Thue Equations and Related Topics

by

Shabnam Akhtari

B.Sc., Sharif University of Technology, 2002
M.Sc., Simon Fraser University, 2004
Ph.D., The University of British Columbia, 2008

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

Doctor of Philosophy

in

The Faculty of Graduate Studies

(Mathematics)

The University Of British Columbia

(Vancouver)

August, 2008

Abstract

Using a classical result of Thue, we give an upper bound for the number of solutions to a family of quartic Thue equations. We also give an upper bound upon the number of solutions to a family of quartic Thue inequalities. Using the Thue-Siegel principle and the theory of linear forms in logarithms, an upper bound is given for general quartic Thue equations.

As an application of the method of Thue-Siegel, we will resolve a conjecture of Walsh to the effect that the Diophantine equation

$$aX^4 - bY^2 = 1,$$

for fixed positive integers a and b, possesses at most two solutions in positive integers X and Y. Since there are infinitely many pairs (a, b) for which two such solutions exist, this result is sharp. It is also effectively proved that for fixed positive integers a and b, there are at most two positive integer solutions to the quartic Diophantine equation

$$aX^4 - bY^2 = 2.$$

We will also study cubic and quartic Thue equations by combining some classical methods from Diophantine analysis with modern geometric ideas.

Table of Contents

Acknowledgements

It is difficult to overstate my gratitude to my Ph.D supervisor, Professor Michael Bennett. Throughout my thesis-writing period, he provided encouragement, support and advice. I would have been lost without his help and stimulating suggestions.

I was delighted to interact with Professor Greg Martin. I enjoyed all graduate courses he offered during my time in UBC. I would like to thank him for being always so kind and helpful.

I was fortunate in having Professor Stephen Choi as my M.Sc supervisor in Simon Fraser University. He is the one who warmly welcomed me in this country and helped me find my way. I am specially thankful to him for his help and advice in finding the right place for my Ph.D study.

I am grateful to Professor David Boyd for spending his valuable time reading my thesis.

I am also grateful to Professor Ebad Mahmoudian, Professor Siavash Shahshahani and Dr. Yahya Tabesh who kindly and unforgettably made my immigration to Canada possible.

I am indebted to Dr. Hadi Jorati for his understanding, for his company and for his honest friendship.

I am very thankful to Dr. Julia Gordon for being such a good listener whenever I needed one.

Words fail me to express my appreciation to my mother, Zahra Hosseini. She is my first math teacher and the creator of my passion for Mathematics. Selfishly, I left her alone in the most difficult time of her life to pursue my graduate study. My absence was not easy for her but she went through it patiently. I owe her everything.

My lovely sisters, Shaghayegh and Nazli Akhtari, exceptionally inspire and enrich my life.

I feel a deep sense of gratitude for my father, Mansour Akhtari. His memory still provides strength and persistent courage. It is to him that I dedicate this work.

Dedication

To the memory of **Baba**.

Statement of Co-Authorship

Chapters 3 and 4 of this thesis is joint work with Dr. Togbe and Dr. Walsh. I used the method explained in Chapter 2 to solve a family of quartic equation which rises from the equation $aX^4 - bY^2 = 2$. This project was suggested to me by Dr. Walsh who had been working with Dr. Togbe on finding an upper bound for the number of integral solutions to the equation $aX^4 - bY^2 = 2$. We give an upper bound upon the number of integral solutions of $aX^4 - bY^2 = 2$ for the first time, combining the result of their previous study on the subject with my method of solving Thue equations.

Chapter 1

Introduction

In 1909, Thue [25] derived the first general sharpening of Liouville's theorem on rational approximation to algebraic numbers, proving, if θ is algebraic of degree $n \geq 3$ and $\epsilon > 0$, that there exists a constant $c(\theta, \epsilon)$ such that

$$\left|\theta - \frac{p}{q}\right| > \frac{c(\theta, \epsilon)}{q^{\frac{n}{2}+1+\epsilon}}$$

for all $p \in \mathbb{Z}$ and $q \in \mathbb{N}$.

In the intervening years, Thue's result has been improved and generalized by several mathematicians. In 1921, Siegel [21] showed that

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{q^{\kappa}} \tag{1.1}$$

has at most finitely many solutions if $\kappa > 2n^{1/2}$. In 1940s, Dyson [10] and Gelfond [13] independently improved this to $\kappa > (2n)^{1/2}$. Finally in 1955, Roth reduced this condition to $\kappa > 2$. Roth's result is best possible, in the sense that we cannot replace the inequality $\kappa > 2$ with $\kappa = 2$. The following theorem is an almost immediate consequence of Thue's result

Theorem 1.0.1 (Thue)**.** *Let $F(x, y)$ be an irreducible binary form in $\mathbb{Z}[x, y]$ of degree at least three and m a nonzero integer, then the equation*

$$F(x, y) = m \tag{1.2}$$

has only finitely many integer solutions (x, y).

To prove this theorem, apply Thue's inequality to the roots of

$$F(x, 1) = 0$$

(see chapter III of [22] for a complete proof). Equations (1.2) are often called Thue equations, in honour of Axel Thue. Another proof of Theorem 1.0.1 was given by Skolem in 1935 [23] using p-adic power series, under certain weak restrictions imposed on F. Nevertheless all of these results, starting from that of Thue, are *ineffective*. In general they do not supply an algorithm to compute all solutions of (1.2). This means that the constant $c(\theta, \epsilon)$ in the Thue theorem, or constants in any other of its improvements, can not be determined explicitly from the proof as can be done in Liouville's theorem. Baker's method (1966) for bounding linear forms in logarithms of algebraic numbers provides an effective, but slight improvement over the Liouville's theorem and thus an explicit upper bound for the solutions of (1.2).

In this thesis, we are mainly interested in upper bounds for the number of solutions to equation (1.2) with degree 4. We will apply ineffective methods similar to those of Thue and Siegel, since they seem to lead to far better estimates in this context than those corresponding to, for instance, the theorem of Roth. In Thue and Siegel's papers, the construction of auxiliary polynomials, at least for some algebraic numbers α, was completely explicit, based on the method of Padé approximations and hypergeometric polynomials. The method of Padé approximations and evaluation of asymptotics of auxiliary polynomials gives precise values for all constants, and allows one to start with a "good" approximation of a relatively small height.

In 1983, J.H. Evertse showed that indeed the number of primitive solutions to (1.2), for irreducible F of degree $n \geq 3$, could be bounded by a function depending only on n and m, but otherwise independent of F. Evertse [12] obtains the bound

$$7^{15\left(\binom{n}{3}m+1\right)^2} + 6 \times 7^{2\binom{n}{3}m(\nu+1)}$$

for the number of primitive solutions of (1.2), where ν is the number of prime factors of the constant term m. This is a special case of Evertse's results as he also treats equations in number fields.

There has developed an extensive body of literature devoted to explicitly solving Thue equations, or bounding the number of such integral solutions; in the latter regard, we mention a result of Bombieri and Schmidt [6]:

Theorem 1.0.2. *If F is an irreducible binary form of degree n and m is a nonzero integer, then the number of primitive solutions to the Diophantine equation (1.2) is not greater than*

$$c_0 n^{1+\nu},$$

where c_0 is an absolute constant, ν is the number of distinct prime factors of m.

Further advances on the number of solutions to Thue equations and inequalities were made by Stewart [24].

Theorem 1.0.3. *Let F be an irreducible binary form of degree n and m be a given integer. The number of solutions of the Thue inequality*

$$|F(x, y)| \leq m$$

is at most

$$nm^{2/n}(1 + \log m^{1/n}).$$

The argument of Bombieri and Schmidt [6] implies that if N is the corresponding upper bound in the special case $m = 1$, then Nn^{ν} is an upper bound for the number of solutions to (1.2). This makes the Thue equation

$$F(x, y) = 1$$

of special interest.

If F is a linear form, $F(x, y) = ax + by$ say, then (1.2) has solutions in integer (x, y) if and only if the greatest common denominator d of a and b divides m. Moreover, if (x_0, y_0) is one solution of (1.2), then the other solutions of (1.2) are given by

$$x = x_0 + \frac{tb}{d}, \quad y = y_0 - \frac{ta}{d},$$

where t runs through the non-zero integers.

If F is a quadratic form of positive discriminant D, then (1.2) has either no solutions or infinitely many. To decide whether (1.2) has solutions or not, one may use the continued fraction expansion of $\sqrt{D}$ (see [14] for details).

If F is a quadratic form of negative discriminant D then (1.2) has at most finitely many solutions. This is because each solution (x, y) to

$$ax^2 + bxy + cy^2 = m$$

will satisfy

$$(2ax + by)^2 - Dy^2 = 4am,$$

thus

$$|y| \leq \left|\frac{4am}{D}\right|^{1/2}.$$

Dirichlet gave an upper bound for the number of solutions to (1.2), when F is a quadratic form with negative discriminant (see [9]).

The first important result on the number of solutions of cubic Thue equations was obtained by Siegel. Nagell [17] and Delone [8] independently showed that (1.2) has at most five solutions in integers x, y where F is a cubic irreducible binary form with negative discriminant. This bound is sharp, for if

$$F(x, y) = x^3 - xy^2 + y^3$$

then F has discriminant -23 and the equation

$$F(x, y) = 1$$

has 5 solutions, namely $(1, 0)$, $(0, 1)$, $(-1, 1)$, $(1, 1)$ and $(4, -3)$. Cubic Thue equations with positive discriminant have been treated in several papers including [11], [5] and [18]. We will adjust and use the ideas and techniques from these three papers to obtain new results for quartic Thue equations.

The problem of determining upper bound for the number of integer points on elliptic curves has received considerable attention. Ljunggren derived remarkable sharp bounds for the number of solutions to various quartic Diophantine equations, particularly those of the shape

$$aX^4 - bY^2 = \pm 1.$$

However, for general a and b, there had previously been no absolute upper bound for the number of integral solutions to

$$aX^4 - bY^2 = 1.$$

In Chapter 2, we will reduce this equation to a quartic Thue inequality and will apply the method of Chapter 1 to solve the inequality.

Mordell [16], shows that all the rational points of a cubic curve

$$f(x, y, z) = 0$$

of genus one, can be found from a finite number by the chord and tangent process. To prove this, he first explains how the problem is equivalent to that of finding the integer solutions in x, y, z of an equation with integer coefficients:

$$ax^4 + bx^3y + cx^2y^2 + dxY^3 + ey^4 = z^2.$$

This fact motivates Chapters 1 and 4 of this thesis. Here we will give a survey of the contents of this thesis.

Chapter 2 [3] is inspired by a paper of J.H. Evertse [11] and its improvement by M.A. Bennett [5], where the method of Thue-Siegel is used to give an upper bound for the number of solutions to cubic Thue equations. In Chapter 1, we give an upper bound for the number of solutions to a family of quartic Thue equations. We also give an upper bound upon the number of solutions to a family of quartic Thue inequalities.

Chapter 3 [2] resolves a conjecture of P.G. Walsh and sharpens classical work of W. Ljunggren. The main result is

Theorem 1.0.4. *Let a and b be positive integers. Then equation*

$$aX^4 - bY^2 = 1 \tag{1.3}$$

has at most two solutions in positive integers (X, Y).

Since there are infinitely many pairs (a, b) for which two such solutions exist, this result is best possible.To obtain the main result of [2] , we have appealed to classical results of Thue from the theory of Diophantine approximation, together with modern refinements, particularly those of Evertse. We apply these techniques to particular families of quartic inequalities (the general machinery is developed in [3]). Similar arguments lead to the result of Chapter 4 [4], on the equation $aX^4 - bY^2 = 2$, which arose from communication with P.G. Walsh. Chapter 5 is a short chapter explaining how the result of Chapter 4 can be extended to a more general family of equations.

In Chapter 6 [1], we combine techniques from Algebraic Number Theory with the theory of linear forms in logarithms (Baker's method), to obtain a clearer view of the geometry of quartic Thue equations. Chapter 4 presents an extension of some geometric ideas of Okazaki [18] and an application of Stewart's method [24] for Thue equations with arbitrary degree n to quartic ones.

In Chapter 7, we will give a survey of the know results for cubic Thue equations and we'll give slight improvment to them. We will study different methods used to give an upper bound for the number of integral solutions to cubic Thue equations.

In Chapter 8, our concluding chapter, we discuss our future plans for research along the lines of this thesis.

Bibliography

[1] S. Akhtari. Geometry of quartic Thue equations. preprint.

[2] S. Akhtari. The Diophantine equation $aX^4 - bY^2 = 1$. to appear in J. Reine Angew. Math. (2008).

[3] S. Akhtari, The method of Thue-Siegel for binary quartic forms. submitted (2007).

[4] S. Akhtari, A. Togbe and G. Walsh. The Diophantine equation $aX^4 - bY^2 = 2$. to appear in Acta. Arith.(2008).

[5] M.A. Bennett. On the representation of unity by binary cubic forms. Trans. Amer. Math. Soc. 353 (2001), 1507-1534.

[6] E. Bombieri and W.M. Schmidt. On Thue's equation. Invent. Math. 88 (1987), 69-81.

[7] G.V. Chudnovsky. On the method of Thue-Siegel. Ann. of Math. II Ser. 117 (1983), 325-382.

[8] B.N. Delone. Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante, Math. Zeitschr. 31 (1930), 1-26.

[9] P.G.L. Dirichlet. Vorlesungen über zahlentheorie, 4th ed., Vieweg & Sohn, Braunschweig (1894).

[10] F.J. Dyson. The approximation of algebraic numbers by rationals, Acta Math.79 (1947), 225-240.

[11] J.H. Evertse. On the representation of integers by binary cubic forms of positive discriminant. Invent. Math.73(1983), 117-138.

[12] J.H. Evertse. Upper bounds for the number of solutions of Diophantine equations. Math. Centrum. Amsterdam(1983).

[13] A.O. Gelfond. Transcendental and Algebraic Numbers. Dover pub. New York (1960).

[14] L.K. Hua. Introduction to Number Theory, Springer Verlag, Berlin, Heidelberg, New York (1982).

[15] W. Ljunggren. On the representation of integers by certain binary cubic and biquadratic forms. Acta. Arith. XVII (1971).

[16] L.J. Mordell. On the rational solutions of indeterminate equations of the 3rd and 4th degrees. Proc. Camb. Phil. Soc.21 (1922), 179-192.

[17] T. Nagell. Darstellung ganzer Zahlen durch bind̈re kubischr formen mit negativer Diskriminante, Math. Zeitscher. 28 (1928), 10-29.

[18] R. Okazaki. Geometry of a cubic Thue equation, Publ. Math. Debrecen. 61 (2002),267-314.

[19] K.F. Roth. Rational approximation to algebraic numbers, Mathematika 2 (1955) 1-20.

[20] C.L. Siegel. Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Wiss. 1 (1929).

[21] C.L. Siegel. Approximation algebraischer Zahlen, Math. Zeitschr. 10 (1921), 173-213.

[22] W.M. Schmidt, Diophantine Approximations and Diophantine Equations, Lecture Notes in Mathematics, Springer Verlag (2000).

[23] Th. Skolem, Einige Sätze über p-adische Potenzreihen mit Anwendung auf gewisse exponentielle Gleichungen, Math. Ann. 111 (1935), 399-424.

[24] C. L. Stewart, On the number of solutions of polynomial congruences and Thue equations, J. Amer. Math. Soc., 4 (1991), 793-838.

[25] A. Thue. Über Annäherungenswerte algebraischen Zahlen. J. reine angew. Math. 135 (1909), 284-305.

Chapter 2

The Method Of Thue-Siegel For Binary Quartic Forms [1]

2.1 Introduction

In 1909, Thue [17] proved that if $F(x, y)$ is an irreducible binary form of degree at least 3 with integer coefficients, and h a nonzero integer, then the equation $F(x, y) = h$ has only finitely many solutions in integers x and y .

In this paper we will consider irreducible binary quartic forms with integer coefficients, i.e. polynomials of the shape

$$F(x, y) = a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4.$$

The discriminant D of F is given by

$$D = a_0^6(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_1 - \alpha_4)^2(\alpha_2 - \alpha_3)^2(\alpha_2 - \alpha_4)^2(\alpha_3 - \alpha_4)^2,$$

where α_1 , α_2, α_3 and α_4 are the roots of

$$F(x, 1) = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4.$$

The invariants of F form a ring, generated by two invariants of weights 4 and 6, namely

$$I = I_F = a_2^2 - 3a_1a_3 + 12a_0a_4$$

and

$$J = J_F = 2a_2^3 - 9a_1a_2a_3 + 27a_1^2a_4 - 72a_0a_2a_4 + 27a_0a_3^2.$$

These are algebraically independent and every invariant is a polynomial in I and J. For the invariant D, we have

$$27D = 4I^3 - J^2.$$

[1] A version of this paper has been submitted for publication. Akhtari. S. The Method Of Thue-Siegel For Binary Quartic Forms.

In what follows, we will just consider the forms F for which the quantity J_F is 0; i.e. for which we have

$$27D = 4I^3.$$

Let h be a positive integer. The number of solutions in integers x and y of the equation

$$|F(x, y)| = h. \tag{2.1}$$

will be the focus of our study in this paper.

Theorem 2.1.1. *Let $F(x, y)$ be an irreducible binary quartic form with integer coefficients and positive discriminant that splits in $\mathbb{R}$. If $J_F = 0$, then the Diophantine equation $|F(x, y)| = 1$ possesses at most 12 solutions in integers x and y (with (x, y) and $(-x, -y)$ regarded as the same) .*

Each positive definite form is equivalent to a reduced form (see [8]). We give the definition of reduced form in section 2.7.

Theorem 2.1.2. *Let $F(x, y)$ be a reduced irreducible binary quartic form with integer coefficients and positive discriminant that splits in $\mathbb{R}$. If $J_F = 0$, then the inequality $|F(x, y)| \leq h$ possesses at most 12 solutions (x, y), with $|y| \geq \frac{2h^{3/4}}{(3I)^{1/8}}$.*

In section 2.2, we will show that to apply a classical theorem of Thue [17] from Diophantine approximation to a quartic form F, one needs to assume $J_F = 0$. Another reason for us to be interested in these results, despite what are apparently quite serious restriction upon F, is that we know important families of quartic forms with these properties. For example a solution to the equation $aX^4 - bY^2 = 1$ gives rise to a solution to the Thue equation

$$x^4 + 4tx^3y - 6tx^2y^2 - 4t^2xy^3 + t^2y^4 = t_1^2,$$

where $t_1 | t$. We have applied the methods of this paper to treat the above Thue equation in [1].

The method of Thue and Siegel based on Padé approximation to binomial functions has been used to study binary cubic forms with positive discriminant, for decades. In 1939, Krechmar [10] showed that when the discriminant of quartic form $F(x, y)$ is sufficiently large ($D_F \gg h^{216/5}$), the equation

$$F(x, y) = h$$

has at most 20 solutions in integers x and y, provided that $J_F = 0$ and all roots of $F(x, 1)$ are real numbers.

2.2 The Method Of Thue-Siegel

The relationship between a system of approximations to an arbitrary cubic irrationality and Padé approximations to $\sqrt[3]{1-x}$ was first established by Thue [19]. Siegel [12], [13] extended Thue's result [19], via hypergeometric polynomials to sharpen the bounds for the number of solutions of Diophantine equation $f(x,y) = k$, for certain binary forms $f(x,y)$ of degree r. He also established bounds for the number of solutions to

$$ax^n - by^n = c,$$

where $n \geq 3$ [14].

To find an upper bound for the number of solutions to $F(x,y) = 1$, we use the method of Thue-Siegel which is based on the following result of Thue.

