pz^2 + 2Bt^2 - As = 2v^2, \end{cases}$$

*Case 4:*

$$\begin{cases} pz^2 + 2Bt^2 + As = 2u^2, \\ pz^2 + 2Bt^2 - As = 2pv^2. \end{cases}$$

*Proof.* In this section, we denote $v_q(x)$ the highest power of a prime number $q$ dividing an integer x.

We show that $\gcd(pz^2 + 2Bt^2 + As, pz^2 + 2Bt^2 - As)$ is either a square or 2 times a square.

Indeed, let $d = \gcd(pz^2 + 2Bt^2 + As, pz^2 + 2Bt^2 - As)$.

Let $n$ be the square-free part of $d$. We want to show that $n = 1$ or $n = 2$.

We have

$$\det \begin{pmatrix} p & 2B & A \\ p & 2B & -A \\ B & 2 & 0 \end{pmatrix} = 4A(p - B^2) = 4A^3.$$

Thus $d | 4A^3$. Hence $n | 4A^3$.

If $n > 1$, then let $q$ be a prime divisor of $n$. We want to show that $q = 2$.

Assume that $q > 2$, then from $n | 4A^3$, we have $q | A$.

Thus

$$s^2 = pz^4 - 4t^4 = (A^2 + B^2)z^4 - 4t^4 \equiv B^2 z^4 - 4t^4 \equiv 0 \mod q.$$

So $q | s$.

Let $v_q(d) = 2r + 1$, then $q^{2r+1} | Bz^2 + 2t^2$.

From

$$q^{2r+1} | pz^2 + 2Bt^2 + As = B^2 z^2 + 2Bt^2 + A^2 z^2 + As = B(Bz^2 + 2t^2) + A(Az^2 + s),$$

we have $q^{2r+1} | A(Az^2 + s)$. Because $q | s, q \nmid z$, we have $q^{2r+1} | A$.

If $v_q(Bz^2 + 2t^2) > 2r + 1$, then from $q | s, q^{2r+1} | A$, we have

$$q^{2r+2} | \gcd(pz^2 + 2Bt^2 + As, pz^2 + 2Bt^2 - As).$$

Thus $v_q(d) > 2r + 1$, a contradiction.

Therefore $v_q(Bz^2 + 2t^2) = 2r + 1$.

From $q > 2$, $\gcd(A, B) = 1$, $\gcd(s, z) = \gcd(s, t) = 1$ and $q | A, s$, we have $q \nmid Bz^2 + 2t^2$.

Therefore $q^{2r+1} || A^2 z^4 + (Bz^2 + 2t^2)(Bz^2 - 2t^2) = s^2$, which is a contradiction.

So $n = 1$ or $n = 2$. $\square$

Now if $4p = g^2 + h^2$, then the equation $X^2 + Y^2 = 4pZ^2$ has a parameterization

$$X : Y : Z = gl^2 - 2hlm - gm^2 : hl^2 + 2glm - hm^2 : l^2 + m^2.$$

Point $(x, y^2, z^2)$ in $X^2 + Y^2 = 4pZ^2$ is parameterized by a pair $(l, m)$ satisfying

$$l : m = gx + hy^2 + Dz^2 : -hx + gy^2 = -hx + gy^2 : -gx - hy^2 + Dz^2.$$

Let

$$\begin{cases} \alpha = gx + hy^2 + Dz^2, \\ \beta = -hx + gy^2, \\ \gamma = -gx - hy^2 + Dz^2. \end{cases}$$

Then

$$\alpha\gamma = \beta^2,$$

and

$$l : m = \alpha : \beta = \beta : \gamma.$$

Thus

$$\begin{aligned} l^2 + m^2 &\equiv \alpha^2 + \beta^2 \mod (\mathbb{Q}^*)^2 \\ &\equiv \alpha^2 + \alpha\gamma \mod (\mathbb{Q}^*)^2 \\ &\equiv \alpha(\alpha + \gamma) \mod (\mathbb{Q}^*)^2 \\ &\equiv \alpha(2Dz^2) \mod (\mathbb{Q}^*)^2 \\ &\equiv 2p\alpha \mod (\mathbb{Q}^*)^2. \end{aligned} \tag{3.3.3}$$

Now, we have $p = A^2 + B^2$, where $8|B$.

Let $g = 2A, h = 2B$, $x = 2s$ and $y = 2t$. Then

$$\alpha = gx + hy^2 + Dz^2 = 4(As + 2Bt^2 + pz^2).$$

Therefore

$$l^2 + m^2 \equiv 2p\alpha \equiv 2p(As + 2Bt^2 + pz^2) \mod (\mathbb{Q}^*)^2. \tag{3.3.4}$$

Now $s^2 + 4t^4 = pz^4$ and $\gcd(x, y, z) = 1$, $z$ and $s$ are odd.

Consider Case 1 in Lemma 3.3.1

$$\begin{cases} pz^2 + 2Bt^2 + As = pu^2, \\ pz^2 + 2Bt^2 - As = v^2. \end{cases}$$

Taking modulo 8, we have

$$\begin{cases} 1 + As \equiv u^2 \mod 8, \\ 1 - As \equiv v^2 \mod 8. \end{cases}$$

$A$ and $s$ are odd, thus $u, v$ are both even, thus $4|1 + As$ and $4|1 - AS$ which is impossible.

So Case 1 is impossible.

Similarly, Case 2 is impossible.

Case 3:

$$\begin{cases} pz^2 + 2Bt^2 + As = 2pu^2, \\ pz^2 + 2Bt^2 - As = 2v^2. \end{cases}$$

Then from (3.3.4)

$$l^2 + m^2 \equiv 2p(As + 2Bt^2 + pz^2) \equiv 4p^2u^2 \equiv 1 \mod (\mathbb{Q}^*)^2.$$

Case 4:

$$\begin{cases} pz^2 + 2Bt^2 + As = 2u^2, \\ pz^2 + 2Bt^2 - As = 2pv^2. \end{cases}$$

Then from (3.3.4),

$$l^2 + m^2 \equiv 2p(As + 2Bt^2 + pz^2) \equiv 4pu^2 \equiv p \mod (\mathbb{Q}^*)^2.$$

So for the curve $D_1\colon x^2 + y^4 = 4pz^4$, we have

$$l^2 + m^2 \equiv 1 \text{ or } p \mod (\mathbb{Q}^*)^2.$$

Now, we consider the curve

$$D_2\colon x^4 + y^2 = 4pz^4.$$

We still have

$$4p = g^2 + h^2,$$

where $g = 2A, h = 2B$, and

$$p = A^2 + B^2,$$

where $B \equiv 0 \mod 8$.

In this case, because $x = 2t, y = 2s$, we have

$$4t^4 + s^2 = pz^4.$$

Now the pair $(l, m)$ satisfies

$$l : m = gx^2 + hy + Dz^2 : -hx^2 + gy = -hx^2 + gy : -gx^2 - hy + Dz^2.$$

By symmetry to the curve $D_1$, we also have

$$l^2 + m^2 \equiv 2p(pz^2 + 2At^2 + Bs) \mod (\mathbb{Q}^*)^2.$$

A similar argument shows that

$$pz^2 + 2At^2 + Bs = pu^2 \text{ or } u^2.$$

Thus

$$l^2 + m^2 \equiv 2 \quad \text{or} \quad 2p \mod (\mathbb{Q}^*)^2.$$

Now, for the curve $D_1\colon x^2 + y^4 = 4pz^4$, we get a pair $(l_1, m_1)$ in which

$$l_1^2 + m_2^2 \equiv 1 \text{ or } p \mod (\mathbb{Q}^*)^2,$$

and for the curve $D_2\colon x^4+y^2=4pz^4$, we get a pair $(l_2,m_2)$ in which

$$l_2^2+m_2^2 \equiv 2 \text{ or } 2p \mod (\mathbb{Q}^*)^2.$$

Thus

$$(l_1^2+m_1^2)(l_2^2+m_2^2) \equiv 2 \text{ or } 2p \mod (\mathbb{Q}^*)^2,$$

hence $(l_1^2+m_1^2)(l_2^2+m_2^2)$ is not a square.

So (3.3.1) has no nontrivial points in any cubic extension of $\mathbb{Q}$. □

### *3.3.2 Equation $x^4+nx^2y^2+y^4=Dz^4$*

This section studies the equation

$$x^4+nx^2y^2+y^4=Dz^4.$$

Bremner [3] proved

**Theorem 3.3.2.** *Let $D$ be a fourth power free integer such that $D$ and $2D$ are not perfect squares. If the rank of the curve $x^2+y^4=Dz^4$ is at most one then the equation*

$$x^4+y^4=Dz^4$$

*does not have any point in any cubic extension of $\mathbb{Q}$.*

We prove the following theorem

**Theorem 3.3.3.** *Let $n,D$ be non-zero integers such that $D$ is fourth power free, $2-n,(2+n)D,(4-n^2)D,$ and $D$ are not perfect squares. Assume that the rank of the curve $x^2+nxy^2+y^4=Dz^4$ is at most one. Then the equation*

$$x^4+nx^2y^2+y^4=Dz^4 \tag{3.3.5}$$

*does not have any nontrivial solution in any odd degree extension of $\mathbb{Q}$ except $xyz=0$. In particular, the equation $x^4+nx^2y^2+y^4=Dz^4$ has no rational solutions except $x=y=z=0$.*

*Proof.* Consider the curve

$$C\colon x^4 + nx^2y^2 + y^4 = Dz^4.$$

By Corollary 6.6, Coray [13], if $C$ has a non-trivial point in an odd degree extension of $\mathbb{Q}$ then $C$ has a non trivial rational point or a cubic point. By Lemma 3.2.1, we only need to show that $C$ has no cubic points.

Because $n^2 - 4 \notin \mathbb{Z}^2$, the equation $X^2 + nXY + Y^2 = DZ^2$ has no rational solution $(X, Y, Z)$ with $XYZ = 0$ except $X = Y = Z = 0$; therefore the condition (3.2.1) is satisfied.

Assume that $C$ has a nontrivial cubic point. Then the curve

$$E_1\colon X^2 + nXy^2 + y^4 = Dz^4$$

has a nontrivial rational point. There are $g, h \in \mathbb{Q}^*$ such that $D = g^2 + ngh^2 + h^4$. The equation

$$X^2 + nXY + Y^2 = DZ^2 \tag{3.3.6}$$

has a parameterization

$$X : Y : Z = (g+nh^2)l^2 + 2h^2lm - gm^2 : -h^2l^2 + 2glm + (ng+h^2)m^2 : l^2 + nlm + m^2, \tag{3.3.7}$$

where

$$l : m = X + gZ : Y + h^2Z. \tag{3.3.8}$$

Let $A = 1 - \frac{n^2}{4}$ and $(a, b) = (g + \frac{n}{2}h^2, h)$.

**Lemma 3.3.2.** *The curve $C_1\colon X^2 + Ay^4 = Dz^4$ has the elliptic curve model*

$$E\colon v^2 = u(u^2 + 4AD)$$

*via the following maps* $\phi\colon C_1 \to E$ *with* $\phi(X, y, z) = (u, v)$*, where*

$$\begin{cases} u = \frac{2(Dz^2 - b^2y^2A + aX)}{(bz-y)^2}, \\ v = \frac{4(aDz^3 + DXz - b^3Xy - aby^3A)}{(bz-y)^3}, \end{cases}$$

*and* $\psi\colon E \to C_1$ *with* $\psi(u, v) = (X, y, z)$*, where*

$$\begin{cases} X = a^3u^3 - 12ab^2ADu^2 - 4a^3ADu + 8bAD(D + Ab^4)v - 16ab^2A^2D^2, \\ y = abv - 2uD + 4ADb^2, \\ z = -2Ab^3 + av - 4bAD. \end{cases}$$

*Proof.* By using Magma [1], we can check that $\phi$ and $\psi$ are inverses of each other and

$$\begin{cases} \phi(a, b, 1) = (0 : 1 : 0), \\ \phi(-a, b, 1) = (\frac{4ADb^2}{a^2}, \frac{-4AD(a^2+2Ab^4)b}{a^3}), \\ \phi(a, -b, 1) = (\frac{a^2}{b^2}, \frac{a(a^2+2Ab^4)}{b^3}), \\ \phi(-a, -b, 1) = (0, 0). \end{cases} \tag{3.3.9}$$

□

We need the following

**Lemma 3.3.3.** *Let* $d$ *be a non-zero integer such that* $d \neq 4$ *and* $-d$ *is not a rational square. Then the group of torsion points on* $y^2 = x(x^2 + d)$ *is* $\{(0, 0), (0, 1, 0)\}$*.*

*Proof.* Prop 6.1, Chapter X, Silverman [18]. □

Because $4AD \neq 4$ and $-4AD = (n^2 - 4)D$ is not a square, by Lemma 3.3.3, the torsion subgroup of $E$ is $\mathbb{Z}/2\mathbb{Z}$ and is generated by $(0, 0)$. So if the rank of $E_1$ is 0, then there are only finitely many points on $E_1$; thus there are only also many finitely many points on $C_1$ via the map

$$\begin{cases} \zeta\colon E_1 \to C_1, \\ \zeta(x,y,z) = (x + \frac{n}{2}y^2, y, z). \end{cases} \tag{3.3.10}$$

The only torsion points on $E$ are $(0,0)$ and $(0:1:0)$; therefore $C_1$ has only 2 rational points, but $C_1$ has at least 4 points $(\pm a, \pm b, 1)$. So if the rank of $E_1$ is 0, then $E_1$ has no rational points except $(0,0,0)$. Therefore $C$ has no point in any cubic extension of $\mathbb{Q}$.

Now consider the case when the rank of $E_1$ is 1. Then the ranks of both $C_1$ and $E$ are one.

Two curves

$$\begin{cases} E_1\colon x^2 + nxy^2 + y^4 = Dz^4, \\ E_2\colon x^4 + nx^2y + y^2 = Dz^4 \end{cases}$$

have rank 1.

A rational triplet $T$ on $C$ gives a pair $(v_1(T), v_2(T))$ on $E_1(\mathbb{Q}) \times E_2(\mathbb{Q})$.

By following Bremner [3], Cassels [11], we only need to find $T$ such that $v_i(T)$ is in the set of the coset reprentatives of $E_i(\mathbb{Q})/2E_i(\mathbb{Q})$ for $i = 1, 2$.

Point $\phi(-a, b, 1) = (\frac{4ADa^2}{b^2}, \frac{a(a^2+2Ab^4)}{b^3})$ is of infinite order because the only non-zero torsion point on $E$ is $(0,0)$. We also have $\psi(-a,b,1)$ is not divisible by 2 because if $\psi(-a,b,1) = 2(u_0, v_0)$ then

$$\frac{4ADb^2}{a^2} = \frac{(4AD - u_0)^2}{(2v_0)^2},$$

which is impossible because $AD = (1 - n^2/4)D$ is not a square. Therefore

$$E(\mathbb{Q}) = \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ and } E(\mathbb{Q})/2E(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z},$$

so the coset representatives of $E(\mathbb{Q})/2E(\mathbb{Q})$ are $(0:1:0)$ and $\psi(-a,b,1)$.

From (3.3.9) and (3.3.10), we have

$$\begin{cases} (\phi\circ\zeta)^{-1}(0,1,0) = \zeta^{-1}(\phi^{-1}(0,1,0)) = \zeta^{-1}(a,b,1) = (a-\frac{n}{2}b^2,b,1) = (g,h,1), \\ (\phi\circ\zeta)^{-1}(0,0,1) = \zeta^{-1}(\phi^{-1}(0,1,0)) = \zeta^{-1}(-a,b,1) = (a-\frac{n}{2}b^2,b,1) = (-g-nh^2,h,1). \end{cases}$$

So the pull backs of $(0:1:0)$ and $(0,0,1)$ on $E_1$ are $(g,h,1)$ and $(-g-nh^2,h,1)$. Thus we only need to find triplet $T$ such that

$$v_1(T) \in \{(g,h,1),(-g-nh^2,h,1)\}. \tag{3.3.11}$$

Similarly, on $E_2$ we only need to consider triplet $T$ such that

$$v_2(T) \in \{(b,a-\frac{n}{2}b^2,b,1),(b,-a-\frac{n}{2}b^2,1)\} = \{(h,g,1),(h,-g-nh^2,1)\}. \tag{3.3.12}$$

The point $(g,h,1)$ on $E_1$ corresponds to the point $(g:h^2:1)$ on $X^2+NXY+Y^2 = DZ^2$. From (3.3.8), $(g:h^2:1)$ is parameterized by

$$l_1 : m_1 = (g+g):(h^2+h^2) = g:h^2.$$

Similarly, point $(-g-nh^2,h,1)$ on $E_1$ corresponds to point $(-g-nh^2,h^2,1)$ on (3.3.6). From (3.3.8), $(-g-nh^2:h:1)$ is parameterized by

$$l_1 : m_1 = (-g-nh^2+g):(h^2+h^2) = -n:2.$$

Because

$$Z(g,h^2) = D \text{ and } Z(-n,2) = 4-n^2,$$

we have

$$Z(l_1,m_1) \mod (\mathbb{Q}^*)^2 \in \{D, 4-n^2\}. \tag{3.3.13}$$

Similarly, points $(h,g,1)$, and $(h,-g-nh^2,1)$ on $E_2$ correspond to points $(h^2,g,1)$ and $(h^2,-g-nh^2,1)$ on (3.3.6) which are parameterized by

$$l_2 : m_2 \in \{1:1,\ h^2+g : -g-(n-1)h^2\}.$$

Because

$$\begin{cases} Z(1,1) = n+2, \\ Z(h^2+g, -g-(n-1)h^2) = (2-n)(g^2+ngh^2+h^4) = (2-n)D, \end{cases},$$

we have

$$Z(l_2, m_2) \mod (\mathbb{Q}^*)^2 \in \{n+2, (2-n)D\}. \tag{3.3.14}$$

From (3.3.13) and (3.3.14), we have

$$Z(l_1, m_1)Z(l_2, m_2) \mod (\mathbb{Q}^*)^2 \in \{(n+2)D, 2-n, (n+2)(4-n^2), (2-n)(4-n^2)D\}.$$

Because $(n+2)(4-n^2) = (2-n)(2+n)^2$ and $(2-n)(4-n^2) = (2-n)^2(2+n)$, we have

$$Z(l_1, m_1)Z(l_2, m_2) \mod (\mathbb{Q}^*)^2 \in \{(n+2)D, 2-n\}.$$

By the assumption on $n, D$ then $(n+2)D$, $2-n$ are not perfect squares. Therefore, $Z(l_1, m_1)Z(l_2, m_2) \notin (\mathbb{Q}^*)^2$, which contradicts Theorem 3.2.1. □

Chapter 4

# THE HILBERT SYMBOL AND APPLICATIONS

## 4.1 Introduction

Let $p$ be a rational prime or the infinite prime and let $a, b \in \mathbb{Q}_p$. The Hilbert symbol $(a,b)_p$ is defined as $(a,b)_p = \begin{cases} 1 \text{ if } z^2 = ax^2 + by^2 \text{ has a non-zero solution } (x,y,z) \in \mathbb{Q}_p^3; \\ -1 \text{ if not.} \end{cases}$

**Theorem 4.1.1.** *For all $a, b$ and $c \in \mathbb{Q}_p$, we have the following*

1, $(a,b)_p(c,b)_p = (ac,b)_p$

2, $\prod_p (a,b)_p = 1$

3, $(a,-a)_p = 1$

4, *if $a = p^\alpha u$ and $b = p^\beta v$, where $p \nmid u, v$, then*

$$(a,b)_p = (-1)^{\alpha\beta\frac{p-1}{2}} (\frac{u}{p})^\beta (\frac{v}{p})^\alpha$$

*for $p > 2$, where $(\frac{-}{p})$ denotes the quadratic residue* $\mod p$*, and*

$$(a,b)_2 = (-1)^{\frac{u-1}{2}\frac{v-1}{2} + \alpha\frac{v^2-1}{8} + \beta\frac{u^2-1}{8}}$$

*for $p = 2$.*

*Proof.* See Chapter III, Serre [17]. □

We also need some knowledge about $p-$adic analysis. See Cassels [12]. In this chapter, we denote both $v_p(n)$ and $\text{ord}_p(n)$ the highest power of a prime $p$ dividing an integer n.

## 4.2 Equation $(x+y+z+w)(1/x+1/y+1/z+1/w)=n$

At the end of their paper Bremner, Guy and Nowakowski [4] conjectured that every positive integer $n>15$ can be presented in the form $(x+y+z+w)(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{w})$, where $x,y,z,w$ are positive integers. But using computer search, Macleod and Bremner did not find solutions in the case $n=4m^2$ or $n=4m^2+4$ when $m\not\equiv 2 \mod 4$. In this section, we will prove the following theorem

**Theorem 4.2.1.** *Let $n$ be a positive integer, $n=4m^2$ or $n=4m^2+4$ with $m\not\equiv 2$ mod 4. Then the equation*

$$n=(x+y+z+w)(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{w})$$

*does not have solutions $x,y,w,z\in\mathbb{Z}^+$.*

**Remark 4.2.1.** *If we allow one of $x,y,z,w$ to be negative then the equation*

$$n=(x+y+z+w)(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{w})$$

*always has a solution, for example:*

$$(w,x,y,z)=(-(n-1)t,\ t^2+t+1,\ (n-1)t(t+1),\ (t+1)(n-1)).$$

**Remark 4.2.2.** *In their paper Bremner and Macleod [7] proved that the equation*

$$n=\frac{x}{y+z}+\frac{y}{z+x}+\frac{z}{x+y}$$

*does not have positive integer solutions when $n$ is a positive odd integer. Michael Stoll [20] gave a different proof for this result using the Hilbert symbol. We will develop Michael Stoll's idea to prove Theorem 4.2.1.*

*The main idea is the following*

**Lemma 4.2.1.** *Let $X,D\in\mathbb{Q}$ such that $D<0$ and $(X,D)_p=1$ for all finite primes $p$. Then $X>0$.*

*Proof.* From Theorem 4.1.1, we have

$$(X, D)_\infty \prod_{p \text{ prime},\, p<\infty} (X, D)_p = 1.$$

Therefore $(X, D)_\infty = 1$. Thus the equation $Xu^2 + Dv^2 = w^2$ has nonzero solutions in $\mathbb{R}^3$. Because $D < 0$, we have $X > 0$.

□

First we need the following theorem

**Theorem 4.2.2.** *Let $n, y, z$ be positive integers such that $n = 4m^2$ or $n = 4m^2 + 4$ with $m \not\equiv 2 \mod 4$. Consider the curve*

$$E\colon Y^2 = X(X^2 + AX + B),$$

*where*

$$A = y^4 - 2ny^3z + (n^2 - 8n - 2)y^2z^2 - 2nyz^3 + z^4,$$
$$B = 16ny^3z^3(y + z)^2.$$

*Let $(X, Y) \in E(\mathbb{Q})$ with $Y \neq 0$. Then*

*(i)for all odd primes $p$*

$$(X, y^2 - (n - 2)yz + z^2)_p = 1,$$

*(ii)in addition,*

$$(X, y^2 - (n - 2)yz + z^2)_2 = 1$$

*in the following cases*

$$n = 4m^2, \quad 4|m \quad \textit{and} \quad 4 \nmid y + z,$$

$$n = 4m^2, \quad 2 \nmid m \quad \textit{and} \quad 4 \nmid y - z,$$

$$n = 4m^2 + 4, \quad 4|m \quad \textit{and} \quad 4 \nmid y - z,$$

$$n = 4m^2 + 4, \quad 2 \nmid m \quad \textit{and} \quad 4 \nmid y + z;$$

*furthermore, if* $y^2 - (n-2)yz + z^2 < 0$ *and* $(X, y^2 - (n-2)yz + z^2)_2 = 1$*, then*

$$X > 0.$$

*Proof.* Let

$$D = y^2 - (n-2)yz + z^2,$$
$$L = y^4 + z^4 - (2n+4)yz(y^2 + z^2) + (n^2 - 12n + 6)y^2z^2.$$

Then

$$A^2 - 4B = D^2L.$$

Let $(X, Y)$ be a rational point on

$$Y^2 = X(X^2 + AX + B) \tag{4.2.1}$$

with $Y \neq 0$.

**Lemma 4.2.2.** *If Theorem 4.2.2 is true when* $\gcd(y, z) = 1$*, then it is true when* $\gcd(y, z) > 1$.

*Proof.* Let $d = \gcd(y, z)$. Then $y = y_1 d, z = z_1 d$ with $\gcd(y_1, z_1) = 1$.
Let $Y_1 = \frac{Y}{d^6}$, $X_1 = \frac{X}{d^4}$. Then from (4.2.1), we have

$$Y_1^2 = X_1(X_1^2 + A_1X_1 + B_1),$$

where

$$\begin{aligned}A_1 =& y_1^4 + z_1^4 - 2ny_1z_1(y_1^2+z_1^2) + (n^2-8n-2)y_1^2z_1^2,\\ B_1 =& 16ny_1^3z_1^3(y_1+z_1)^2,\end{aligned}$$

Let $D_1 = y_1^2 - (n-2)y_1z_1 + z_1^2$. Then for every prime p, we have

$$(X, D)_p = (d^4X_1, d^2D_1)_p = (X_1, D_1)_p.$$

Therefore if $(X_1, D_1)_p = 1$ then $(X, D)_p = 1$.

□

Now we assume that $\gcd(y, z) = 1$.

(i)We want to show

$$(X, D)_p = 1 \quad \forall \text{ odd primes p.}$$

The equation

$$Bu^2 + Dv^2 = \theta^2$$

has a non-trivial solution $(u, v, \theta) = (1, 4yz(y+z), 4yz(y+z)^2)$; thus

$$(B, D)_p = 1 \quad \forall \text{ primes p.} \tag{4.2.2}$$

If $x \notin \mathbb{Z}_p$, then let $X = p^{-r}X_0$ with $p \nmid X_0, r > 0$.

From (4.2.1) we have

$$Y^2 = \frac{X_0(X_0^2 + p^rAX_0 + p^{2r}B)}{p^{3r}}.$$

Thus $r$ is even and

$$\square = X_0(X_0^2 + p^rAX_0 + p^{2r}B).$$

Here $\square$ means a square in the field we are working in. Taking $\mod p$, we have

$$\square \equiv X_0 \mod p.$$

Thus $X_0 \in \mathbb{Z}_p^2$. Therefore

$$(X, D)_p = (p^r X_0, D)_p = 1.$$

Now we consider the case $X \in \mathbb{Z}_p$.

**Lemma 4.2.3.** *Theorem 4.2.2 holds when $n = 4m^2$.*

*Proof.*

Case 1:

$$p \nmid X.$$

Case 1.1: $p \nmid D$, then $X, D$ are units in $\mathbb{Z}_p$. Thus $(X, D)_p = 1$.

Case 1.2: $p | D$, we have

$$X^2 + AX + B = (X + \frac{A}{2})^2 - \frac{LD^2}{4} \equiv (X + \frac{A}{2})^2 \mod p. \tag{4.2.3}$$

- $p | A$ then $p \nmid X + \frac{A}{2}$, thus from (4.2.3), we have $X^2 + AX + B \in \mathbb{Z}_p^2$; therefore

$$(X, D)_p = (X^2 + AX + B, D)_p = 1.$$

- $p \nmid A$.

If $p \nmid X + \frac{A}{2}$, then from (4.2.3), $X^2 + AX + B \in \mathbb{Z}_p^2$. Thus

$$(X, D)_p = (X^2 + AX + B, D)_p = 1.$$

If $p | X + \frac{A}{2}$, then from $p | D$, we have

$$y^2 + z^2 \equiv (n - 2)yz \mod p.$$

Thus

$$A = (y^2 + z^2)^2 - 2nyz(y^2 + z^2) + (n^2 - 8n - 4)y^2z^2$$
$$\equiv ((n-2)^2 - 2n(n-2) + (n^2 - 8n - 4))y^2z^2$$
$$\equiv -8ny^2z^2 \mod p.$$

$$\Rightarrow X \equiv -\frac{A}{2} \equiv 4ny^2z^2 \equiv (4myz)^2 \mod p.$$

$$\Rightarrow X \in \mathbb{Z}_p^2 \quad (\text{ because } p \nmid X \text{ }).$$

$$\Rightarrow (X, D)_p = 1.$$

Case 2:

$$p|X.$$

Case 2.1:

$$p \nmid yz(y+z).$$

The equation

$$(X^2 + AX + B)u^2 + Dv^2 = \theta^2$$

has a nontrivial solution $(1, 4yz(y+z), 4yz(y+z)^2) \mod p$, thus it has a nontrivial solution in $\mathbb{Q}_p$.

$$\Rightarrow (X^2 + AX + B, D)_p = 1.$$

$$\Rightarrow (X, D)_p = (X^2 + AX + B, D)_p = 1.$$

Case 2.2:

$$p|yz(y+z).$$

Case 2.2.1: $p|yz$.

Because $\gcd(y, z) = 1$, we have

$$D = y^2 + z^2 - (n-2)yz \equiv y^2 \quad \text{or } z^2 \not\equiv 0 \mod p.$$

Thus $D \in \mathbb{Z}_p^2$ and $(X, D)_p = 1$.

Case 2.2.2: $p \nmid yz$, then $p|y+z$. Therefore

$$D = y^2 + z^2 - (n-2)yz \equiv -nyz \equiv 4m^2y^2 \mod p. \tag{4.2.4}$$

We only need to consider $p|m$; otherwise $D \in \mathbb{Z}_p^2$ and hence $(X, D)_p = 1$.

Let $r = v_p(m)$, $s = v_p(y+z)$, $m = p^r m_1$, $y + z = p^s t$, where $r, s > 0$, $p \nmid m_1, t$.

♦ $r > s$, then

$$D = (y+z)^2 - nyz = p^{2s}(t^2 - 4p^{2r-2s}m_1^2 yz).$$

Because $p \nmid t$, we have $D \in \mathbb{Z}_p^2$. Thus $(X, D)_p = 1$.

♦ $r < s$, then

$$D = p^{2r}(p^{2s-2r}t^2 - 4m_1^2 yz) = p^{2r}D_1,$$

where

$$D_1 = p^{2s-2r}t^2 - 4m_1^2 yz \equiv 4m_1^2 y^2 \mod p.$$

Because $p \nmid m_1, y$, we have $D_1 \in \mathbb{Z}_p^2$. Thus

$$(X, D)_p = (X, p^{2r}D_1)_p = 1.$$

♦ $r = s$, then

$$B = 16ny^3z^3(y+z)^2 = 64p^{4r}m_1^2(yz)^3t^2$$

$$\Rightarrow v_p(B) = 4r.$$

$$
\begin{aligned}
A &= (y^2 - z^2)^2 - 8m^2yz(y^2+z^2) + (16m^4 - 32m^2)y^2z^2 \\
&= (y+z)^2(y-z)^2 - 8m^2yz(y+z)^2 + 16m^2(m^2-1)y^2z^2 \\
&= p^{2r}t^2(y-z)^2 - 8m_1^2yzt^2p^{4r} + 16m_1^2(p^{2r}m_1^2 - 1)p^2ry^2z^2 \\
&= p^{2r}(t^2(y-z)^2 - 8m_1^2yzt^2p^{2r} + 16m_1^2(p^{2r}m_1^2-1)y^2z^2) \\
&= p^{2r}A_1,
\end{aligned}
$$

where

$$
\begin{aligned}
A_1 &= t^2(y-z)^2 - 8m_1^2yzt^2p^{2r} + 16m_1^2(p^{2r}m_1^2-1)y^2z^2 \\
&\equiv t^2(y-z)^2 - 16m_1^2y^2z^2 \mod p.
\end{aligned}
\tag{4.2.5}
$$

Thus

$$v_p(A) \geq 2r.$$

Let $\alpha = v_p(X)$, $\beta = v_p(A)$, $B_0 = 64m_1^2(yz)^3t^2$. Then $A = p^\beta A_0$, $X = p^\alpha X_0$ with $\alpha > 0$, $\beta \geq 2r$, and $p \nmid X_0, A_0, B_0$.

We have

$$Y^2 = p^\alpha X_0(p^{2\alpha}X_0^2 + p^{\alpha+\beta}X_0A_0 + p^{4r}B_0). \tag{4.2.6}$$

If $\boxed{\alpha < 2r}$, then from (4.2.6), we have

$$Y^2 = p^{3\alpha}X_0(X_0^2 + p^{\beta-\alpha}A_0X_0 + p^{4r-2\alpha}B_0).$$

Because $\beta \geq 2r > \alpha$ and $4r - 2\alpha > 0$, we have $3\alpha = v_p(X(X^2 + AX + B))$. Thus $2|\alpha$. Therefore $\alpha \leq 2r - 2$.

Now we have

$$\square = X_0(X_0^2 + p^{\beta-\alpha}X_0A_0 + p^{4r-2\alpha}B_0). \tag{4.2.7}$$

Taking $\mod p$, we have $X_0^3 \equiv \square \mod p$. Thus $X_0 \in \mathbb{Z}_p^2$, hence $X = p^\alpha X_0 \in \mathbb{Z}_p^2$. Therefore $(X, D)_p = 1$.

If $\boxed{\alpha = 2r}$, then $v_p(X) = 2r$.

We have $D = p^{2r}(t^2 - 4m_1^2yz) = p^{2r}D_1$.

• If $p \nmid D_1$, then $v_p(D) = 2r = v_p(X)$. Because $X_0, D_1$ are units in $\mathbb{Z}_p$, we have

$$(X, D)_p = (p^{2r}X_0, p^{2r}D_1)_p = (X_0, D_1)_p = 1.$$

• If $p|D_1$, then because $z \equiv -y \mod p$, we have

$$t^2 \equiv 4m_1^2yz \equiv -4m_1^2y^2 \mod p. \tag{4.2.8}$$

From (4.2.5), we have

$$\begin{aligned} A_1 &\equiv t^2(y-z)^2 - 16m_1^2y^2z^2 \equiv 4t^2y^2 - 16m_1^2y^4 \\ &\equiv -32m_1^2y^4 \mod p. \end{aligned} \tag{4.2.9}$$

Because $p \nmid y$ and $p \nmid m_1$, we have $p \nmid A_1$. Thus $A_0 = A_1$, so $\beta = v_p(A) = 2r$.

From (4.2.6), we have

$$\square = X_0(X_0^2 + X_0A_0 + B_0).$$

$\diamond$ $p \nmid X_0 + \frac{A_0}{2}$. We have

$$p^{4r}D_1^2L = D^2L = A^2 - 4B = p^{4r}(A_0^2 - 4B_0).$$

Thus

$$D_1^2L = A_0^2 - 4B_0.$$

Therefore

$$p|A_0^2 - 4B_0.$$

Thus

$$X_0^2 + A_0X_0 + B_0 \equiv (X_0 + \frac{A_0}{2})^2 \mod p.$$

Because $p \nmid X_0 + \frac{A_0}{2}$, we have $X_0^2 + A_0X_0 + B_0 \in \mathbb{Z}_p^2$. Hence $X_0 \in \mathbb{Z}_p^2$

$$\Rightarrow (X, D)_p = (p^{2r}X_0, D)_p = 1.$$

$\diamond$ $p|X_0 + \frac{A_0}{2}$, then $X_0 \equiv -\frac{A_0}{2} \mod p$.

Because $A_0 = A_1$, from (4.2.9), we have

$$X_0 \equiv -\frac{A_1}{2} \equiv \frac{-32m_1^2y^4}{2} \equiv 16m_1^2y^4 \mod p.$$

Thus $X_0 \in \mathbb{Z}_p^2$. Therefore $(X, D)_p = (p^{2r}X_0, D)_p = 1$.

$\boxed{\alpha > 2r}$, then from (4.2.6), we have

$$Y^2 = p^{4r+\alpha}X_0(p^{2\alpha-4r}X_0^2 + p^{\alpha+\beta-4r}A_0X_0 + B_0).$$

Because $2\alpha - 4r > 0$ and $\alpha + \beta - 4r > 0$, we have $4r + \alpha = v_p(X(X^2 + AX + B))$. Therefore $2|\alpha$, hence $\alpha \geq 2r + 2$. So $X_0B_0 \equiv \square \mod p$. Now

$$\square = X_0(p^{2\alpha-4r}X_0^2 + p^{\alpha+\beta-4r}A_0X_0 + B_0).$$

Therefore $X_0B_0 \in \mathbb{Q}_p^2$. Thus

$$(XB, D)_p = (p^{\alpha+4r}X_0B_0, D)_p = 1.$$

From (4.2.2), we have $(B, D)_p = 1$. So $(X, D)_p = 1$. $\square$

**Lemma 4.2.4.** *Theorem 4.2.2 is true when $n = 4m^2 + 4$.*

*Proof.*

**Case 1:**

$$p \nmid X.$$

If $p \nmid D$, then $X, D$ are both units in $\mathbb{Z}_p$, thus $(X, D)_p = 1$. We only need to consider $p|D$.

$\blacklozenge$ $p \nmid X + \frac{A}{2}$, then

$$X^2 + AX + B = (X + \frac{A}{2})^2 - \frac{LD^2}{4} \equiv (X + \frac{A}{2})^2 \mod p.$$

Thus $X^2 + AX + B \in \mathbb{Q}_p^2$, therefore $(X, D)_p = (X^2 + AX + B, D)_p = 1$.

♦ $p | X + \frac{A}{2}$, then $p \nmid A$. Because $p | LD^2 = A^2 - 4B$ and $p | A$, we have $p \nmid B = 16ny^3z^2(y+z)^2$. So $p \nmid yz$.

From $p | D$, we have $y^2 + z^2 \equiv (n-2)yz \mod p$. Thus

$$\begin{aligned} A &= (y^2+z^2)^2 - 2nyz(y^2+z^2) + (n^2-8n-4)y^2z^2 \\ &\equiv ((n-2)^2 - 2n(n-2) + (n^2-8n-4))y^2z^2 \\ &\equiv -8ny^2z^2 \mod p. \end{aligned}$$

Therefore

$$X \equiv -\frac{A}{2} \equiv -\frac{-8ny^2z^2}{2} = 4ny^2z^2 \mod p.$$

Because $p \nmid A$, we have $p \nmid nyz$.

• $p \nmid 2m$.

Because $p \nmid yz$, $p | D = (y-z)^2 - 4m^2yz$, we have $p \nmid y - z$. Thus

$$yz \equiv (\frac{y-z}{2m})^2 \equiv \square \mod p.$$

Furthermore, because

$$(y+z)^2 \equiv nyz \not\equiv 0 \mod p,$$

we have

$$n \equiv \square \mod p.$$

Therefore

$$X \equiv 4ny^2z^2 \equiv \square \mod p.$$

So $X \in \mathbb{Q}_p^2$. Thus $(X, D)_p = 1$.

• $p|2m$, then $n = 4m^2 + 4 \equiv 4 \mod p$, thus

$$X \equiv 4ny^2z^2 \equiv (4yz)^2 \mod p$$

So $X$ is a p-adic square, and $(X, D)_p = 1$.

**Case 2**

$$p|X.$$

**Case 2.1**

$$p \nmid yz(y+z).$$

The equation

$$(X^2 + AX + B)u^2 + Dv^2 = \theta^2$$

has a nontrivial solution $(1, 4yz(y+z), 4yz(y+z)^2) \mod p$, thus it has a nontrivial solution in $\mathbb{Q}_p$. Therefore $(X^2 + AX + B, D)_p = 1$.

Because $(X, D)_p = (X^2 + AX + B, D)_p$, we have $(X, D)_p = 1$.

**Case 2.2**

$$p|yz(y+z).$$

♦ $p|yz$, then $p|y$ and $p \nmid z$, or $p|z$ and $p \nmid y$.

Then

$$D = y^2 + z^2 - (n-2)yz \equiv \square \not\equiv 0 \mod p$$

Therefore $D \in \mathbb{Z}_p^2$. Hence $(X, D)_p = 1$.

♦ $p \nmid yz$, then $p|y+z$.

**Case 2.2.1:** $p \nmid D$.

Because $y \equiv -z \mod p$, we have

$$D = (y+z)^2 - nyz \equiv ny^2 \mod p.$$

Thus $p \nmid n$. We have

$$\begin{aligned} A &= y^4 + z^4 - 2yz(y^2+z^2) + (n^2-8n-2)y^2z^2 \\ &\equiv 2y^4 + 4ny^4 + (n^2-8n-2)y^4 \mod p \\ &\equiv n(n-4)y^4 \equiv n(4m^2y^4) \mod p. \end{aligned} \tag{4.2.10}$$

♦ $p|m$,then $n = 4m^2 + 4 \equiv 4 \mod p$. Thus

$$D \equiv ny^2 \equiv 4y^2 \mod p.$$

Therefore $D \in \mathbb{Q}_p^2$ and $(X, D)_p = 1$.

♦ $p \nmid m$, then from (4.2.10) we have $p \nmid A$.

Let $y + z = p^\alpha t$ with $p \nmid t$. Then

$$B = 16ny^3z^3(y+z)^2 = p^{2\alpha}B_0,$$

where $p \nmid B_0$.

Let $X = p^s X_0$ with $p \nmid X_0$. Then

$$Y^2 = p^s X_0(p^{2s}X_0^2 + p^s X_0 A + p^{2\alpha}B_0).$$

- $s < 2\alpha$, then $2s = v_p(X(X^2 + AX + B))$, and we have

$$\square = X_0(p^s X_0^2 + X_0 A + p^{2\alpha - s}).$$

Therefore $X_o^2 A \equiv \square \mod p$. Thus

$$A \equiv \square \mod p. \tag{4.2.11}$$

From (4.2.10) and (4.2.11), we have

$$n \equiv \square \mod p.$$

Therefore

$$D \equiv ny^2 \equiv \square \mod p.$$

Hence $D \in \mathbb{Z}_p^2$, and $(X, D)_p = 1$.

• $s > 2\alpha$, then $s + 2\alpha = v_p(X(X^2 + AX + B))$. Thus $s$ is even.

So

$$v_p(X) \equiv v_p(D) \equiv 0 \mod 2.$$

Therefore

$$(X, D)_p = 1.$$

• $s = 2\alpha$, then because $X_0, D$ are units in $\mathbb{Z}_p$, we have

$$(X, D)_p = (p^{2\alpha} X_0, D)_p = (X_0, D)_p = 1.$$

**Case 2.2.2:** $p|D$.

Because $p \nmid yz$, $p|D = (y+z)^2 - nyz$. By the assumption, $p|n$ and $p|y+z$.

Let $y + z = p^u s$ and $n = 4p^v t$, where $p \nmid s, t$. Then

$$D = p^{2u}s^2 - 4p^v tyz. \tag{4.2.12}$$

If $v > 2u$, then $D = p^{2u}(s^2 - 4p^{v-2u}tyz)$. Because $p \nmid s^2 - 4p^{v-2u}tyz$, $D \in \mathbb{Q}_p^2$. Therefore $(X, D)_p = 1$. So we only need to consider the case $v \leq 2u$.

$$\boxed{v < 2u}$$

Then

$$D = p^v(p^{2u-v}s^2 - 4tyz) = p^v D_0,$$

where

$$D_0 = p^{2u-v}s^2 - 4tyz \equiv -4tyz \equiv 4ty^2 \not\equiv 0 \mod p. \tag{4.2.13}$$

We have

$$\begin{aligned} A &= (y+z)^2(y-z)^2 - 2nyz(y+z)^2 + n(n-4)(yz)^2 \\ &= (y-z)^2 p^{2u}s^2 - 8p^v t.p^{2u}s^2 yz + 16(tp^v-1)p^v t(yz)^2 \\ &= p^v((y-z)^2 p^{2u-v}s^2 - 8tp^{2u}s^2 yz + 16(tp^v-1)(yz)^2). \end{aligned}$$

Thus $A = p^v A_0$, where

$$\begin{aligned} A_0 &= (y-z)^2 p^{2u-v}s^2 - 8tp^{2u}s^2 yz + 16t(tp^v-1)(yz)^2 \\ &\equiv -16t(yz)^2 \mod p. \end{aligned} \tag{4.2.14}$$

We also have

$$B = 16n(yz)^3(y+z)^2 = 64p^{u+2v}t(yz)^3 s^2 = p^{u+2v}B_0 \text{ with } p \nmid B_0 = 64t(yz)^3 s^2.$$

Let $X = p^\alpha X_0$ with $p \nmid X_0$.

Then

$$Y^2 = p^\alpha X_0(p^{2\alpha}X_0^2 + p^{\alpha+v}A_0 X_0 + p^{2u+v}B_0). \tag{4.2.15}$$

•If $\alpha < v$, then $3\alpha = v_p(X(X^2+AX+B))$. Thus $2|\alpha$ and

$$\square = X_0(X_0^2 + p^{v-\alpha}A_0 X_0 + p^{2u+v-2\alpha}).$$

Therefore $X_0 \equiv \square \mod p$. Thus $X_0 \in \mathbb{Z}_p^2$. $\alpha$ is even, so

$$(X, D)_p = (p^\alpha X_0, D)_p = 1.$$

• If $\alpha = v$, then

$$Y^2 = p^{3v}X_0(X_0^2 + A_0 X_0 + p^{2u-v}). \tag{4.2.16}$$

If $\alpha$ is even then $v$ is even. Because $X_0, D_0$ are units in $\mathbb{Z}_p^2$, we have

$$(X, D)_p = (p^\alpha X_0, p^v D_0) = 1.$$

If $\alpha$ is odd, then $3v$ is odd. Because $2u - v > 0$, from (4.2.16), we have

$$p | X_0^2 + A_0 X_0.$$

Therefore

$$X_0 \equiv -A_0 \mod p. \tag{4.2.17}$$

From (4.2.13), (4.2.14), (4.2.17), we have

$$X_0 D_0 \equiv 64 t^2 (yz)^2 y^2 \mod p.$$

Therefore

$$(X, D)_p = (p^\alpha X_0, p^v D_0)_p = (-1)^\alpha (-1)^v (\frac{X_0}{p})^v (\frac{D_0}{p})^\alpha = (-1)^{2\alpha} (\frac{X_0 D_0}{p})^v = 1.$$

•If $v < \alpha < 2u$, then $2\alpha, v + 2u > \alpha + v$. From (4.2.15), we have $v_p(X(X^2 + AX + B)) = 2\alpha + v$. Thus $2|v$. We now have

$$\square = X_0(p^{\alpha - v} X_0^2 + A_0 X_0 + p^{2u-\alpha} B_0).$$

Taking $\mod p$, we have

$$\square \equiv A_0 \mod p.$$

From (4.2.14), $A_0 \equiv -16t(yz)^2 \mod p$, thus

$$-t \equiv \square \mod p.$$

Because $p | m^2 + 1$, we have $-1 \equiv \square \mod p$. Therefore

$$D_0 \equiv -4ty^2 \equiv \square \mod p.$$

Thus $D_0 \in \mathbb{Z}_p^2$. $2|v$, so $D = p^v D_0 \in \mathbb{Q}_p^2$. Hence $(X, D)_p = 1$.