Lemma 2.2.1. *Suppose that $P(x)$ is a polynomial of degree n and there is a quadratic polynomial $U(x)$ such that*

$$U(x)P''(x) - (n-1)U'(x)P'(x) + \frac{n(n-1)}{2}U''(x)P(x) = 0. \tag{2.2}$$

Let

$$Y(x) = 2U(x)P'(x) - nU'(x)P(x)$$

and

$$h = \frac{n^2-1}{4}\big(U'(x)^2 - 2U(x)U''(x)\big).$$

Consider the recurrences

$$P_{r+1}(x) = k_r Y(x)P_r(x) - P(x)^2 P_{r-1}(x);$$

$$Q_{r+1}(x) = k_r Y(x)Q_r(x) - P(x)^2 Q_{r-1}(x),$$

with the initial conditions

$$P_0(x) = Q_0(x) = \frac{2}{3}h,$$

$$P_1(x) = U(x)P'(x) - \frac{n-1}{2}U'(x)P(x),$$

$$Q_1(x) = xP_1(x) - U(x)P(x),$$

where

$$c_1 = \frac{3}{2},\ c_2 = \frac{2(2n-1)(2n+1)}{3(n-1)(n+1)}h,\ k_r c_r = \frac{2r+1}{2}$$

and

$$\frac{c_{r+1}-c_{r-1}}{k_r} = 2h\frac{n^2}{(n-1)(n+1)}.$$

Then polynomials $P_r(x)$, $Q_r(x)$ are of degree $rn+1$ and satisfy equation

$$\alpha P_r(x) - Q_r(x) = (x-\alpha)^{2r+1}R_r(x)$$

for a polynomial $R_r(x)$.

To apply Theorem 2.2.1 to the polynomial $P(x) = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$, suppose that for a quadratic polynomial $U(x) = u_2x^2 + u_1x + u_0$, we have

$$\begin{aligned} 0 &= U(x)P''(x) - 3U'(x)P'(x) + 6U''(x)P(x) \\ &= (12a_0u_0 - 3a_1u_1 + 2a_2u_2)x^2 + (6a_1u_0 - 4a_2u_1 + 6a_3u_2)x \\ &\quad +2a_2u_0 - 3a_3u_1 + 12a_4u_2. \end{aligned}$$

This implies that

$$\begin{pmatrix} 12a_0 & -3a_1 & 2a_2 \\ 3a_1 & -2a_2 & 3a_3 \\ 2a_2 & -3a_3 & 12a_4 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \end{pmatrix} = 0.$$

Therefore,

$$\begin{aligned} &\det \begin{pmatrix} 12a_0 & -3a_1 & 2a_2 \\ 3a_1 & -2a_2 & 3a_3 \\ 2a_2 & -3a_3 & 12a_4 \end{pmatrix} \\ &= 4(2a_2^3 - 9a_1a_2a_3 + 27a_1^2a_4 - 72a_0a_2a_4 + 27a_0a_3^2) \\ &= 4J = 0. \end{aligned}$$

In this paper, we always suppose that $J = 0$. In section 2.5, we will show that if $J_F = 0$ then there are linear forms $\xi = \xi(x,y)$ and $\eta = \eta(x,y)$ so that

$$F(x,y) = \frac{-1}{8\sqrt{3IA_4}}\left(\xi^4 - \eta^4\right).$$

We will use Padé approximation via hypergeometric polynomials to approximate $\frac{\eta}{\xi}$ with rational numbers. The main idea here is to replace the construction of a family of dense approximations to $\frac{\xi}{\eta}$, by a family of rational approximations to the function $(1-z)^{1/4}$. Consider the system of linear forms $R_r(z) = -Q_r(z) + (1-z)^{1/4}P_r(z)$ that approximate $(1-z)^{1/4}$ at $z=0$, such that $R_r(z) = z^{2r+1}\bar{R}_r(z)$, $\bar{R}_r(z)$ is regular at $z=0$, and $P_r(z)$ and $Q_r(z)$ are polynomials of degree r. Thue [16], [18] explicitly found polynomials $P_r(z)$ and $Q_r(z)$ (see Lemma 2.2.1) and Siegel [12] identified them in terms of hypergeometric polynomials. Refining the method of Siegel, Evertse [9] used the theory of hypergeometric functions to give an upper bound for the number of solutions to the equation $f(x,y)=1$, where f is a cubic binary form with positive discriminant. Here we adjust Lemma 4 of [9] for quartic forms.

Lemma 2.2.2. *Let r, g be integers with $r \geq 1$, $g \in \{0,1\}$. Put*

$$\begin{aligned} A_{r,g}(z) &= \sum_{m=0}^{r} \binom{r-g+\frac{1}{4}}{m}\binom{2r-g-m}{r-g}(-z)^m, \\ B_{r,g}(z) &= \sum_{m=0}^{r-g} \binom{r-\frac{1}{4}}{m}\binom{2r-g-m}{r}(-z)^m. \end{aligned} \tag{2.3}$$

(i) There exists a power series $F_{r,g}(z)$ such that for all complex numbers z with $|z|<1$

$$A_{r,g}(z) - (1-z)^{1/4}B_{r,g}(z) = z^{2r+1-g}F_{r,g}(z) \tag{2.4}$$

and

$$|F_{r,g}(z)| \leq \frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}}(1-|z|)^{-\frac{1}{2}(2r+1-g)}. \tag{2.5}$$

(ii) For all complex numbers z with $|1-z| \leq 1$ we have

$$|A_{r,g}(z)| \leq \binom{2r-g}{r}. \tag{2.6}$$

(iii) For all complex numbers $z \neq 0$ and for $h \in \{1,0\}$ we have

$$A_{r,0}(z)B_{r+h,1}(z) \neq A_{r+h,1}(z)B_{r,0}(z). \tag{2.7}$$

Proof. This lemma has been proven in [1]. □

2.3 Equivalent Forms

We will call forms F_1 and F_2 equivalent if they are equivalent under $SL_2(\mathbb{Z})$-action (i.e. if there exist integers b, c, d and e such that

$$F_1(bx + cy, dx + ey) = F_2(x, y)$$

for all x and y, where $be - cd = \pm 1$). Denote by N_F the number of solutions in integers x and y of the Diophantine equation

$$|F(x, y)| = h.$$

Note that if F_1 and F_2 are equivalent, then $N_{F_1} = N_{F_2}$, $I_{F_1} = I_{F_2}$ and $J_{F_1} = J_{F_2}$.

Let us define, for a quartic form F, an associated quartic form, the Hessian H, by

$$H(x, y) = \frac{\delta^2 F}{\delta x^2}\frac{\delta^2 F}{\delta y^2} - \left(\frac{\delta^2 F}{\delta x \delta y}\right)^2.$$

Then

$$H(x, y) = A_0 x^4 + A_1 x^3 y + A_2 x^2 y^2 + A_3 x y^3 + A_4 y^4,$$

where

$$\begin{aligned} A_0 &= 3(8a_0a_2 - 3a_1^2), \\ A_1 &= 12(6a_0a_3 - a_1a_2), \\ A_2 &= 6(3a_1a_3 + 24a_0a_4 - 2a_2^2), \\ A_3 &= 12(6a_1a_4 - a_2a_3), \\ A_4 &= 3(8a_2a_4 - 3a_3^2). \end{aligned} \tag{2.8}$$

We have the following identities (see Proposition 5 of [8]):

$$I_H = 12^2 I_F^2, \tag{2.9}$$

$$J_H = 12^3(2I_F^3 - J_F^2)$$

and

$$D_H = 12^6 J_F^2 D_F,$$

where H is the Hessian of F and D_F, D_H are the discriminants of F and H, respectively . We note that

$$A_0A_3^2 - A_4A_1^2 = 12^3(a_0a_3^2 - a_4a_1^2)J_F$$

and

$$A_3^3 + 8A_1A_4^2 - 4A_2A_3A_4 = 12^3(a_3^3 + 8a_1a_4^2 - 4a_2a_3a_4)J_F.$$

When $J_F = 0$, we obtain

$$\begin{aligned} A_0A_3^2 &= A_4A_1^2, \\ A_3^3 + 8A_1A_4^2 &= 4A_2A_3A_4. \end{aligned} \tag{2.10}$$

Therefore,

$$\begin{aligned} H(x,y) &= A_0x^4 + A_1x^3y + A_2x^2y^2 + A_3xy^3 + A_4y^4 \\ &= \frac{1}{4A_3^2A_4}(2A_1A_4x^2 + A_3^2xy + 2A_4A_3y^2)^2, \end{aligned}$$

when $A_3A_4 \neq 0$. Whereby, from (2.9),

$$\left|A_3^4 - 16A_1A_4^2A_3\right| = \left|48A_3^2A_4I_F\right|. \tag{2.11}$$

In order to make good use of the above identities, we prove the following lemma:

Lemma 2.3.1. *Let $F(x,y)$ be a quartic form with $J_F = 0$. There exists a form equivalent to $F(x,y)$, for which $A_3A_4 \neq 0$.*

Proof. If $A_4 = 0$, then by (2.10) we have $A_4 = A_3 = 0$ and therefore,

$$H(x,y) = x^2(A_0x^2 + A_1xy + A_2y^2).$$

Let

$$x = mX + lY$$

and

$$y = pX + qY,$$

where m, l, p and q are integers satisfying $mq - lp = \pm 1$. Suppose that $\phi(X,Y)$ is equivalent to $F(x,y)$ under this substitution with Hessian

$$H_\phi(X,Y) = A'_0X^4 + A'_1X^3Y + A'_2X^2Y^2 + A'_3XY^3 + A'_4Y^4.$$

We have,

$$A'_4 = H_\phi(0,1) = H_F(l,q) = l^2(A_0l^2 + A_1lq + A_2q^2).$$

We have assumed that $F(x,y)$ is irreducible, hence $H_F(x,y)$ is not identically zero. Therefore, the integers l and q can be chosen so that $A'_4 \neq 0$.

Let $t \in \mathbb{Z}$ and put

$$M = m + lt,$$

$$P = p + qt.$$

Let $\phi(X, Y)$ be the equivalent form to $F(x, y)$ under the substitution

$$x = MX + lY$$

and

$$y = PX + qY.$$

Then

$$\begin{aligned} A'_3 &= 4Ml^3A_0 + (l^3P + 3Ml^2q)A_1 + (2l^2Pq + 2Mlq^2)A_2 \\ &\quad +(q^3M + 3Pq^2l)A_3 + 4Pq^3A_4 \\ &= (m + lt)(4l^3A_0 + 3l^2qA_1 + 2lq^2A_2 + q^3A_3) \\ &\quad +(p + qt)(l^3A_1 + 2l^2qA_2 + 3lq^2A_3 + 4q^3A_4) \\ &= K + 4t(l^4A_0 + l^3qA_1 + l^2q^2A_2 + lq^3A_3 + q^4A_4) \\ &= K + 4tA'_4. \end{aligned}$$

Since $A'_4 \neq 0$, the integer t can be chosen so that $A'_3 \neq 0$. □

In the following, we will show that $F(x, y)$ or one of its equivalences (under $GL_2(\mathbb{Z})$-action) satisfies

$$|A_4| < 4I.$$

From now on, we will suppose that $A_3A_4 \neq 0$. Let

$$x = mX + lY$$

and

$$y = pX + qY,$$

where m, l, p and q are integers satisfying $mq - lp = \pm 1$. Let $\phi(X, Y)$ be equivalent to $F(x, y)$ under this substitution and

$$\phi(X, Y) = a'_0X^4 + a'_1X^3Y + a'_2X^2Y^2 + a'_3XY^3 + a'_4Y^4.$$

We observe that

$$A'_4 = H_\phi(0, 1) = H_F(l, q),$$

where $H_\phi(X, Y) = A'_0X^4 + A'_1X^3Y + A'_2X^2Y^2 + A'_3XY^3 + A'_4Y^4$.

To continue, we will be in need of the following Proposition due to Hermite.

Proposition 2.3.2. *Suppose that* $f_{11}x^2 + 2f_{12}xy + f_{22}y^2$ *is a binary form with* $D = f_{11}f_{22} - f_{12}^2 \neq 0$. *Then there is an integer pair* $(u_1, u_2) \neq (0, 0)$ *for which*

$$0 < |f_{11}u_1^2 + 2f_{12}u_1u_2 + f_{22}u_1^2| < \sqrt{\frac{4}{3}|D|}.$$

Proof. See [5], page 31. □

Proposition 2.3.2 implies that we can choose l and q, such that

$$\begin{aligned} 0 < |A_4'| &= \frac{1}{|4A_3^2A_4|}(2A_1A_4l^2 + A_3^2lq + 2A_4A_3q^2)^2 \\ &< \frac{1}{|4A_3^2A_4|}\left|\frac{1}{3}(A_3^4 - 16A_1A_4^2A_3)\right| \\ &= 4I, \end{aligned}$$

where the last equality comes from (2.11).

2.4 Reduction To A Diagonal Form

Our goal in this section will be to reduce the problem at hand to consideration of diagonal forms over a suitable imaginary quadratic field. The method of Thue-Siegel is particularly well suited for application to such forms. We will show that

Lemma 2.4.1. *Let* F *be the binary form in Theorem 2.1.1. Then*

$$F(x, y) = \frac{1}{96A_3^2A_4\sqrt{-3I}}\left(\xi^4(x, y) - \eta^4(x, y)\right),$$

where ξ *and* η *are complex conjugate linear forms in* x *and* y.

Let $H(x, y) = A_0x^4 + A_1x^3y + A_2x^2y^2 + A_3xy^3 + A_4y^4$ with $A_3A_4 \neq 0$, be the Hessian of $F(x, y)$. Suppose that

$$x = m\xi + l\eta$$

and

$$y = p\xi + q\eta,$$

with

$$\xi(x, y)\eta(x, y) = 2A_1A_4x^2 + A_3^2xy + 2A_4A_3y^2,$$

for some m, l, p, $q \in \mathbb{C}$. Let $\Delta = mq - lp$. Therefore,

$$\begin{aligned} F(x,y) &= F(m\xi + l\eta, p\xi + q\eta) \\ &= a_0'\xi^4 + a_1'\xi^3\eta + a_2'\xi^2\eta^2 + a_3'\xi\eta^3 + a_4'\eta^4 \\ &= \Phi(\xi,\eta) \end{aligned}$$

and $\xi = \lambda(\alpha x + \beta y)$, $\eta = \mu(\gamma x + \delta y)$ and $\lambda\mu = 1$ (the values of λ and μ will be determined later). The Hessian $H'(\xi,\eta)$ of $\Phi(\xi,\eta)$ satisfies

$$\begin{aligned} H'(\xi,\eta) &= A_0'\xi^4 + A_1'\xi^3\eta + A_2'\xi^2\eta^2 + A_3'\xi\eta^3 + A_4'\eta^4 \\ &= \Delta^2 H(x,y) = \frac{\Delta^2}{4A_3^2A_4}\xi^2\eta^2. \end{aligned}$$

Hence,

$$A_0' = A_1' = A_3' = A_4' = 0; \quad A_2' = \Delta^2\frac{1}{4A_3^2A_4}. \tag{2.12}$$

On the other hand,

$$A_0' = 3(8a_0'a_2' - 3a_1'^2)$$

and

$$A_1' = 12(6a_0'a_3' - a_1'a_2').$$

It is easy to check that for any form $F(x,y)$,

$$-10a_4A_0 + 2a_3A_1 - a_2A_2 + a_1A_3 - 2a_0A_4 = 6J.$$

So, for $\Phi(\xi,\eta)$, we obtain

$$-10a_4'A_0' + 2a_3'A_1' - a_2'A_2' + a_1'A_3' - 2a_0'A_4' = 6J_\Phi = 6\Delta^6 J_F = 0,$$

where a_i' are the coefficients of Φ and A_i' are the coefficients of its Hessian. Therefore, by (2.12),

$$a_2' = 0$$

and by (2.8),

$$a_1' = a_3' = 0,$$

whereby,

$$F(x,y) = \Phi(\xi,\eta) = a_0'\xi^4 + a_4'\eta^4.$$

Our goal now is to determine the value of λ and $\mu = \frac{1}{\lambda}$ in $\xi = \lambda(\alpha x + \beta y)$ and $\eta = \mu(\gamma x + \delta y)$, so that $a_4' = -a_0'$. We have

$$a_0' = F(m,p) = F\left(\frac{-\delta p}{\gamma}, p\right) = \frac{p^4}{\gamma^4}F(-\delta,\gamma)$$

and

$$a'_4 = F(l,q) = F\left(\frac{-\beta q}{\alpha}, q\right) = \frac{q^4}{\alpha^4}F(-\beta,\alpha).$$

Also

$$\begin{pmatrix} m & l \\ p & q \end{pmatrix}\begin{pmatrix} \lambda\alpha & \lambda\beta \\ \mu\gamma & \mu\delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

whereby,

$$q = -\frac{\lambda p \alpha}{\mu\gamma}.$$

Therefore, to obtain $-a'_0 = a'_4$, we may take λ and μ so that

$$\mu^8 = \frac{\mu^4}{\lambda^4} = -\frac{F(-\beta,\alpha)}{F(\delta,-\gamma)}.$$

We have shown that $F(x,y)$ can be written as $a'_0\left(\xi^4(x,y) - \eta^4(x,y)\right)$, where

$$\xi = \lambda(\alpha x + \beta y),\ \ \eta = \mu(\gamma x + \delta y) \tag{2.13}$$

and $\lambda\mu = 1$. It remains to calculate the value of a'_0. Using (2.12) and (2.8), we get

$$A'_2 = \Delta^2 \frac{1}{4A_3^2 A_4} = 6(3a'_1a'_3 + 24a'_0a'_4 - 2a'^2_2) = 144a'_0a'_4.$$

Substituting a'_4 by $-a'_0$, we obtain

$$a'^2_0 = -\frac{\Delta^2}{24^2A_3^2A_4} = -\frac{1}{(\alpha\delta - \beta\gamma)^2 24^2 A_3^2 A_4}.$$

To calculate $(\alpha\delta - \beta\gamma)^2$, we recall that

$$2A_1A_4x^2 + A_3^2xy + 2A_3A_4y^2 = (\alpha x + \beta y)(\gamma x + \delta y),$$

consequently, by (2.11),

$$(\alpha\delta - \beta\gamma)^2 = A_3^4 - 16A_1A_4^2A_3 = 48A_3^2A_4I \tag{2.14}$$

and therefore,

$$a'_0 = \pm\frac{1}{96A_3^2A_4\sqrt{-3I}},$$

where $I = I_F$.

We will assume, without loss of generality, that

$$a'_0 = \frac{1}{96A_3^2A_4\sqrt{-3I}}. \tag{2.15}$$

For the binary form $F(x, y)$ with Hessian $H(x, y)$, the sextic covariant $Q(x, y)$ is defined by

$$Q(x, y) = \frac{\delta F}{\delta x}.\frac{\delta H}{\delta y} - \frac{\delta F}{\delta y}.\frac{\delta H}{\delta x}.$$

Since we have taken $H(x, y) = \frac{1}{4A_3^2A_4}(2A_1A_4x^2 + A_3^2xy + 2A_4A_3y^2)^2$, we may write

$$Q(x, y) = \frac{1}{2A_3^2A_4}(2A_1A_4x^2 + A_3^2xy + 2A_4A_3y^2).\psi(x, y),$$

where

$$\psi(x, y) = (A_3^2x + 4A_3A_4y)\frac{\delta F}{\delta x} - (4A_1A_4x + A_3^2y)\frac{\delta F}{\delta y}.$$

We have (see equation (25) of [8])

$$16H^3 + 9Q^2 = 4^4 \times 3^3IHF^2.$$

Let us set

$$W(x, y) = 2A_1A_4x^2 + A_3^2xy + 2A_4A_3y^2$$

to get

$$Q(x, y) = \frac{1}{2A_3^2A_4}W(x, y)\psi(x, y)$$

and

$$W^4(x, y) + 9A_3^2A_4\psi^2(x, y) = 4^4 \times 3^3IA_3^4A_4^2F^2(x, y). \tag{2.16}$$

Since $W(x, y) = \xi\eta$ and $F(x, y) = a'_0(\xi^4 - \eta^4)$, (2.16) implies that

$$(\xi^4 + \eta^4)^2 = -36A_3^2A_4\psi^2(x, y) \tag{2.17}$$

and therefore, by (2.10)

$$\xi^4 + \eta^4 = \pm\frac{6A_3^2}{A_1}\sqrt{-A_0}\psi(x, y).$$

Note that if all roots of $F(x, 1)$ are real then $I > 0$ and $A_0 < 0$ (see [7], Exercise 1 on page 217). So for every $x, y \in \mathbb{Z}$, there is $b \in \mathbb{Q}$, such that

$$\xi^4(x, y) + \eta^4(x, y) = b\sqrt{-A_0}.$$

We have also seen that for integers $x, y \in \mathbb{Z}$, there is $a \in \mathbb{Z}$ such that

$$\xi^4(x,y) - \eta^4(x,y) = i\, a\sqrt{3I}.$$

Therefore, for integers x, y, the quantities $\xi^4(x,y)$ and $\eta^4(x,y)$ are complex conjugates and integral in $\mathbb{Q}\left(\sqrt{-A_0}, \sqrt{-3I}\right)$. Moreover, $\sqrt{-A_0}\,\xi^4(x,y)$ and $\sqrt{-A_0}\,\eta^4(x,y)$ are algebraic integers in $\mathbb{Q}\left(\sqrt{A_0 I/3}\right)$. We will work in the number field $\mathbf{K} = \mathbb{Q}\left(\sqrt{A_0 I/3}\right)$. We also have, for every pair of integers (x,y),

$$\begin{aligned}\frac{\xi^4(x,y)}{\eta^4(x,y)} &= \frac{b\sqrt{-A_0} + ia\sqrt{3I}}{b\sqrt{-A_0} - ia\sqrt{3I}} \\ &= \frac{-A_0 b^2 - 3a^2 I + i6ab\sqrt{-A_0 I/3}}{-A_0 b^2 + 3a^2 I},\end{aligned}$$

where $b \in \mathbb{Q}$ and $a \in \mathbb{Z}$ depend on (x,y). Therefore,

$$\frac{\xi^4(x,y)}{\eta^4(x,y)} \in \mathbb{Q}(\sqrt{A_0 I/3}),$$

for integers x and y. Note that, in (2.13), we started with two linear forms and continued with their fourth powers. Let the linear form $\xi = \xi(x,y)$ be a fourth root of $\xi^4(x,y)$ and define

$$\eta(x,y) = \bar{\xi}(x,y).$$

Indeed, $\eta(x,y)$ is a fourth root of η^4. Hence, when $F(x,1)$ splits in $\mathbb{R}$, we can define the complex conjugate linear forms $\xi(x,y)$ and $\eta(x,y)$, so that

$$\xi^4 - \eta^4 = 96A_3^2 A_4\sqrt{-3I}F(x,y)$$

and

$$|\xi\eta| = \left|2A_1A_4x^2 + A_3^2xy + 2A_4A_3y^2\right|.$$

Observe that if the pair (ξ, η) satisfies the above identities, then there are precisely three others satisfying these identities, given by $(i\xi, -i\eta)$, $(-\xi, -\eta)$ and $(-i\xi, i\eta)$, where $i = \sqrt{-1}$. We will, however, work with (ξ, η), a fixed choice of complex conjugate forms. Let (x_1, y_1) and (x_2, y_2) be two distinct pairs of integers. Then we have

$$\begin{pmatrix} \lambda\alpha & \lambda\beta \\ \mu\gamma & \mu\delta \end{pmatrix}\begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} = \begin{pmatrix} \xi_1 & \xi_2 \\ \eta_1 & \eta_2 \end{pmatrix}.$$

If $x_1y_2 - x_2y_1$ is a nonzero integer then by (2.14), we get

$$|\xi_1\eta_2 - \xi_2\eta_1| = |(\alpha\delta - \beta\gamma)(x_1y_2 - x_2y_1)| \geq \frac{12A_3^2}{|A_1|}\sqrt{\frac{|IA_0|}{3}}. \tag{2.18}$$

2.5 Resolvent Forms

Suppose that ξ and η are linear forms in Lemma 2.4.1. Let us define

$$\xi' = \frac{\xi}{(12A_3^2)^{1/4}|A_4|^{1/8}}$$

and

$$\eta' = \frac{\eta}{(12A_3^2)^{1/4}|A_4|^{1/8}},$$

so that

$$F(x,y) = \frac{-1}{8\sqrt{3IA_4}}\left(\xi'^4(x,y) - \eta'^4(x,y)\right).$$

From (2.8), it is easy to see that all coefficients of $W^2(x,y) = (4A_3^2A_4)H(x,y)$ are multiples of $12A_3^2|A_4|$. By (2.16), we conclude that all coefficients of $\psi^2(x,y)$ are multiples of $16A_3^2|A_4|$. Using (2.17), we conclude that the real part of ξ^4 has the factor $12A_3^2A_4$. Since $\xi^4 - \eta^4 = a_0'F$, by (2.15), the imaginary part of ξ^4 has also the factor $12A_3^2A_4$. So, for $x, y \in \mathbb{Z}$, we have

$$\frac{\xi^4}{|12A_3^2A_4|}, \frac{\eta^4}{|12A_3^2A_4|} \in \mathbb{Q}\left(\sqrt{-A_0}, \sqrt{-3I}\right).$$

By (2.10),

$$\frac{\sqrt{-A_4}\,\xi^4}{|12A_3^2A_4|}, \frac{\sqrt{-A_4}\eta^4}{|12A_3^2A_4|} \in \mathbb{Q}\left(\sqrt{A_0I/3}\right),$$

for $x, y \in \mathbb{Z}$. From now on, we will consider the following diagonal form representation for F:

$$F(x,y) = \frac{-1}{8\sqrt{3IA_4}}\left(\xi^4(x,y) - \eta^4(x,y)\right). \tag{2.19}$$

For this new choice of ξ and η, we have

$$|\xi\eta| = \left|\frac{2A_1A_4x^2 + A_3^2xy + 2A_4A_3y^2}{\sqrt{12A_3^2\sqrt{|A_4|}}}\right| = \sqrt{\frac{H\sqrt{|A_4|}}{3}}. \tag{2.20}$$

From (2.18), we have

$$|\xi_1\eta_2 - \xi_2\eta_1| \geq 2\sqrt{I}\,|A_4|^{1/4}. \tag{2.21}$$

We also have

$$\xi^4(x,y) = \frac{\pm\psi(x,y)}{4A_4} \pm 4F(x,y)\sqrt{3IA_4}. \tag{2.22}$$

Lemma 2.4.1 can hence be restated as follows:

Lemma 2.5.1. *Let F be the binary form in Theorem 2.1.1. Then*

$$F(x,y) = \frac{1}{8\sqrt{3IA_4}}\left(\xi^4(x,y) - \eta^4(x,y)\right),$$

where ξ and η are complex conjugate linear forms in x and y. Furthermore, for integers x, y we have

$$\xi^4, \eta^4 \in \mathbb{Q}\left(\sqrt{A_0 I/3}\right).$$

Note that by (2.10),

$$\mathbb{Q}(\sqrt{A_0 I/3}) = \mathbb{Q}(\sqrt{A_4 I/3}).$$

We call a pair of complex conjugates ξ and η satisfying the above identities a pair of *resolvent forms*, and note that if (ξ, η) is one pair, there are precisely three others, given by $(i\xi, -i\eta)$, $(-\xi, -\eta)$ and $(-i\xi, i\eta)$, where $i = \sqrt{-1}$. We will, however, work with (ξ, η), a fixed pair of resolvent forms. Let ω be a fourth root of unity (for some $j \in \{1, 2, 3, 4\}$, let $\omega = e^{\frac{2j\pi i}{4}}$). We say that the integer pair (x, y) is *related* to ω if

$$\left|\omega - \frac{\eta(x,y)}{\xi(x,y)}\right| = \min_{0\leq k\leq 3}\left|e^{2k\pi i/4} - \frac{\eta(x,y)}{\xi(x,y)}\right|.$$

Let us define $z = 1 - \left(\frac{\eta(x,y)}{\xi(x,y)}\right)^4$, where (ξ, η) is a fixed pair of resolvent forms (in other words, $\frac{\eta}{\xi}$ is a fourth root of $(1-z)$). We have

$$|1 - z| = 1 \quad , \quad |z| < 2.$$

Lemma 2.5.2. *Let ω be a fourth root of unity and the integral pair (x, y) satisfies*

$$F(x,y) = \frac{-1}{8\sqrt{3IA_4}}(\xi^4(x,y) - \eta^4(x,y)) = h,$$

with

$$\left|\omega - \frac{\eta(x,y)}{\xi(x,y)}\right| = \min_{0\leq k\leq 3}\left|e^{2k\pi i/4} - \frac{\eta(x,y)}{\xi(x,y)}\right|.$$

If $|z| \geq 1$ then

$$\left|\omega - \frac{\eta(x,y)}{\xi(x,y)}\right| \leq |z|. \tag{2.23}$$

If $|z| < 1$ then

$$\left|\omega - \frac{\eta(x,y)}{\xi(x,y)}\right| < \frac{\pi}{12}|z|. \tag{2.24}$$

Proof. If

$$1 \le z = \prod_{0 \le k \le 3} \left| e^{2k\pi i/4} - \frac{\eta(x,y)}{\xi(x,y)} \right|,$$

then

$$\left| \omega - \frac{\eta(x,y)}{\xi(x,y)} \right| = \min_{0 \le k \le 3} \left| e^{2k\pi i/4} - \frac{\eta(x,y)}{\xi(x,y)} \right| \le z.$$

Now suppose that $|z| < 1$. Let

$$4\theta = \arg\left(\frac{\eta(x,y)^4}{\xi(x,y)^4} \right).$$

We have

$$\sqrt{2 - 2\cos(4\theta)} = |z| < 1.$$

Therefore, $|\theta| < \frac{\pi}{12}$. Since

$$\left| \omega - \frac{\eta(x,y)}{\xi(x,y)} \right| \le |\theta|,$$

we obtain

$$\left| \omega - \frac{\eta(x,y)}{\xi(x,y)} \right| \le \frac{1}{4} \frac{|4\theta|}{\sqrt{2 - 2\cos(4\theta)}} \left| 1 - \frac{\eta(x,y)^4}{\xi(x,y)^4} \right|.$$

From the fact that $\frac{|4\theta|}{\sqrt{2-2\cos(4\theta)}} < \frac{\pi}{3}$ whenever $0 < |\theta| < \frac{\pi}{12}$, we conclude

$$\left| \omega - \frac{\eta(x,y)}{\xi(x,y)} \right| < \frac{\pi}{12}|z|,$$

as desired. □

2.6 Gap Principles For The Thue Equation

Suppose that we have distinct solutions to $|F(x,y)| \le h$ indexed by i, say (x_i, y_i), related to ω with $|\xi(x_{i+1}, y_{i+1})| \ge |\xi(x_i, y_i)|$. For concision, we will write $\eta_i = \eta(x_i, y_i)$ and $\xi_i = \xi(x_i, y_i)$. By (2.21),

$$|\xi_i \eta_{i+1} - \xi_{i+1} \eta_i| \ge 2\sqrt{I}\, |A_4|^{1/4}.$$

On the other hand, by (2.23) and (2.24), we have

$$\begin{aligned}|\xi_i\eta_{i+1} - \xi_{i+1}\eta_i| &= |\xi_i(\eta_{i+1} - \omega\xi_{i+1}) - \xi_{i+1}(\eta_i - \omega\xi_i)| \\ &\leq 8h\sqrt{|3I\,A_4|}\left(\frac{|\xi_i|}{|\xi_{i+1}^3|} + \frac{|\xi_{i+1}|}{|\xi_i^3|}\right) \\ &\leq 8h\sqrt{|3I\,A_4|}\left(2\frac{|\xi_{i+1}|}{|\xi_i^3|}\right),\end{aligned}$$

since we assumed $|\xi_i| \leq |\xi_{i+1}|$. Combining this with (2.21), we conclude

$$|\xi_{i+1}| \geq \frac{1}{8\sqrt{3}h\ |A_4|^{1/4}}|\xi_i|^3. \tag{2.25}$$

Let us now assume that there are 4 distinct solutions to $|F(x, y)| = h$ related to a fixed choice of ω, corresponding to ξ_{-1}, ξ_0, ξ_1 and ξ_2, where $|\xi_{-1}| < |\xi_0| < |\xi_1| < |\xi_2|$. We will deduce a contradiction, which shows that at most 3 such solutions can exist under certain assumptions. By (2.25),

$$|z_{j+1}| \leq \frac{|z_j|^3 192h^2}{I},$$

where $z_i = 1 - \frac{\eta_i^4}{\xi_i^4} = \frac{\pm 8h\sqrt{3I\,A_4}}{\xi_i^4}$. Since $|z_{-1}| \leq 2$, if $I > 1536h^2$ then $|z_0|$, $|z_1|$, $|z_2| < 1$. Suppose that $|z_0| < 1$. By (2.23) and (2.24),

$$\begin{aligned}|\xi_{-1}\eta_0 - \xi_0\eta_{-1}| &= |\xi_{-1}(\omega\eta_0 - \xi_0) - \xi_0(\omega\eta_{-1} - \xi_{-1})| \\ &< 8h(1 + \frac{\pi}{12})\sqrt{|3I\,A_4|}\left(\frac{|\xi_0|}{|\xi_{-1}^3|}\right).\end{aligned}$$

Combining this with (2.21), we conclude

$$|\xi_0| > \frac{\sqrt{3}}{(12 + \pi)h\ |A_4|^{1/4}}|\xi_{-1}|^3.$$

Similarly, we get

$$\begin{aligned}&|\xi_0\eta_1 - \xi_1\eta_0| = |\xi_0(\omega\eta_1 - \xi_1) - \xi_1(\omega\eta_0 - \xi_0)| \\ < \ &8h\sqrt{|3I\,A_4|}\frac{\pi}{12}\left(\frac{|\xi_0|}{|\xi_1^3|} + \frac{|\xi_1|}{|\xi_0^3|}\right) \leq \frac{4\pi}{3}h\sqrt{|3I\,A_4|}\left(\frac{|\xi_1|}{|\xi_0^3|}\right),\end{aligned}$$

which leads to

$$|\xi_1| > \frac{\sqrt{3}}{2\pi h\ |A_4|^{1/4}}|\xi_0|^3 > \frac{9}{2\pi h^4(12 + \pi)^3\ |A_4|}|\xi_{-1}|^9. \tag{2.26}$$

Note that $\left|\frac{8h\sqrt{|3I\,A_4|}}{\xi_{-1}^4}\right| = |z_{-1}| = \left|1 - \left(\frac{\eta_{-1}}{\xi_{-1}}\right)^4\right| \leq 2$ and therefore,

$$|\xi_{-1}|^4 > 4h\sqrt{|3I\,A_4|}. \tag{2.27}$$

Thus, when $I > 1536h^2$ we have

$$|\xi_1| > I^{\frac{9}{8}} \frac{9\left(4\sqrt{3}\right)^{9/4} |A_4|^{9/8}}{2\pi(12+\pi)^3 h^{7/4}\ |A_4|} > 0.06\,\frac{I^{\frac{9}{8}}\ |A_4|^{1/8}}{h^{7/4}}. \tag{2.28}$$

2.7 Gap Principles For The Thue Inequality

In Section 2.3, we have shown that the Hessian of F satisfies the following formula.

$$\begin{aligned} H(x,y) &= A_0x^4 + A_1x^3y + A_2x^2y^2 + A_3xy^3 + A_4y^4 \\ &= \frac{1}{4A_3^2A_4}(2A_1A_4x^2 + A_3^2xy + 2A_4A_3y^2)^2. \end{aligned}$$

In fact, it is known (see page 78 of [8]) that for any quartic form $F(x,y)$ with $J=0$, the algebraic covariant $\frac{-1}{9}H(x,y)$ is the square of a quadratic form, say

$$\frac{-1}{9}H(x,y) = m^2(x,y).$$

The polynomial $m(x) = m(x,1)$ is a positive definite quadratic. We say that the quartic form $F(x,y) = a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4$ with positive discriminant is *reduced* if and only if the positive definite quadratic form $m(x,y)$ is reduced. Here, we remark that the real quadratic form $f(x,y) = ax^2 + bxy + cy^2$ is called *reduced* if

$$|b| \leq a \leq c.$$

Suppose that our quartic form $F(x,y)$ is reduced. We assume that $y \neq 0$. Put

$$m(x,y) = y^2m(z) = y^2\left(Az^2 + Bz + C\right),$$

where $z = \frac{x}{y}$. Note that $m(z)$ assumes a minimum equal to $\frac{4AC-B^2}{4A}$ at $z = \frac{-B}{2A}$. Since $m(x,y) = \frac{1}{|36A_3^2A_4|}(2A_1A_4x^2 + A_3^2xy + 2A_4A_3y^2)^2$, by (2.11), we get

$$4AC - B^2 = \frac{16A_1A_3A_4^2 - A_3^4}{36A_3^2A_4} = \frac{4}{3}I.$$

Since $m(x,y)$ is reduced, we have

$$A^2 \leq AC \leq \frac{1}{3}(4AC - B^2) = \frac{4}{9}I.$$

Therefore,

$$m(x,y) \geq \frac{\sqrt{I}}{2}y^2,$$

Hence, we have shown that

Lemma 2.7.1. *If the quartic form $F(x,y)$ in Theorem 2.1.2 is reduced, then for its Hessian $H(x,y)$ we have*

$$|H(x,y)| \geq \frac{9}{4}\,Iy^4.$$

So we can assume that $|H(x,y)| \geq 12h^3\sqrt{3I}$ when looking for pairs of solutions (x,y) with $|y| \geq \frac{2h^{3/4}}{(3I)^{1/8}}$.

Suppose that we have distinct solutions to $|F(x,y)| \leq h$ indexed by i, say (x_i, y_i), related to ω with $|\xi(x_{i+1}, y_{i+1})| \geq |\xi(x_i, y_i)|$. Let

$$F(x_i, y_i) = h_i,\ F(x_{i+1}, y_{i+1}) = h_{i+1}.$$

Since $|h_i|, |h_{i+1}| < h$, (2.25) still holds and we have

$$|\xi_{i+1}| \geq \frac{1}{8\sqrt{3}h\ |A_4|^{1/4}}|\xi_i|^3.$$

Let us now assume that there are 4 distinct solutions to $|F(x,y)| \leq h$ related to a fixed choice of ω, corresponding to ξ_{-1}, ξ_0, ξ_1 and ξ_2, where $|\xi_{-1}| < |\xi_0| < |\xi_1| < |\xi_2|$ and $F(x_j, y_j) = h_j$. We will deduce a contradiction. By (2.25) and since $|h_j| < h$,

$$|z_{j+1}| \leq \frac{|z_j|^3 192h^5}{I},$$

where $z_i = 1 - \frac{\eta_i^4}{\xi_i^4} = \frac{-8h_i\sqrt{3IA_4}}{\xi_i^4}$. Since $|z_{-1}| \leq 2$, if $I > 1536h^5$ then $|z_0|$, $|z_1|$, $|z_2| < 1$. Suppose that $I > 1536h^5$ then similar to section 2.6, we can prove that inequalities (2.26) hold and we have

$$|\xi_1| > \frac{3}{2\pi h\,|A_4|^{1/4}}|\xi_0|^3 > \frac{9\sqrt{3}}{2\pi h^4(12+\pi)^3\,|A_4|}|\xi_{-1}|^9.$$

Let us now assume that

$$|H(x_{-1}, y_{-1})| \geq 12\frac{h^3\sqrt{3I}}{|A_3^2 A_4|}.$$

Then by (2.20),

$$|\xi_{-1}|^4 \geq 4h^3\sqrt{|3IA_4|}.$$

Note that under this assumption, we have $|z_{-1}| < 1$ and

$$|\xi_1| > (4\sqrt{3})^{9/4} I^{\frac{9}{8}} h^{11/4}\ |A_4|^{1/8} \left(\frac{3}{2\pi}\right)^4 > 0.1 h^{11/4} I^{\frac{9}{8}}\ |A_4|^{1/8}. \qquad (2.29)$$

2.8 Some Algebraic Numbers

Combining the polynomials $A_{r,g}$ and $B_{r,g}$ in Lemma 2.2.2 with the resolvent forms, we will consider the complex sequences $\Sigma_{r,g}$ given by

$$\Sigma_{r,g} = \frac{\eta_2}{\xi_2} A_{r,g}(z_1) - \frac{\eta_1}{\xi_1} B_{r,g}(z_1)$$

where $z_1 = 1 - \eta_1^4/\xi_1^4$. For any pair of integers (x, y), $\xi^4(x, y)$ and $\eta^4(x, y)$ are algebraic integers in $\mathbb{Q}(\sqrt{A_0 I/3})$(see Lemma 2.5.1). We have seen that $A_0 < 0$ and one can assume $A_3 A_4 \neq 0$. Therefore from (2.10), we have $A_1 \neq 0$. Define

$$\Lambda_{r,g} = (9|A_4|)^{\frac{1-g}{4}}\ \xi_1^{4r} \xi_1^{1-g} \xi_2 \Sigma_{r,g}.$$

We will show that $\Lambda_{r,g}$ is either an integer in $\mathbb{Q}(\sqrt{\frac{A_0 I}{3}})$ or a fourth root of such an integer. If $\Lambda_{r,g} \neq 0$, this provides a lower bound upon $|\Lambda_{r,g}|$.