•If $\alpha = 2u$, then

$$Y^2 = p^{4u+v}(p^{2u-v} X_0^2 + A_0 X_0 + B_0).$$

$\diamond$ $p \nmid A_0X_0 + B_0$, then $4u + v = v_2(X(X^2 + AX + B))$. Thus $v$ is even.

$$\Rightarrow v_p(X) \equiv v_p(D) \equiv 0 \mod 2$$

$$\Rightarrow (X, D)_p = 1.$$

$\diamond$ $p|A_0X_0 + B_0$. Because

$$A_0 \equiv -16t(yz)^2 \mod p,$$

$$B_0 \equiv 64t(yz)^3s^2 \mod p,$$

we have

$$64t(yz)^3s^2 - 16t(yz)^2X_0 \equiv 0 \mod p.$$

Therefore

$$X_0 \equiv 4yzs^2 \equiv -4y^2s^2 \equiv 4m^2y^2s^2 \mod p \quad (\text{ because } p|m^2+1 \text{ }).$$

Thus $X_0 \in \mathbb{Z}_p^2$, so $X = p^{2u}X_0 \in \mathbb{Q}_p^2$. Therefore $(X, D)_p = 1$.

• If $\alpha > 2u$, then $2\alpha > \alpha + v > 2u + v$. We have

$$Y^2 = p^{\alpha+v+2u}X_0(p^{2\alpha-v-2u}X_0^2 + p^{\alpha-2u}A_0X_0 + B_0).$$

Thus $2|\alpha + v$.

If $v$ is even, then $\alpha$ is even. Thus

$$(X, D)_p = (p^\alpha X_0, p^v D_0)_p = (X_0, D_0)_p = 1.$$

If $v$ is odd, then $\alpha$ is odd. We have

$$\square = X_0(p^{2\alpha-v-2u}X_0^2 + p^{\alpha-2u}A_0X_0 + B_0).$$

Taking $\mod p$, we have $X_0B_0 \equiv \square \mod p$, thus $(X_0B_0, D)_p = 1$.

We have $XB = p^{\alpha+v+2u}X_0B_0$ and $2|\alpha + v$, thus $(BX, D)_p = 1$.

From (4.2.2), we have $(B,D)_p = 1$. Therefore $(X,D)_p = 1$.

If

$$\boxed{v = 2u},$$

then

$$D = p^{2u}(s^2 - 4tyz) = p^{2u} D_0,$$

where

$$D_0 = s^2 - 4tyz.$$

We have

$$\begin{aligned} A &= (y-z)^2(y+z)^2 - 2nyz(y+z)^2 + n(n-4)(yz)^2 \\ &= p^{2u}((y-z)^2 s^2 - 8tp^{2u}yz + 16tm^2(yz)^2). \end{aligned}$$

Thus $A = p^{2u} A_0$, where

$$\begin{aligned} A_0 &\equiv (y-z)^2 s^2 - 16ty^4 \mod p \\ &\equiv 4y^2(s^2 - 4ty^4) \mod p \end{aligned} \tag{4.2.18}$$

(because $z \equiv -y \mod p$ and $m^2 \equiv -1 \mod p$).

We also have

$$B = p^{4u} B_0,$$

where $B_0 = 64m_1(yz)^3 s^2$, $p \nmid B_0$.

Let $X = p^{\alpha} X_0$, $p \nmid X_0$. Then

$$Y^2 = p^{\alpha} X_0 (p^{2\alpha} X_0^2 + p^{\alpha+2u} A_0 X_0 + p^{4u} B_0). \tag{4.2.19}$$

If $\alpha < 2u$, then $v_p(X(X^2 + AX + B)) = 3\alpha$. Thus $2|\alpha$. We have

$$\square = X_0(X_0^2 + p^{2u-\alpha} A_0 X_0 + p^{4u-\alpha} B_0).$$

Taking $\mod p$, we have $X_0 \equiv \square \mod p$, thus $X_0 \in \mathbb{Z}_p^2$. Thus $X \in \mathbb{Q}_p^2$. Hence

$$(X,D)_p = 1.$$

If $\alpha = 2u$, then from (4.2.19), we have

$$\square = X_0(X_0^2 + A_0X_0 + B_0).$$

$\Diamond$ $p \nmid D_0 = s^2 - 4tyz$, then $v_p(D) = v_p(X) = 2u$. Thus

$$(X, D)_p = (p^{2u}X_0, p^{2u}D_0)_p = 1.$$

$\Diamond$ $p|D_0$, then

$$s^2 \equiv 4tyz \mod p.$$

We have

$$p^{4u}(A_0^2 - 4B_0) = A^2 - 4B = D^2L = p^{4u}D_0^2L.$$

Thus

$$A_0^2 - 4B_0 \equiv 0 \mod p.$$

Therefore

$$X_0^2 + A_0X_0 + B_0 \equiv (X_0 + \frac{A_0}{2})^2 \mod p.$$

If $p \nmid X_0 + \frac{A_0}{2}$, then $p \nmid X_0^2 + A_0X_0 + B_0$. Thus $X_0^2 + A_0X_0 + B_0 \in \mathbb{Z}_p^2$, hence $X_0 \in Z_p^2$. Thus $(X_0, D)_p = 1$, so $(X, D)_p = 1$.

If $p|X_0 + \frac{A_0}{2}$, then

$$X_0 \equiv -\frac{A_0}{2} \mod p.$$

We have $z \equiv -y \mod p$, so

$$s^2 \equiv 4tyz \equiv -4ty^2 \mod p.$$

Thus from (4.2.18), we have

$$A_0 \equiv (y - z)^2 s^2 - 16ty^4 \equiv -32ty^4 \mod p.$$

Therefore

$$\begin{aligned} X_0 &\equiv -\frac{A_0}{2} \\ &\equiv 16ty^4 \equiv -4(4ty^2)y^2 \mod p \\ &\equiv -4s^2y^2 \equiv 4m^2s^2t^2 \mod p \end{aligned}$$

(because $ty^2 \equiv s^2 \mod p$ and $-1 \equiv m^2 \mod p$).

Thus $X_0 \in \mathbb{Z}_p^2$. So $(X, D)_p = (p^{2u}X_0, D)_p = 1$.

If $\alpha > 2u$, then $2\alpha > \alpha + 2u > 4u$.

From (4.2.19), we have $4u + \alpha = v_p(X(X^2 + AX + B))$, thus $\alpha$ is even and

$$\square = X_0(p^{2\alpha-4u}X_0^2 + p^{\alpha-2u}A_1X_0 + B_0).$$

Taking $\mod p$, we have

$$X_0B_0 \equiv \square \mod p.$$

Thus $X_0B_0 \in Z_p^2$. Hence $XB = p^{\alpha+4u}X_0B_0 \in \mathbb{Q}_p^2$, thus $(XB, D)_p = 1$. From (4.2.2) we have $(B, D)_p = 1$, therefore $(X, D)_p = 1$.

(ii)

First we show that $(X, D)_2 = 1$ in each case.

**Case 1:**

$$n = 4m^2, \quad 4|m \quad \text{and} \quad 4 \nmid y + z.$$

We have

$$D = (y + z)^2 - 4m^2yz.$$

If $2 \nmid y + z$, then $D \equiv 1 \mod 8$.

If $2|y + z$ and $4 \nmid y + z$, then $D = 4(1 \mod 8)$.

Thus $D \in \mathbb{Q}_2^2$ and hence $(X, D)_2 = 1$.

**Case 2:**

$$n = 4m^2, \quad 2 \nmid m \text{ and } \quad 4 \nmid y - z.$$

We have

$$D = (y - z)^2 - 4(m^2 - 1)yz.$$

If $2 \nmid y - z$, then $D \equiv 1 \mod 8$.

If $2|y - z$, then $D = 4(1 \mod 8)$.

Thus $D \in \mathbb{Q}_2^2$ and hence $(X, D)_2 = 1$.

**Case 3:**

$$n = 4m^2 + 4, \quad 4|m \quad \text{and} \quad 4 \nmid y - z.$$

We have

$$D = (y - z)^2 - 4m^2yz.$$

If $2 \nmid y - z$, then $D \equiv 1 \mod 8$.

If $2|y - z$, then $D = 4(1 \mod 8)$.

Thus $D \in \mathbb{Z}_2^2$, and hence $(X, D)_2 = 1$.

**Case 4:**

$$n = 4m^2 + 4, \quad 2 \nmid m \quad \text{and} \quad 4 \nmid y + z.$$

We have

$$D = (y + z)^2 - 4(m^2 + 1)yz.$$

If $2 \nmid y + z$, then because $2|m^2 + 1$, $D \equiv 1 \mod 8$.

If $2|y + z$ and $4 \nmid y + z$, then we have 2 subcases:

**Case 4.1:** $y, z$ are odd.

Because $4 \nmid y + z$, we have $y \equiv z \mod 4$. Thus $yz \equiv 1 \mod 4$, thus

$$D = 4D_0, \quad \text{where} \quad D_0 \equiv -1 \mod 8.$$

Let $m^2+1=2m_1$, $y+z=2t$, $2\nmid m_1, t$. Then

$$B=64(m^2+1)(yz)^3(y+z)^2=2^9B_0,$$

where $B_0=m_1(yz)^3t^2$.

We have

$$\begin{aligned}A&=(y^2-z^2)^2-2nyz(y+z)^2+n(n-4)(yz)^2\\&=(y-z)^2(y+z)^2-8(m^2+1)(y+z)^2+16(m^2+1)(m^2)(yz)^2.\end{aligned}$$

Let $y-z=4s$. Then

$$\begin{aligned}A&=(4s)^2(2t)^2-8(2m_1)(2t)^2+16(2m_1)(m^2)(yz)^2\\&=2^5(2s^2t^2-2m_1t^2+m_1m^2(yz)^2)\\&=2^5A_0,\end{aligned}\tag{4.2.20}$$

where

$$A_0=2s^2t^2-2m_1t^2+m_1m^2(yz)^2.$$

Let $X=2^kX_0$ with $2\nmid X_0$.

If $k<0$, then we have

$$Y^2=\frac{X_0(X_0^2+2^{5-k}X_0A_0+2^{9-2k}B_0}{2^{-3k}}.$$

Thus $2v_2(Y)=-3k\Rightarrow 2|k$, and

$$\square=X_0(X_0^2+2^{5-k}X_0A_0+2^{9-2k}B_0).$$

Taking $\mod 8$, we have

$$X_0\equiv\square \mod 8$$

$$\Rightarrow X=2^kX_0\in\mathbb{Q}_2^2$$

$$\Rightarrow (X,D)_2=1.$$

We now assume that $k \geq 0$.

We have

$$Y^2 = 2^k X_0(2^{2k} X_0^2 + 2^{5+k} A_0 X_0 + 2^9 B_0). \tag{4.2.21}$$

• $k < 4$, then from (4.2.21), we have $3k = v_2(X(X^2 + AX + B))$, so $2|k$. Thus $k \leq 2$. Now

$$\square = X_0(X_0^2 + 2^{5-k} A_0 + 2^{9-2k} B_0).$$

Because $k \leq 2$, taking $\mod 8$, we have

$$\square = X_0 \mod 8.$$

Thus $X_0 \in \mathbb{Z}_2^2$, hence $X = 2^k X_0 \in \mathbb{Q}_2^2$, therefore $\Rightarrow (X, D)_2 = 1$.

•If $k = 4$, then

$$\square = X_0(X_0^2 + 2A_0 X_0 + 2B_0)$$

Taking $\mod 4$, we have

$$1 \equiv X_0 + 2A_0 + 2X_0 B_0 \mod 4.$$

Because $A_0 + X_0 B_0 \equiv 0 \mod 2$, we have

$$1 \equiv X_0 \mod 4.$$

So $X = 2^4 X_0$ and $D = 2^2 D_0$, where $X_0 \equiv 1 \mod 4$ and $D_o \equiv -1 \mod 8$. Thus

$$(X, D)_2 = (2^4 X_0, 2^2 D_0)_2 = 2^{\frac{X_0-1}{2}\frac{D_0-1}{2} + 4\frac{D_0^2-1}{8} + 2\frac{X_0^2-1}{8}} = 1.$$

•If $k \geq 5$, then $9 + k = v_2(X(X^2 + AX + B))$. Thus $2 \nmid k$.

We have

$$\square = X_0(2^{2k-9} X_0^2 + 2^{k-4} A_0 + B_0). \tag{4.2.22}$$

•If $k = 5$, then

$$\square = X_0(2X_0^2 + 2A_0X_0 + B_0).$$

Taking $\mod 4$, we have

$$1 \equiv X_0B_0 + 2X_0 + 2A_0 \mod 4.$$

Because $X_0 + A_0 \equiv 0 \mod 2$, we have

$$X_0B_0 \equiv 1 \mod 4.$$

Because $D_0 \equiv -1 \mod 8$, we have

$$(X_0B_0, D_0)_2 = (-1)^{\frac{X_0-1}{2}\frac{D_0-1}{2}} = 1$$

$$\Rightarrow (4X_0B_0, D_0)_2 = 1. \tag{4.2.23}$$

On the other hand

$$1 = (B, D)_2 = (2^9B_0, 2^2D_0)_2 = (2B_0, D_0)_2,$$

thus

$$(2B_0, D_0)_2 = 1. \tag{4.2.24}$$

From (4.2.23) and (4.2.24), we have

$$(2X_0, D_0)_2 = 1.$$

Therefore

$$(X, D)_2 = (2^5X_0, 2^2D_0)_2 = 1.$$

• If $k > 5$, then because $2 \nmid k$, we have $k \geq 7$. Taking $\mod 8$ in (4.2.22) gives

$$1 \equiv X_0B_0 \mod 8.$$

Thus $X_0B_0 \in \mathbb{Z}_2^2$. Hence $XB = 2^{9+k}X_0B_0 \in \mathbb{Q}_2^2$. Thus $(XB, D)_2 = 1$. Further, $(B, D)_p = 1$ for all primes $p$, we have $(B, D)_2 = 1$. So $(X, D)_2 = 1$.

When $D < 0$, from Lemma 4.2.1, we have $X > 0$. $\square$

□

Now we will prove our Theorem 4.2.1.

*Proof.* Assume $(x, y, z, w)$ is a positive integer solution to

$$n = (x + y + z + w)(\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{w}) \tag{4.2.25}$$

with $\gcd(x, y, z, w) = 1$.

**Lemma 4.2.5.** *$(n - 2)yz - y^2 - z^2 > 0$.*

*Proof.* Using the Cauchy-Schwarz inequality (see Sedrakyan and Sedrakyan [16]), we have

$$n \geq (\sqrt{\frac{x}{x}} + \sqrt{\frac{w}{w}} + \sqrt{\frac{y}{z}} + \sqrt{\frac{z}{y}})^2 = (2 + \frac{y+z}{\sqrt{yz}})^2$$
$$\Rightarrow (\sqrt{n} - 2)\sqrt{yz} \geq y + z$$
$$\Rightarrow (n - 4\sqrt{n} + 2)yz \geq y^2 + z^2$$
$$\Rightarrow (n - 2)yz > (n - 4\sqrt{n} + 2)yz \geq y^2 + z^2$$
$$\Rightarrow (n - 2)yz - y^2 - z^2 > 0.$$

□

Write (4.2.25) as

$$(y+z)(x+w)xw+yz(x^2+w^2)+(y^2-(n-4)yz+z^2)xw+yz(y+z)(x+w) = 0. \tag{4.2.26}$$

Regarding (4.2.26) as an affine curve in $x, w$ over $\mathbb{Q}(y, z)$. Then (4.2.26) has a projective model $(x : w : d)$

$$C\colon (y+z)(x+w)xw+yz(x^2+w^2)d+(y^2-(n-4)yz+z^2)xwd+yz(y+z)(x+w)d^2 = 0.$$

**Lemma 4.2.6.** *$C$ is birationally isomorphic to the curve*

$$F\colon V^2T = U^3 + AU^2T + BUT^2,$$

*where*

$$A = y^4 + z^4 - 2nyz(y^2+z^2) + (n^2-8n-2)y^2z^2,$$

$$B = 16ny^3z^3(y+z)^2,$$

*via the following maps*

$$\phi\colon F \to C,$$

$$\phi(U:V:T) = (V+DU : -V+DU : 2(y+z)(U-4ny^2z^2T)),$$

$$\psi\colon C \to F,$$

$$\psi(x:y:d) = (\frac{x+w}{2D} : \frac{x-w}{2} : \frac{(x+w)(y+z)-dD}{8nD(y+z)y^2z^2}).$$

*Proof.* We can check $\phi$ and $\psi$ are inverses of each other using Magma [1]. □

We seek rational points $(U:V:T)$ on $F$ such that $\phi(U:V:T)$ satisfies $d \neq 0, x/d > 0, w/d > 0$, thus

$$\begin{cases} U - 4ny^2z^2T \neq 0, \\ \frac{V-DU}{2(y+z)(U-4ny^2z^2T)} > 0, \\ \frac{-V-DU}{2(y+z)(U-4ny^2z^2T)} > 0. \end{cases}$$

Point $(0:1:0)$ does not satisfy $U - 4ny^2z^2T \neq 0$; thus $T \neq 0$. When $T \neq 0$, $F$ has the affine model

$$E\colon Y^2 = X(X^2 + AX + B), \tag{4.2.27}$$

where

$$X = \frac{U}{T}, \quad Y = \frac{V}{T},$$

$$A = y^4 + z^4 - 2nyz(y^2+z^2) + (n^2-8n-2)y^2z^2,$$

$$B = 16ny^3z^3(y+z)^2.$$

**Lemma 4.2.7.** *Let* $(X, Y)$ *be a point on* (4.2.27) *such that*

$$\begin{cases} 2(y+z)(X-4ny^2z^2) \neq 0, \\ \frac{Y-DX}{2(y+z)(X-4ny^2z^2)} > 0, \\ \frac{-Y-DX}{2(y+z)(X-4ny^2z^2)} > 0. \end{cases} \tag{4.2.28}$$

*Then* $X < 0$.

*Proof.* From (4.2.28), we have

$$0 < D^2X^2 - Y^2 = -X(X - 4ny^2z^2)(X - 4yz(y+z)^2). \tag{4.2.29}$$

Because $D = y^2 - (n-2)yz + z^2 < 0$, $4ny^2z^2 > 4yz(y+z)^2$, (4.2.29) implies that

$$X < 0 \quad \text{or} \quad 4yz(y+z)^2 < X < 4ny^2z^2.$$

If $X > 0$, then $4yz(y+z)^2 < X < 4ny^2z^2$; then from (4.2.28), we have $Y - DX < 0$ and $-Y - DX < 0$. Thus $-2DX < 0$, impossible because $X > 0, D < 0$. Therefore, $X < 0$.

□

**Case 1:**

$$n = 4m^2 \quad \text{and} \quad 4|m.$$

If

$$x + y \equiv x + z \equiv z + w \equiv y + z \equiv y + w \equiv z + w \equiv 0 \mod 4,$$

then

$$x \equiv y \equiv z \equiv w \mod 4.$$

Further, $4 \nmid x + y$, so

$$x \equiv y \equiv z \equiv w \equiv 0 \mod 2.$$

Therefore $\gcd(x, y, z, w) > 1$, which is not possible.

Without loss of generality, we can assume that $4 \nmid y + z$.

Now applying Theorem 4.2.2 to $n = 4m^2, \quad 4|m, \quad 4 \nmid y + z$, we have $Y = 0$.

Because

$$\psi(x : y : d) = (\frac{x + w}{2D} : \frac{x - w}{2D} : \frac{(x + w)(y + z) - dD}{8nD(y + z)y^2z^2}),$$

$Y = 0$ implies $x = w$.

So when $4 \nmid y + z$, then $x = w$.

• If $4 \nmid x + y$, then from the above argument, we have $z = w$. Therefore $y = z = w$.

(4.2.25) becomes

$$n = \frac{(x + 3y)(y + 3x)}{xy} = 10 + \frac{3(x^2 + y^2)}{xy}.$$

Because $\gcd(x, y, z, w) = 1$, we have $\gcd(x, y) = 1$. Therefore $\gcd(x^2 + y^2, xy) = 1$. So $xy|3$. Thus $(x, y) = (1, 3)$ or $(3, 1)$, and $n = 16$ or $n = 20$.

• If $4 \nmid x + z$, then similarly we get $n = 16$ or $n = 20$.

• If $4|x + y$ and $4|x + z$, then $4|2x + y + z$.

Because $4 \nmid y + z$, we have $4 \nmid 2x = x + w$. Applying Theorem 4.2.2 again for $(x, w)$ in the stead of $(y, z)$, we have $y = z$.

Therefore

$$n = \frac{4(x + y)^2}{xy}.$$

Thus $xy|4(x + y)^2$. Because $\gcd(x, y) = 1$, we have $\gcd(xy, (x + y)^2) = 1$. thus $xy|4$. From $4|x + y$, we have $x = y = 2$, so $x = y = z = w = 2$, which contradicts $\gcd(x, y, z, w) = 1$.

So there are no solutions in positive integers of (4.2.25).

**Case 2:**

$$n = 4m^2 \quad \text{and} \quad 2 \nmid m.$$

If

$$x \equiv y \equiv z \equiv w \mod 4,$$

then because $\gcd(x, y, z, w) = 1$, we have

$$x \equiv y \equiv z \equiv w \equiv \pm 1 \mod 4.$$

From

$$nxyzw = (x + y + z + w)(xyz + xyw + xzw + yzw),$$

we have

$$nxyzw \equiv 0 \mod 16,$$

so $2|m$, which is not possible.

Without loss of generality, we assume that $4 \nmid y - z$. Applying Theorem 4.2.2 to $n = 4m^2, \quad 2 \nmid m \quad \text{and} \quad 4 \nmid y - z$, we have $x = w$.

•If $4 \nmid x - y$ (or $4 \nmid x - z$), then by a similar argument, we have $z = w$ or $y = w$.

If $z = w$, then $x = z = w$. We have

$$n = \frac{(3x + y)(x + 3y)}{xy}.$$

Similar to **Case 1**, $n = 16$ or $20$.

If $y = w$ then $x = w = y$. Thus $n = 16$ or $20$.

• If $4|x - y$ and $4|x - z$, then $4|y - z$, which contradicts $4 \nmid y - z$.

**Case 3:**

$$n = 4m^2 + 4 \quad \text{and} \quad 4|m.$$

Similar to **Case 2**, we can assume $4 \nmid y - z$. Applying Theorem 4.2.2 to $n = 4m^2 + 4$ and $4 \nmid y - z$ we have $x = w$, which leads to $n = 16$ or $20$.