Lemma 2.8.1. *The linear forms*

$$\frac{\xi}{\xi(1,0)}, \frac{\eta}{\eta(1,0)}$$

have their coefficients in $\mathbb{Q}(\sqrt{A_0 I/3})$.

Proof. By (2.10) and (2.14), we have

$$\alpha\delta - \beta\gamma = \pm\sqrt{A_3^4 - 16A_1 A_4^2 A_3} = \pm\frac{4A_3^2}{A_1}\sqrt{3IA_0} = \frac{12A_3^2}{A_1}\sqrt{\frac{IA_0}{3}}.$$

Since

$$\begin{aligned} 2A_1A_4x^2 + A_3^2xy + 2A_3A_4y^2 &= (\alpha x + \beta y)(\gamma x + \delta y) \\ &= \sqrt{12A_3^2\sqrt{|A_4|}}\xi(x,y)\eta(x,y), \end{aligned}$$

we conclude that $\alpha\gamma$, $\beta\delta$, $\alpha\delta + \beta\gamma \in \mathbb{Z}$. Thus, for integral pair (s,t), we obtain

$$\frac{\xi(s,t)}{\xi(1,0)}, \frac{\eta(s,t)}{\eta(1,0)} \in \mathbb{Q}(\sqrt{A_0I/3})[s,t].$$

□

Lemma 2.8.2. *If (x_1,y_1) and (x_2,y_2) are two pairs of rational integers then the numbers*

$$\sqrt{3|A_4|^{1/2}}\xi(x_1,y_1)\eta(x_2,y_2),$$

$$\xi(x_1,y_1)^3\xi(x_2,y_2)$$

and

$$\eta(x_1,y_1)^3\eta(x_2,y_2)$$

are integers in $\mathbb{Q}(\sqrt{A_0I/3})$.

Proof. For any pair of integers (x,y), Lemma 2.8.1 implies that

$$\frac{\xi(x,y)}{\xi(1,0)} \in \mathbb{Q}(\sqrt{A_0I/3}).$$

Thus,

$$\frac{\xi(x_1,y_1)}{\xi(x_2,y_2)} \in \mathbb{Q}(\sqrt{A_0I/3}).$$

Since

$$\sqrt{3|A_4|^{1/2}}\xi(x_2,y_2)\eta(x_2,y_2) = \frac{W(x_2,y_2)}{2|A_3|} \in \mathbb{Q},$$

the algebraic integer $\sqrt{3|A_4|}\xi(x_1,y_1)\eta(x_2,y_2)$ belongs to $\mathbb{Q}(\sqrt{A_0I/3})$.
Let $\xi(x,y) = \epsilon_1 x + \epsilon_2 y$. Clearly, ϵ_1 and ϵ_2 are algebraic integers and so are ϵ_1^4, $\epsilon_1^3\epsilon_2$, $\epsilon_1^2\epsilon_2^2$, $\epsilon_1\epsilon_2^3$ and ϵ_2^4. Since ξ^4 is an integer in $\mathbb{Q}(\sqrt{A_0I/3})$, we conclude that ϵ_1^4, $\epsilon_1^3\epsilon_2$, $\epsilon_1^2\epsilon_2^2$, $\epsilon_1\epsilon_2^3$ and ϵ_2^4 are all algebraic integers in $\mathbb{Q}(\sqrt{A_0I/3})$.
$\xi(x_1,y_1)^3\xi(x_2,y_2)$ is an integer in $\mathbb{Q}(\sqrt{A_0I/3})$, because it can be written as a linear combination with rational integer coefficients in ϵ_1^4 , $\epsilon_1^3\epsilon_2$, $\epsilon_1^2\epsilon_2^2$, $\epsilon_1\epsilon_2^3$ and ϵ_2^4.
We can similarly show that that $\eta(x_1,y_1)^3\eta(x_2,y_2)$ is also an integer in $\mathbb{Q}(\sqrt{A_0I/3})$. □

Let $\mathbf{K} = \mathbb{Q}(\sqrt{A_4 I/3})$ and $\mathbf{O_K}$ be its ring of integers. Note that by (2.10)

$$\mathbb{Q}(\sqrt{A_4 I/3}) = \mathbb{Q}(\sqrt{A_0 I/3}).$$

We put

$$\mathbf{O} = \{\frac{m + n\sqrt{A_4 I/3}}{2} \in \mathbf{O_K} \quad | \quad m, n \in \mathbb{Z}\}.$$

It is easy to check that $\mathbf{O}$ is a subring of $\mathbf{O_K}$. Let d be the largest square-free divisor of $A_0 I/3$. From the well-known characterization of algebraic integers in quadratic fields, we have

$$\mathbf{O_K} = \{a + b\,\frac{1+\sqrt{d}}{2} \quad | \quad a, b \in \mathbb{Z}\} \qquad \text{if} \qquad d \equiv 1 \mod 4$$

and

$$\mathbf{O_K} = \{a + b\sqrt{d} \quad | \quad a, b \in \mathbb{Z}\} \qquad \text{if} \qquad d \equiv 2, 3 \mod 4.$$

Therefore,

$$\theta \in \mathbf{O} \qquad \text{if and only if} \qquad \theta \in \mathbf{O_K}, \quad \theta - \bar{\theta} \in \mathbb{Z}(\sqrt{A_4 I/3}), \tag{2.30}$$

where $\bar{\theta}$ is the complex conjugate of θ. This implies that

$$|\theta| \geq |\operatorname{Im}\theta| \geq \frac{1}{2}(\sqrt{A_4 I/3}). \tag{2.31}$$

Lemma 2.8.3. *If (x_1, y_1) and (x_2, y_2) are two pairs of rational integers then the numbers*

$$\sqrt{3|A_4|^{1/2}}\xi(x_1, y_1)\eta(x_2, y_2),$$

$$\xi(x_1, y_1)^3\xi(x_2, y_2)$$

and

$$\eta(x_1, y_1)^3\eta(x_2, y_2)$$

belong to $\mathbf{O}$.

Proof. For pairs of integers (x_1, y_1) and (x_2, y_2), we know

$$\sqrt{3|A_4|^{1/2}}\xi(x_1, y_1)\eta(x_2, y_2),$$

and

$$\sqrt{3|A_4|^{1/2}}\xi(x_2, y_2)\eta(x_1, y_1),$$

are complex conjugate elements of $\mathbf{O_K}$. By the definition of the resolvent forms ξ and η in Section 2.5 and (2.14), the transformation $(x, y) \to (\xi, \eta)$ has determinant

$$\pm \frac{4A_3\sqrt{3IA_4}}{2\sqrt{3}A_3\,|A_4|^{1/4}}.$$

Therefore

$$\sqrt{3|A_4|^{1/2}}\xi(x_1, y_1)\eta(x_2, y_2) - \sqrt{3|A_4|^{1/2}}\xi(x_2, y_2)\eta(x_1, y_1) = \pm 2\sqrt{3IA_4}.$$

By (2.30), this implies

$$\sqrt{3|A_4|^{1/2}}\xi(x_1, y_1)\eta(x_2, y_2) \in \mathbf{O}.$$

Let $\xi(x, y) = \epsilon_1 x + \epsilon_2 y$. Since

$$\begin{aligned} & \epsilon_1^4 x^4 + 4\epsilon_1^3\epsilon_2 x^3 y + 6\epsilon_1^2\epsilon_2^2 x^2 y^2 + 4\epsilon_1\epsilon_2^3 x y^3 + \epsilon_2^4 y^4 \\ = \; & \xi^4(x, y), \end{aligned}$$

and by (2.22),

$$\xi^4(x, y) = \frac{\pm\psi(x, y)}{4A_4} \pm 4F(x, y)\sqrt{3IA_4},$$

we have ϵ_1^4, $4\epsilon_1^3\epsilon_2$, $6\epsilon_1^2\epsilon_2^2$, $4\epsilon_1\epsilon_2^3$ and ϵ_2^4 are elements of $\mathbf{O}$ and their imaginary parts have factor 12. From the proof of Lemma 2.8.2, ϵ_1^4 , $\epsilon_1^3\epsilon_2$, $\epsilon_1^2\epsilon_2^2$, $\epsilon_1\epsilon_2^3$ and ϵ_2^4 are algebraic integers. Therefore, by (2.30), ϵ_1^4 , $\epsilon_1^3\epsilon_2$, $\epsilon_1^2\epsilon_2^2$, $\epsilon_1\epsilon_2^3$ and ϵ_2^4 are elements of $\mathbf{O}$. So $\xi(x_1, y_1)^3\xi(x_2, y_2)$ belongs to $\mathbf{O}$, because it can be written as a linear combination with rational integer coefficients in ϵ_1^4 , $\epsilon_1^3\epsilon_2$, $\epsilon_1^2\epsilon_2^2$, $\epsilon_1\epsilon_2^3$ and ϵ_2^4.
We can similarly prove the lemma for $\eta(x_1, y_1)^3\eta(x_2, y_2)$. □

For every polynomial $P(z) = a_n z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$, we define

$$P^*(x, y) = x^n P(y/x) = a_0 x^n + a_1 x^{n-1} y + \ldots + a_{n-1} x y^{n-1} + a_n y^n.$$

Let $A_{r,g}$ and $B_{r,g}$ be as in (2.3) and

$$C_{r,g}(z) = A_{r,g}(1 - z),\ D_{r,g}(z) = B_{r,g}(1 - z),$$

where $A_{r,g}$ and $B_{r,g}$ are the polynomials in Lemma 2.2.2. For $z \neq 0$, we have $D_{r,0}(z) = z^r C_{r,0}(z^{-1})$, hence

$$\begin{aligned} A^*_{r,0}(z, z-\bar{z}) &= z^r A_{r,0}(1-\frac{\bar{z}}{z}) = z^r C_{r,0}(\frac{\bar{z}}{z}) \\ &= \bar{z}^r D_{r,0}(\frac{z}{\bar{z}}) = \bar{z}^r B_{r,0}(1-\frac{z}{\bar{z}}) \\ &= B^*_{r,0}(\bar{z}, \bar{z}-z) = \bar{B}^*_{r,0}(z, z-\bar{z}). \end{aligned} \tag{2.32}$$

Lemma 2.8.4. *For any pair of integers (x, y), the numbers*

$$A^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$$

and

$$B^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$$

belong to **O**.

Proof. It is clear that

$$A^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$$

and

$$B^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$$

belong to $\mathbb{Q}(\sqrt{A_0 I/3})$. So we need only show that they are integers in $\mathbb{Q}(\sqrt{A_0 I/3})$. This follows immediately from Lemma 4.1 of [6] since

$$\xi^4(x,y) - \eta^4(x,y) = -8h\sqrt{3IA_4}F(x,y).$$

□

We now proceed to show that for any $r \in \mathbb{Z}$, $\Lambda_{r,0}$ and $\Lambda^4_{r,1}$ are in **O**.

$$\begin{aligned} \Lambda_{r,g} &= (9|A_4|)^{\frac{1-g}{4}} \xi_1^{4r} \xi_1^{1-g} \xi_2 \Sigma_{r,g} \\ &= (9|A_4|)^{\frac{1-g}{4}} \left(\xi_1^{1-g} \eta_2 A^*_{r,g}(\xi_1^4, \xi_1^4 - \eta_1^4) - \xi_1^{3g} \xi_2 \eta_1 B^*_{r,g}(\xi_1^4, \xi_1^4 - \eta_1^4) \right). \end{aligned}$$

By Lemma 2.8.2 and (2.32), $\Lambda_{r,0} \in \mathbb{Z}.\sqrt{A_0 I/3}$. By Lemma 2.8.3 and Lemma 2.8.4, $\Lambda^4_{r,1}$ belongs to **O**. Next we will show that $\Lambda^4_{r,1}$ is not a rational integer when $\Sigma_{r,1}$ is nonzero. We have

$$\Sigma_{r,g} = \frac{\eta_2}{\xi_2} A_{r,g}(z_1) - \frac{\eta_1}{\xi_1} B_{r,g}(z_1) = \frac{\eta}{\xi} \left[\frac{\eta_2/\eta}{\xi_2/\xi} A_{r,g}(z_1) - \frac{\eta_1/\eta}{\xi_1/\xi} B_{r,g}(z_1) \right],$$

where $\eta = \eta(1,0)$ and $\xi = \xi(1,0)$. By Lemmas 2.8.1 and 2.8.4, $\frac{\eta_2/\eta}{\xi_2/\xi}A_{r,g}(z_1) - \frac{\eta_1/\eta}{\xi_1/\xi}B_{r,g}(z_1) \in \mathbb{Q}(\sqrt{A_0 I/3})$. Hence

$$\mathfrak{f} = \mathbb{Q}(\sqrt{A_0 I/3}, \Sigma_{r,g}) = \mathbb{Q}(\sqrt{A_0 I/3}, \frac{\xi}{\eta}).$$

If we choose complex number X so that $\xi(X,1) = \eta(X,1)$ then by Lemma 2.8.1, $X \in \mathfrak{f}$. We have $F(X,1) = \frac{-1}{8\sqrt{3IA_4}}(\xi^4(X,1) - \eta^4(X,1)) = 0$. Since we have assumed that F is irreducible and has only real roots, the number A_0 is negative, and therefore, X has degree 4 over $\mathbb{Q}(\sqrt{A_0 I/3})$.We also know that

$$X \in \mathfrak{f} = \mathbb{Q}(\sqrt{A_0 I/3})(\Sigma_{r,g}).$$

Thus, $\Sigma_{r,g}$ must have degree 4 over $\mathbb{Q}(\sqrt{A_0 I/3})$. Now suppose $\Lambda_{r,1}^4 \in \mathbb{Z}$. Then we have for some $\rho \in \{\pm 1, \pm i\}$, that $\Lambda_{r,1} = \rho\bar{\Lambda}_{r,1}$. Hence by Lemma 2.8.2

$$\begin{aligned}
\Sigma_{r,1} &= \xi_1^{-4r}\xi_2^{-1}\rho\bar{\Lambda}_{r,1} \\
&= \xi_1^{-4r}\xi_2^{-1}\eta_1^{4r}\eta_2\rho\left(\frac{\xi_2}{\eta_2}A_{r,1}\left(1-\frac{\xi_1^4}{\eta_1^4}\right) - \frac{\xi_1}{\eta_1}B_{r,1}\left(1-\frac{\xi_1^4}{\eta_1^4}\right)\right) \\
&= \xi_1^{-4r}\xi_2^{-1}\eta_1^{4r}\eta_2\rho\left(\frac{\xi_2}{\eta_2}A_{r,1}\left(1-\frac{\xi_1^4}{\eta_1^4}\right) - \frac{\xi_1}{\eta_1}B_{r,1}\left(1-\frac{\xi_1^4}{\eta_1^4}\right)\right) \\
&= \rho\frac{\eta_1^{4r}}{\xi_1^{4r}}\left(A_{r,1}\left(1-\frac{\xi_1^4}{\eta_1^4}\right) - \frac{\xi_1\eta_2}{\xi_2\eta_1}B_{r,1}\left(1-\frac{\xi_1^4}{\eta_1^4}\right)\right).
\end{aligned}$$

This, together with Lemmas 2.8.2 and 2.8.4, implies that

$$\Sigma_{r,1} \in \mathbb{Q}(\sqrt{A_0 I/3}, \rho),$$

which contradicts the fact that $\Sigma_{r,1}$ has degree 4 over $\mathbb{Q}(\sqrt{A_0 I/3})$ $(\rho \in \{\pm 1, \pm i\}$). We conclude that $\Lambda_{r,1}$ can not be a rational integer.

Therefore, by (2.31), we may conclude that if $\Lambda_{r,g} \neq 0$, then for $g \in \{0,1\}$

$$|\Lambda_{r,g}| \geq 2^{\frac{-g}{4}}(-A_4 I/3)^{\frac{1}{2}-\frac{3g}{8}}. \tag{2.33}$$

2.9 Approximating Polynomials

In order to apply (2.21), we must make sure that $\Lambda_{r,g}$ or equivalently $\Sigma_{r,g}$ does not vanish. First we will show that for small r, $\Sigma_{r,0} \neq 0$.

Lemma 2.9.1. *Suppose that* (x, y) *is a pair of solutions to* $F(x, y) = \pm 1$ *with* $I > 1536$ *or a pair of solutions to* $|F(x, y)| \leq h$ *with* $|y| > \frac{2h^{3/4}}{(3I)^{1/8}}$ *. For this pair of solutions and* $r \in \{1, 2, 3, 4, 5\}$*, we have*

$$\Sigma_{r,0} \neq 0.$$

Proof. Let $r \in \{1, 2, 3, 4, 5\}$. Suppose that $\Sigma_{r,0} = 0$. From (2.4), we can find for each r, a polynomial $F_r(z) \in \mathbb{Z}[z]$, satisfying

$$A_{r,0}(z)^4 - (1 - z)B_{r,0}^4 = z^{2r+1}F_r(z).$$

In fact, we have

$$A_1(z) = 4A_{1,0}(z) = 8 - 5z,$$

$$B_1(z) = 4B_{1,0}(z) = 8 - 3z,$$

$$F_1(z) = 320 - 320z + 81z^2,$$

$$A_2(z) = \frac{32}{3}A_{2,0}(z) = 64 - 72z + 15z^2,$$

$$B_2(z) = \frac{32}{3}B_{2,0}(z) = 64 - 56z + 7z^2,$$

$$F_2(z) = 86016 - 172032z + 114624z^2 - 28608z^3 + 2401z^4,$$

$$A_3(z) = 128A_{3,0}(z) = 2560 - 4160z + 1872z^2 - 195z^3,$$

$$B_3(z) = 128B_{3,0}(z) = 2560 - 3520z + 1232z^2 - 77z^3,$$

$$\begin{aligned} F_3(z) = \quad & 14057472000 - 42172416000z \\ & +48483635200z^2 - 26679910400z^3 \\ & +7150266240z^4 - 839047040z^5 \\ & +35153041z^6, \end{aligned}$$

$$\begin{aligned} A_4(z) &= \frac{2048}{5}A_{4,0}(z) \\ &= 28672 - 60928z + 42432z^2 - 10608z^3 + 663z^4, \end{aligned}$$

$$\begin{aligned} B_4(z) &= \frac{2048}{5}B_{4,0}(z) \\ &= 28672 - 53760z + 31680z^2 - 6160z^3 + 231z^4, \end{aligned}$$

$$\begin{aligned} F_4(z) = \quad & 13989396348928 - 55957585395712z \\ & +91916125077504z^2 - 79896826347520z^3 \\ & +39463764078592z^4 - 11050000539648z^5 \\ & +1648475542656z^6 - 113348764800z^7 \\ & +2847396321z^8, \end{aligned}$$

$$\begin{aligned} A_5(z) &= \frac{8192}{21} A_{5,0}(z) \\ &= 98304 - 258048z + 243712z^2 \\ &\quad -99008z^3 + 15912z^4 - 663z^5, \end{aligned}$$

$$\begin{aligned} B_5(z) &= \frac{8192}{21} B_{5,0}(z) \\ &= 98304 - 233472z + 194560z^2 \\ &\quad -66880z^3 + 8360z^4 - 209z^5. \end{aligned}$$

and

$$\begin{aligned} F_5(z) = \quad & 121733331812352 - 608666659061760z \\ & +1301756554248192z^2 - 1555026262622208z^3 \\ & +1136607561252864z^4 - 523630732640256z^5 \\ & +151029162176512z^6 - 26204424888320z^7 \\ & +2515441608384z^8 - 113971885760z^9 \\ & +1908029761z^{10}. \end{aligned}$$

We also define A_r^* and B_r^* via

$$A_r^*(x,y) = x^r A_r(y/x),$$

and

$$B_r^*(x,y) = x^r B_r(y/x).$$

Since $\Sigma_{r,0}$ is assumed to be zero,

$$\frac{\eta_2^4}{\xi_2^4} = \frac{\eta_1^4 (B_r^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4}{\xi_1^4 (A_r^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4}.$$

Let $\mathfrak{I}_r$ be the integral ideal in $\mathbb{Q}(\sqrt{IA_0/3})$ generated by $\xi_1^4(A^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4$ and $\eta_1^4(B^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4$ and $N(\mathfrak{I}_r)$ be the absolute norm of $\mathfrak{I}_r$. Since the ideal generated by $\xi_1^4(A_r^*(\xi_1^4,\xi_1^4-\eta_1^4))^4-\eta_1^4(B_r^*(\xi_1^4,\xi_1^4-\eta_1^4))^4$ divides $(\xi_2^4-\eta_2^4).\mathfrak{I}_r$, we obtain

$$\begin{aligned}&|\xi_1|^{4(4r+1)}|A_r^4(z_1)-(1-z_1)B_r^4(z_1)|\\ =\ &|\xi_1^4(A_r^*(\xi_1^4,\xi_1^4-\eta_1^4))^4-\eta_1^4(B_r^*(\xi_1^4,\xi_1^4-\eta_1^4))^4.\end{aligned}$$

Since $\mathfrak{I}_r$ is contained in an imaginary quadratic field, by (2.15), we get

$$|\xi_1|^{4(4r+1)}|A_r^4(z_1)-(1-z_1)B_r^4(z_1)|\leq N(\mathfrak{I}_r)^{1/2}|\xi_2^4-\eta_2^4|$$

By (2.4),

$$A_r^4(z_1)-(1-z_1)B_r^4(z_1)=z_1^{2r+1}F_r(z_1),$$

and so we conclude

$$|z_1|^{2r+1}|F_r(z_1)|\leq N(\mathfrak{I}_r)^{1/2}|\xi_2^4-\eta_2^4||\xi_1|^{-4(4r+1)};$$

i.e.

$$1\leq\frac{N(\mathfrak{I}_r)^{1/2}|\xi_2^4-\eta_2^4||\xi_1|^{-4(4r+1)}}{|z_1|^{2r+1}|F_r(z_1)|}.$$

Since $\xi_1^4=(\xi_1^4-\eta_1^4)(1-\frac{\eta_1^4}{\xi_1^4})^{-1}=(\xi_1^4-\eta_1^4)z_1^{-1}$ we obtain

$$1\leq\frac{N(\mathfrak{I}_r)^{1/2}|\xi_2^4-\eta_2^4||\xi_1^4-\eta_1^4|^{-4r-1}|z_1|^{2r}}{|F_r(z_1)|}.$$

Noting that $|z_1|=\left|\xi_1^{-4}\right|\left|\xi_1^4-\eta_1^4\right|$ and $\left|\xi_i^4-\eta_i^4\right|=\left|8h\sqrt{3IA_4}F(x,y)\right|$, we obtain for $r\in\{1,2,3,4,5\}$,

$$|\xi_1|^{8r}\leq\frac{(N(\mathfrak{I}_r)^{1/2}|\xi_1^4-\eta_1^4|^{-4r-1})|8h\sqrt{3IA_4}|^{2r+1}}{|F_r(z_1)|}.\tag{2.34}$$

To estimate $N(\mathfrak{I}_r)^{1/2}$, we choose a finite extension $\mathbf{M}$ of $\mathbb{Q}(\sqrt{A_0I/3})$ so that the ideal generated by ξ_1^4 and $\xi_1^4-\eta_1^4$ in $\mathbf{M}$ is a principal ideal, with generator p, say. We denote the extension of $\mathfrak{I}_r$ to $\mathbf{M}$, by $\mathfrak{I}'_r$. Let $\mathfrak{r}_r$ be the ideal in $\mathbf{M}$ generated by $A_r^*(u,v)$ and $B_r^*(u,v)$, where $u=\frac{\xi_1^4}{p}$ and $v=\frac{\xi_1^4-\eta_1^4}{p}$. Since $A_r^*(x,x-y)=B_r^*(y,y-x)$,

$$\begin{aligned}p^{4r+1}\mathfrak{r}_r^4B_r^*(0,1)^4\ &\subset\ p^{4r+1}\mathfrak{r}_r^4(u,B_r^*(0,v)^4)(u-v,B_r^*(0,v)^4)\\ &\subset\ p^{4r+1}\mathfrak{r}_r^4(u,B_r^*(0,v)^4)(u-v,A_r^*(v,v)^4)\\ &\subset\ p^{4r+1}\mathfrak{r}_r^4(u,u-v)(u,B_r^*(u,v)^4)(u-v,A_r^*(u,v)^4)\\ &\subset\ p^{4r+1}(uA^*(u,v)^4,(u-v)B_r^*(u,v)^4)=\mathfrak{I}'_r,\end{aligned}\tag{2.35}$$

where $(m_1, \ldots, m_n)$ denote the ideal in $\mathbf{M}$ generated by $m_1, \ldots, m_n$.

We have

$$A_1^*(x,y) - B_1^*(x,y) = -2y.$$

Therefore,

$$2(v) \subset (A_1^*(u,v), B_1^*(u,v)) \subset \mathfrak{r}_1,$$

where (v) is the ideal generated by v in $\mathbf{M}$. Since $B_1^*(0,1) = -3$, it follows from (2.35) that

$$1296(\xi_1^4 - \eta_1^4)^5 \subset 1296p(\xi_1^4 - \eta_1^4)^4 = p^5 16 v^4 B_1^*(0,1)^4 \subset \mathfrak{I}_1'.$$

For $r = 2$, we first observe that

$$B_1^*(x,y)A_2^*(x,y) - A_1^*(x,y)B_2^*(x,y) = -10y^3$$

and

$$(-32x + 7y)A_2^*(x,y) - (-32x + 15y)B_2^*(x,y) = 80xy^2.$$

Therefore, by (2.35) we have

$$80(v)^2 \subset (-10v^3, 80uv^2) \subset (A_2^*(u,v), B_2^*(u,v)) \subset \mathfrak{r}_2.$$

Since $B_2^*(0,1) = 7$, we have

$$80^4 \times 7^4(\xi_1^4 - \eta_1^4)^9 \subset 80^4 \times 7^4 p(\xi_1^4 - \eta_1^4)^8 = 80^4 p^9 v^8 B_2^*(0,1)^4 \subset \mathfrak{I}_2'.$$

When $r = 3$, we have

$$B_2^*(x,y)A_3^*(x,y) - A_2^*(x,y)B_3^*(x,y) = -210y^5$$

$$\begin{aligned} & (1616x^2 - 1078xy + 77y^2)A_3^*(x,y) \\ - \quad & (1616x^2 - 1482xy + 195y^2)B_3^*(x,y) \\ = \quad & -16800x^2y^3. \end{aligned}$$

Substituting 77 for $B_3^*(0,1)$, we conclude

$$\begin{aligned} & 16800^4 \times 77^4(\xi_1^4 - \eta_1^4)^{13} \subset 16800^4 \times 77^4 p(\xi_1^4 - \eta_1^4)^{12} \\ = \quad & 16800^4 p^{13} v^{12} B_3^*(0,1)^4 \subset \mathfrak{I}_3'. \end{aligned}$$

For $r = 4$, setting

$$\begin{aligned} G_4(x,y) &= 14178304x^3 - 15889280x^2y + 4071760xy^2 - 162393y^3, \\ H_4(x,y) &= 14178304x^3 - 19433856x^2y + 6714864xy^2 - 466089y^3, \end{aligned}$$

we may verify that

$$B_3^*(x,y)A_4^*(x,y) - A_3^*(x,y)B_4^*(x,y) = -6006y^7$$

and

$$G_4(x,y)A_4^*(x,y) - H_4(x,y)B_4^*(x,y) = -150678528y^4x^3.$$

This implies that

$$150678528^4 \times 231^4(\xi_1^4 - \eta_1^4)^{17} \subset 150678528^4 \times 231^4 p(\xi_1^4 - \eta_1^4)^{16}.$$

Since this latter quantity is equal to $150678528^4 p^{17} v^{16} B_4^*(0,1)^4$, it follows that

$$150678528^4 \times 231^4(\xi_1^4 - \eta_1^4)^{17} \subset \mathfrak{I}_4'.$$

Finally, for $r = 5$, we have

$$B_4^*(x,y)A_5^*(x,y) - A_4^*(x,y)B_5^*(x,y) = -14586y^7$$

and

$$G_5(x,y)A_5^*(x,y) - H_5(x,y)B_5^*(x,y) = -134424576y^5x^4,$$

where

$$\begin{aligned} & G_5(x,y) \\ = \; & 43706368x^4 - 69346048x^3y + 32767856x^2y^2 \\ & -4764782xy^3 + 123519y^4, \end{aligned}$$

$$\begin{aligned} & H_5(x,y) \\ = \; & 43706368x^4 - 80272640x^3y + 46006896x^2y^2 \\ & -8845746xy^3 + 391833y^4. \end{aligned}$$

This implies that

$$134424576^4 \times 209^4(\xi_1^4 - \eta_1^4)^{21} \subset 134424576^4 \times 209^4 p(\xi_1^4 - \eta_1^4)^{20}$$

whereby

$$134424576^4 \times 209^4(\xi_1^4 - \eta_1^4)^{21} \subset 134424576^4 p^{21} v^{20} B_5^*(0,1)^4 \subset \mathfrak{I}_5'.$$

From the preceding arguments, we are thus able to deduce the following series of inequalities :

$$N(\mathfrak{I}_1)^{1/2}|\xi_1^4 - \eta_1^4|^{-5} \leq 1296,$$

$$N(\mathfrak{I}_2)^{1/2}|\xi_1^4 - \eta_1^4|^{-9} \leq 560^4,$$
$$N(\mathfrak{I}_3)^{1/2}|\xi_1^4 - \eta_1^4|^{-13} \leq (77 \times 16800)^4,$$
$$N(\mathfrak{I}_4)^{1/2}|\xi_1^4 - \eta_1^4|^{-17} \leq (231 \times 150678528)^4$$

and

$$N(\mathfrak{I}_5)^{1/2}|\xi_1^4 - \eta_1^4|^{-21} \leq (134424576 \times 209)^4.$$

Substituting any of these in (2.34) provides a contradiction to inequality (2.28) when $I > 1536$ and a contradition to (2.29) when $|y| > \frac{2h^{3/4}}{(3I)^{1/8}}$. Note that under both assumptions $I > 1536$ and $|y| > \frac{2h^{3/4}}{(3I)^{1/8}}$, the function z is small. This makes $|F_r(z)|$ large enough for our contradictions. □

Lemma 2.9.2. *If $r \in \mathbb{N}$ and $h \in \{0, 1\}$, then at most one of $\{\Sigma_{r,0}, \Sigma_{r+h,1}\}$ can vanish.*

Proof. Let r be a positive integer and $h \in \{0, 1\}$. Following an argument of Bennett [3], we define the matrix $\mathbf{M}$:

$$\mathbf{M} = \begin{pmatrix} A_{r,0}(z_1) & A_{r+h,1}(z_1) & \frac{\eta_1}{\xi_1} \\ A_{r,0}(z_1) & A_{r+h,1}(z_1) & \frac{\eta_1}{\xi_1} \\ B_{r,0}(z_1) & B_{r+h,1}(z_1) & \frac{\eta_2}{\xi_2} \end{pmatrix}.$$

The determinant of $\mathbf{M}$ is zero because it has two identical rows. Expanding along the first row, we get

$$\begin{aligned} 0 \;=\; & A_{r,0}(z_1)\Sigma_{r+h,1} - A_{r+h,1}(z_1)\Sigma_{r,0} \\ & + \frac{\eta_2}{\xi_2}(A_{r,0}(z_1)B_{r+h,1}(z_1) - A_{r+h,1}(z_1)B_{r,0}(z_1)). \end{aligned}$$

If $\Sigma_{r,0} = 0$ and $\Sigma_{r+h,1} = 0$ then $A_{r,0}(z_1)B_{r+h,1}(z_1) - A_{r+h,1}(z_1)B_{r,0}(z_1) = 0$ which contradicts part (iii) of Lemma 2.2.2. □

2.10 An Auxiliary Lemma

We now combine the upper bound for $\Lambda_{r,g}$ obtained in (2.33) with the lower bounds from Lemma 2.2.2 to prove the following lemma.

Lemma 2.10.1. *If $\Sigma_{r,g} \neq 0$, then*

$$c_1(r, g)|\xi_1|^{4r+1-g}|\xi_2|^{-3} + c_2(r, g)|\xi_1|^{-4r-3(1-g)}|\xi_2| > 1,$$

where we may take

$$c_1(1,0) = 4\sqrt{3}\,\pi h\,|A_4|^{1/4}$$

and

$$c_2(1,0) = 27\,h^3\left(\frac{3}{|A_4|^{1/2}}\right)^{1/2}(9\sqrt{3I\,|A_4|})^2\frac{5}{128}$$

and for $(r,g) \neq (1,0)$,

$$c_1(r,g) = 2\sqrt{3\pi}\,h\,|A_4|^{1/4}\left(\frac{|A_4|^{1/2}}{3}\right)^{g/4}\frac{4^r}{\sqrt{r}}$$

and

$$c_2(r,g) =$$
$$27\sqrt{3}\,h^{2r+1-g}\,|A_4|^{1/4}\left(\frac{|A_4|^{1/2}}{3}\right)^{g/4}(9\sqrt{3I\,|A_4|})^{2r-g}\frac{\sqrt{2}}{\sqrt{r}\pi 4^r}.$$

Proof. By the definition of $\Lambda_{r,g}$ and (2.4), we can write

$$|\Lambda_{r,g}| = (9|A_4|)^{(1-g)/4}|\xi_1|^{4r+1-g}|\xi_2|\left|(\frac{\eta_2}{\xi_2}-\omega)A_{r,g}(z_1)+\omega z_1^{2r+1-g}F_{r,g}(z_1)\right|.$$

Since $|1-z_1| = 1$, $|z_1| \leq 1$ and $|z_i| = \frac{8h\sqrt{3I}}{|\xi_i^4|}$, by (2.5), (2.6) and inequality (2.24), we have

$$|\Lambda_{r,g}| \leq (9|A_4|)^{(1-g)/4}|\xi_1|^{4r+1-g}|\xi_2|\,\mathfrak{L}, \tag{2.36}$$

where $\mathfrak{L}$ is equal to

$$\binom{2r-g}{r}\frac{2\pi h\sqrt{3I\,|A_4|}}{3|\xi_2^4|}+\frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}}\left(\frac{9h\sqrt{3I\,|A_4|}}{|\xi_1^4|}\right)^{2r+1-g}.$$

Comparing this with (2.33), we obtain

$$c_1(r,g)|\xi_1|^{4r+1-g}|\xi_2|^{-3}+c_2(r,g)|\xi_1|^{-4r-3(1-g)}|\xi_2| > 1,$$

where we may take c_1 and c_2 so that

$$c_1(r,g) \geq$$
$$2\sqrt{3}\pi\,h\,|A_4|^{1/4}\left(\frac{|A_4|^{1/2}}{3}\right)^{g/4}\binom{2r}{r}$$

and

$$c_2(r,g) \geq$$
$$27\sqrt{3}\, h^{2r+1-g}\, |A_4|^{1/4} \left(\frac{|A_4|^{1/2}}{3}\right)^{g/4} (9\sqrt{3I\,|A_4|})^{2r-g} \frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}}.$$

Substituting $r = 1$ and $g = 0$, we get the desired values for $c_1(1,0)$ and $c_2(1,0)$. Let us apply the following version of Stirling's formula (see Theorem (5.44) of [15]):

$$\frac{1}{2\sqrt{k}}4^k \leq \binom{2k}{k} < \frac{1}{\sqrt{\pi k}}4^k,$$

for $k \in \mathbb{N}$. This leads to the stated choice of c_1 immediately.

To evaluate $c_2(r,g)$, we first note that

$$\binom{2r+1-g}{r} \geq \binom{2r}{r} \geq \frac{4^r}{2\sqrt{r}}.$$

Next we will show that

$$\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r} < \frac{1}{\sqrt{2\pi r}}, \tag{2.37}$$

for $r \in \mathbb{N}$ and $g \in \{0,1\}$, whence we may conclude that

$$\frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}} < \frac{\sqrt{2}}{\sqrt{r}\pi 4^r}.$$

This leads immediately to the stated choice of c_2. It remains to show (2.37). Let us set

$$X_r = \binom{r-3/4}{r}\binom{r-1/4}{r} = \frac{y_r}{r},$$

whereby

$$X_{r+1} = \binom{r+1/4}{r+1}\binom{r+3/4}{r+1} = \left(\frac{r^2+r+2/9}{r^2+r}\right)\frac{y_r}{r+1}.$$

This implies

$$y_1 = 3/16\ ,\ y_r = \frac{3}{16}\prod_{k=1}^{r-1}\frac{k^2+k+3/16}{k^2+k}.$$

Since

$$\prod_{k=1}^{\infty}\frac{k^2+k+3/16}{k^2+k} = \frac{16}{3\Gamma(1/4)\Gamma(3/4)} = \frac{16}{3\sqrt{2}\pi},$$

we obtain

$$X_r < \frac{1}{\sqrt{2\pi r}}.$$

For $r \in \mathbb{N}$, we have

$$\binom{r-3/4}{r} > \binom{r+1/4}{r+1}.$$

So when $g \in \{0, 1\}$,

$$\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r} \leq X_r,$$

which completes the proof. □

2.11 Proof of Theorem 2.1.2

Let us now assume that there are 4 distinct solutions (x_i, y_i) to reduced form

$$|F(x,y)| \leq h$$

related to ω with $|y_i| > \frac{h^{3/4}}{(3I)^{1/8}}$, corresponding to ξ_{-1}, ξ_0, ξ_1 and ξ_2, where we have ordered these in nondecreasing modulus. From (2.29) and Lemma 2.7.1, we have

$$|\xi_1| > 0.1\,|A_4|^{1/8}\,I^{9/8}h^{11/4}.$$

We will deduce a contradiction, implying that at most 3 such solutions can exist. Then Theorem 2.1.1 will be proven, since there are 4 choices of ω.

We will show that $|\xi_2|$ is arbitrarily large in relation to $|\xi_1|$. This contradicts (2.29).