**Case 4:**

$$n = 4m^4 + 4 \quad \text{and} \quad 2 \nmid m.$$

Similar to **Case 1**, we can asusme $4 \nmid y+z$. Applying Theorem 4.2.2 to $n = 4m^2$ and $4 \nmid y+z$, we have $x = w$, which leads to $n = 16$ or $20$. $\square$

## 4.3 Equation $\frac{x}{y} + p\frac{y}{z} + \frac{z}{w} + p\frac{w}{x} = 8pn$

In this section, we will prove the following theorem

**Theorem 4.3.1.** *Let $p = 1$ or $p$ be an odd prime such that $p \equiv 1 \mod 8$. Then for every positive integer $n$, the equation*

$$\frac{x}{y} + p\frac{y}{z} + \frac{z}{w} + p\frac{w}{x} = 8pn \tag{4.3.1}$$

*does not have solutions $x, y, z, w \in \mathbb{Z}^+$.*

*Proof.* Assume that $(x, y, z, w)$ is a positive integer solution of (4.3.1) with $\gcd(x, y, z, w) = 1$.

Write the equation (4.3.1) as

$$x^2zw + py^2wx + z^2xy + pw^2yz - 8npxyzw = 0. \tag{4.3.2}$$

We fix $x, z$ then (4.3.2) is an affine curve $F(y, w)$ in $\mathbb{Q}(x, z)$ with the projective model

$$C\colon pxwy^2 + pw^2yz + (xz^2y + x^2zw)d^2 - 8npxzywd = 0.$$

We need the following lemma

**Lemma 4.3.1.** *Let $p = 1$ or $p$ be a prime and $p \equiv 1 \mod 8$. Let $n, x, z \in \mathbb{Z}^+$ and $(u, v) \in \mathbb{Q}^2$ with $v \neq 0$ such that*

$$E\colon v^2 = u(u^2 + Au + B), \tag{4.3.3}$$

*where*

$$\begin{aligned} A &= pxz(16n^2pxz - x^2 - z^2), \\ B &= p^2x^4z^4. \end{aligned}$$

*Let* $D(x,z) = x^2 + z^2 - 2xz(8pn^2 - 1)$ *and* $H(x,z) = x^2 + z^2 - 2xz(8pn^2 + 1)$*. Then*

$$(D,u)_q = (H,u)_q = 1 \quad \forall \quad primes \quad q > 2.$$

*In addition:*

$$(D,u)_2 = (D,u)_\infty = 1 \quad if \quad 4 \nmid x + z,$$

*and*

$$(H,u)_2 = (H,u)_\infty = 1 \quad if \quad 4 \nmid x - z.$$

*Proof.* In this section, we denote $\mathrm{ord}_q(x)$ the highest power of a prime number $q$ dividing an integer $x$.

Let $d = \gcd(x,z)$. Then $x = dx_1$, $y = dy_1$, where $x_1, z_1 \in \mathbb{Z}^+$ and $\gcd(x_1, z_1) = 1$.

Let $u_1 = \frac{u}{d^4}$ and $v_1 = \frac{v}{d^6}$. From (4.3.3), we have

$$v_1^2 = u_1(u_1^2 + x_1z_1(16pn^2x_1z_1 - x_1^2 - z_1^2)),$$

and for all $q$ prime

$$(D,u)_q = (d^2(x_1^2 + z_1^2 - 2(8pn^2 - 1)x_1z_1), d^4u_1)_q = (D_1, u_1)_q,$$

and

$$(H,u)_q = (d^2(x_1^2 + z_1^2 - 2(8pn^2 + 1)x_1z_1, d^4u_1)_q = (H_1, u_1)_q,$$

where $D_1 = x_1^2 + z_1^2 - 2(8n^2 - 1)x_1z_1$ and $H_1 = x_1^2 + z_1^2 - 2p(8pn^2 + 1)x_1z_1$.

Also if $4 \nmid x + z$, then $4 \nmid x_1 + z_1$, and if $4 \nmid x - z$, then $4 \nmid x_1 - z_1$; therefore we only need to prove Lemma 4.3.1 when $\gcd(x,z) = 1$.

If $D(x,z) = 0$, then $(8pn^2 - 1)^2 - 1$ is a perfect square. Equation $a^2 - 1 = b^2$ in integers has only solution $|a| = 1$ and $b = 0$, but $8pn^2 - 1 \neq \pm 1$, therefore $H(x,z) \neq 0$. Similarly, $H(x,z) \neq 0$. Let $q$ be an odd prime. We want to show

$$(u,D)_q = 1.$$

If $u \notin \mathbb{Z}_q$ then $u = q^{-r}u_0$ with $r \in \mathbb{Z}^+$ and $u_0$ is a unit in $\mathbb{Z}_p$. From (4.3.3), we have

$$v^2 = \frac{u_0(u_0^2 + q^r A u_0 + q^{2r} B)}{q^{3r}},$$

$$3r = \mathrm{ord}_q(v^2) = 2\mathrm{ord}_q(v).$$

Thus $r$ is even and

$$u_0(u_0^2 + q^r A u_0 + q^{2r} B) = \square \in \mathbb{Z}_q^2.$$

Taking $\mod q$ gives $u_0 \equiv \square \mod q$, thus $u_0 \in \mathbb{Z}_q^2$. $2|v$, so $u \in \mathbb{Q}_q^2$. Hence $(D, u)_q = 1$.

We only need to consider $u \in \mathbb{Z}_q$.

**Case 1:** $p \nmid u$.

If $q \nmid D$, then both $u, D$ are units in $\mathbb{Z}_q$, thus $(u, D)_q = 1$.

If $q|D$, then

$$x^2 + z^2 \equiv 2(8pn^2 - 1)xz \mod q.$$

$$\Rightarrow \quad (x+z)^2 \equiv 16pn^2xz \mod q.$$

We have

$$u^2 + Au + B = (u + \frac{A}{2})^2 - \frac{p^2x^2z^2HD}{4} \equiv (u + \frac{A}{2})^2 \mod q.$$

If $q \nmid u + \frac{A}{2}$, then $u^2 + Au + B \in \mathbb{Z}_q^2$. Thus from $v^2 = u(u^2 + Au + B)$, we have $u \in \mathbb{Z}_q^2$, so $(u, D)_q = 1$.

If $q|u + \frac{A}{2}$, then $u \equiv -\frac{A}{2} \mod q$. Thus $q \nmid A$. $q|D$, so

$$A = pxz(16pn^2xz - x^2 - z^2) = pxz(-D + 2xz) \equiv 2px^2z^2 \mod q.$$

Because $q \nmid u$, $q \nmid A$, we have $q \nmid 2px^2z^2$.

From $v^2 = u(u^2 + Au + B)$ and $q \nmid u$, we have $2|\mathrm{ord}_q(u^2 + Au + B)$. Now $q \nmid 2pxz$, so

$\gcd(D, H) = 1$.

Let $k = \text{ord}_q(D)$. If $2|k$, then $D = q^k D_1$ with $q \nmid D_1$, so

$$(u, D)_q = (u, q^k D_1)_q = (u, D_1)_q = 1.$$

If $2 \nmid k$ then let $S = u + \frac{A}{2}$ and $T = \frac{HD}{4}$. Because $\gcd(H, D) = 1$ and $q|D$, we have $\text{ord}_q(T) = \text{ord}_q(D) = k$. Let $S = q^l S_1, T = q^k T_1$ with $q \nmid S_1, T_1$. Then from

$$2|\text{ord}_q(u^2 + Au + B) = \text{ord}_q(S^2 + T) = \text{ord}_q(q^{2l} S_1^2 + q^k T_1),$$

we have $2l < k$. Thus $u^2 + Au + B = q^{2l}(S_1^2 + q^{k-2l} T) \in \mathbb{Q}_q^2$. Hence $u = \frac{v^2}{S^2+T} \in \mathbb{Q}_q^2$. So $(u, D)_q = 1$.

**Case 2:** $q|u$.

**Case 2.1:** $q \nmid pxz$.

Equation $(u^2 + Au + B)\alpha^2 + D\beta^2 = \gamma^2$ has a solution $(1, 0, px^2z^2) \mod q$. Thus it has a nontrivial solution in $\mathbb{Q}_q$. Therefore

$$(u^2 + Au + B, D)_q = 1.$$

Because $u(u^2 + Au + B) = v^2 \neq 0$, we also have $(u, D)_q = 1$.

**Case 2.2:** $q|pxz$.

If $q|xz$, then because $\gcd(x, z) = 1$, we have $q \nmid D = x^2 + z^2 - 2p(8n^2 - 1)yz$ and $D \equiv \square \mod q$, hence $D \in \mathbb{Z}_q^2$; therefore $(u, D)_q = 1$.

If $q \nmid xz$, then $q = p$ and $p \nmid xz$.

Let $u = p^s$, where $s > 0$ and $p \nmid u_1$. Then

$$v^2 = p^s u_1(p^{2s} u_1^2 + Ap^s u_1 + p^2 x^4 z^4). \tag{4.3.4}$$

If $s \geq 2$, then from (4.3.4), we have $2\text{ord}_p(v) = s + 2$. Thus $2|s$. We now have

$$\square = u_1(p^{2s-2} u_1^2 + Ap^{s-2} u_1 + x^4 z^4).$$

$p|A$, so taking $\mod p$ gives $\Box \equiv u_1x^4z^4$. Therefore $u_1 \in \mathbb{Z}_q^2$. Thus

$$(u, D)_p = (2^s u_1, D)_p = 1.$$

If $s = 1$, then

$$v^2 = pu_1(p^2u_1^2 + pAu_1 + p^2x^4z^4).$$

$$\Rightarrow \quad v^2 = p^3u_1(u_1^2 + xz(16pn^2xz - x^2 - z^2)u_1 + x^4z^4)$$

$$\Rightarrow \quad p|u_1^2 + xz(-x^2 - z^2)u_1 + x^4z^4 = (u_1 - x^3z)(u_1 - xz^3).$$

Thus

$$u_1 \equiv x^3z \mod p \quad \text{or } u_1 \equiv xz^3 \mod p. \tag{4.3.5}$$

We have

$$D = (x+z)^2 - 16pn^2xz \equiv (x+z)^2 \mod p,$$

so if $p \nmid x + z$, then $D \in \mathbb{Z}_p^2$, hence $(u, D)_p = 1$.

If $p|x + z$, let $x + z = p^r f$, where $r > 0$ and $p \nmid f$, then

$$D = p(p^{2r-1}f^2 - 16n^2xz).$$

If $p \nmid n$, then $D = p(\Box \mod p)$. So $D = pD_1^2$, where $D_1 \in \mathbb{Z}_p$.

From (4.3.5), if $u_1 \equiv x^3z \mod p$, we have

$$\begin{aligned}(u, D)_p = (pu_1, pD_1^2)_p = (pu_1, p)_p = (-1)^{\frac{p-1}{2}}(\frac{u_1}{p}) \\ = (\frac{x^3z}{p}) = (\frac{-x^4}{p}) = (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = 1.\end{aligned} \tag{4.3.6}$$

Similarly,if $u_1 \equiv xz^3 \mod p$, then $(u, D)_p = 1$.

If $p|n$, let $n = p^t n_1$, where $t > 0$ and $p \nmid n_1$, then

$$D = p^{2r}f^2 - 16p^{2t+1}xz. \tag{4.3.7}$$

If $r \leq t$, then

$$D = p^{2r}(f^2 - 16p^{2t+1-2r}n_1^2xz)$$

Thus $D \in \mathbb{Z}_p^2$, and $(u, D)_p = 1$.

If $r > t$, then

$$D = p^{2s+1}(p^{2r-2t-1}f^2 - 16n_1^2 xz).$$

Because $-16n_1^2 xz \equiv 16n_1^2 x^2 \mod p$, we have $D = p^{2s+1}D_2^2$, where $D_2 \in \mathbb{Z}_p$. Therefore

$$(u, D)_p = (pu_1, p^{2r+1}D_2^2)_p = (pu_1, p)_p.$$

Similar to (4.3.6), we have $(pu_1, p)_p = 1$, thus $(u, D)_p = 1$.

Now we prove that if $4 \nmid x + z$ then $(D, u)_2 = 1$.

We have $D = (x + z)^2 - 16pn^2 xz$.

If $2 \nmid x + z$, then $D \equiv 1 \mod 8$, so $D \in \mathbb{Z}_2^2$, hence $(D, u)_2 = 1$.

If $2 | x + z$, then because $4 \nmid x + z$, we have $x + z = 2h$, $2 \nmid h$. So $D = 4(h^2 - 4pn^2 xz)$.

If $2|n$, then $h^2 - 4pn^2 xz \equiv 1 \mod 8$, thus $D \in \mathbb{Z}_2^2$.

If $2 \nmid n$, then $pn^2 xz \equiv 1 \mod 4$, so $h^2 - 4pn^2 xz \equiv 5 \mod 8$.

Thus $D = 4D_1$, where $D_1 \equiv 5 \mod 8$.

Let $u = 2^r u_1$. Then

$$v^2 = 2^r u_1(2^{2r}u_1^2 + 2^r A u_1 + B).$$

If $r \geq 3$, then

$$2^{2r}u_1^2 + 2^r A u_1 + B \equiv B = p^2 x^4 z^4 \equiv 1 \mod 8.$$

Thus $r = 2\mathrm{ord}_2(v)$. Now

$$\square = u_1(2^{2r}u_1^2 + 2^r A u_1 + B).$$

So $u_1 \equiv 1 \mod 8$. Thus $u_1 \in \mathbb{Z}_2^2$, so $u = 2^r u_1 \in \mathbb{Z}_2^2$, hence $(u, D)_2 = 1$.

If $r < 0$, then

$$v^2 = \frac{u_1(u_1^2 + 2^{-r}Au_1 + 2^{-2r}B)}{2^{-3r}}.$$

So $2|3r$, hence $2|r$. Thus $r \leq -2$. Taking $\mod 8$ gives $u_1 \equiv 1 \mod 8$. Thus $u_1 \in \mathbb{Z}_2$, so $u \in \mathbb{Z}_2^2$. Thus $(u, D)_2 = 1$.

So we only need to consider $r \in \{0, 1, 2\}$.

If $r = 2$, then

$$v^2 = 2^2 u_1(2^4 u_1^2 + 2^2 A u_1 + B).$$

Taking $\mod 8$ gives $u_1 \equiv 1 \mod 8$. So $u = 2^2(1 \mod 8) \in \mathbb{Z}_2^2$, hence $(u, D)_2 = 1$.

If $r = 1$, then

$$v^2 = 2u_1(4u_1^2 + 2Au_1 + B).$$

So $1 = 2\text{ord}_2(v)$, impossible.

If $r = 0$, then $u = u_1$ and $D = 2^2 D_1$, where $D_1 \equiv 5 \mod 8$. Therefore

$$(u, D)_2 = (u_1, 2^2 D_1)_2 = (u_1, D_1)_2 = (-1)^{\frac{u_1-1}{2}\frac{D-1}{2}} = 1.$$

So if $4 \nmid x + z$, then $(D, u)_2 = 1$.

Because

$$(D, u)_\infty \prod_{q \text{ prime},\ q<\infty} = 1,$$

we also have $(u, D)_\infty = 1$.

Next we show that if $q$ is an odd prime, then $(H, u)_q = 1$.

Because $A^2 - 4B = p^2 x^2 z^2 DH$, we have

$$v^2 = u((u + \frac{A}{2})^2 - DH(\frac{pxz}{2})^2).$$

So

$$u\alpha^2 - uDH\beta^2 = v^2,$$

where $\alpha = u + \frac{A}{2}$ and $\beta = \frac{pxz}{2}$. So

$$(u, -uHD)_q = 1.$$

But $(u,-u)_q = 1$ and $(u,D)_q = 1$, therefore

$$(u,H)_q = 1.$$

Now we will show that $(u,H)_2 = 1$ if $4 \nmid x-z$.

If $2 \nmid x-z$, then

$$H = (x-z)^2 - 16pn^2xz \equiv 1 \mod 8.$$

Thus $H \in \mathbb{Z}_2^2$, hence $(u,H)_2 = 1$.

If $2|x-z$ and $4 \nmid x-z$, then $x-z = 2k$ and $H = 4(k^2 - 4pn^2xz)$, where $2 \nmid k$.

If $2|n$, then

$$k^2 - 4pn^2xz \equiv 1 \mod 8.$$

Thus $H \in \mathbb{Z}_2^2$ and $(u,H)_2 = 1$.

If $2 \nmid n$, then

$$k^2 - 4pn^2xz \equiv 1 - 4 \equiv 5 \mod 8,$$

so $H = 4H_1$, where $H_1 \equiv 5 \mod 8$.

Let $u = 2^r u_1$. Then

$$v^2 = 2^r u_1(2^{2r}u_1^2 + 2^r Au_1 + B).$$

If $r \geq 3$, then

$$2^{2r}u_1^2 + 2^r Au_1 + B \equiv 1 \mod 8.$$

Hence $\in \mathbb{Z}_2^2$, thus $u = 2^r u_1 \in \mathbb{Z}_2^2$. So $(u,H)_2 = 1$.

If $r < 0$, then

$$v^2 = \frac{u_1(u_1^2 + 2^{-r}Au_1 + 2^{-2r}B)}{2^{-3r}}.$$

Therefore $2|r$. Thus $r \leq -2$. Taking $\mod 8$ gives $u_1 \equiv 1 \mod 8$, thus $u_1 \in \mathbb{Z}_2$, so $u \in \mathbb{Z}_2^2$. Thus $(u,H)_2 = 1$.

So we only need to consider $r \in \{0, 1, 2\}$.

If $r = 2$, then

$$v^2 = 2^2 u_1 (2^4 u_1^2 + 2^2 A u_1 + B).$$

Taking $\mod 8$, we have $u_1 \equiv 1 \mod 8$, so $u \in \mathbb{Z}_2^2$, hence $(u, H)_2 = 1$.

If $r = 1$, then $v^2 = 2u_1(4u_1^2 + 2Au_1 + B)$, impossible $\mod 2$.

If $r = 0$, then $u = u_1$ and $H = 2^2 H_1$, where $H_1 \equiv 5 \mod 8$, therefore

$$(u, H)_2 = (u_1, 2^2 H_1)_2 = (u_1, H_1)_2 = (-1)^{\frac{u_1 - 1}{2} \frac{H_1 - 1}{2}} = 1.$$

From

$$(u, H)_\infty \prod (u, H)_{\text{q prime}, \, q < \infty} = 1,$$

we have $(u, H)_\infty = 1$. □

From $\frac{x}{y} + \frac{py}{z} + \frac{z}{w} + \frac{pw}{x} = 8np$, we have

$$x^2 zw + py^2 wx + z^2 xy + pw^2 yz - 8npxyzw = 0.$$

**Lemma 4.3.2.** *$x^2 - 2(8pn^2 - 1)xz + z^2 < 0$ and $y^2 - 2(8pn^2 - 1)yw + w^2 < 0$.*

*Proof.* Using the AM-GM inequality, we have

$$\begin{aligned} 8pn = (\frac{x}{y} + \frac{pw}{x}) + (\frac{py}{z} + \frac{z}{w}) &\geq 2\sqrt{\frac{x}{y}\frac{pw}{x}} + 2\sqrt{\frac{py}{z}\frac{z}{w}} \\ &= 2\sqrt{p}\frac{y + w}{\sqrt{yw}} \end{aligned}$$

$$\Rightarrow \quad 4n\sqrt{pyw} \geq y + w$$

$$\Rightarrow \quad y^2 - 2(8pn^2 - 1)yw + w^2 \leq 0.$$

Similarly, we have

$$\begin{aligned} 8np = (\frac{x}{y} + \frac{py}{z}) + (\frac{z}{w} + \frac{pw}{x}) &\geq 2(\sqrt{\frac{x}{y}\frac{py}{z}} + \sqrt{\frac{z}{w}\frac{pw}{x}}) \\ &= 2\sqrt{p}\frac{x + z}{\sqrt{xz}} \end{aligned}$$

$$\Rightarrow \quad 4n\sqrt{pxz} \geq x + z$$

$$\Rightarrow \quad x^2 - 2(8pn^2 - 1)xz + z^2 \leq 0.$$

Because $(8pn^2 - 1)^2 - 1$ is not a square, so $y^2 - 2(8pn^2 - 1)yw + w^2 < 0$ and $x^2 - 2(8pn^2 - 1)xz + z^2 < 0$. □

Fix $x, z$ and consider the equation $F_{x,z} = 0$, where

$$F_{x,z}(Y, W, d) = pxWY^2 + pW^2Yz + (xz^2Y + x^2zW)d^2 - 8npxzYWd.$$

Then $F_{x,z}$ has points $(y, w, 1)$ and $(0, 1, 0)$.

**Lemma 4.3.3.** *$F_{x,z}$ is birationally isomorphic to the curve*

$$E_{x,z}\colon v^2 = u(u^2 + Au + B),$$

*where*

$$\begin{cases} A = pxz(16n^2pxz - x^2 - z^2), \\ B = p^2x^4z^4, \end{cases}$$

*via the following maps*

$$\begin{cases} \phi\colon F_{x,z} \to E_{x,z}, \quad \psi\colon E_{x,z} \to F_{x,z}, \\ \phi(Y : W : d) = (\frac{-x^2z^2Wp}{Y}, \frac{x^3z^2W(4nxzd - xY - zW)}{Yd}), \\ \psi(u, v) = (px^2z^2(4nxzu + pv) : -u(4nxznu + pv) : zu(u - px^3z)), \end{cases}$$

*where $\phi(0 : 1 : 0) = (0 : 1 : 0)$.*

*Proof.* We can check that $\psi$ and $\phi$ are inverses of each other using Magma [1]. □

We seek for point $(u, v)$ on $E_{x,z}$ such that $\psi(u, v) = (Y : W : d)$ satisfying $d \neq 0$, $\frac{Y}{d} > 0$ and $\frac{w}{d} > 0$. If $u = 0$, then $v = 0$. Because $\psi(0, 0) = (1 : 0 : 0)$, we have $u \neq 0$.

Therefore

$$\begin{cases} u \neq 0, \\ \frac{px^2z(4nxzu+pv)}{u(u-px^3z)} > 0, \\ -\frac{4xznu+pv}{u-px^3z} > 0. \end{cases} \tag{4.3.8}$$

From (4.3.8) and $px^2z > 0$, we have $u < 0$.

Let

$$(u_0, v_0) = \phi(y : w : 1) = (\frac{-x^2z^2wp}{y}, \frac{x^3z^2w(4nxz - xy - zw)}{y}). \tag{4.3.9}$$

Let $D(l,m) = l^2 + m^2 - 2lm(8pn^2 - 1)$ and $H(l,m) = l^2 + m^2 - 2lm(8pn^2 + 1)$. Then because $(8pn^2 - 1)^2 - 1$ and $(8pn^2 + 1)^2 - 1$ are not perfect squares, we have $G(l,m), H(l,n) \neq 0$ for all $m, n \in \mathbb{Q}^*$.

If $v_0 \neq 0$, then

• if $4 \nmid x + z$, from the Lemma 4.3.1, we have $(D(x,z), u_0)_\infty = 1$. But $D(x,z) < 0$ by Lemma 4.2.5, so $u_0 > 0$, contradicting $u_0 < 0$.

• if $4 \nmid x - z$, from the Lemma 4.3.1, we have $(H(x,z), u_0)_\infty = 1$. Because $H(x,z) < D(x,z) < 0$, we have $u_0 > 0$, contradicting $u_0 < 0$.

So there are no solutions to (4.3.1) if $4 \nmid x + z$ or $4 \nmid x - z$.

We now consider the case $4|x + z$ and $4|x - z$. Then $x = 2x_1$ and $z = 2z_1$, where $2 \nmid x_1, z_1$. Then $4 \nmid x_1 + z_1$ or $4 \nmid x_1 - z_1$. From $v_0^2 = u_0(u_0^2 + Au_0 + B)$, we have

$$(\frac{v_0}{2^6})^2 = \frac{u_0}{2^4}((\frac{u_0}{2^4})^2 + A_1\frac{u_0}{2^4} + B_1),$$

where $A_1 = px_1z_1(16pn^2x_1z_1 - x_1^2 - z_1^2)$ and $B_1 = p^2x_1^4z_1^4$.

Now $4 \nmid x_1 - z_1$ or $4 \nmid x_1 + z_1$, so we have $(D(x_1,z_1), \frac{u_0}{2^4})_2 = 1$ or $(H(x_1,z_1), \frac{u_0}{2^4})_2 = 1$. But we also have

$$(D(x,z), u_0)_2 = (2^2D(x_1,z_1), 2^4\frac{u_0}{2^4})_2 = (D(x_1,z_1), \frac{u_0}{2^4})_2,$$

and similarly

$$(H(x,z),u_0)_2 = (H(x_1,z_1),\frac{u_0}{2^4})_2.$$

So we have $(D(x,z),u_0)_2 = 1$ or $(H(x,z),u_0)_2 = 1$, which implies $u_0 > 0$, contradicting $u_0 < 0$.

Therefore $v_0 = 0$ . From (4.3.9), we have

$$4nxz - xy - zw = 0. \tag{4.3.10}$$

$$\Rightarrow \frac{y}{z} + \frac{w}{x} = 4n.$$

$$\Rightarrow \frac{x}{y} + \frac{z}{w} = 4np. \tag{4.3.11}$$

Now fix y,w and consider the equation $F_{y,w}(X,Z,d) = 0$, where

$$F_{y,w}(X,Z,d) = X^2yZ + py^2Zwd^2 + Z^2wX + pw^2Xyd^2 - 8npXZdyw. \tag{4.3.12}$$

Then $F_{y,w}(0,1,0) = F_{y,w}(x,z,1) = 0$.

**Lemma 4.3.4.** *$F_{y,w}$ is birationally isomorphic to the curve*

$$E_{y,w}\colon v^2 = u(u^2 + Au + B),$$

*where*

$$\begin{cases} A = pyw(16n^2pyw - y^2 - w^2), \\ B = p^2y^4w^4, \end{cases}$$

*via the following maps*

$$\begin{cases} \alpha\colon F_{y,w} \to E_{y,w}, \quad \gamma\colon E_{y,w} \to F_{y,w}, \\ \alpha(X:Z:d) = (\frac{-w^2pZy^2}{X}, \frac{-py^2w^2Z(Xy+Zw-4npywd)}{Xd}), \\ \beta(u,v) = (pw^2(4npywu+v) : -u(4npywu+v) : wu(u-py^3w)), \end{cases}$$

*where $\alpha(0:1:0) = (0:1:0)$ and $\beta(0,0) = (1:0:0)$.*

*Proof.* We can check that $\alpha$ and $\beta$ are inverses of each other using Magma [1]. $\square$

We seek for point $(u, v)$ on $E_{y,w}$ such that $\psi(u, v) = (X : Z : d)$ satisfying $d \neq 0$, $\frac{X}{d} > 0$ and $\frac{Z}{d} > 0$. If $d = 0$, then from (4.3.12), we have

$$X^2yZ + Z^2wX = 0.$$

Thus $(X : Z : d) = (1 : 0 : 0)$ or $(X : Z : d) = (0 : 1 : 0)$.

Using Magma [1], we have $\alpha(1 : 0 : 0) = (0 : 0 : 1)$ and $\alpha(0 : 1 : 0) = (0 : 1 : 0)$. So in order for $\psi(u, v) = (X : Z : d)$ to satisfy $d \neq 0$, $\frac{X}{d} > 0$ and $\frac{Z}{d} > 0$, we have

$$\begin{cases} u \neq 0, \\ \frac{pw(4npywu+v)}{u(u-py^3w)} > 0, \\ -\frac{4npywu+v}{w(u-py^3w)} > 0. \end{cases} \tag{4.3.13}$$

From (4.3.13), we have $u < 0$.

Let

$$(u_1, v_1) = \alpha(x : z : 1) = (\frac{-py^2w^2z}{x}, \frac{-py^2w^2z(yx + wz - 4npyw)}{x}). \tag{4.3.14}$$

If $v_1 \neq 0$, then

• if $4 \nmid y+w$, from the Lemma 4.3.1, we have $(D(y, w), u_1)_\infty = 1$, thus $u_1 > 0$ because $D(y, w) < 0$ by Lemma 4.2.5. This contradicts $u_1 < 0$.

• if $4 \nmid y - w$, from the Lemma 4.3.1, we have $(H(y, w), u_1)_\infty = 1$, thus $u_1 > 0$, because $H(y, w) < D(y, w) < 0$. This contradicts $u_1 < 0$.

Therefore there are no solutions to (4.3.1) if $4 \nmid y + w$ or $4 \nmid y - w$.

We now consider the case $4|y + w$ and $4|y - w$. Then $y = 2y_1$ and $w = 2w_1$,where $2 \nmid y_1, w_1$. Then $4 \nmid y_1 + w_1$ or $4 \nmid y_1 - w_1$. By the same argument, we still have $(D(y, w), u_1)_\infty = 1$ or $(H(y, w), u_1)_\infty = 1$. This implies $u_1 > 0$, which contradicts

$u_1 < 0$.

Therefore $v_1 = 0$. From (4.3.14), we have

$$xy + zw - 4npyw = 0. \tag{4.3.15}$$

From (4.3.10) and (4.3.15), we have

$$4nxz = 4npyw.$$

$$\Rightarrow \frac{x}{y}\frac{z}{w} = p. \tag{4.3.16}$$

From (4.3.11) and (4.3.16), we have

$$(4np)^2 - 4p = (\frac{x}{y} - \frac{z}{w})^2.$$

Thus $4n^2p^2 - p \in \mathbb{Q}^2$, hence $4n^2p^2 - p \in \mathbb{Z}^2$. This is not possible because $p^2 \nmid 4n^2p^2 - p$. Therefore, there are no positive integer solutions to (4.3.1).

□

The above proof still works when $p = 1$, therefore we have the following theorem

**Theorem 4.3.2.** *Let $n$ be a positive integer then the equation*

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{w} + \frac{w}{x} = 8n$$

*does not have solutions $(x, y, z, w)$ in positive integers.*

**Remark 4.3.1.** *Theorem 4.3.1 was suggested by Professor Andrew Bremner. It gives an infinite family of surfaces which does not have positive integer solutions. We can investigate the family*

$$(Ax + By + Cz + Dw)(\frac{E}{x} + \frac{F}{y} + \frac{G}{z} + \frac{H}{w}) = n,$$

*where* $A, B, C, D, E, F, G,$ *and* $H$ *are positive integers. The conjecture here is that for each tuple* $(A, B, C, D, E, F, G, H) \in (\mathbb{Z}^+)^8$ *there is a polynomial function* $n = n(A, B, C, D, E, F, G, H)$ *such that the equation*

$$(Ax + By + Cz + Dw)(\frac{E}{x} + \frac{F}{y} + \frac{G}{z} + \frac{H}{w}) = n(A, B, C, D, E, F, G, H)$$

*does not have positive integer solutions.* $(x + y + z + w)(\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{w}) = n$ *with* $n = 4m^2$ *or* $n = 4m^2 + 4$, $m \not\equiv 2 \mod 4$ *and* $\frac{x}{y} + p\frac{y}{z} + \frac{z}{w} + p\frac{w}{x} = 8pn$ *with* $p = 1$ *or* $p$ *is a prime* $\equiv 1 \mod 8$ *are apparently the only known two examples.*

### 4.4 Equation $x^4 + 7y^4 = 14z^4 + 18w^4$

The family of surfaces $ax^4 + by^4 = cz^4 + dw^4$, where $a, b, c, d \in \mathbb{Z}$ and $abcd \in \mathbb{Z}^2$, has been studied extensively by Swinnerton-Dyer [21] and Bright [9, 8]. The only known examples which are everywhere locally solvable but have no rational points are apparently

$$2x^4 + 6y^4 = 9z^4 + 12w^4, \quad 4x^4 + 9y^4 = 8z^4 + 8w^4$$

and the family

$$x^4 + 4y^4 = d(z^4 + w^4),$$

where $d > 0$, $d \equiv 2 \mod 16$, no prime $p \equiv 3 \mod 4$ divides $d$, no prime $p \equiv 5 \mod 8$ divides $d$ to an odd power, and $r \equiv \pm 3 \mod 8$, where $d = r^2 + s^2$. The other known examples when $abcd$ is not a perfect square given by Bright [9] are

$$x^4 + y^4 = 6z^4 + 12w^4, \quad x^4 + 47y^4 = 103z^4 + 17.47.103w^4.$$

It is unknown whether these surfaces have non-trivial points in cubic extensions of $\mathbb{Q}$ or not. In this section, we will show that the surface $x^4 + 7y^4 = 14z^4 + 18w^4$ is unsolvable in the rational numbers, everywhere locally solvable, and solvable in a cubic and other odd degree number fields. The example was suggested by Professor Andrew Bremner and the proof uses the ideas from Swinnerton-Dyer [21].

**Lemma 4.4.1.** *There are infinitely many pairs $(P, Q)$ of positive integers satisfying the following condition*

*i, every prime factor of $PQ$ is congruent to* $1$ *mod* $24$,

*ii, if $p$ is a prime divisor of $P$ then $2Q^2$ is a quadratic residue mod $p$,*

*iii, if $q$ is a prime divisor of $Q$ then $-7P^2$ is a quadratic residue mod $q$.*

*Proof.* Take $Q = 1$. By Theorem 9.1, Cox [14] there are infinitely many primes $p$ of the form $p = 9u^2+64v^2$. Now we take $P$ to be products of primes $p$ of form $p = 9u^2+64v^2$. Let $p|P$, then $p = 9u^2 + 64v^2$. So $p \equiv 1 \mod 24$. Also $p = (3u)^2 + (8v)^2$. By Proposition 6.6, Chapter X, Silverman [18], 2 is a biquadratic residue mod $p$. Therefore $2Q^2$ is a biquadratic residue mod p.

□

**Theorem 4.4.1.** *Let $(P, Q)$ be a pair of positive integers satisfying the conditions of Lemma 4.4.1. Then the equation*

$$x^4 + 7P^2y^4 = 14P^2Q^2z^4 + 18Q^2w^4 \tag{4.4.1}$$

*is locally solvable for every prime number $p$, but has only integer solution $x = y = z = w = 0$.*

*Proof.* First we show that (4.4.1) is everywhere locally solvable. By Lemma 5.2, Bright [8], it is enough to show this for $p = 2, 3, 5, 7$ and $p|PQ$.

In $\mathbb{Q}_2$, we have the point $(x, y, z, w) = (0, 0, 3, \sqrt[4]{-63P^2})$.

In $\mathbb{Q}_3$, we have the point $(x, y, z, w) = (\sqrt[4]{(7Q^2 - 1)P^2}, 1, 1, 0)$.

In $\mathbb{Q}_5$, we have the point $(x, y, z, w) = (0, \sqrt[4]{2Q^2(7P^2 + 9)/(7P^2)}, 1, 1)$ when $(P^2, Q^2) \equiv$

$(1,1) \mod 5$, the point $(\sqrt[4]{14P^2Q^2+18Q^2-7P^2}, 1, 1, 1)$ when $(P^2, Q^2) \equiv (1,4)$ or $(4,1) \mod 5$, and the point $(\sqrt[4]{2Q^2(7P^2+9)}, 0, 1, 1)$ when $(P^2, Q^2) \equiv (4,4) \mod 5$.

In $\mathbb{Q}_7$, we have the point $(x, y, z, w) = (\sqrt[4]{18}\sqrt{(\frac{Q}{7})}, 0, 0, 1)$.

In $\mathbb{Q}_p$, where $p|P$, we have the point $(x, y, z, w) = (\sqrt[4]{2Q^2}\sqrt{3}, 0, 0, 1)$.

In $\mathbb{Q}_q$, where $q|Q$, we have the point $(x, y, z, w) = (\sqrt[4]{-7P^2}, 1, 0, 0)$.

Let $(x_0, x_1, x_2, x_3)$ be an integer solution of (3.4.1) with $\gcd(x_0, x_1, x_2, x_3) = 1$.

If $x_0 = 0$ then by considering $\mod 3$, (4.4.1) gives $3|x_1^4 + x_2^4$. Thus $3|x_1, x_2$, hence $3|x_3$. Therefore $3|\gcd(x_0, x_1, x_2, x_3)$.

So $x_0 \neq 0$. Similarly, we have $x_1, x_2, x_3 \neq 0$.

Now (4.4.1) has the form

$$7(x_0^2+x_1^2-4PQx_2^2)(x_0^2+Px_1^2+4PQx_2^2)+(x_0^2-7Px_1^2+12Qx_3^2)(x_0^2-7Px_1^2-12Qx_3^2) = 0.$$

So there exist non zero, coprime integers $u, v$ such that

$$u(x_0^2 - 7Px_1^2 + 12Qx_3^2) + 7v(x_0^2 + Px_1^2 - 4PQx_2^2) = 0,$$

$$u(x_0^2 + Px_1^2 + 4PQx_2^2) - v(x_0^2 - 7Px_1^2 - 12Qx_3^2) = 0.$$

Eliminating $x_0, x_1, x_2, x_3$ respectively, we get

$$(u^2 - 2uv - 7v^2)x_0^2 + (u^2 + 14uv - 7v^2)Px_1^2 + 4(u^2 + 7v^2)PQx_2^2 = 0, \quad (4.4.2)$$

$$(u^2 + 14uv - 7v^2)x_0^2 - 7(u^2 - 2uv - 7v^2)Px_1^2 + 12(u^2 + 7v^2)Qx_3^2 = 0, \quad (4.4.3)$$

$$2(u^2 + 7v^2)x_0^2 + 7(u^2 - 2uv - 7v^2)PQx_2^2 + 3(u^2 + 14uv - 7v^2)Qx_3^2 = 0, \quad (4.4.4)$$

$$-2(u^2 + 7v^2)Px_1^2 - (u^2 + 14uv - 7v^2)PQx_2^2 + 3(u^2 - 2uv - 7v^2)Qx_3^2 = 0. \quad (4.4.5)$$

Let $A = u^2 - 2uv - 7v^2$, $B = u^2 + 14uv - 7v^2$, $C = u^2 + 7v^2$. Then we have

$$Ax_0^2 + BPx_1^2 + 4CPQx_2^2 = 0, \quad (4.4.6)$$

$$Bx_0^2 - 7APx_1^2 + 12CQx_3^2 = 0, \quad (4.4.7)$$

$$2Cx_0^2 + 7APQx_2^2 + 3BQx_3^2 = 0, \tag{4.4.8}$$

$$-2CPx_1^2 - BPQx_2^2 + 3AQx_3^2 = 0. \tag{4.4.9}$$

Notice that $A, B, C \neq 0$.

The only prime divisors of Disc$(ABC)$ are 2 and 7.

Let $S = \{2, 3, 7, \infty\}$.

Write (4.4.6) in the form

$$-ABPx_0^2 - BCQ(2Px_2)^2 = (BPx_1)^2.$$

Thus for every prime $p$, then $(-ABP, -BCQ)_p = 1$.

For $p \notin S$ and $p|C$, then $p$ is odd and $p \nmid A, B$ because $p \nmid$ Disc$(ABC)$. Therefore $(-ABP, -BQ)_p = 1$. Thus

$$(-ABP, C)_p = 1 \ \forall p|C, \ p \notin S. \tag{4.4.10}$$

Similarly, writing (4.4.9) in the form $(3ABP)(Qx_3)^2 - (2BCQ)(Px_1)^2 = (BPQx_2)^2$, it follows that for $p \notin S$ and $p|C$, then

$$(3ABP, -2BCQ)_p = 1,$$

and

$$(3ABP, C)_p = 1. \tag{4.4.11}$$

From (4.4.10) and (4.4.11), $\forall p \notin S$, $p|C$

$$(-3, C)_p = 1.$$

Let $p \notin S$ and $p \not| C$. Then both $-3$ and $C$ are units in $\mathbb{Z}_p$, thus

$$(-3, C)_p = 1.$$

From the product formula of the Hilbert symbol

$$\prod_{p\in S}(-3,C)_p\prod_{p\notin S}(-3,C)_p=1.$$

Therefore

$$(-3,u^2+7v^2)_2(-3,u^2+7v^2)_3(-3,u^2+7v^2)_7(-3,u^2+7v^2)_\infty=1. \qquad (4.4.12)$$

Let $u^2+7v^2=2^m\alpha$, where $m\in\mathbb{N}$ and $\alpha$ is odd.

We have the following lemma

**Lemma 4.4.2.** $3|uv$ *and* $2\not|m$.

*Proof.* If $3\not|uv$, then $u^2\equiv v^2\equiv 1 \mod 3$. Reducing (4.4.3) $\mod 3$ gives

$$-uvx_0^2-uvx_1^2\equiv 0 \mod 3$$

thus $3|x_0,x_1$.

Now $3|x_0$, reducing (4.4.4) $\mod 3$ gives

$$uvx_2^2\equiv 0 \mod 3.$$

So $3|x_2$. Reducing (4.4.5) $\mod 3$ gives $9|3x_3^2$, thus $3|x_3$. From (4.4.1), $3|x_1$. Therefore $\gcd(x_0,x_1,x_2,x_3)>1$, a contradiction. So $3|uv$.

Assume that $2|m$ then $m=2n$ with $n\in\mathbb{N}$.

If $2|u$ and $2\nmid v$, then by looking at (4.4.3) mod 4, we have $x_0^2+x_1^2\equiv 0 \mod 4$, thus $2|x_0,x_1$.

Now $2|x_0$, by looking at (4.4.4) mod 4, we have $-x_2^2-x_3^2\equiv 0 \mod 4$, thus $2|x_2,x_3$.

So $2|\gcd(x_0,x_1,x_2,x_3)$, a contradiction.

If $2\nmid u$ and $2|v$, then by looking at (4.4.2) and (4.4.4) mod 4, we have $2|\gcd(x_0,x_1,x_2,x_3)$, a contradiction.

So $2\nmid uv$.

Case 1: $u \not\equiv v \pmod 4$. Let $u - v = 2\alpha$, where $\alpha$ odd.

Then $u^2 - 2uv - 7v^2 = (u-v)^2 - 8v^2 = 4(a^2 - 2v^2) = 4(-1 \mod 8)$. Thus

$$u^2 - 2uv - 7v^2 = -\beta^2, \tag{4.4.13}$$

where $\beta \in \mathbb{Q}_2^*$.

$u^2 + 14uv - 7v^2 = (u-v)^2 + 16uv - 8v^2 = 4(a^2 + 4uv - 2v^2) = 4(3 \mod 8)$, so

$$u^2 + 14uv - 7v^2 = 4(8k+3), \tag{4.4.14}$$

where $k \in Z$.

From (4.4.2), (4.4.13) and (4.4.14), we have

$$-\beta^2 x_0^2 + 4(8k+3)Px_1^2 + \alpha 2^{2n+2} PQx_2^2 = 0.$$

$$\Rightarrow \quad (8k+3)P(2x_1)^2 + \alpha PQ(2^{n+1}x_2)^2 = (\beta x_0)^2.$$

Because $P \equiv Q \equiv 1 \mod 8$, so $P$, $Q$ are squares in $\mathbb{Q}_2^*$. Hence

$$(8k+3, \alpha)_2 = ((8k+3)P, \alpha PQ)_2 = 1.$$

Because $(8k+3, \alpha)_2 = (-1)^{\frac{8k+3-1}{2}\frac{\alpha-1}{2}} = (-1)^{\frac{\alpha-1}{2}}$, we have

$$\alpha \equiv 1 \mod 4. \tag{4.4.15}$$

In (4.4.3), we have $-7 \equiv 1 \mod 8$. So $-7 = \gamma^2$, where $\gamma \in \mathbb{Q}_2^*$. So (4.4.3) becomes

$$4(8k+3)x_0^2 + \gamma^2(-\beta^2)Px_1^2 + 3\alpha Q 2^{2n+2} x_3^2 = 0.$$

$$\Rightarrow (8k+3)(2x_0)^2 + (3\alpha Q)(2^{n+1}x_3)^2 = P(\gamma\beta x_1)^2.$$

$P, Q$ are squares in $\mathbb{Q}_2^*$, so

$$(8k+3, 3\alpha)_2 = (8k+3, 3\alpha Q)_2 = 1.$$

Thus

$$3\alpha \equiv 1 \mod 4,$$

which contradicts (4.4.15).

Case 2: $u \equiv v \mod 4$.

If $8|u-v$, then $u-v=8l$, where $l \in \mathbb{Z}$. Thus

$$u^2+7v^2=(v+8l)^2+7v^2=8(8l^2+2lv+v^2)=8(1 \mod 2).$$

So $m=3$ is an odd number, hence $8 \not| u-v$.

Let $u-v=4b$, where $2 \not| b$. Then

$$u^2-2uv-7v^2=(u-v)^2-8v^2=8(2b^2-v^2)=2^3(1 \mod 8).$$

So $u^2-2uv-7v^2=2^3c^2$, where $c \in \mathbb{Q}_2^*$.

$$u^2+14uv-7v^2=(u-v)^2+16uv-8v^2=8(2b^2+2uv-v^2)=8(3 \mod 8),$$

so $u^2+14uv-7v^2=8(8h+3)$ with $h \in \mathbb{Z}$.

(4.4.2) becomes

$$8c^2x_0^2+8(8h+3)Px_1^2+\alpha 2^{2n+2}PQx_2^2=0.$$

$$\Rightarrow \quad -(8h+3)P(4x_1)^2-2\alpha PQ(2^{n+1}x_2)^2=(4cx_0)^2.$$

$P,Q$ are squares in $\mathbb{Q}_2^*$, so

$$(-8h-3,-2\alpha)_2=1.$$

On the other hand

$$(-8h-3,-2\alpha)_2=(-1)^{\frac{-8h-3-1}{2}\frac{-\alpha-1}{2}+\frac{(8h+3)^2-1}{8}}=(-1)^{8h^2+6h+1}=-1,$$

a contradiction. $\square$

We have $-3 \equiv 2^2 \pmod 7$, thus $-3 \in (\mathbb{Q}_7^*)^2$. Hence

$$(-3, u^2 + 7v^2)_7 = 1.$$

Also $u^2 + 7v^2 > 0$, thus

$$(-3, u^2 + 7v^2)_\infty = 1.$$

From $3|uv$ and $\gcd(u, v) = 1$, we have $u^2 + 7v^2 \in (\mathbb{Q}_3^*)^2$, hence

$$(-3, u^2 + 7v^2)_3 = 1.$$

From $2 \nmid m$, we have

$$(-3, u^2 + 7v^2)_2 = (-3, 2^m\alpha)_2 = (-1)^{\frac{m-1}{2}\frac{-3-1}{2} + \frac{m((-3)^2-1)}{8}} = -1.$$

Therefore,

$$\prod_{p\in\{2,3,7,\infty\}} (-3, u^2 + 7v^2)_p = -1,$$

which contradicts to (4.4.12). □

In Theorem 4.4.1, let $P = Q = 1$. Then we have the following theorem

**Theorem 4.4.2.** *Consider the surface* $S\colon x^4 + 7y^4 = 14z^4 + 18w^4$. *Then* $S$ *is everywhere locally solvable, and* $S$ *has no rational points except* $(0, 0, 0, 0)$. *For every odd integer* $n \geq 3$, *there is a number field* $K$ *of degree* $n$ *such that* $S$ *has a nontrivial point in* $K$.