Lemma 2.11.1. *Let $F(x,y)$ be the quartic form in Theorem 2.1.2. Suppose that (x_1, y_1) and (x_2, y_2) are 2 pairs of solutions to $|F(x,y)| \leq h$, both related to ω, a fixed fourth root unity, with*

$$0.1\,|A_4|^{1/8}\,h^{11/4}I^{9/8} < |\xi_1| < |\xi_2|,$$

where $\xi_j = \xi(x_j, y_j)$. Then, for each positive integer r,

$$|\xi_2| > \frac{4^r\sqrt{r}}{27\sqrt{3}\,|A_4|^{1/8}\,h^{2r+1}}(9\sqrt{3I\,|A_4|})^{-2r}|\xi_1|^{4r+3}.$$

Proof. By (2.26), $|\xi_2| \geq \frac{3|\xi_1|^3}{2\pi h|A_4|^{1/4}}$. This implies

$$c_1(1,0)|\xi_1|^5|\xi_2|^{-3} \leq 4\,h^4\pi \times 12^{3/2}\sqrt{3}\,|A_4|^{1/2}\,|\xi_1|^{-4}$$

Therefore, by (2.29) and from the fact that $|A_4| < 4I$, we obtain

$$c_1(1,0)|\xi_1|^5|\xi_2|^{-3} < 0.01$$

Lemma 2.9.1 implies that $\Sigma_{1,0} \neq 0$. So we may apply Lemma 2.10.1 to get

$$c_2(1,0)I^3|\xi_1|^{-7}|\xi_2| > 0.99.$$

One may now conclude that

$$|\xi_2| > \frac{0.99}{c_2(1,0)}|\xi_1|^7 > 0.93\,h^{-3}\left(\frac{3}{|A_4|^{1/2}}\right)^{-1/2}(9\sqrt{3I\,|A_4|})^{-2}|\xi_1|^7.$$

This proves the lemma for $r = 1$. Moreover, we may conclude that

$$c_1(2,0)|\xi_1|^9|\xi_2|^{-3} < \frac{18\,h^{10}\sqrt{\pi} \times 16 \times (5 \times 27)^3}{\sqrt{2}|A_4|127^3}\left(9\sqrt{3I\,|A_4|}\right)^6|\xi_1|^{-12}.$$

Since $|A_4| \leq 4I$, by (2.29) we have

$$c_1(2,0)|\xi_1|^9|\xi_2|^{-3} < 0.1.$$

Via Lemmas 2.10.1 and 2.9.1, we obtain

$$|\xi_2| > \frac{0.9}{c_2(1,0)}|\xi_1|^{11}.$$

This leads to the proof of the Lemma for $r = 2$, after substituting the value of $c_2(2,0)$. To complete the proof, we use induction on r. Suppose that for some $r \geq 2$,

$$|\xi_2| > \frac{4^r\sqrt{r}}{27\sqrt{3}\,|A_4|^{1/8}\,h^{2r+1}}(9\sqrt{3I\,|A_4|})^{-2r}|\xi_1|^{4r+3}.$$

Then

$$c_1(r+1,0)|\xi_1|^{4r+5}|\xi_2|^{-3} < \frac{18\sqrt{\pi} \times 27^3\,|A_4|^{1/8}\,h^{6r+4}}{4^{2r-1}\sqrt{(r+1)}r\sqrt{r}}\left(9\sqrt{3I\,|A_4|}\right)^{6r}|\xi_1|^{-8r-4}.$$

By (2.29), we have

$$c_1(r+1,0)|\xi_1|^{4r+5}|\xi_2|^{-3} < 0.1.$$

If $\Sigma_{r+1,0} \neq 0$, then by Lemma 2.10.1,

$$c_2(r+1,0)|\xi_1|^{-4(r+1)-3}|\xi_2| > 0.9.$$

Hence,

$$\begin{aligned} |\xi_2| &> \frac{0.9}{c_2(r+1,0)}|\xi_1|^{4(r+1)+3} \\ &> \frac{4^{r+1}\sqrt{r+1}}{27\,h^{2r+3}}\left(\frac{|A_4|^{1/2}}{3}\right)^{1/2}(9\sqrt{3I})^{-2r-2}|\xi_1|^{4r+7}. \end{aligned}$$

If, however, $\Sigma_{r+1,0} = 0$, then by Lemma 2.9.2, both $\Sigma_{r+1,1}$ and $\Sigma_{r+2,1}$ are both non-zero and by Lemma 2.9.1, we have $r > 5$. Using the induction hypothesis, we get

$$c_1(r+1,1)|\xi_1|^{4r+4}|\xi_2|^{-3} < 0.01$$

and thus by Lemma 2.10.1, (2.10) and (2.28), we conclude

$$c_2(r+1,1)|\xi_1|^{-4r-4}|\xi_2| > 0.99.$$

So, we obtain

$$|\xi_2| > \frac{4^{r+1}\sqrt{r+1}}{27\,h^{2r+2}\,|A_4|^{1/8}\,3^{1/4}}\left(9\sqrt{3I\,|A_4|}\right)^{-2r-1}|\xi_1|^{4(r+1)}.$$

Consequently, $c_1(r+2,1)|\xi_1|^{4r+8}|\xi_2|^{-3}$ is less than

$$\frac{2\sqrt{\pi}\times 27\left(3\,|A_4|^{1/2}\right)\left(9\sqrt{3I\,|A_4|}\right)^{6r+3}h^{6r+7}}{4^{2r+1}(r+1)\sqrt{(r+1)\,(r+2)}}|\xi_1|^{-8r-4} < 0.1.$$

A final application of Lemma 2.10.1 implies

$$c_2(r+2,1)|\xi_1|^{-4r-8}|\xi_2| > 0.9$$

or

$$|\xi_2| > \frac{0.9}{c_2(r+2,1)}|\xi_1|^{4r+8}.$$

It follows that

$$|\xi_2| > \frac{\sqrt{r+2}\,4^{r+2}}{27}\frac{|A_4|^{1/8}}{3^{1/4}h^{2r+4}}\left(9\sqrt{3I\,|A_4|}\right)^{-2r-3}|\xi_1|^{4(r+1)+4}.$$

Since $|\xi_1| > 0.1I^{9/8}h^{11/4}\,|A_4|^{1/8}$, we conclude that

$$|\xi_2| > \frac{4^{r+1}\sqrt{r+1}}{27\sqrt{3}\,|A_4|^{1/8}}(9\sqrt{3I\,|A_4|})^{-2r-2}|\xi_1|^{4r+7}.$$

□

2.12 Representation Of Unity By $F(x, y)$

2.12.1 The Proof Of Theorem 2.1.1 for $I > 1536$

Let us now assume that there are 4 distinct solutions to $|F(x, y)| = 1$ related to ω, corresponding to ξ_{-1} , ξ_0 , ξ_1 and ξ_2, where we have ordered these in nondecreasing modulus. From (2.28), we have

$$|\xi_1| > 0.06\,I^{9/8}.$$

Similar to Lemma 2.11.1, one can show that for $I > 1536$,

$$|\xi_2| > \frac{4^r\sqrt{r}}{27\sqrt{3}\,|A_4|^{1/8}}(9\sqrt{3I\,|A_4|})^{-2r}|\xi_1|^{4r+3}.$$

This, together with (2.28), provides a contradiction when $I > 1536$. So we conclude that related to each fourth root of unity, there are at most 3 solutions to equation (2.1). Since there are 4 such roots of unity, we conclude Theorem 2.1.1 when $I > 1536$.

2.12.2 Forms With Small Discriminant

To finish the proof of Theorem 2.1.1, we need to study the quartic forms $F(x, y) = a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4$ with $0 < I_F \leq 1536$ and $A_0 = 3(8a_0a_2 - 3a_1^2) < 0$. Quartic forms with $I > 0$ and $A_0 < 0$ are called forms of type 2 (signature $(4, 0)$) in [8].

We followed an algorithm of Cremona, in section 4.6 of [8], which gives all inequivalent integer quartics with given invariant I and $J = 0$. Using Magma, we counted the number of solutions to

$$|F(x, y)| = 1$$

for all reduced quartic forms F with $I_F \leq 1536$ and $J_F = 0$. Regarding (x, y) and $(-x, -y)$ as the same, we didn't find any form F for which there are more than 4 solutions to $F(x, y) = \pm 1$. We have solved about 1200 equations

$$|F(x, y)| = 1.$$

Our algorithm is not efficient in the sense that it solves more than one equation from some equivalent classes. We finish this paper by giving some examples with $I_F \leq 1536$ and $J_F = 0$, for which

$$F(x, y) = \pm 1$$

has 4 solutions:
If

$$F(x, y) = x^4 - 12x^2y^2 + 16xy^3 + 4y^4$$

then

$$F(x, y) = 1$$

has 4 solutions $(5, 2)$, $(1, 3)$, $(1, 1)$, $(1, 0)$ and the equation

$$F(x, y) = -1$$

has no solution.
If

$$F(x, y) = 4x^4 - 12x^2y^2 - 8xy^3 - y^4$$

then

$$F(x, y) = 1$$

has no solution and the equation

$$F(x, y) = -1$$

has 4 solutions $(-3, 5)$, $(-1, 1)$, $(0, 1)$, $(2, 1)$.
For the folowing forms the equation

$$|F(x, y)| = 1$$

has 4 solutions:
If

$$F(x, y) = x^4 - x^3y - 6x^2y^2 + xy^3 + y^4$$

then the solutions are:

$$(-1, 0), (0, 1), (-1, 2), (2, 1).$$

If

$$F(x, y) = 4x^4 - 6x^3y - 3x^2y^2 + 5xy^3 - y^4$$

then the solutions are

$$(-1, 1), (2, 3), (0, 1), (1, 1).$$

Bibliography

[1] S. Akhtari. The Diophantine equation $aX^4 - bY^2 = 1$. (2007), to appear in J. Reine Angew. Math.

[2] S. Akhtari and G. Walsh. The Diophantine equation $aX^4 - bY^2 = 2$. (2007), to appear in Acta. Arith.

[3] M.A. Bennett. On the representation of unity by binary cubic forms. Trans. Amer. Math. Soc. 353 (2001), 1507-1534.

[4] E. Bombieri and W.M. Schmidt. On Thue's equation. Invent. Math. 88 (1987), 69-81.

[5] J.W. Cassels. An Introduction to the Geometry of Numbers. Springer-Verlag,1959.

[6] G.V. Chudnovsky. On the method of Thue-Siegel. Ann. Math. II Ser. 117 (1983), 325-382.

[7] H. Cohen, A Course in Computational Algebraic Number Theory, 3rd corrected printing, Graduate Texts in Mathematics 138 (Springer-Verlag, 1996).

[8] J.E. Cremona. Reduction of binary cubic and quartic forms. London Math Soc. J. Comput. Math 2 (1999), 62-92.

[9] J.H. Evertse. On the representation of integers by binary cubic forms of positive discriminant. Invent. Math.73(1983), 117-138.

[10] V. Krechmar. On the superior bound of the number of representations of an integer by binary forms of the fourth degree (Russian). Bull. Acad. Sci. URSS, Ser. Math. (1939), 289-302

[11] W. Ljunggren. On the representation of integers by certain binary cubic and biquadratic forms. Acta. Arith. XVII (1971)

[12] C.L. Siegel. Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Wiss. 1 (1929).

[13] C.L. Siegel. Einige Erläuterungen zu Thues Untersuchungen über Annäherungswerte algebraischer Zahlen und diophantische Gleichungen, Akad. D. Wiss. in Gottingen , Math.-Phys. Klasse 1970. no 8, (1970), 169-195.

[14] C.L. Siegel. Die Gleichung $ax^n - by^n = c$, Math. Ann. 114 (1937), 57-68.

[15] K. Stromberg. An Introduction to Classical Real Analysis. Wadsworth international mathematical series, 1981.

[16] A. Thue. Bemerkungen über gewisse Näherungsbrüche algebraischer Zahlen, Kra. Vidensk. Selsk. Skrifter. I. Mat. Nat. Kl. (1908), no 3, Kra, 1908.

[17] A. Thue. Über Annäherungenswerte algebraischer Zahlen. J. reine angew. Math. 135 (1909), 284-305.

[18] A. Thue. Über rationale Annäherungswerte der reellen Wuzel der ganzen Funktion dritten Grades $x^3 - ax - b$. Kra. Vidensk. Selsk. Skrifter. I. Mat. Nat. Kl. (1908), no. 6, Kra, 1908.

[19] A.Thue. Ein Fundamental theorem zur Bestimmunhg von Annäherungs-werten aller Wurzeln gewisser ganzer Funktionen. J. Reine Angew. Mat. 138 (1910), 96-108.

Chapter 3

The Diophantine equation $aX^4 - bY^2 = 1$ [2]

3.1 Introduction

In a series of papers over nearly forty years, Ljunggren (see e.g. [11], [12], [13], [14] and [15]) derived remarkable sharp bounds for the number of solutions to various quartic Diophantine equations, particularly those of the shape

$$aX^4 - bY^2 = \pm 1, \tag{3.1}$$

typically via sophisticated application of Skolem's p-adic method. More recently, there has been a resurgence of interest in Ljunggren's work; results along these lines are well surveyed in the paper of Walsh [26]. By way of example, using lower bounds for linear forms in logarithms, together with an assortment of elementary arguments, Bennett and Walsh [2] showed that the equation

$$aX^4 - bY^2 = 1 \tag{3.2}$$

has at most one solution in positive integers X and Y, when a is an integral square and b is a positive integer. For general a and b, however, there is no absolute upper bound for the number of integral solutions to (3.2) available in the literature, unless one makes strong additional assumptions (see e.g. [2], [3], [5], [7], [14], [15] and [22]). This lies in sharp contrast to the situation for the apparently similar equation

$$aX^4 - bY^2 = -1 \tag{3.3}$$

where Ljunggren [12] was able to bound the number of positive integral solutions by 2 for arbitrary fixed a and b. Moreover, it appears that the techniques employed to treat equation (3.3) and, in special cases, (3.2), do not lead to results for (3.2) in general.

[2] A version of this chapter has been accepted for publication. Akhtari. S. The Diophantine equation $aX^4 - bY^2 = 1$. to appear in J. Reine Angew. Math.

It is our goal in this paper to rectify this situation. To be precise, we will prove the following

Theorem 3.1.1. *Let a and b be positive integers. Then equation (3.2) has at most two solutions in positive integers (X, Y).*

This resolves a conjecture of Walsh (see [2], [3], [7] and [26]), which had been suggested by computations and assorted heuristics. Since there are infinitely many pairs (a, b) for which two such solutions exist (see Section 3.2), this result is best possible.

To prove this, we will appeal to classical results of Thue [21] from the theory of Diophantine approximation, together with modern refinements, particularly those of Evertse [8]. Such an approach, based on Padé approximation to binomial functions, has been used in a number of previous works to explicitly solve Thue inequalities and equations (see e.g. [3], [5], [9], [22], [23], [24]) or to bound the number of such solutions (see e.g. [1], [8], [10]). We will apply similar techniques to a certain family of quartic inequalities.

3.2 An Equivalent Problem

Let a denote a non-square positive integer, and b a positive integer for which the quadratic equation

$$aX^2 - bY^2 = 1 \tag{3.4}$$

is solvable in positive integers X and Y. Let (v, w) be a pair of positive solutions to (3.4) so that

$$\tau = v\sqrt{a} + w\sqrt{b} > 1,$$

and τ is minimal with this property. All solutions in positive integers of (3.4) are given by (v_{2k+1}, w_{2k+1}), where

$$\tau^{2k+1} = v_{2k+1}\sqrt{a} + w_{2k+1}\sqrt{b} \qquad (k \geq 0)$$

(see [25] for a proof). Solving the quartic equation (3.2) is thus equivalent to the problem of determining all squares in the sequence $\{v_{2k+1}\}$. One can find a proof of the following result in [16].

Proposition 3.2.1. *If v_{2k+1} is a square for some $k \geq 0$, then v_1 is also a square.*

Let us assume that equation (3.2) is solvable. Proposition 3.2.1 implies that $\tau = \tau(a,b)$ is of the form $\tau = x^2\sqrt{a} + w\sqrt{b}$. We have

$$\tau = \sqrt{t+1} + \sqrt{t},$$

where $t = ax^4 - 1$. Thus, for $k \geq 0$

$$\tau^{2k+1} = V_{2k+1}\sqrt{t+1} + W_{2k+1}\sqrt{t},$$

where $V_{2k+1} = \frac{v_{2k+1}}{v_1}$. Hence, by Proposition 3.2.1, v_{2k+1} is a square if and only if V_{2k+1} is a square. In other words, in order to bound the number of positive integer solutions to an equation of the form $aX^4 - bY^2 = 1$, it is sufficient to determine an upper bound for the number of integer solutions to Diophantine equations of the shape

$$(t+1)X^4 - tY^2 = 1. \tag{3.5}$$

The main result of [3] is the following.

Proposition 3.2.2. *Let m be a positive integer. Then the only positive integral solutions to the equation*

$$(m^2+m+1)X^4 - (m^2+m)Y^2 = 1$$

are given by $(X,Y) = (1,1)$ and $(X,Y) = (2m+1, 4m^2+4m+3)$.

In fact, these are the only values of t for which equation (3.5) is known to have as many as two positive solutions (suggesting a stronger version of Theorem 3.1.1). Note that if $V_3 = z^2$, where z is a positive integer, then since $V_3 = 1 + 4t$, we have

$$4t = z^2 - 1 = (z-1)(z+1)$$

and therefore there exist positive integers m and n such that $t = mn$, $2m = z-1$ and $2n = z+1$. We conclude, therefore, that $n = m+1$ and $t = m^2+m$. Proposition 3.2.2 thus implies the following.

Corollary 3.2.3. *If V_3 is a square then for any $k > 1$, V_{2k+1} is not a square and there are only 2 solutions to equation (3.5) in positive integers X and Y.*

As it transpires, we will need to account for the possibility of V_{2k+1} being square, for odd values of k. The preceding result handles the case $k = 1$. For $k = 3$ and $k = 5$, we will appeal to

Lemma 3.2.4. *If $t > 204$, then neither V_7 nor V_{11} is an integral square.*

Proof. The equation $z^2 = V_7 = 64t^3 + 80t^2 + 24t + 1$ was treated independently using the function faintp on SIMATH and IntegralPoints on MAGMA, and found to have only the solutions corresponding to $t = 0$ and $t = 1$. For the case $z^2 = V_{11}$, we first put $x = 4t$, and see that the desired result will follow by determining the set of rational points on the curve $z^2 = x^5 + 9x^4 + 28x^3 + 35x^2 + 15x + 1$. The proof now follows exactly as the proof for the case $M^2 = U_{11}$ on pages $8 - 10$ of [4], but with $x = P^2$ and $Q = -1$, as the proof therein does not take into account the fact that P^2 is a square.. ☐

3.3 Reduction To A Family Of Thue Equations

We will begin by applying an argument of Togbe, Voutier and Walsh [22] to reduce (3.5) to a family of Thue equations. We subsequently apply the method of Thue-Siegel to find an upper bound for the number of solutions to this family. Let

$$P(x, y) = x^4 + 4tx^3y - 6tx^2y^2 - 4t^2xy^3 + t^2y^4.$$

The following is a modified version of Proposition 2.1 of [22]. We will include a proof primarily for completeness (and since we will have need of one of the inequalities derived therein).

Proposition 3.3.1. *Let t be a positive integer such that $t \neq m^2 + m$ for all $m \in \mathbb{Z}$. If $(X, Y) \neq (1, 1)$ is a positive integer solution to equation (3.5), then there is a solution in coprime positive integers (x, y) to the equation*

$$P(x, y) = t_1^2,$$

where t_1 divides t, $t_1 \leq \sqrt{t}$ and $xy > 64t^3$.

Proof. For $k \geq 0$, let us define τ, V_{2k+1} and W_{2k+1} as in Section 3.2, and choose T_k and U_k to satisfy

$$\tau^{2k} = T_k + U_k\sqrt{t(t+1)}.$$

Assume that $V_{2k+1} = z^2$ for some integer $z > 1$. We will suppose that k is odd, $k = 2n + 1$ say, as the case that k is even is similar and discussed in [22]. When $k = 2n + 1$,

$$V_{4n+3} = z^2 = V_{2n+2}^2 + V_{2n+1}^2 = tU_{n+1}^2 + V_{2n+1}^2,$$

with, via Corollary 3.2.3, $n > 0$. Thus

$$tU_n^2 = z^2 - V_{2n+1}^2 = tU_n^2 = z^2 - (T_n + tU_n)^2.$$

Since

$$U_{n+1} = 2T_n + (2t+1)U_n$$

and $\gcd(U_n, T_n) = 1$, we have

$$\gcd(U_{n+1}, T_n + tU_n) = 1$$

and hence there exist positive integers G, H, t_1, t_2, with $U_{n+1} = 2GH$ and $t = t_1 t_2$, such that

$$z - (T_n + tU_n) = 2t_1G^2 \quad \text{and} \quad z + (T_n + tU_n) = 2t_2H^2.$$

Therefore,

$$T_n + tU_n = t_2H^2 - t_1G^2,$$

and since

$$2GH = U_{n+1} = 2T_n + (2t+1)U_n,$$

we deduce that

$$U_n = 2GH - 2t_2H^2 + 2t_1G^2$$

and

$$T_n = t_2H^2 - t_1G^2 - t(2GH - 2t_2H^2 + 2t_1G^2).$$

Substituting for T_n and U_n in the equation $T_n^2 - t(t+1)U_n^2 = 1$, we obtain the equation

$$t_1^2G^4 - 4tt_1G^3H - 6tG^2H^2 + 4tt_2GH^3 + t_2^2H^4 = 1.$$

Multiplying both sides by t_1^2 and taking $x = -t_1G$, $y = H$, we find that x and y are coprime positive integers satisfying $P(x, y) = t_1^2$. To complete the proof, we observe that, since Lemma 3.2.4 and Corollary 3.2.3 imply that $n \geq 3$,

$$xy = t_1GH = \frac{t_1}{2}U_{n+1} \geq \frac{t_1}{2}U_4 > 64t^3. \tag{3.6}$$

□

Our focus for the remainder of the paper will be to find, for fixed t, an upper bound upon the number of coprime positive integral solutions to the constrained inequality

$$0 < P(x, y) \leq t^2, \quad xy > 64t^3. \tag{3.7}$$

We should note that for $t \leq 204$, Theorem 3.1.1 with $(a, b) = (t+1, t)$ has been verified in [22]. Here and henceforth, therefore, we will assume that $t > 204$. To proceed, let $\xi = \xi(x, y)$ and $\eta = \eta(x, y)$ be linear functions of (x, y) so that

$$\xi^4 = 4\,(\sqrt{-t}+1)(x - \sqrt{-t}y)^4 \quad \text{and} \quad \eta^4 = 4\,(\sqrt{-t}-1)(x + \sqrt{-t}y)^4.$$

We call (ξ, η), a pair of *resolvent forms*. Note that

$$P(x, y) = \frac{1}{8}(\xi^4 - \eta^4)$$

and if (ξ, η) is a pair of resolvent forms then there are precisely three others with distinct ratios, say $(-\xi, \eta)$, $(i\xi, \eta)$ and $(-i\xi, \eta)$. Let ω be a fourth root of unity, (ξ, η) a fixed pair of resolvent forms and set

$$z = 1 - \left(\frac{\eta(x, y)}{\xi(x, y)}\right)^4.$$

We say that the integer pair (x, y) is *related* to ω if

$$\left|\omega - \frac{\eta(x, y)}{\xi(x, y)}\right| < \frac{\pi}{12}|z|.$$

It turns out that each nontrivial solution (x, y) to (3.7) is related to a fourth root of unity :

Lemma 3.3.2. *Suppose that (x, y) is a positive integral solution to inequality (3.7), with*

$$\left|\omega_j - \frac{\eta(x, y)}{\xi(x, y)}\right| = \min_{0 \leq k \leq 3} \left|e^{k\pi i/2} - \frac{\eta(x, y)}{\xi(x, y)}\right|.$$

Then

$$|\omega_j - \frac{\eta(x, y)}{\xi(x, y)}| < \frac{\pi}{12}|z(x, y)|. \tag{3.8}$$

Proof. We begin by noting that

$$|z| = \left|\frac{\xi^4 - \eta^4}{\xi^4}\right| = \frac{8\,P(x, y)}{|\xi^4|},$$

and, from $xy \neq 0$,

$$|\xi^4(x, y)| \geq 4(\sqrt{1+t})^5,$$

whereby

$$|z| \leq \frac{2t^2}{(\sqrt{t+1})^5} < 1.$$

Since $\eta = -\bar{\xi}$, it follows that

$$\left|\frac{\eta}{\xi}\right| = 1, \quad |1 - z| = 1.$$

Now let $4\theta = \arg\left(\frac{\eta(x,y)^4}{\xi(x,y)^4}\right)$. We have

$$\sqrt{2 - 2\cos(4\theta)} = |z| < 1,$$

and so $|\theta| < \frac{\pi}{12}$. Since

$$\left|\omega_j - \frac{\eta(x,y)}{\xi(x,y)}\right| \leq |\theta|,$$

it follows that

$$\left|\omega_j - \frac{\eta(x,y)}{\xi(x,y)}\right| \leq \frac{1}{4}\frac{|4\theta|}{\sqrt{2 - 2\cos(4\theta)}}\left|1 - \frac{\eta(x,y)^4}{\xi(x,y)^4}\right|.$$

From the fact that $\frac{|4\theta|}{\sqrt{2-2\cos(4\theta)}} < \frac{\pi}{3}$ whenever $0 < |\theta| < \frac{\pi}{12}$, we obtain inequality (3.8), as desired. □

This lemma shows that each integer pair (x, y) is related to precisely one fourth root of unity. Let us fix such a fourth root, say ω, and suppose that we have distinct coprime positive solutions (x_1, y_1) and (x_2, y_2) to inequality (3.7), each related to ω. We will assume, as we may, that $|\xi(x_2, y_2)| \geq |\xi(x_1, y_1)|$. For concision, we will write $\eta_i = \eta(x_i, y_i)$ and $\xi_i = \xi(x_i, y_i)$. Before we move into the heart of our proof, we will mention a pair of results that will be the starting point for our later proving that (x_1, y_1) and (x_2, y_2) are far apart in height.

Since

$$|z| = \frac{8P(x,y)}{|\xi|^4} \leq \frac{8t^2}{|\xi|^4}, \tag{3.9}$$

it follows from (3.8) that

$$\begin{aligned} |\xi_1\eta_2 - \xi_2\eta_1| &= |\xi_1(\eta_2 - \omega\xi_2) - \xi_2(\eta_1 - \omega\xi_1)| \\ &\leq \frac{2\pi}{3}t^2\left(\frac{|\xi_1|}{|\xi_2^3|} + \frac{|\xi_2|}{|\xi_1^3|}\right) \\ &\leq \frac{4\pi t^2\,|\xi_2|}{3|\xi_1^3|}. \end{aligned} \tag{3.10}$$

On the other hand, choosing our fourth root appropriately, we have

$$\begin{pmatrix} \sqrt{2}(\sqrt{-t}+1)^{1/4} & -\sqrt{2}(\sqrt{-t}+1)^{1/4}\sqrt{-t} \\ \sqrt{2}(\sqrt{-t}-1)^{1/4} & \sqrt{2}(\sqrt{-t}-1)^{1/4}\sqrt{-t} \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$$
$$= \begin{pmatrix} \xi_1 & \xi_2 \\ \eta_1 & \eta_2 \end{pmatrix}$$

and so

$$|\xi_1\eta_2 - \xi_2\eta_1| = \left|4(t+1)^{1/4}\sqrt{t}\,(x_1y_2 - x_2y_1)\right|.$$

Since $x_1y_2 - x_2y_1$ is a nonzero integer (recall that we assumed $\gcd(x_i, y_i) = 1$), we have

$$|\xi_1\eta_2 - \xi_2\eta_1| \geq 4\sqrt{t}\,(t+1)^{1/4} \tag{3.11}$$

and thus, combining (3.10) and (3.11), we conclude that if (x_1, y_1) and (x_2, y_2) are distinct solutions to (3.7), related to ω, with $|\xi(x_2, y_2)| \geq |\xi(x_1, y_1)|$ then

$$|\xi_2| > \frac{3}{\pi} t^{-5/4}\,|\xi_1|^3. \tag{3.12}$$

As a final preliminary result, we have the following lemma, whose proof is an immediate consequence of the definition of resolvent forms :

Lemma 3.3.3. *If (x_1, y_1) and (x_2, y_2) are two pairs of rational integers then*

$$\frac{\xi(x_1,y_1)\eta(x_2,y_2)}{(-t-1)^{1/4}}, \quad \xi(x_1,y_1)^3\xi(x_2,y_2) \quad \text{and} \quad \eta(x_1,y_1)^3\eta(x_2,y_2)$$

are integers in $\mathbb{Q}(\sqrt{-t})$.

3.4 Padé Approximation

The main focus of this section is to construct a family of dense approximations to ξ/η from rational function approximations to the binomial function $(1-z)^{1/4}$. Consider the system of linear forms

$$R_r(z) = -Q_r(z) + (1-z)^{1/4}P_r(z),$$

where $R_r(z) = z^{2r+1}\bar{R}_r(z)$, $\bar{R}_r(z)$ is regular at $z = 0$, and $P_r(z)$ and $Q_r(z)$ are polynomials of degree r. Thue [19], [20] explicitly found polynomials $P_r(z)$ and $Q_r(z)$ that satisfy such a relationship, and Siegel [17] identified them in terms of hypergeometric polynomials. Refining the work of Thue and Siegel, Evertse [8] used the theory of hypergeometric functions to sharpen Siegel's upper bound for the number of solutions to the equation $f(x,y) = 1$, where f is a cubic binary form with positive discriminant. In this paper, we will apply similar arguments to certain quartic forms.

We begin with some preliminaries on hypergeometric functions. A *hypergeometric function* is a power series of the shape

$$F(\alpha,\beta,\gamma,z) = 1 + \sum_{n=1}^{\infty} \frac{\alpha(\alpha+1)\cdots(\alpha+n-1)\beta(\beta+1)\cdots(\beta+n-1)}{\gamma(\gamma+1)\cdots(\gamma+n-1)n!} z^n.$$

Here z is a complex variable and α, β and γ are complex constants. If α or β is a non-positive integer and m is the smallest integer such that

$$\alpha(\alpha+1)\cdots(\alpha+m)\beta(\beta+1)\cdots(\beta+m) = 0,$$

then $F(\alpha,\beta,\gamma,z)$ is a polynomial in z of degree m. Furthermore, if γ is a non-positive integer, we will assume that at least one of α and β is also a non-positive integer, smaller than γ.

We note that $F(\alpha,\beta,\gamma,z)$ converges for $|z| < 1$. By a result of Gauss, if α, β and γ are real with $\gamma > \alpha + \beta$ and γ, $\gamma - \alpha$ and $\gamma - \beta$ are not non-positive integers, then $F(\alpha,\beta,\gamma,z)$ converges for $z = 1$ and we have

$$F(\alpha,\beta,\gamma,1) = \frac{\Gamma(\gamma)\Gamma(\gamma-\alpha-\beta)}{\Gamma(\gamma-\alpha)\Gamma(\gamma-\beta)}.$$

For future use, it is worth noting that the hypergeometric function $F(\alpha,\beta,\gamma,z)$ satisfies the differential equation

$$z(1-z)\frac{d^2F}{dz^2} + (\gamma - (1+\alpha+\beta)z)\frac{dF}{dz} - \alpha\beta F = 0. \tag{3.13}$$

Our family of dense approximations to ξ/η are as given in the following lemma; their connection to hypergeometric functions will be made apparent later.

Lemma 3.4.1. *Let r be a positive integer and $g \in \{0,1\}$. Put*

$$\begin{aligned} A_{r,g}(z) &= \sum_{m=0}^{r} \binom{r-g+\frac{1}{4}}{m}\binom{2r-g-m}{r-g}(-z)^m, \\ B_{r,g}(z) &= \sum_{m=0}^{r-g} \binom{r-\frac{1}{4}}{m}\binom{2r-g-m}{r}(-z)^m. \end{aligned} \tag{3.14}$$

(i) There exists a power series $F_{r,g}(z)$ *such that for all complex numbers* z *with* $|z| < 1$

$$A_{r,g}(z) - (1-z)^{1/4} B_{r,g}(z) = z^{2r+1-g} F_{r,g}(z) \tag{3.15}$$

and

$$|F_{r,g}(z)| \leq \frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}} (1-|z|)^{-\frac{1}{2}(2r+1-g)}. \tag{3.16}$$

(ii) For all complex numbers z *with* $|1-z| \leq 1$ *we have*

$$|A_{r,g}(z)| \leq \binom{2r-g}{r}. \tag{3.17}$$

(iii) For all complex numbers $z \neq 0$ *and for* $h \in \{1, 0\}$ *we have*

$$A_{r,0}(z) B_{r+h,1,1}(z) \neq A_{r+h,1}(z) B_{r,0}(z). \tag{3.18}$$

Proof. Put

$$C_{r,g}(z) = \sum_{m=0}^{r} \binom{r-1/4}{r-m} \binom{r-g+1/4}{m} z^m$$

and

$$D_{r,g} = \sum_{m=0}^{r-g} \binom{r-1/4}{m} \binom{r-g+1/4}{r-g+m} z^m.$$

Note that, in terms of hypergeometric functions,

$$A_{r,g}(z) = \binom{2r-g}{r} F(-1/4 - r + g, -r, -2r + g, z),$$

$$B_{r,g}(z) = \binom{2r-g}{r-g} F(1/4 - r, -r + g, -2r + g, z),$$

$$C_{r,g}(z) = \binom{r-1/4}{r} F(-1/4 - r + g, -r, 3/4, z)$$

and

$$D_{r,g}(z) = \binom{r-g+1/4}{r-g} F(1/4 - r, -r + g, 5/4, z),$$

We will begin by proving that

$$C_{r,g}(z) = A_{r,g}(1-z), \ D_{r,g}(z) = B_{r,g}(1-z).$$

The power series $F(z) = \sum_{m=0}^{\infty} a_m z^m$ is a solution to the differential equation (3.13) precisely when

$$(n+1)(\gamma+n)a_{n+1} = (\alpha+n)(\beta+n)a_n \text{ for } n = 0, 1, 2, \ldots. \tag{3.19}$$

Both $A_{r,g}(1-z)$ and $C_{r,g}(z)$ satisfy (3.13) with $\alpha = -1/4 - r + g$, $\beta = -r$, $\gamma = 3/4$. Since γ is not a non-positive integer, all coefficient a_i of power series $y(z)$ are determined by a_0. Hence the solution space of (3.13) is one-dimensional. Therefore, $A_{r,g}(1-z)$ and $C_{r,g}(z)$ are linearly dependent. On equating the coefficients of z^r in

$$(1+z)^{2r+g} = (1+z)^{r-1/4}(1+z)^{r-g+1/4},$$

we find that

$$C_{r,g}(1) = \sum_{m=0}^{r} \binom{r-1/4}{r-m}\binom{r-g+1/4}{m} = \binom{2r-g}{r} = A_{r,g}(0),$$

and hence $C_{r,g}(z) = A_{r,g}(1-z)$. Similarly, $D_{r,g}(z) = B_{r,g}(1-z)$. One can easily observe that $C_{r,g}(z)$ has positive coefficients. Hence when $|1-z| \leq 1$,

$$|A_{r,g}(z)| = |C_{r,g}(1-z)| \leq C_{r,g}(1) = A_{r,g}(0) = \binom{2r-g}{r}.$$

This proves part (ii) of our lemma.

To prove (3.15), we define

$$G_{r,g}(z) = F(r+1-g, r+3/4, 2r+2-g, z)$$

and notice that, for $|z| < 1$, the functions $A_{r,g}(z)$, $(1-z)^{1/4}B_{r,g}(z)$ and $z^{2r+1-g}G_{r,g}(z)$ satisfy (3.13) with $\alpha = -1/4 - r + g$, $\beta = -r$, $\gamma = -2r + g$. Suppose

$$G_{r,g}(z) = \sum_{m=0}^{\infty} g_m z^m.$$

We have $g_0 = 1$ and, for $m \geq 0$,

$$\begin{aligned} \frac{g_{m+1}}{g_m} &= \frac{(r+1-g+m)(r+3/4+m)}{(m+1)(2r+2-g+m)} \\ &\leq \frac{r+1/2-g/2+m}{m+1} \\ &= \frac{(-1)^{m+1}\binom{-r-1/2+g/2}{m+1}}{(-1)^m\binom{-r-1/2+g/2}{m}}. \end{aligned}$$

Therefore,

$$\begin{aligned} |G_{r,g}(z)| &\le \sum_{m=0}^{r} \binom{-r-1/2+g/2}{m} (-|z|)^m \\ &= (1-|z|)^{-\frac{1}{2}(2r+1-g)}. \end{aligned}$$

Since $r \ge 1$ and $g \in \{0,1\}$, $\gamma = -2r+g$ is a negative integer. By (3.19), If $F(z) = \sum_{m=0}^{\infty} a_m z^m$ is a solution to (3.13), then since a_0 and a_{2r-g+1} may vary independently, the solution space of (3.13) is two-dimensional. Therefore, there are constants c_1, c_2 and c_3, not all zero, such that

$$c_1 A_{r,g}(z) + c_2(1-z)^{1/4} B_{r,g}(z) + c_3 z^{2r+1-g} G_{r,g}(z) = 0.$$

Letting $z=0$, since $A_{r,g}(0) = B_{r,g}(0) \neq 0$, we find that $c_1 = -c_2 \neq 0$. We may thus assume $c_1 = 1$. Substituting $z=1$ in above identity thus yields $c_3 = -\frac{A_{r,g}(z)}{G_{r,g}(z)}$, whence

$$F_{r,g}(z) = A_{r,g}(1) G_{r,g}(1)^{-1} G_{r,g}(z).$$

In order to complete the proof of part (i), note that, by (3.13), we have

$$\begin{aligned} A_{r,g}(1) G_{r,g}(1)^{-1} &= \binom{r-1/4}{r} \frac{\Gamma(r+1)\Gamma(r+5/4-g)}{\Gamma(2r+2-g)\Gamma(1/4)} \\ &= \frac{\binom{r-1/4}{r}\binom{r-g+1/4}{r+1-g}}{\binom{2r+1-g}{r}}. \end{aligned}$$

It remains to prove part (iii). By (3.15),

$$A_{r,0}(z) B_{r+h,1}(z) - A_{r+h,1}(z) B_{r,0}(z) = z^{2r+h} P_{r,h}(z),$$

where $P_{r,h}(z)$ is a power series. However, the left hand side of the above identity is a polynomial of degree at most $2r+h$, and so $P_{r,h}$ must be a constant. Letting $z=1$, we obtain that $P_{r,h}$ is not 0. Therefore,

$$A_{r,0}(z) B_{r+h,1}(z) - A_{r+h,1}(z) B_{r,0}(z) = 0$$

if and only if $z = 0$. □

3.5 Some Algebraic Numbers

Combining our polynomials of the previous section with the resolvent forms defined in Section 3.3, we will consider the complex sequences $\Sigma_{r,g}$ given by

$$\Sigma_{r,g} = \frac{\eta_2}{\xi_2} A_{r,g}(z_1) - (-1)^r \frac{\eta_1}{\xi_1} B_{r,g}(z_1)$$

where $z_1 = 1 - \eta_1^4/\xi_1^4$. Define

$$\Lambda_{r,g} = \frac{\xi_1^{4r+1-g} \xi_2}{(-t-1)^{1/4}} \Sigma_{r,g}.$$

Let $\mathbf{O_K}$ be the ring of integers of the number field $\mathbf{K} = \mathbb{Q}(\sqrt{-t})$. Put

$$\mathbf{O} = \{ \frac{m + n\sqrt{-t}}{2} \in \mathbf{O_K} \quad | \quad m, n \in \mathbb{Z} \}.$$

It is easy to check that $\mathbf{O}$ is a subring of $\mathbf{O_K}$. Let d be the largest square-free divisor of t. From the well-known characterization of algebraic integers in quadratic fields, we have

$$\mathbf{O_K} = \{ a + b\, \frac{1 + \sqrt{-d}}{2} \quad | \quad a, b \in \mathbb{Z} \} \qquad \text{if} \qquad d \equiv 1 \mod 4$$

and

$$\mathbf{O_K} = \{ a + b\sqrt{-d} \quad | \quad a, b \in \mathbb{Z} \} \qquad \text{if} \qquad d \equiv 2, 3 \mod 4.$$

Therefore,

$$\theta \in \mathbf{O} \qquad \text{if and only if} \qquad \theta \in \mathbf{O_K}, \quad \theta - \bar{\theta} \in \mathbb{Z}.\sqrt{-t}, \tag{3.20}$$

where $\bar{\theta}$ is the complex conjugate of θ. This implies that

$$|\theta| \geq |\ \mathrm{Im}\ \theta| \geq \frac{1}{2}(\sqrt{t}). \tag{3.21}$$

We will show that $\Lambda_{r,g}$ is either in $\mathbf{O}$ or a fourth root of such an algebraic integer. If $\Lambda_{r,g} \neq 0$, this provides a lower bound upon $|\Lambda_{r,g}|$. In conjunction with the inequalities derived in Lemma 3.4.1, this will induce a strong "gap principle", guaranteeing that solutions to inequality (3.7) must, in a certain sense, increase rapidly in height.

For a polynomial $P(z)$ of degree n, we will denote by

$$P^*(x, y) = x^n P(y/x)$$

an associated binary form. Let $A_{r,g}$ and $B_{r,g}$ be as in (3.14) and, as in the proof of Lemma 3.4.1, set

$$C_{r,g}(z) = A_{r,g}(1-z) \quad \text{and} \quad D_{r,g}(z) = B_{r,g}(1-z).$$

For $z \neq 0$, we have $D_{r,0}(z) = z^r C_{r,0}(z^{-1})$, hence

$$\begin{aligned} A^*_{r,0}(z, z+\bar{z}) &= z^r A_{r,0}\left(1+\frac{\bar{z}}{z}\right) = z^r C_{r,0}\left(\frac{-\bar{z}}{z}\right) \\ &= (-1)^r \bar{z}^r D_{r,0}\left(\frac{-z}{\bar{z}}\right) = (-1)^r \bar{z}^r B_{r,0}\left(1+\frac{z}{\bar{z}}\right) \\ &= (-1)^r B^*_{r,0}(\bar{z}, \bar{z}+z) = (-1)^r \bar{B}^*_{r,0}(z, z+\bar{z}). \end{aligned} \tag{3.22}$$

Lemma 3.5.1. *For any pair of integers (x,y), both*

$$A^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$$

and

$$B^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$$

are contained in the subring $\mathbf{O}$.