*Proof.* The proof in Theorem 4.4.1 works when $P = Q = 1$ so we only need to show for each odd integer $n \geq 3$, there is a number field $K$ of degree $n$ such that $S$ has a nontrivial point in $K$. $S$ has a point $(x_0, y_0, z_0, w_0) = (2\theta^2+2\theta, 2\theta, \theta^2+1, \theta^2-1)$, where $\theta$ satisfies $\theta^3 + \theta^2 - 1 = 0$. The point $(x_0, y_0, z_0, w_0)$ lies in the plane $L:\ x = y + z + w$. $L$ cuts $S$ in an absolutely irreducible quartic curve $C$ of genus 3, having points in a cubic field, giving rise to a positive divisor of degree 3 on $C$. By Theorem 6.1, Coray [13], $C$ contains positive divisors of every odd degree at least 3; and then the second statement in Theorem 4.4.1 follows. $\square$

# REFERENCES

[1] W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system. I. The user language.* J. Symbolic Comput. 24(3-4): 235-265, 1997.

[2] A. Bremner,D. J. Lewis, P. Morton, *Some varieties with points only in a field extension.* Arch. Math. 43 (1984), no. 4, 344-350.

[3] A. Bremner, *Some quartic curves with no points in any cubic field.* Proc. London Math. Soc. (3) 52 (1986), no. 2, 193-214.

[4] A. Bremner, R. K. Guy, and R. J. Nowakowski, *Which integers are representable as the product of the sum of three integers with the sum of their reciprocals.* Math. Comp. 61 (1993), no. 203, 117-130.

[5] A. Bremner, R. K. Guy,*Two more representation problems.*Proc. Edinburgh Math. Soc. Vol.40 (1997), 1-17.

[6] A. Bremner, and N. Tzanakis, *On the equation* $Y^2 = X^6 + k$. Ann. Sci. Math. Quebec 35 (2011), no. 2, 153-174.

[7] A. Bremner and M. MacLeod, *An unusual cubic representation problem.* Ann. Math. Inform. 43 (2014), 29-41.

[8] M. Bright, *Computations on diagonal quartic surfaces.* Ph.D dissertation, University of Cambridge, 2002.

[9] M. Bright, *Brauer groups of diagonal quartic surfaces.* J. Symbolic Comput. 41 (2006), no. 5, 544-558.

[10] S. Brueggeman, *Integers representable by* $\frac{(x+y+z)^3}{xyz}$. Internat. J. Math. Sci, Vol.21(1998), no.1, 107-116.

[11] J. W. S. Cassels, *The arithmetic of certain quartic curves.* Proc. Roy. Soc. Edinburgh Sect. A 100 (1985), no. 3-4, 201-218.

[12] J. W. S. Cassels, *Local fields.* London Mathematical Society Student Texts, 3. Cambridge University Press, Cambridge, 1986.

[13] D. F. Coray, *Algebraic points on cubic hypersurfaces.* Acta Arith, 30 (1976), 267-296.

[14] D. A. Cox, *Primes of the form* $x^2 + ny^2$*, Fermat, class field theory, and complex multiplication. Second edition.* John Wiley and Sons, Inc., Hoboken, NJ, 2013.

[15] E. V. Flynn and J. L. Wetherell, *Finding rational points on bielliptic genus 2 curves,* Manuscripta Math. 100:4 (1999), 519-533.

[16] H. Sedrakyan, and N. Sedrakyan, *Algebraic inequalities.* Problem Books in Mathematics. Springer (2018).

[17] J. -P. Serre, *A Course in Arithmetic.* Graduate Texts in Mathematics, Vol 7, Springer (1973).

[18] J. H. Silverman, *The arithmetic of elliptic curves. Second edition.* Graduate Texts in Mathematics 106, Springer (2009).

[19] S. Siksek and M. Stoll, *Partial descent on hyperelliptic curves and the generalized Fermat equation* $x^3 + y^4 + z^5 = 0$*,* Bull. London Math. Soc. 44:1 (2012), 151-166.

[20] M. Stoll,
`https://mathoverflow.net/questions/227713/estimating-the-size-of-solutions-of-a-diophantine-equation`

[21] H. P. F. Swinnerton-Dyer, *Arithmetic of diagonal quartic surfaces II.* Proc. London Math. Soc. (3) 80 (2000), 513-544.

# APPENDIX A

## EQUATION $(X + Y + Z + W)(1/X + 1/Y + 1/Z + 1/W) = N$

I would like to thank Professor Andrew Bremner for allowing me to use his computation tables.

Table A.1: Solutions Of $(x+y+z+w)(1/x+1/y+1/z+1/w) = n$

| | | | | | |
|---|---|---|---|---|---|
| 16 | (1, 1, 1, 1 ) | 17 | ( 2, 3, 3, 4 ) | 18 | ( 1, 1, 2, 2 ) |
| 19 | ( 5, 8, 12, 15 ) | 20 | ( 1, 1, 1, 3 ) | 21 | ( 8, 14, 15, 35 ) |
| 22 | ( 1, 1, 2, 4 ) | 23 | ( 76, 220, 285, 385 ) | 24 | ( 1, 2, 3, 6 ) |
| 25 | ( 1, 1, 4, 4 ) | 26 | ( 20, 27, 39, 130) | 27 | ( 3, 7, 8, 24 ) |
| 28 | ( 2, 9, 10, 15 ) | 29 | ( 1, 1, 4, 6 ) | 30 | ( 2, 3, 10, 15 ) |
| 31 | ( 1, 4, 5, 10 ) | 32 | ( 1, 2, 6, 9 ) | 33 | ( 12, 35, 51, 140 ) |
| 34 | ( 6, 35, 40, 63 ) | 35 | ( 8, 45, 63, 84 ) | 36 | * |
| 37 | ( 1, 3, 8, 12 ) | 38 | ( 2, 3, 15, 20 ) | 39 | ( 4, 18, 20, 63 ) |
| 40 | * | 41 | ( 1, 5, 12, 12 ) | 42 | ( 1, 1, 4, 12 ) |
| 43 | ( 5, 14, 44, 77 ) | 44 | ( 2, 14, 15, 35 ) | 45 | ( 1, 1, 6, 12 ) |
| 46 | ( 6, 35, 78, 91 ) | 47 | ( 6, 28, 51, 119 ) | 48 | ( 1, 1, 3, 15 ) |
| 49 | ( 1, 2, 5, 20 ) | 50 | ( 1, 2, 9, 18 ) | 51 | ( 35, 77, 480, 528 ) |
| 52 | ( 1, 3, 4, 24 ) | 53 | ( 2, 4, 9, 45 ) | 54 | ( 1, 3, 8, 24 ) |
| 55 | ( 9, 44, 77, 234 ) | 56 | ( 6, 78, 91, 105 ) | 57 | ( 3, 6, 40, 56 ) |
| 58 | ( 2, 11, 20, 55 ) | 59 | ( 6, 65, 104, 120 ) | 60 | ( 3, 5, 6, 70 ) |
| 61 | ( 2, 7, 15, 60 ) | 62 | ( 3, 16, 45, 80 ) | 63 | ( 3, 12, 50, 75 ) |
| 64 | * | 65 | ( 2, 9, 44, 44 ) | 66 | ( 2, 2, 5, 45 ) |
| 67 | ( 1, 4, 20, 25 ) | 68 | * | 69 | ( 24, 140, 561, 595 ) |
| 70 | ( 1, 6, 21, 28 ) | 71 | ( 1, 10, 21, 28 ) | 72 | ( 1, 4, 21, 28 ) |
| 73 | ( 5, 44, 45, 198 ) | 74 | ( 28, 33, 209, 756 ) | 75 | ( 4, 7, 78, 91 ) |
| 76 | ( 1, 7, 10, 42 ) | 77 | ( 1, 5, 18, 36 ) | 78 | ( 1, 6, 28, 28 ) |
| 79 | ( 1, 3, 24, 28 ) | 80 | ( 1, 5, 9, 45 ) | 81 | ( 3, 6, 20, 116 ) |
| 82 | ( 7, 24, 112, 273 ) | 83 | ( 8, 78, 129, 344 ) | 84 | ( 1, 3, 5, 45 ) |
| 85 | ( 1, 18, 20, 36 ) | 86 | ( 5, 28, 30, 252 ) | 87 | ( 2, 4, 15, 84 ) |
| 88 | ( 2, 9, 22, 99 ) | 89 | ( 1, 1, 12, 28 ) | 90 | ( 3, 21, 80, 120 ) |
| 91 | ( 20, 21, 261, 580 ) | 92 | ( 1, 3, 12, 48 ) | 93 | ( 3, 7, 30, 140 ) |
| 94 | ( 1, 5, 8, 56 ) | 95 | ( 3, 8, 88, 99 ) | 96 | ( 1, 7, 30, 42 ) |
| 97 | ( 5, 20, 21, 276 ) | 98 | ( 1, 18, 33, 36 ) | 99 | ( 1, 4, 20, 50 ) |
| 100 | * | 101 | ( 7, 15, 220, 220 ) | 102 | ( 5, 9, 16, 240 ) |
| 103 | ( 5, 92, 110, 253 ) | 104 | * | 105 | ( 2, 44, 44, 99 ) |

| | | | | | |
|---|---|---|---|---|---|
| 106 | ( 1, 9, 20, 60 ) | 107 | ( 2, 11, 20, 132 ) | 108 | ( 3, 40, 105, 140 ) |
| 109 | ( 5, 12, 63, 280 ) | 110 | ( 14, 168, 248, 903 ) | 111 | ( 45, 60, 385, 2156 ) |
| 112 | ( 1, 14, 35, 50 ) | 113 | ( 1, 3, 16, 60 ) | 114 | ( 7, 102, 231, 374 ) |
| 115 | ( 2, 9, 52, 117 ) | 116 | ( 2, 9, 39, 130 ) | 117 | ( 1, 3, 24, 56 ) |
| 118 | ( 1, 1, 12, 42 ) | 119 | ( 2, 4, 63, 84 ) | 120 | ( 1, 2, 12, 60 ) |
| 121 | ( 1, 21, 28, 60 ) | 122 | ( 1, 12, 13, 78 ) | 123 | ( 3, 36, 136, 153 ) |
| 124 | ( 9, 154, 273, 572 ) | 125 | ( 2, 9, 13, 156 ) | 126 | ( 1, 2, 10, 65 ) |
| 127 | ( 1, 8, 27, 72 ) | 128 | ( 3, 11, 35, 231 ) | 129 | ( 1, 9, 14, 84 ) |
| 130 | ( 1, 5, 28, 70 ) | 131 | ( 7, 15, 60, 492 ) | 132 | ( 1, 2, 18, 63 ) |
| 133 | ( 5, 96, 195, 312 ) | 134 | ( 5, 8, 65, 312 ) | 135 | ( 5, 68, 102, 420 ) |
| 136 | ( 3, 11, 110, 186 ) | 137 | ( 2, 13, 57, 156 ) | 138 | ( 3, 7, 90, 180 ) |
| 139 | ( 3, 17, 80, 240 ) | 140 | ( 7, 160, 189, 540 ) | 141 | ( 3, 8, 88, 198 ) |
| 142 | ( 3, 7, 24, 238 ) | 143 | ( 1, 3, 40, 60 ) | 144 | ( 1, 21, 33, 77 ) |
| 145 | ( 3, 10, 156, 156 ) | 146 | ( 4, 5, 126, 180 ) | 147 | ( 1, 14, 33, 84 ) |
| 148 | ( 5, 7, 13, 325 ) | 149 | ( 4, 15, 152, 285 ) | 150 | ( 1, 14, 36, 84 ) |
| 151 | ( 4, 13, 85, 340 ) | 152 | ( 2, 7, 18, 189 ) | 153 | ( 4, 4, 102, 187 ) |
| 154 | ( 1, 2, 24, 72 ) | 155 | ( 8, 28, 315, 585 ) | 156 | ( 6, 42, 95, 627 ) |
| 157 | ( 1, 14, 25, 100 ) | 158 | ( 5, 11, 192, 320 ) | 159 | ( 3, 10, 140, 204 ) |
| 160 | ( 2, 49, 54, 189 ) | 161 | ( 5, 9, 210, 280 ) | 162 | ( 1, 2, 8, 88 ) |
| 163 | ( 5, 195, 256, 312 ) | 164 | ( 1, 6, 15, 110 ) | 165 | ( 3, 55, 84, 308 ) |
| 166 | ( 1, 21, 66, 66 ) | 167 | ( 5, 12, 165, 390 ) | 168 | ( 2, 7, 54, 189 ) |
| 169 | ( 1, 4, 25, 100 ) | 170 | ( 11, 15, 352, 672 ) | 171 | ( 2, 3, 75, 120 ) |
| 172 | ( 1, 24, 45, 90 ) | 173 | ( 4, 20, 27, 459 ) | 174 | ( 3, 14, 19, 342 ) |
| 175 | ( 2, 24, 136, 153 ) | 176 | ( 3, 25, 207, 225 ) | 177 | ( 6, 63, 315, 560 ) |
| 178 | ( 8, 24, 55, 870 ) | 179 | ( 12, 165, 590, 1180 ) | 180 | ( 1, 8, 56, 91 ) |
| 181 | ( 1, 4, 30, 105 ) | 182 | ( 1, 5, 18, 120 ) | 183 | ( 7, 160, 240, 777 ) |
| 184 | ( 4, 6, 75, 340 ) | 185 | ( 1, 18, 76, 76 ) | 186 | ( 2, 35, 95, 210 ) |
| 187 | ( 2, 56, 104, 189 ) | 188 | ( 7, 217, 264, 744 ) | 189 | ( 5, 195, 312, 384 ) |

| | | | | | |
|---|---|---|---|---|---|
| 190 | ( 2, 5, 18, 225 ) | 191 | ( 5, 36, 369, 410 ) | 192 | ( 3, 42, 200, 280 ) |
| 193 | ( 4, 35, 40, 553 ) | 194 | ( 12, 35, 188, 1410 ) | 195 | ( 4, 40, 264, 385 ) |
| 196 | * | 197 | ( 1, 7, 48, 112 ) | 198 | ( 9, 34, 45, 1122 ) |
| 199 | ( 2, 15, 68, 255 ) | 200 | * | 201 | ( 5, 20, 84, 654 ) |
| 202 | ( 1, 4, 14, 133 ) | 203 | ( 1, 10, 52, 117 ) | 204 | ( 1, 10, 39, 130 ) |
| 205 | ( 1, 1, 28, 70 ) | 206 | ( 3, 8, 165, 264 ) | 207 | ( 1, 5, 42, 120 ) |
| 208 | ( 2, 54, 147, 189 ) | 209 | ( 4, 189, 297, 308 ) | 210 | ( 5, 6, 77, 462 ) |
| 211 | ( 2, 15, 63, 280 ) | 212 | ( 1, 1, 15, 85 ) | 213 | ( 1, 10, 13, 156 ) |
| 214 | ( 2, 5, 42, 245 ) | 215 | ( 2, 27, 147, 216 ) | 216 | ( 3, 28, 69, 460 ) |
| 217 | ( 1, 8, 72, 108 ) | 218 | ( 1, 15, 16, 160 ) | 219 | ( 3, 7, 140, 300 ) |
| 220 | ( 1, 6, 13, 156 ) | 221 | ( 4, 184, 312, 345 ) | 222 | ( 5, 28, 396, 495 ) |
| 223 | ( 1, 4, 70, 100 ) | 224 | ( 3, 5, 42, 350 ) | 225 | ( 1, 20, 84, 105 ) |
| 226 | ( 10, 45, 792, 968 ) | 227 | ( 1, 13, 34, 156 ) | 228 | ( 1, 10, 22, 165 ) |
| 229 | ( 2, 12, 140, 231 ) | 230 | ( 1, 2, 42, 105 ) | 231 | ( 3, 8, 220, 264 ) |
| 232 | ( 1, 4, 13, 156 ) | 233 | ( 13, 405, 660, 1782 ) | 234 | ( 1, 48, 70, 105 ) |
| 235 | ( 4, 210, 245, 441 ) | 236 | ( 4, 100, 259, 525 ) | 237 | ( 3, 35, 90, 504 ) |
| 238 | ( 2, 10, 13, 325 ) | 239 | ( 4, 135, 351, 420 ) | 240 | ( 2, 9, 10, 315 ) |
| 241 | ( 1, 40, 69, 120 ) | 242 | ( 1, 5, 72, 120 ) | 243 | ( 5, 35, 88, 880 ) |
| 244 | ( 4, 21, 175, 600 ) | 245 | ( 1, 9, 20, 180 ) | 246 | ( 2, 55, 90, 315 ) |
| 247 | ( 5, 22, 341, 620 ) | 248 | ( 1, 18, 38, 171 ) | 249 | ( 5, 12, 352, 495 ) |
| 250 | ( 2, 5, 98, 245 ) | 251 | ( 2, 21, 105, 320 ) | 252 | ( 1, 14, 84, 132 ) |
| 253 | ( 1, 6, 20, 180 ) | 254 | ( 3, 114, 247, 364 ) | 255 | ( 4, 39, 87, 754 ) |
| 256 | * | 257 | ( 6, 287, 364, 819 ) | 258 | ( 5, 36, 246, 820 ) |
| 259 | ( 2, 11, 104, 312 ) | 260 | * | 261 | ( 3, 40, 42, 595 ) |
| 262 | ( 1, 7, 48, 168 ) | 263 | ( 3, 184, 228, 345 ) | 264 | ( 1, 35, 90, 126 ) |
| 265 | ( 5, 231, 420, 616 ) | 266 | ( 3, 195, 286, 286 ) | 267 | ( 3, 16, 33, 572 ) |
| 268 | ( 13, 15, 336, 1456 ) | 269 | ( 1, 20, 105, 126 ) | 270 | ( 3, 39, 98, 588 ) |

| | | | | | |
|---|---|---|---|---|---|
| 271 | ( 4, 45, 441, 490 ) | 272 | ( 6, 9, 34, 833 ) | 273 | ( 3, 115, 204, 460 ) |
| 274 | ( 1, 28, 91, 140 ) | 275 | ( 1, 3, 28, 168 ) | 276 | ( 2, 76, 165, 285 ) |
| 277 | ( 191, 836, 1463, 36290 ) | 278 | ( 10, 21, 360, 1449 ) | 279 | ( 7, 380, 570, 924 ) |
| 280 | ( 1, 3, 30, 170 ) | 281 | ( 10, 27, 80, 1755 ) | 282 | ( 6, 35, 259, 1110 ) |
| 283 | ( 1, 3, 48, 156 ) | 284 | ( 3, 5, 96, 416 ) | 285 | ( 3, 84, 290, 435 ) |
| 286 | ( 6, 275, 555, 814 ) | 287 | ( 1, 9, 44, 198 ) | 288 | ( 1, 8, 18, 216 ) |
| 289 | ( 1, 12, 22, 220 ) | 290 | ( 3, 10, 91, 546 ) | 291 | ( 11, 200, 300, 2409 ) |
| 292 | ( 5, 8, 187, 680 ) | 293 | ( 3, 35, 380, 380 ) | 294 | ( 1, 8, 27, 216 ) |
| 295 | ( 1, 10, 88, 165 ) | 296 | ( 4, 7, 189, 540 ) | 297 | ( 2, 33, 253, 264 ) |
| 298 | ( 8, 170, 561, 1496 ) | 299 | ( 3, 220, 316, 330 ) | 300 | ( 2, 78, 91, 399 ) |
| 301 | ( 4, 11, 130, 715 ) | 302 | ( 4, 168, 273, 712 ) | 303 | ( 5, 70, 72, 1176 ) |
| 304 | ( 1, 9, 11, 231 ) | 305 | ( 4, 15, 399, 532 ) | 306 | ( 6, 57, 665, 910 ) |
| 307 | ( 3, 44, 108, 682 ) | 308 | ( 4, 69, 460, 615 ) | 309 | ( 1, 48, 72, 176 ) |
| 310 | ( 1, 5, 22, 220 ) | 311 | ( 1, 8, 45, 216 ) | 312 | ( 9, 91, 990, 1430 ) |
| 313 | ( 1, 12, 120, 152 ) | 314 | ( 2, 45, 185, 360 ) | 315 | ( 2, 11, 160, 352 ) |
| 316 | ( 3, 4, 45, 468 ) | 317 | ( 6, 115, 135, 1472 ) | 318 | ( 1, 24, 75, 200 ) |
| 319 | ( 5, 19, 32, 1064 ) | 320 | ( 6, 105, 820, 861 ) | 321 | ( 18, 117, 1860, 2945 ) |
| 322 | ( 4, 15, 93, 868 ) | 323 | ( 1, 4, 100, 150 ) | 324 | * |
| 325 | ( 1, 72, 88, 154 ) | 326 | ( 1, 56, 90, 168 ) | 327 | ( 1, 21, 132, 154 ) |
| 328 | * | 329 | ( 12, 92, 182, 3003 ) | 330 | ( 3, 60, 340, 527 ) |
| 331 | ( 1, 6, 105, 168 ) | 332 | ( 3, 100, 220, 627 ) | 333 | ( 2, 24, 39, 520 ) |
| 334 | ( 3, 11, 126, 630 ) | 335 | ( 1, 10, 85, 204 ) | 336 | ( 1, 20, 84, 210 ) |
| 337 | ( 1, 34, 136, 152 ) | 338 | ( 4, 13, 340, 663 ) | 339 | ( 2, 9, 69, 460 ) |
| 340 | ( 1, 10, 34, 255 ) | 341 | ( 1, 56, 105, 168 ) | 342 | ( 1, 9, 126, 168 ) |

| | | | | | |
|---|---|---|---|---|---|
| 343 | ( 1, 10, 132, 165 ) | 344 | ( 2, 6, 33, 451 ) | 345 | ( 3, 120, 187, 680 ) |
| 346 | ( 1, 20, 104, 200 ) | 347 | ( 3, 13, 192, 624 ) | 348 | ( 3, 138, 391, 476 ) |
| 349 | ( 18, 204, 1036, 4403) | 350 | ( 1, 21, 154, 154 ) | 351 | ( 1, 3, 96, 160 ) |
| 352 | ( 3, 176, 416, 429 ) | 353 | ( 1, 45, 90, 204 ) | 354 | ( 1, 66, 66, 209 ) |
| 355 | ( 7, 352, 416, 1612 ) | 356 | ( 6, 77, 825, 1050 ) | 357 | ( 1, 5, 120, 168 ) |
| 358 | ( 2, 21, 266, 357 ) | 359 | ( 20, 111, 814, 4995 ) | 360 | ( 2, 21, 175, 450 ) |
| 361 | ( 2, 55, 132, 495 ) | 362 | ( 2, 27, 259, 378 ) | 363 | ( 5, 285, 672, 798 ) |
| 364 | ( 1, 3, 16, 240 ) | 365 | ( 1, 5, 84, 210 ) | 366 | ( 4, 45, 294, 980 ) |
| 367 | ( 3, 65, 432, 540 ) | 368 | ( 1, 15, 40, 280 ) | 369 | ( 5, 7, 56, 952 ) |
| 370 | ( 17, 21, 492, 2870 ) | 371 | ( 3, 65, 104, 860 ) | 372 | ( 2, 25, 108, 540 ) |
| 373 | ( 4, 40, 43, 1160 ) | 374 | ( 2, 65, 180, 468 ) | 375 | ( 4, 57, 660, 665 ) |
| 376 | ( 3, 65, 212, 780 ) | 377 | ( 3, 22, 220, 735 ) | 378 | ( 3, 35, 190, 798 ) |
| 379 | ( 3, 40, 129, 860 ) | 380 | ( 3, 85, 400, 600 ) | 381 | ( 5, 378, 385, 1080 ) |
| 382 | ( 1, 2, 28, 217 ) | 383 | ( 7, 259, 1110, 1204 ) | 384 | ( 1, 21, 65, 273 ) |
| 385 | ( 7, 300, 700, 1590 ) | 386 | ( 5, 24, 213, 1320 ) | 387 | ( 8, 264, 924, 1771 ) |
| 388 | ( 1, 77, 135, 165 ) | 389 | ( 4, 84, 330, 1045 ) | 390 | ( 6, 420, 645, 1204 ) |
| 391 | ( 4, 5, 116, 725 ) | 392 | ( 3, 16, 465, 496 ) | 393 | ( 6, 36, 100, 1775 ) |
| 394 | ( 8, 377, 840, 1820 ) | 395 | ( 1, 24, 150, 200 ) | 396 | ( 5, 51, 238, 1470 ) |
| 397 | ( 140, 1365, 1980, 43758 ) | 398 | ( 9, 20, 580, 1827 ) | 399 | ( 1, 12, 117, 234 ) |
| 400 | ( 3, 39, 299, 759 ) | 401 | ( 3, 39, 140, 910 ) | 402 | ( 1, 1, 42, 154 ) |
| 403 | ( 3, 4, 180, 495 ) | 404 | ( 1, 9, 25, 315 ) | 405 | ( 4, 5, 420, 462 ) |
| 406 | ( 9, 11, 420, 1540 ) | 407 | ( 1, 13, 156, 204 ) | 408 | ( 2, 114, 247, 429 ) |
| 409 | ( 2, 35, 252, 476 ) | 410 | ( 2, 60, 93, 620 ) | 411 | ( 5, 60, 117, 1638 ) |
| 412 | ( 1, 14, 66, 297 ) | 413 | ( 5, 145, 696, 1128 ) | 414 | ( 5, 210, 258, 1505 ) |

| | | | | | |
|---|---|---|---|---|---|
| 415 | ( 21, 80, 2132, 4592 ) | 416 | ( 1, 20, 33, 330 ) | 417 | ( 4, 36, 510, 935 ) |
| 418 | ( 1, 26, 33, 330 ) | 419 | ( 3, 133, 504, 576 ) | 420 | ( 2, 57, 60, 665 ) |
| 421 | ( 3, 44, 55, 1020 ) | 422 | ( 7, 24, 248, 1953 ) | 423 | ( 2, 7, 20, 580 ) |
| 424 | ( 5, 17, 140, 1428 ) | 425 | ( 4, 68, 81, 1377 ) | 426 | ( 35, 52, 1209, 7440 ) |
| 427 | ( 3, 23, 112, 966 ) | 428 | ( 1, 45, 138, 230 ) | 429 | ( 2, 28, 33, 693 ) |
| 430 | ( 3, 110, 132, 980 ) | 431 | ( 3, 13, 384, 640 ) | 432 | ( 5, 420, 533, 1148 ) |
| 433 | ( 44, 126, 2035, 11655 ) | 434 | ( 9, 68, 112, 3024 ) | 435 | (1, 7, 16, 336 ) |
| 436 | ( 1, 40, 50, 325 ) | 437o | ( 1, 6, 57, 304 ) | 438 | ( 5, 10, 72, 1305 ) |
| 439 | ( 105, 700, 13754, 25116 ) | 440 | ( 4, 7, 165, 924 ) | 441 | ( 75, 114, 6251, 13300 ) |
| 442 | ( 1, 35, 48, 336 ) | 443 | ( 9, 35, 264, 2772 ) | 444 | ( 1, 6, 33, 330 ) |
| 445 | ( 2, 140, 341, 385 ) | 446 | ( 231, 434, 4275, 59850 ) | 447 | ( 7, 224, 1056, 1716 ) |
| 448 | ( 1, 15, 35, 357 ) | 449 | ( 4, 170, 276, 1275 ) | 450 | ( 2, 85, 290, 493 ) |
| 451 | ( 5, 32, 480, 1410 ) | 452 | ( 2, 45, 94, 705 ) | 453 | ( 4, 30, 35, 1380 ) |
| 454 | ( 5, 90, 665, 1368 ) | 455 | ( 1, 56, 96, 288 ) | 456 | ( 1, 14, 90, 315 ) |
| 457 | ( 3, 19, 36, 1044 ) | 458 | ( 5, 60, 493, 1530 ) | 459 | ( 5, 136, 1020, 1032 ) |
| 460 | ( 5, 17, 300, 1428 ) | 461 | ( 3, 12, 140, 930 ) | 462 | ( 6, 344, 840, 1505 ) |
| 463 | ( 1, 11, 52, 352 ) | 464 | ( 35, 38, 896, 7296 ) | 465 | ( 5, 170, 561, 1496 ) |
| 466 | ( 5, 9, 196, 1260 ) | 467 | ( 2, 84, 301, 516 ) | 468 | ( 1, 8, 36, 360 ) |
| 469 | ( 8, 25, 264, 2475 ) | 470 | ( 2, 120, 305, 488 ) | 471 | ( 77, 168, 7880, 16500 ) |
| 472 | ( 1, 9, 66, 342 ) | 473 | ( 1, 24, 200, 225 ) | 474 | ( 4, 323, 399, 1122 ) |
| 475 | ( 3, 112, 210, 1040 ) | 476 | ( 39, 238, 360, 13923 ) | 477 | ( 1, 58, 144, 261 ) |
| 478 | ( 2, 5, 105, 560 ) | 479 | ( 1, 2, 60, 252 ) | 480 | ( 3, 5, 14, 770 ) |
| 481 | ( 8, 27, 945, 1960 ) | 482 | ( 4, 460, 621, 805 ) | 483 | ( 1, 5, 60, 330 ) |
| 484 | * | 485 | ( 84, 7315, 14345, 18120 ) | 486 | ( 2, 25, 264, 600 ) |

| | | | | | |
|---|---|---|---|---|---|
| 487 | ( 1, 8, 156, 264 ) | 488 | * | 489 | ( 1, 21, 132, 308 ) |
| 490 | ( 1, 76, 76, 323 ) | 491 | ( 8, 495, 1122, 2200 ) | 492 | ( 3, 68, 252, 1071 ) |
| 493 | ( 4, 209, 513, 1188 ) | 494 | ( 5, 18, 129, 1720 ) | 495 | ( 3, 104, 504, 819 ) |
| 496 | ( 4, 231, 390, 1300 ) | 497 | ( 1, 34, 84, 357 ) | 498 | ( 2, 180, 325, 468 ) |
| 499 | ( 3, 34, 315, 1008 ) | 500 | ( 1, 12, 78, 364 ) | 501 | ( 5, 54, 564, 1645 ) |
| 502 | ( 2, 2, 45, 441 ) | 503 | ( 7, 87, 690, 2436 ) | 504 | ( 2, 21, 29, 812 ) |
| 505 | ( 1, 110, 144, 240 ) | 506 | ( 5, 740, 740, 999 ) | 507 | ( 3, 26, 504, 819 ) |
| 508 | ( 4, 415, 660, 913 ) | 509 | ( 1, 1, 70, 180 ) | 510 | ( 31, 70, 1030, 9579 ) |
| 511 | ( 7, 20, 1071, 1530 ) | 512 | ( 2, 45, 47, 846 ) | 513 | ( 3, 88, 196, 1176 ) |
| 514 | ( 2, 231, 280, 495 ) | 515 | ( 7, 87, 770, 2436 ) | 516 | ( 3, 34, 63, 1260 ) |
| 517 | ( 2, 65, 140, 780 ) | 518 | ( 5, 90, 209, 2090 ) | 519 | ( 5, 129, 618, 1720 ) |
| 520 | ( 3, 184, 363, 968 ) | 521 | ( 1, 28, 70, 396 ) | 522 | ( 3, 4, 140, 735 ) |
| 523 | ( 9, 309, 1442, 2772 ) | 524 | ( 40, 1015, 7105, 11832 ) | 525 | ( 1, 4, 36, 369 ) |
| 526 | ( 2, 11, 187, 680 ) | 527 | ( 7, 32, 1248, 1716 ) | 528 | ( 5, 30, 799, 1410 ) |
| 529 | ( 2, 65, 165, 780 ) | 530 | ( 2, 3, 175, 450 ) | 531 | ( 3, 25, 196, 1176 ) |
| 532 | ( 3, 72, 680, 765 ) | 533 | ( 1, 42, 172, 301 ) | 534 | ( 1, 3, 84, 308 ) |
| 535 | ( 2, 152, 264, 627 ) | 536 | ( 2, 35, 308, 660 ) | 537 | ( 1, 72, 200, 252 ) |
| 538 | ( 4, 30, 645, 1204 ) | 539 | ( 11, 15, 902, 2460 ) | 540 | ( 18, 19, 1683, 3230 ) |
| 541 | ( 5, 525, 636, 1484 ) | 542 | ( 3, 55, 680, 792 ) | 543 | ( 1, 21, 68, 420 ) |
| 544 | ( 2, 11, 182, 715 ) | 545 | ( 119, 420, 550, 42075 ) | 546 | ( 3, 168, 665, 760 ) |
| 547 | ( 4, 27, 155, 1674 ) | 548 | ( 1, 42, 236, 252 ) | 549 | ( 4, 9, 68, 1377 ) |
| 550 | ( 8, 25, 792, 2475 ) | 551 | ( 219, 660, 5110, 81620 ) | 552 | ( 1, 84, 140, 315 ) |
| 553 | ( 2, 35, 259, 740 ) | 554 | ( 1, 12, 156, 338 ) | 555 | ( 9, 58, 1885, 2340 ) |

| | | | | | |
|---|---|---|---|---|---|
| 556 | ( 3, 112, 225, 1260 ) | 557 | ( 4, 9, 80, 1395 ) | 558 | ( 1, 77, 182, 286 ) |
| 559 | ( 12, 686, 1311, 4508 ) | 560 | ( 1, 9, 175, 315 ) | 561 | ( 1, 8, 216, 270 ) |
| 562 | ( 5, 609, 812, 1334 ) | 563 | ( 3, 4, 290, 660 ) | 564 | ( 6, 261, 580, 2420 ) |
| 565 | ( 15, 27, 350, 4900 ) | 566 | ( 4, 494, 585, 1140 ) | 567 | ( 20, 105, 174, 8372 ) |
| 568 | ( 1, 15, 160, 352 ) | 569 | ( 4, 117, 484, 1573 ) | 570 | ( 3, 114, 608, 928 ) |
| 571 | ( 1, 21, 140, 378 ) | 572 | ( 1, 2, 105, 270 ) | 573 | ( 4, 20, 333, 1530 ) |
| 574 | ( 5, 62, 705, 1860 ) | 575 | ( 3, 56, 630, 936 ) | 576 | * |
| 577 | ( 7, 105, 720, 2912 ) | 578 | ( 1, 9, 50, 450 ) | 579 | ( 7, 228, 437, 3192 ) |
| 580 | * | 581 | ( 7, 88, 280, 3300 ) | 582 | ( 1, 54, 224, 288 ) |
| 583 | ( 5, 87, 112, 2436 ) | 584 | ( 7, 300, 1708, 1950 ) | 585 | ( 1, 4, 30, 420 ) |
| 586 | ( 8, 111, 140, 3885 ) | 587 | ( 5, 245, 504, 2088 ) | 588 | ( 1, 30, 69, 460 ) |
| 589 | ( 1, 32, 45, 480 ) | 590 | ( 2, 28, 105, 945 ) | 591 | ( 17, 1428, 4100, 4305 ) |
| 592 | ( 1, 9, 48, 464 ) | 593 | ( 5, 36, 820, 1722 ) | 594 | ( 2, 84, 161, 897 ) |
| 595 | ( 4, 145, 580, 1566 ) | 596 | ( 3, 36, 720, 880 ) | 597 | ( 9, 126, 1540, 3300 ) |
| 598 | ( 1, 72, 192, 320 ) | 599 | ( 1, 32, 57, 480 ) | 600 | ( 1, 10, 115, 414 ) |
| 601 | ( 10, 55, 112, 4543 ) | 602 | ( 3, 252, 442, 1071 ) | 603 | ( 1, 10, 69, 460 ) |
| 604 | ( 20, 84, 679, 8730 ) | 605 | ( 1, 21, 130, 420 ) | 606 | ( 7, 35, 1326, 2142 ) |
| 607 | ( 5, 22, 245, 2156 ) | 608 | ( 6, 88, 231, 3003 ) | 609 | ( 1, 12, 56, 483 ) |
| 610 | ( 1, 10, 154, 385 ) | 611 | ( 4, 84, 162, 2025 ) | 612 | ( 1, 48, 210, 336 ) |
| 613 | ( 3, 336, 678, 791 ) | 614 | ( 1, 54, 77, 462 ) | 615 | ( 35, 187, 1890, 15708) |
| 616 | ( 4, 39, 144, 1989 ) | 617 | ( 3, 20, 418, 1155 ) | 618 | ( 2, 33, 280, 840 ) |
| 619 | ( 3, 65, 88, 1560 ) | 620 | ( 88, 621, 11891, 34776 ) | 621 | ( 2, 220, 444, 555 ) |
| 622 | ( 4, 13, 172, 1677 ) | 623 | ( 90, 561, 16380, 30940 ) | 624 | ( 2, 28, 300, 825 ) |

| | | | | | |
|---|---|---|---|---|---|
| 625 | ( 4, 81, 84, 2106 ) | 626 | ( 1, 16, 208, 360 ) | 627 | ( 1, 4, 70, 420 ) |
| 628 | ( 6, 80, 91, 3120 ) | 629 | ( 35, 1110, 1628, 18095 ) | 630 | ( 7, 18, 875, 2250 ) |
| 631 | ( 5, 240, 1240, 1584 ) | 632 | ( 4, 39, 405, 1820 ) | 633 | ( 19, 399, 3528, 7448 ) |
| 634 | ( 19, 1260, 1386, 9020 ) | 635 | ( 7, 16, 385, 2640 ) | 636 | ( 5, 12, 564, 1645 ) |
| 637 | ( 3, 32, 837, 864 ) | 638 | ( 1, 9, 180, 380 ) | 639 | ( 5, 377, 592, 2146 ) |
| 640 | ( 1, 76, 220, 330 ) | 641 | ( 39, 1144, 3504, 19184 ) | 642 | ( 2, 20, 23, 1035 ) |
| 643 | ( 11, 836, 1547, 4522 ) | 644 | ( 5, 72, 371, 2520 ) | 645 | ( 2, 207, 264, 792 ) |
| 646 | ( 17, 30, 1245, 5644 ) | 647 | ( 1, 30, 124, 465 ) | 648 | ( 1, 68, 85, 476 ) |
| 649 | ( 3, 336, 560, 1015 ) | 650 | ( 1, 21, 198, 396 ) | 651 | ( 22, 225, 2780, 9900 ) |
| 652 | ( 1, 19, 56, 532 ) | 653 | ( 5, 28, 111, 2520 ) | 654 | ( 1, 14, 60, 525 ) |
| 655 | ( 2, 57, 84, 1092 ) | 656 | ( 39, 364, 4340, 18135 ) | 657 | ( 8, 21, 145, 3480 ) |
| 658 | ( 6, 49, 225, 3150 ) | 659 | ( 2, 31, 84, 1092 ) | 660 | ( 4, 209, 504, 1848 ) |
| 661 | ( 5, 20, 884, 1717 ) | 662 | ( 1, 90, 234, 325 ) | 663 | ( 17, 52, 1716, 6630 ) |
| 664 | ( 17, 87, 3944, 5336 ) | 665 | ( 4, 318, 420, 1855 ) | 666 | ( 1, 21, 56, 546 ) |
| 667 | ( 7, 48, 1452, 2541 ) | 668 | ( 26, 2070, 5895, 9039 ) | 669 | ( 4, 48, 784, 1617 ) |
| 670 | ( 4, 20, 405, 1782 ) | 671 | ( 7, 8, 360, 2100 ) | 672 | ( 4, 476, 969, 1197 ) |
| 673 | ( 37, 168, 620, 18600 ) | 674 | ( 3, 150, 716, 1100 ) | 675 | ( 19, 126, 1740, 9135 ) |
| 676 | * | 677 | ( 1, 3, 140, 360 ) | 678 | ( 7, 55, 576, 3520 ) |
| 679 | ( 4, 31, 616, 1736 ) | 680 | * | 681 | ( 40, 1060, 1749, 22792 ) |
| 682 | ( 1, 10, 220, 385 ) | 683 | ( 33, 176, 2091, 16400 ) | 684 | ( 104, 1107, 29848, 33579 ) |
| 685 | ( 88, 425, 6732, 42075 ) | 686 | ( 21, 1295, 3420, 9324 ) | 687 | ( 1, 15, 240, 384 ) |
| 688 | ( 3, 16, 171, 1520 ) | 689 | ( 3, 3, 130, 884 ) | 690 | ( 10, 972, 1215, 4563 ) |
| 691 | ( 5, 21, 518, 2220 ) | 692 | ( 21, 2847, 3796, 7644 ) | 693 | ( 5, 52, 62, 2821 ) |

| | | | | | |
|---|---|---|---|---|---|
| 694 | ( 15, 1703, 1950, 6550 ) | 695 | ( 29, 5661, 6660, 7540 ) | 696 | ( 3, 121, 690, 1210 ) |
| 697 | ( 4, 56, 696, 1827 ) | 698 | ( 126, 420, 5915, 59995 ) | 699 | ( 11, 525, 1320, 5600 ) |
| 700 | ( 3, 75, 372, 1550 ) | 701 | ( 2, 299, 299, 780 ) | 702 | ( 2, 63, 468, 819 ) |
| 703 | ( 2, 12, 364, 819 ) | 704 | ( 1, 18, 63, 574 ) | 705 | ( 60, 175, 517, 28200 ) |
| 706 | ( 13, 28, 1365, 4810 ) | 707 | ( 9, 280, 1666, 4165 ) | 708 | ( 1, 24, 200, 450 ) |
| 709 | ( 6, 455, 819, 2880 ) | 710 | ( 1, 45, 230, 414 ) | 711 | ( 120, 1240, 6479, 68541 ) |
| 712 | ( 1, 56, 132, 504 ) | 713 | ( 4, 665, 1005, 1140 ) | 714 | ( 2, 3, 195, 650 ) |
| 715 | ( 5, 184, 221, 2990 ) | 716 | ( 7, 116, 1740, 2835 ) | 717 | ( 3, 175, 620, 1302 ) |
| 718 | ( 7, 1200, 1800, 1953 ) | 719 | ( 3, 175, 372, 1550 ) | 720 | ( 5, 72, 742, 2520 ) |
| 721 | ( 2, 40, 504, 819 ) | 722 | ( 1, 4, 99, 468 ) | 723 | ( 69, 588, 12719, 30968) |
| 724 | ( 1, 22, 33, 616 ) | 725 | ( 1, 15, 96, 560 ) | 726 | ( 1, 120, 234, 360 ) |
| 727 | ( 20, 455, 2964, 10374 ) | 728 | ( 11, 210, 715, 6552 ) | 729 | ( 1, 6, 44, 561 ) |
| 730 | ( 11, 594, 2295, 4930 ) | 731 | ( 2, 20, 132, 1155 ) | 732 | ( 3, 27, 248, 1674 ) |
| 733 | ( 3, 220, 310, 1612 ) | 734 | ( 1, 28, 58, 609 ) | 735 | ( 15, 74, 780, 8140 ) |
| 736 | ( 5, 6, 108, 1836 ) | 737 | ( 1, 24, 222, 456 ) | 738 | ( 1, 12, 156, 507 ) |
| 739 | ( 11, 209, 1508, 5928 ) | 740 | ( 21, 210, 4235, 9570 ) | 741 | ( 5, 16, 420, 2352 ) |
| 742 | ( 1, 77, 286, 364 ) | 743 | ( 31, 60, 684, 13950 ) | 744 | ( 3, 91, 416, 1632 ) |
| 745 | ( 2, 28, 315, 1035 ) | 746 | ( 1, 35, 180, 504 ) | 747 | ( 3, 28, 39, 1820 ) |
| 748 | ( 4, 265, 420, 2226 ) | 749 | ( 4, 25, 225, 2286 ) | 750 | ( 3, 99, 682, 1386 ) |
| 751 | ( 36, 3510, 10244, 12805 ) | 752 | ( 2, 3, 50, 825 ) | 753 | ( 2, 85, 204, 1164 ) |
| 754 | ( 2, 168, 357, 952 ) | 755 | ( 1, 155, 168, 420 ) | 756 | ( 3, 186, 280, 1736 ) |
| 757 | ( 2, 9, 528, 693 ) | 758 | ( 18, 2392, 5405, 5640 ) | 759 | ( 4, 231, 658, 2068 ) |
| 760 | ( 6, 215, 595, 3570 ) | 761 | ( 3, 52, 660, 1430 ) | 762 | ( 70, 1925, 5700, 43092 ) |

| | | | | | |
|---|---|---|---|---|---|
| 763 | ( 2, 95, 380, 1007 ) | 764 | ( 1, 8, 216, 450 ) | 765 | ( 3, 231, 616, 1400 ) |
| 766 | ( 12, 42, 55, 5995 ) | 767 | ( 12, 37, 126, 6300 ) | 768 | ( 4, 425, 1020, 1575 ) |
| 769 | ( 1, 35, 112, 592 ) | 770 | ( 1, 21, 88, 616 ) | 771 | ( 3, 104, 143, 1950 ) |
| 772 | ( 3, 650, 660, 975 ) | 773 | ( 49, 834, 973, 32248 ) | 774 | ( 1, 2, 65, 442 ) |
| 775 | ( 1, 84, 171, 504 ) | 776 | ( 1, 20, 294, 420 ) | 777 | ( 6, 91, 644, 3588 ) |
| 778 | ( 1, 30, 93, 620 ) | 779 | ( 3, 55, 870, 1276 ) | 780 | ( 1, 10, 165, 528 ) |
| 781 | ( 8, 665, 2520, 2945 ) | 782 | ( 2, 95, 266, 1155 ) | 783 | ( 34, 3575, 3927, 18564 ) |
| 784 | ( 1, 33, 209, 513 ) | 785 | ( 105, 2788, 22176, 53856 ) | 786 | ( 2, 75, 175, 1260 ) |
| 787 | ( 3, 408, 822, 1096 ) | 788 | ( 3, 217, 385, 1705 ) | 789 | ( 12, 812, 986, 7395 ) |
| 790 | ( 5, 36, 820, 2583 ) | 791 | ( 3, 70, 567, 1620 ) | 792 | ( 1, 39, 312, 416 ) |
| 793 | ( 19, 28, 3948, 4935 ) | 794 | ( 3, 39, 858, 1300 ) | 795 | ( 1, 4, 100, 525 ) |
| 796 | ( 3, 44, 660, 1515 ) | 797 | ( 3, 247, 380, 1710 ) | 798 | ( 1, 20, 315, 420 ) |
| 799 | ( 1, 22, 184, 552 ) | 800 | ( 78, 1155, 3014, 52745) | 801 | ( 1, 33, 120, 616 ) |
| 802 | ( 3, 84, 282, 1927 ) | 803 | ( 104, 561, 595, 60060 ) | 804 | ( 3, 110, 195, 2002 ) |
| 805 | ( 1, 2, 92, 437 ) | 806 | ( 45, 755, 4032, 28992 ) | 807 | ( 1, 48, 147, 588 ) |
| 808 | ( 1, 18, 171, 570 ) | 809 | ( 63, 124, 279, 28892 ) | 810 | ( 2, 210, 265, 1113 ) |
| 811 | ( 15, 540, 1708, 9455 ) | 812 | ( 1, 32, 270, 480 ) | 813 | ( 14, 132, 2409, 7665 ) |
| 814 | ( 23, 1130, 4068, 12995 ) | 815 | ( 9, 1270, 2540, 3420 ) | 816 | ( 3, 7, 325, 1365 ) |
| 817 | ( 34, 2457, 11908, 12852 ) | 818 | ( 45, 63, 3220, 17940 ) | 819 | ( 16, 33, 490, 8085 ) |
| 820 | ( 1, 51, 340, 408 ) | 821 | ( 60, 603, 1615, 41004 ) | 822 | ( 4, 264, 737, 2211 ) |
| 823 | ( 4, 29, 212, 2597 ) | 824 | ( 5, 1170, 1261, 1638 ) | 825 | ( 3, 98, 315, 1960 ) |
| 826 | ( 4, 140, 585, 2457 ) | 827 | ( 21, 86, 1712, 11984 ) | 828 | ( 20, 3289, 3588, 9438 ) |
| 829 | ( 6, 32, 555, 3552) | 830 | ( 5, 8, 105, 2360 ) | 831 | ( 41, 1640, 2120, 28779 ) |

| | | | | | |
|---|---|---|---|---|---|
| 832 | ( 2, 99, 385, 1134 ) | 833 | ( 1, 90, 260, 468 ) | 834 | ( 1, 21, 308, 462 ) |
| 835 | ( 29, 1092, 3689, 18564 ) | 836 | ( 3, 351, 621, 1495 ) | 837 | ( 3, 8, 484, 1320 ) |
| 838 | ( 64, 960, 19425, 29575 ) | 839 | ( 80, 1008, 8449, 52020 ) | 840 | ( 2, 100, 255, 1275 ) |
| 841 | ( 3, 140, 910, 1404 ) | 842 | ( 1, 92, 252, 483 ) | 843 | ( 1560, 637, 8, 4410 ) |
| 844 | ( 5, 492, 777, 2870 ) | 845 | ( 2, 63, 300, 1260 ) | 846 | ( 3, 210, 568, 1704 ) |
| 847 | ( 1, 8, 84, 651 ) | 848 | ( 1, 90, 156, 585 ) | 849 | ( 7, 165, 1176, 4312 ) |
| 850 | ( 1, 9, 180, 570 ) | 851 | ( 60, 2041, 22765, 24492 ) | 852 | ( 1, 84, 248, 504 ) |
| 853 | ( 105, 280, 16058, 48285 ) | 854 | ( 3, 16, 276, 1840 ) | 855 | ( 1, 11, 352, 416 ) |
| 856 | ( 15, 602, 1435, 10332 ) | 857 | ( 1, 16, 55, 720 ) | 858 | ( 8, 115, 360, 5796 ) |
| 859 | ( 8, 176, 187, 5936 ) | 860 | ( 3, 11, 616, 1386 ) | 861 | ( 7, 1071, 1122, 3740 ) |
| 862 | ( 12, 364, 1326, 8211 ) | 863 | ( 35, 54, 540, 16983 ) | 864 | ( 1, 6, 140, 588 ) |
| 865 | ( 10, 611, 2340, 5499 ) | 866 | ( 75, 2599, 20566, 39550 ) | 867 | ( 8, 475, 2100, 4200 ) |
| 868 | ( 3, 8, 129, 1720 ) | 869 | ( 1, 18, 280, 520 ) | 870 | ( 6, 296, 888, 3885 ) |
| 871 | ( 8, 1643, 2015, 3224 ) | 872 | ( 3, 14, 595, 1530 ) | 873 | ( 2, 195, 364, 1155 ) |
| 874 | ( 2, 315, 400, 1008 ) | 875 | ( 4, 87, 798, 2436 ) | 876 | ( 792, 12760, 20, 3393 ) |
| 877 | ( 1, 4, 72, 616 ) | 878 | ( 20, 24, 141, 8695 ) | 879 | ( 1, 65, 132, 660 ) |
| 880 | ( 18, 70, 1155, 11187 ) | 881 | ( 122, 168, 17400, 44225 ) | 882 | ( 3, 660, 935, 1020 ) |
| 883 | ( 20, 3589, 5994, 7857 ) | 884 | ( 9, 1332, 1406, 5092 ) | 885 | ( 1, 42, 301, 516 ) |
| 886 | ( 1, 32, 342, 480 ) | 887 | ( 65, 494, 1505, 46956 ) | 888 | ( 3, 130, 819, 1638 ) |
| 889 | ( 3, 462, 616, 1551 ) | 890 | ( 2, 11, 155, 1320 ) | 891 | ( 1, 144, 315, 420 ) |
| 892 | ( 2, 45, 235, 1410 ) | 893 | ( 3, 329, 420, 1880 ) | 894 | ( 1, 96, 288, 495 ) |
| 895 | ( 66, 280, 18165, 29064 ) | 896 | ( 9, 10, 1595, 2610 ) | 897 | ( 2, 273, 572, 924 ) |
| 898 | ( 35, 5060, 6020, 19866 ) | 899 | ( 1, 84, 357, 442 ) | 900 | * |

| | | | | | |
|---|---|---|---|---|---|
| 901 | ( 4, 35, 690, 2484 ) | 902 | ( 8, 104, 1911, 4641 ) | 903 | ( 6, 11, 40, 3135 ) |
| 904 | * | 905 | ( 5, 594, 1705, 2160 ) | 906 | ( 3, 8, 110, 1815 ) |
| 907 | ( 1, 51, 208, 624 ) | 908 | ( 2, 33, 105, 1540 ) | 909 | ( 11, 440, 2365, 6880 ) |
| 910 | ( 3, 70, 532, 1995 ) | 911 | ( 9, 180, 2660, 4921 ) | 912 | ( 1, 5, 225, 525 ) |
| 913 | ( 5439, 37, 12, 2744 ) | 914 | ( 21, 57, 1196, 12558 ) | 915 | ( 5, 222, 280, 3885 ) |
| 916 | ( 84, 445, 7476, 56035 ) | 917 | ( 2, 21, 184, 1449 ) | 918 | ( 3, 25, 1100, 1320 ) |
| 919 | ( 23, 189, 616, 17388 ) | 920 | ( 1, 48, 231, 616 ) | 921 | ( 29, 534, 812, 23100 ) |
| 922 | ( 5, 308, 1892, 2310 ) | 923 | ( 2, 68, 735, 980 ) | 924 | ( 5, 75, 1932, 2300 ) |
| 925 | ( 3, 44, 846, 1692 ) | 926 | ( 1, 12, 225, 612 ) | 927 | ( 39, 2812, 3515, 28860 ) |
| 928 | ( 2, 175, 450, 1197 ) | 929 | ( 2, 48, 51, 1616 ) | 930 | ( 1, 35, 360, 504 ) |
| 931 | ( 2, 44, 460, 1265 ) | 932 | ( 2, 33, 82, 1599 ) | 933 | ( 17, 29, 170, 9180 ) |
| 934 | ( 2, 52, 81, 1620 ) | 935 | ( 3, 220, 627, 1900 ) | 936 | ( 1, 42, 357, 510 ) |
| 937 | ( 13, 1428, 4774, 5797 ) | 938 | ( 3, 52, 440, 2145 ) | 939 | ( 1, 60, 122, 732 ) |
| 940 | ( 13, 16, 611, 6016 ) | 941 | ( 17, 493, 1740, 13050 ) | 942 | ( 1, 33, 330, 546 ) |
| 943 | ( 11, 63, 2016, 6688 ) | 944 | ( 2, 165, 246, 1435 ) | 945 | ( 3, 156, 371, 2226 ) |
| 946 | ( 1, 5, 48, 720 ) | 947 | ( 6052, 1869, 17, 7938 ) | 948 | ( 1, 40, 60, 808 ) |
| 949 | ( 2, 41, 85, 1640 ) | 950 | ( 3, 9, 828, 1288 ) | 951 | ( 7, 48, 1320, 4400 ) |
| 952 | ( 1, 14, 153, 714 ) | 953 | ( 99, 172, 24390, 34959 ) | 954 | ( 3, 77, 528, 2128 ) |
| 955 | ( 3, 390, 624, 1808 ) | 956 | ( 17, 135, 4522, 9690 ) | 957 | ( 7, 408, 1938, 4199 ) |
| 958 | ( 10, 265, 649, 8162 ) | 959 | ( 8, 315, 2850, 4275 ) | 960 | ( 1, 3, 13, 663 ) |
| 961 | ( 10, 204, 1605, 7276 ) | 962 | ( 1, 44, 297, 594 ) | 963 | ( 5, 765, 990, 2992 ) |
| 964 | ( 14, 18, 1683, 5831 ) | 965 | ( 3, 507, 660, 1690 ) | 966 | ( 3, 15, 140, 2212 ) |
| 967 | ( 1, 23, 160, 736 ) | 968 | ( 2, 25, 405, 1350 ) | 969 | ( 8, 90, 175, 6552 ) |

| | | | | | |
|---|---|---|---|---|---|
| 970 | ( 11, 1155, 1908, 7420 ) | 971 | ( 1, 4, 105, 660 ) | 972 | ( 1, 14, 34, 833 ) |
| 973 | ( 3, 115, 132, 2530 ) | 974 | ( 118, 177, 294, 54929 ) | 975 | ( 14, 99, 2296, 9471 ) |
| 976 | ( 1, 84, 350, 525 ) | 977 | ( 17, 1295, 6720, 8288 ) | 978 | ( 5, 69, 1242, 3220 ) |
| 979 | ( 35, 59, 3920, 17346 ) | 980 | ( 1, 17, 135, 765 ) | 981 | ( 3, 195, 242, 2420 ) |
| 982 | ( 94, 4756, 9541, 75153 ) | 983 | ( 16, 83, 360, 12240 ) | 984 | ( 1, 20, 36, 855 ) |
| 985 | ( 3, 112, 240, 2485 ) | 986 | ( 11, 440, 984, 9020 ) | 987 | ( 66, 2604, 9548, 50809 ) |
| 988 | ( 3, 165, 440, 2280 ) | 989 | ( 2, 175, 180, 1575 ) | 990 | ( 11, 231, 3990, 6118 ) |
| 991 | ( 40, 1265, 9867, 27048 ) | 992 | ( 2, 69, 860, 989 ) | 993 | ( 13, 21, 2808, 5096 ) |
| 994 | ( 1, 112, 272, 595 ) | 995 | ( 3, 200, 1200, 1525 ) | 996 | ( 2, 75, 805, 1050 ) |
| 997 | ( 1, 88, 178, 712 ) | 998 | ( 76, 1368, 7301, 62328 ) | 999 | ( 2, 9, 693, 924 ) |
| 1000 | ( 1, 10, 24, 840 ) | | | | |

We computed solutions of the title equation for $n = 4m^2$, $m \equiv 2 \pmod 4$, in the range $n < 20000$, and found solutions in all cases except $n = 10000$ and $n = 15376$; see Table A.2. Further, for $n = 4m^2 + 4$, $m \equiv 2 \pmod 4$, we were able to find solutions in all cases where $n < 20000$; see Table A.3.

Table A.2: Solutions Of $(x+y+z+w)(1/x+1/y+1/z+1/w) = 4m^2,\ m \equiv 2 \pmod 4$

| $n$ | $m$ | $(x, y, z, w)$ | $n$ | $m$ | $(x, y, z, w)$ |
|---|---|---|---|---|---|
| 144 | 6 | (1,21,33,77) | 400 | 10 | (3, 39, 299, 759) |
| 784 | 14 | (1,33,209,513) | 1296 | 18 | (47, 55, 1095, 30879) |
| 1936 | 22 | (17, 1813, 2205, 28305) | 2704 | 26 | (3, 651, 2415, 4991) |
| 3600 | 30 | (45, 133, 3605, 116109) | 4624 | 34 | (1, 25, 169, 4225) |
| 5776 | 38 | (1, 81, 1325, 4293) | 7056 | 42 | (1235, 2639, 735315, 5189223) |
| 8464 | 46 | (1, 121, 385, 7865) | 10000 | 50 | |
| 11664 | 54 | (5, 561, 4245, 52921) | 13456 | 58 | (13, 16245, 53361, 105105) |
| 15376 | 62 | | 17424 | 66 | (65, 4305, 5265, 1092609) |
| 19600 | 70 | (9, 589, 1833, 170469) | | | |

Table A.3: Solutions Of $(x+y+z+w)(1/x+1/y+1/z+1/w) = 4m^2+4,\ m \equiv 2 \pmod 4$

| $n$ | $m$ | $(x, y, z, w)$ | $n$ | $m$ | $(x, y, z, w)$ |
|---|---|---|---|---|---|
| 148 | 6 | (5,7,13,325) | 404 | 10 | (1,9,25,315) |
| 788 | 14 | (3, 217, 385, 1705) | 1300 | 18 | (5, 637, 1615, 4165) |
| 1940 | 22 | (1, 11, 51, 1683) | 2708 | 26 | (7, 759, 2479, 15477) |
| 3604 | 30 | (1, 91, 161, 3289) | 4628 | 34 | (13, 21, 285, 35815) |
| 5780 | 38 | (5, 29, 1653, 22895) | 7060 | 42 | (43, 121, 88451, 135235), |
| 8468 | 46 | (35, 2171, 54275, 234969) | 10004 | 50 | (1, 51, 1131, 8619) |
| 11668 | 54 | (25,41475,45899,203931) | 13460 | 58 | (55, 189, 70455, 502335) |
| 15380 | 62 | (1, 3219, 4995, 7155) | 17428 | 66 | (27, 125307, 155601, 189371) |
| 19604 | 70 | (123, 459, 2425, 1825443) | | | |

# APPENDIX B

# EQUATION $X^4 + Y^4 = DZ^4$

In both Theorem 3.3.2 and Theorem 3.3.3, we require the condition that the rank of some curves is at most 1. We give a table where cubic points are found when the rank of the curve $x^4 + y^2 = Dz^4$ is at least 2. Finding solutions to $x^4 + y^4 = Dz^4$ in cubic number fields is not easy. Our approach here is to find the cubic number field of the form $at^3 + bt^2 + xt + d$, which was proposed in Bremner [3] and Cassels [11]. We looked for cubic fields $at^3 + bt^2 + ct + d = 0$, where the equation $x^4 + y^4 = Dz^4$ has solutions. To proceed in this way, we searched for rational points in some 64 degree homogeneous variables. Computational results support the conjecture that when the rank of $x^4 + y^2 = Dz^4$ is at least 2, then there always exists a cubic point, but this seems every difficult to prove. The computation is recorded in the following table.

Table B.1: Solutions Of $x^4 + y^4 = Dz^4$, $z = t^2 + 1$

| D | Cubic equations defining t | x | y |
|---|---|---|---|
| 1777 | $-\frac{5320687}{602320}t^3 + \frac{1241317}{602320}t^2 + \frac{2597617}{602320}t + 1$ | $\frac{1}{53098}(-888723t^2 + 1558403t + 117662)$ | $\frac{1}{191}(-764t^2 + 5102t + 788)$ |
| 1873 | $-\frac{532076238522349807}{4350827579604821674}t^3 + \frac{868069163214966164}{4350827579604821674}t^2 - \frac{503067684125840327 9}{4350827579604821674}t + 1$ | $-\frac{606437152469148}{103858567341425}t^2 - \frac{128177543406547}{103858567341425}t + \frac{529523869513673}{103858567341425}$ | $-\frac{149980402}{82089865}t^2 + \frac{1608906352}{82089865}t - \frac{2946041588}{82089865}$ |
| 1889 | $\frac{340464146921478811383 6}{7601169982050224925503377}t^3 + \frac{37392986272364699738394 01}{3040467992820089970201350 8}t^2 - \frac{5358841821246864376216483}{7601169982050224925503377}t + 1$ | $-\frac{3465276609095076 88}{77363288673972050}t^2 + \frac{1695621331731884835 7}{77363288673972050}t - \frac{44941517494280046162}{77363288673972050}$ | $-\frac{3508429512}{604901640}t^2 - \frac{1943705195747}{604901640}t + \frac{5514042765442}{604901640}$ |
| 2753 | $\frac{143265249566 4}{40800233234177}t^3 + \frac{32707381153769}{40800233234177}t^2 + \frac{59802385215158}{40800233234177}t + 1$ | $-\frac{112040214}{12653550}t^2 - \frac{437879971}{12653550}t - \frac{31092181}{12653550}$ | $-\frac{572936}{204620}t^2 - \frac{5041589}{204620}t - \frac{6361759}{204620}$ |
| 2801 | $-\frac{784719925160}{5214612456061}t^3 + \frac{6219693961004}{5214612456061}t^2 + \frac{11669679283964}{5214612456061}t + 1$ | $-\frac{14760380}{11613750}t^2 - \frac{200447838}{11613750}t - \frac{27372889}{11613750}$ | $-\frac{5086835}{455835}t^2 + \frac{15189576}{455835}t + \frac{15663158}{455835}$ |
| 3137 | $-\frac{519948}{96557}t^3 + \frac{949533}{96557}t^2 - \frac{278842}{96557}t + 1$ | $-\frac{3199956}{137160}t^2 + \frac{4088495}{137160}t - \frac{826609}{137160}$ | $-\frac{5402}{254}t^2 + \frac{4301}{254}t + \frac{179}{254}$ |
| 3229 | $\frac{1575576}{2137801}t^3 + \frac{23094361}{2137801}t^2 + \frac{13652618}{2137801}t + 1$ | $-\frac{718}{1283}t^2 + \frac{127006}{1283}t + \frac{38350}{1283}$ | $-\frac{180}{36}t^2 - \frac{4751}{36}t - \frac{1451}{36}$ |
| 3649 | $-\frac{155738}{23409}t^3 + \frac{261473}{23409}t^2 - \frac{3508}{1377}t + 1$ | $-\frac{13334}{1275}t^2 + \frac{35251}{1275}t - \frac{4641}{1275}$ | $-\frac{15373}{675}t^2 + \frac{11447}{675}t + \frac{648}{675}$ |
| 4001 | $\frac{49472722}{29393679}t^3 + \frac{12826189}{1799613}t^2 + \frac{43710244}{9797893}t + 1$ | $-\frac{950274}{56433}t^2 - \frac{1795724}{56433}t - \frac{366516}{56433}$ | $-\frac{3549}{507}t^2 - \frac{23807}{507}t - \frac{8694}{507}$ |
| 4993 | $\frac{13625408059306986314693496}{66609356791482944932125159 53}t^3 + \frac{6217520526390261465182872 16}{6660935679148294493212515953}t^2 - \frac{4255745377389670505965077888}{6660935679148294493212515953}t + 1$ | $-\frac{533778361685908739 4}{813010109053557850}t^2 + \frac{754411007184061994 34}{813010109053557850}t - \frac{11615979628206349853 1}{813010109053557850}$ | $-\frac{346777873328}{177348640510}t^2 - \frac{260452641702 12}{177348640510}t + \frac{81613818831463}{177348640510}$ |
| 6353 | $-\frac{368030872}{674441021}t^3 + \frac{1558384512}{674441021}t^2 - \frac{1774757484}{674441021}t + 1$ | $-\frac{2683308664}{82123770}t^2 + \frac{7103733136}{82123770}t - \frac{4114661791}{82123770}$ | $-\frac{14446986}{483650}t^2 + \frac{30633054}{483650}t - \frac{10160939}{483650}$ |
| 6481 | $-\frac{110440}{7569}t^3 + \frac{15801}{841}t^2 - \frac{15238}{7569}t + 1$ | $-\frac{527}{20}t^2 + \frac{31983}{800}t - \frac{2393}{800}$ | $-3t^2 + \frac{387}{20}t + \frac{63}{20}$ |

| | | | |
|---|---|---|---|
| 7522 | $\frac{1761021915246340562 5}{3465265940169438989 21}t^3+\frac{1737862275421434926875}{346526594016943898921}t^2-\frac{138833387475741406719}{31502417637903990811}t+1$ | $-\frac{10145220196827}{2307626943028}t^2+\frac{300937570118302}{2307626943028}t-\frac{131724269039407}{2307626943028}$ | $-\frac{6282377092855625}{647248491480800}t^2-\frac{47530814249370002}{647248491480800}t+\frac{21414917567843063}{647248491480800}$ |
| 7537 | $\frac{-478793115}{140014628}t^3+\frac{877971339}{70007314}t^2+\frac{852368421}{140014628}t+1$ | $-\frac{152981}{7738}t^2+\frac{363105}{7738}t+\frac{80442}{7738}$ | $-\frac{6390}{1065}t^2+\frac{60906}{1065}t+\frac{15466}{1065}$ |
| 8882 | $-\frac{1253189307829367199225017199610 7}{857209049554969488421624727333 17}t^3+\frac{4552548623402371404179458646258 3}{857209049554969488421624727333 17}t^2+\frac{775403571441021980099814111907 93}{857209049554969488421624727333 17}t+1$ | $+\frac{120389005864572635737212 7}{159902332875541342451838}t^2-\frac{366957684224509975216477 8}{159902332875541342451838}t-\frac{846666671828542465486121 9}{159902332875541342451838}$ | $+\frac{900259362351500941}{141938281994105982}t^2-\frac{1326247943951450118}{141938281994105982}t-\frac{332102859432140333}{141938281994105982}$ |
| 9281 | $-\frac{123119}{4682}t^3+\frac{158196}{2341}t^2-\frac{74015}{4682}t+1$ | $\frac{1}{29}(-5654t^2+14435t-1735)$ | $\frac{1}{23}(-92t^2+t-30)$ |
| 9596 | $-\frac{1808627180499}{25009857744533}t^3+-\frac{844612424797}{25009857744533}t^2+\frac{18094138210859}{25009857744533}t+1$ | $-\frac{344224782153}{54286633458}t^2+\frac{743427722104}{54286633458}t+\frac{178784756189}{54286633458}$ | $-\frac{11977557}{736922}t^2+\frac{1682696}{736922}t+\frac{44517537}{736922}$ |
| 9649 | $\frac{2204102626544}{19142972461433}t^3+\frac{15989802592176}{19142972461433}t^2+\frac{1595414088193}{19142972461433}t+1$ | $-\frac{4122916}{437990}t^2+\frac{624389}{437990}t-\frac{2085339}{437990}$ | $-\frac{13075520107}{2371559425}t^2+\frac{9334335848}{2371559425}t-\frac{28125830693}{2371559425}$ |