Proof. It is clear that

$$A^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$$

and

$$B^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$$

belong to $\mathbb{Q}(\sqrt{-t})$; we need only show that they are of the shape $\frac{m+n\sqrt{-t}}{2}$. From the definitions of $A^*_{r,g}(x,y)$, $B^*_{r,g}(x,y)$, $\xi(x,y)$ and $\eta(x,y)$ (in particular, since $\xi^4(x,y) - \eta^4(x,y) = 8P(x,y)$), this is an immediate consequence of Lemma 4.1 of [6], which, in this case, implies that

$$\binom{a/4}{n} 8^n$$

is, for fixed nonnegative integers a and n, a rational integer. □

We now proceed to show that $\Lambda_{r,g}$ has the desired property. We have

$$\Lambda_{r,g} = \frac{\xi_1^{1-g}\eta_2}{(-t-1)^{1/4}} A^*_{r,g}(\xi^4, \xi^4 - \eta^4) - \frac{(-1)^r \xi_1^{2g}\xi_2\eta_1}{(-t-1)^{1/4}} B^*_{r,g}(\xi^4, \xi^4 - \eta^4).$$

By Lemmas 3.3.3, 3.5.1 and (3.22), $\Lambda_{r,0} \in \mathbb{Z}\sqrt{-t}$. Similarly, Lemmas 3.3.3 and 3.5.1 imply that $\Lambda_{r,1}^4$ is an algebraic integer in $\mathbb{Q}(\sqrt{-t})$. It can also be easily seen, from the definition of ξ and η, that $\Lambda_{r,1}^4$ belongs to $\mathbf{O}$. We claim that it is not a rational integer. To see this, let us start by noting that

$$\frac{\Sigma_{r,g}}{(-t-1)^{1/4}} = \\ \frac{\eta_2}{\xi_2}A_{r,g}(z_1) - (-1)^r\frac{\eta_1}{\xi_1}B_{r,g}(z_1) = \\ \frac{\eta}{\xi}\big(\frac{\eta_2/\eta}{\xi_2/\xi}A_{r,g}(z_1) - (-1)^r\frac{\eta_1/\eta}{\xi_1/\xi}B_{r,g}(z_1)\big),$$

where $\eta = (\sqrt{-t}-1)^{1/4}$ and $\xi = (\sqrt{-t}+1)^{1/4}$. By Lemma 3.5.1,

$$\frac{\eta_2/\eta}{\xi_2/\xi}A_{r,g}(z_1) - (-1)^r\frac{\eta_1/\eta}{\xi_1/\xi}B_{r,g}(z_1) \in \mathbb{Q}(\sqrt{-t})$$

and so

$$\begin{aligned} \mathfrak{f} = \mathbb{Q}(\sqrt{-t}, \Sigma_{r,g}) &= \mathbb{Q}(\sqrt{-t}, (-t-1)^{1/4}\frac{\eta}{\xi}) \\ &= \mathbb{Q}(\sqrt{-t}, (-t+1-2\sqrt{-t})^{1/4}). \end{aligned} \tag{3.23}$$

If we choose a complex number X so that $\xi(X,1) = \eta(X,1)$ then $X \in \mathfrak{f}$ and

$$P(X,1) = \frac{1}{8}(\xi^4(X,1) - \eta^4(X,1)) = 0.$$

Since we have assumed that P is irreducible, X and $\Sigma_{r,g}$ both have degree 4 over $\mathbb{Q}(\sqrt{-t})$.

Suppose that $\Lambda_{r,1}^4 \in \mathbb{Z}$. Then we have for some $\rho, \rho_1 \in \{\pm 1, \pm i\}$, that $\Lambda_{r,1} = \rho\bar{\Lambda}_{r,1}$ and $(-t-1)^{1/4} = \rho_1\overline{(-t-1)^{1/4})}$, whence, from Lemma 3.3.3,

$$\begin{aligned} \Sigma_{r,1} &= (-t-1)^{1/4}\xi_1^{-4r}\xi_2^{-1}\rho\bar{\Lambda}_{r,1} \\ &= \xi_1^{-4r}\xi_2^{-1}\eta_1^{4r}\eta_2\rho\rho_1\left(\frac{\xi_2}{\eta_2}A_{r,1}\left(1-\frac{\xi^4}{\eta^4}\right) - (-1)^r\frac{\xi_1}{\eta_1}B_{r,1}\left(1-\frac{\xi^4}{\eta^4}\right)\right) \\ &= \rho\rho_1\frac{\eta_1^{4r}}{\xi_1^{4r}}\left(A_{r,1}\left(1-\frac{\xi_1^4}{\eta_1^4}\right) - (-1)^r\frac{\xi_1\eta_2}{\xi_2\eta_1}B_{r,1}\left(1-\frac{\xi_1^4}{\eta_1^4}\right)\right). \end{aligned}$$

This together with Lemmas 3.3.3 and 3.5.1 imply that $\Sigma_{r,1} \in \mathbb{Q}(\sqrt{-t}, \rho\rho_1)$, which contradicts the fact that $\Sigma_{r,1}$ has degree 4 over $\mathbb{Q}(\sqrt{-t})$. We conclude that $\Lambda_{r,1}$ can not be a rational integer.

Therefore, we conclude that, if $\Lambda_{r,g} \neq 0$, $g \in \{0,1\}$, then

$$|\Lambda_{r,g}| \geq 2^{\frac{-g}{4}}\ t^{\frac{1}{2}-\frac{3g}{8}}. \tag{3.24}$$

3.6 Three Auxiliary Lemmas

We will now combine inequality (3.24) with upper bounds from Lemma 3.4.1 to show that solutions to (3.7) are widely spaced :

Lemma 3.6.1. *If $\Sigma_{r,g} \neq 0$, then*

$$c_1(r,g)\,|\xi_1|^{4r+1-g}|\xi_2|^{-3} + c_2(r,g)\,|\xi_1|^{-4r-3(1-g)}|\xi_2| > 1,$$

where we may take

$$c_1(r,g) = \frac{2^{2r+1+g/4}}{\sqrt{\pi r}}\, t^{5/4+3g/8}$$

and

$$c_2(r,g) = \frac{2^{1/2+g/4-2r}3^{4r+2-2g}}{\pi\sqrt{r}} t^{4r+5/4-13g/8}.$$

Proof. By (3.15), we can write

$$\left|(t+1)^{1/4}\,\Lambda_{r,g}\right| = |\xi_1|^{4r+1-g}|\xi_2|\ \left|\left(\frac{\eta_2}{\xi_2} - \omega\right) A_{r,g}(z_1) + \omega z_1^{2r+1-g} F_{r,g}(z_1)\right|.$$

Since $|1 - z_1| = 1$ and $|z_1| \leq 1$, from (3.8), (3.9), (3.16), (3.17), and the inequality

$$|\xi_1|^4 > 4\,(1+t)^{5/2},$$

we have

$$\left|(t+1)^{1/4}\,\Lambda_{r,g}\right| \leq |\xi_1|^{4r+1-g}|\xi_2|\mathfrak{L},$$

where $\mathfrak{L}$ is equal to

$$\binom{2r-g}{r}\frac{2t^2}{|\xi_2^4|}\frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}}\left(\frac{9t^2}{|\xi_1^4|}\right)^{2r+1-g}.$$

Comparing this with (3.24), we obtain

$$c_1(r,g)\,|\xi_1|^{4r+1-g}|\xi_2|^{-3} + c_2(r,g)\,|\xi_1|^{-4r-3(1-g)}|\xi_2| > 1,$$

where we may take c_1 and c_2 so that

$$c_1(r,g) \geq 2^{1+g/4}\,t^{5/4+3g/8}\binom{2r}{r}$$

and

$$c_2(r,g) \geq 2^{g/4}\, 3^{4r+2-2g}\, t^{4r+5/4-13g/8}\, \frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}}.$$

Applying the following version of Stirling's formula (see Theorem (5.44) of [18])

$$\frac{1}{2\sqrt{k}}4^k \leq \binom{2k}{k} < \frac{1}{\sqrt{\pi k}}4^k,$$

(valid for $k \in \mathbb{N}$) leads immediately to the stated choice of c_1.

To evaluate $c_2(r,g)$, we begin by noting that

$$\binom{2r+1-g}{r} \geq \binom{2r}{r} \geq \frac{4^r}{2\sqrt{r}}.$$

Next we will show that

$$\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r} < \frac{1}{\sqrt{2}\pi r},$$

for $r \in \mathbb{N}$ and $g \in \{0,1\}$, whence we may conclude that

$$\frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}} < \frac{\sqrt{2}}{\sqrt{r}\pi 4^r}.$$

This gives the desired value for $c_2(r,g)$. To bound $\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}$, first we note that

$$\binom{r-3/4}{r} > \binom{r+1/4}{r+1},$$

for $r \in \mathbb{N}$. Put

$$X_r = \binom{r-3/4}{r}\binom{r-1/4}{r} = \frac{y_r}{r},$$

whereby

$$X_{r+1} = \binom{r+1/4}{r+1}\binom{r+3/4}{r+1} = \left(\frac{r^2+r+2/9}{r^2+r}\right)\frac{y_r}{r+1}.$$

Hence,

$$y_1 = 3/16\ ,\ y_r = 3/16\prod_{k=1}^{r-1}\frac{k^2+k+3/16}{k^2+k}.$$

Since

$$\prod_{k=1}^{\infty}\frac{k^2+k+3/16}{k^2+k} = \frac{16}{3\Gamma(1/4)\Gamma(3/4)} = \frac{16}{3\sqrt{2}\pi},$$

we obtain

$$X_r < \frac{1}{\sqrt{2\pi r}},$$

which completes the proof. □

We will also have need of the following :

Lemma 3.6.2. *If $r \in \mathbb{N}$ and $h \in \{0,1\}$, then at most one of $\{\Sigma_{r,0}, \Sigma_{r+h,1}\}$ can vanish.*

Proof. Let r be a positive integer and $h \in \{0,1\}$. Following an argument of Bennett [1], we define the matrix $\mathbf{M}$:

$$\mathbf{M} = \begin{pmatrix} A_{r,0}(z_1) & A_{r+h,1}(z_1) & (-1)^r \frac{\eta_1}{\xi_1} \\ A_{r,0}(z_1) & A_{r+h,1}(z_1) & (-1)^r \frac{\eta_1}{\xi_1} \\ B_{r,0}(z_1) & B_{r+h,1}(z_1) & \frac{\eta_2}{\xi_2} \end{pmatrix}.$$

The determinant of $\mathbf{M}$ is zero because it has two identical rows. Expanding along the first row, we find that

$$\begin{aligned} & A_{r,0}(z_1)\Sigma_{r+h,1} - A_{r+h,1}(z_1)\Sigma_{r,0} \\ + \quad & (-1)^r \frac{\eta_1}{\xi_1}(A_{r,0}(z_1)B_{r+h,1}(z_1) - A_{r+h,1}(z_1)B_{r,0}(z_1)) \end{aligned}$$

vanishes and hence if $\Sigma_{r,0} = \Sigma_{r+h,1} = 0$, then

$$A_{r,0}(z_1)B_{r+h,1}(z_1) - A_{r+h,1}(z_1)B_{r,0}(z_1) = 0,$$

contradicting part (iii) of Lemma 3.4.1. □

Our final result of this section follows similar lines to an argument of Evertse [8]. We show :

Lemma 3.6.3. *Suppose that $t > 204$. For $r \in \{1,2,3,4,5\}$, we have*

$$\Sigma_{r,0} \neq 0.$$

Proof. Let $r \in \{1,2,3,4,5\}$ and suppose that $\Sigma_{r,0} = 0$. From (3.15), for each r, the polynomial

$$A_{r,0}(z)^4 - (1-z)B_{r,0}^4$$

has a zero at 0 of order at least $2r+1$. We can thus find polynomials $A_r(z), B_r(z)$ and $F_r(z) \in \mathbb{Z}[z]$, satisfying

$$A_r(z)^4 - (1-z)B_r^4 = z^{2r+1}F_r(z).$$

In fact, we have

$$A_1(z) = 4A_{1,0}(z) = 8 - 5z,$$

$$B_1(z) = 4B_{1,0}(z) = 8 - 3z,$$

$$F_1(z) = 320 - 320z + 81z^2,$$

$$A_2(z) = \frac{32}{3}A_{2,0}(z) = 64 - 72z + 15z^2,$$

$$B_2(z) = \frac{32}{3}B_{2,0}(z) = 64 - 56z + 7z^2,$$

$$F_2(z) = 86016 - 172032z + 114624z^2 - 28608z^3 + 2401z^4,$$

$$A_3(z) = 128A_{3,0}(z) = 2560 - 4160z + 1872z^2 - 195z^3,$$

$$B_3(z) = 128B_{3,0}(z) = 2560 - 3520z + 1232z^2 - 77z^3,$$

$$\begin{aligned} F_3(z) = & \quad 14057472000 - 42172416000z \\ & + \; 48483635200z^2 - 26679910400z^3 \\ & \quad +7150266240z^4 - 839047040z^5 \\ & + \; 35153041z^6, \end{aligned}$$

$$A_4(z) = \frac{2048}{5}A_{4,0}(z) = 28672 - 60928z + 42432z^2 - 10608z^3 + 663z^4,$$

$$B_4(z) = \frac{2048}{5}B_{4,0}(z) = 28672 - 53760z + 31680z^2 - 6160z^3 + 231z^4,$$

$$\begin{aligned} F_4(z) = & \quad 13989396348928 - 55957585395712z \\ & + \; 91916125077504z^2 - 79896826347520z^3 \\ & + \; 39463764078592z^4 - 11050000539648z^5 \\ & + \; 1648475542656z^6 - 113348764800z^7 \\ & + \; 2847396321z^8, \end{aligned}$$

$$\begin{aligned} A_5(z) & = \frac{8192}{21}A_{5,0}(z) \\ & = 98304 - 258048z + 243712z^2 - 99008z^3 + 15912z^4 - 663z^5, \end{aligned}$$

$$\begin{aligned} B_5(z) & = \frac{8192}{21}B_{5,0}(z) \\ & = 98304 - 233472z + 194560z^2 - 66880z^3 + 8360z^4 - 209z^5. \end{aligned}$$

and

$$\begin{aligned} F_5(z) = & \quad 121733331812352 - 608666659061760z \\ & + \quad 1301756554248192z^2 - 1555026262622208z^3 \\ & + \quad 1136607561252864z^4 - 523630732640256z^5 \\ & + \quad 151029162176512z^6 - 26204424888320z^7 \\ & + \quad 2515441608384z^8 - 113971885760z^9 \\ & + \quad 1908029761z^{10}. \end{aligned}$$

We also define A_r^* and B_r^* via

$$A_r^*(x,y) = x^r A_r(y/x) \quad \text{and} \quad B_r^*(x,y) = x^r B_r(y/x).$$

Since $\Sigma_{r,0}$ is assumed to be zero,

$$\frac{\eta_2^4}{\xi_2^4} = \frac{\eta_1^4 (B_r^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4}{\xi_1^4 (A_r^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4}.$$

Let $\mathfrak{I}_r$ be the integral ideal in $\mathbb{Q}(\sqrt{-t})$ generated by $\xi_1^4(A_r^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4$ and $\eta_1^4(B_r^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4$, and $N(\mathfrak{I}_r)$ be the absolute norm of $\mathfrak{I}_r$. Since the ideal generated by $\xi_1^4(A_r^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4 - \eta_1^4(B_r^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4$ divides $(\xi_2^4 - \eta_2^4)\mathfrak{I}_r$, we obtain

$$\begin{aligned} & |\xi_1|^{4(4r+1)} \left| A_r^4(z_1) - (1 - z_1) B_r^4(z_1) \right| = \\ & \left| \xi_1^4 (A_r^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4 - \eta_1^4 (B_r^*(\xi_1^4, \xi_1^4 - \eta_1^4))^4 \right| . \end{aligned}$$

From the fact that $\mathfrak{I}_r$ is contained in an imaginary quadratic field,

$$|\xi_1|^{4(4r+1)} |A_r^4(z_1) - (1 - z_1) B_r^4(z_1)| \le N(\mathfrak{I}_r)^{1/2} |\xi_2^4 - \eta_2^4|.$$

By (3.15),

$$A_r^4(z_1) - (1 - z_1) B_r^4(z_1) = z_1^{2r+1} F_r(z_1),$$

so we may conclude

$$|z_1|^{2r+1} |F_r(z_1)| \le N(\mathfrak{I}_r)^{1/2} |\xi_2^4 - \eta_2^4| |\xi_1|^{-4(4r+1)};$$

i.e.

$$1 \le \frac{N(\mathfrak{I}_r)^{1/2} |\xi_2^4 - \eta_2^4| |\xi_1|^{-4(4r+1)}}{|z_1|^{2r+1} |F_r(z_1)|}.$$

Since $|z_1| = |\xi_1^{-4}| |\xi_1^4 - \eta_1^4|$ and $|\xi_i^4 - \eta_i^4| = 8P(x,y)$, it follows after a little work that

$$|\xi_1|^{8r} \le N(\mathfrak{I}_r)^{1/2} \left| \xi_1^4 - \eta_1^4 \right|^{-4r-1} (8P(x,y))^{2r+1} |F_r(z_1)|^{-1} . \tag{3.25}$$

To estimate $N(\mathfrak{I}_r)^{1/2}$, we choose a finite extension $\mathbf{M}$ of $\mathbb{Q}(\sqrt{-t})$ so that the ideal generated by ξ_1^4 and $\xi_1^4 - \eta_1^4$ in $\mathbf{M}$ is a principal ideal, with generator p, say. We denote the extension of $\mathfrak{I}_r$ to $\mathbf{M}$, by $\mathfrak{I}'_r$. Let $\mathfrak{r}_r$ be the ideal in $\mathbf{M}$ generated by $A_r^*(u,v)$ and $B_r^*(u,v)$, where $u = \frac{\xi_1^4}{p}$ and $v = \frac{\xi_1^4 - \eta_1^4}{p}$. Since $A_r^*(x, x-y) = B_r^*(y, y-x)$,

$$\begin{aligned} p^{4r+1}\mathfrak{r}_r^4 B_r^*(0,1)^4 &\subset p^{4r+1}\mathfrak{r}_r^4(u, B_r^*(0,v)^4)(u-v, B_r^*(0,v)^4) \\ &\subset p^{4r+1}\mathfrak{r}_r^4(u, B_r^*(0,v)^4)(u-v, A_r^*(v,v)^4) \\ &\subset p^{4r+1}\mathfrak{r}_r^4(u, u-v)(u, B_r^*(u,v)^4)(u-v, A_r^*(u,v)^4) \\ &\subset p^{4r+1}(uA^*(u,v)^4, (u-v)B_r^*(u,v)^4) = \mathfrak{I}'_r, \end{aligned} \tag{3.26}$$

where $(m_1, \ldots, m_n)$ denote the ideal in $\mathbf{M}$ generated by $m_1, \ldots, m_n$.

We have

$$A_1^*(x,y) - B_1^*(x,y) = -2y.$$

Therefore,

$$2(v) \subset (A_1^*(u,v), B_1^*(u,v)) \subset \mathfrak{r}_1,$$

where (v) is the ideal generated by v in $\mathbf{M}$. Since $B_1^*(0,1) = -3$, it follows from (3.26) that

$$1296(\xi_1^4 - \eta_1^4)^5 \subset 1296p(\xi_1^4 - \eta_1^4)^4 = p^5 16v^4 B_1^*(0,1)^4 \subset \mathfrak{I}'_1.$$

For $r = 2$, we first observe that

$$B_1^*(x,y)A_2^*(x,y) - A_1^*(x,y)B_2^*(x,y) = -10y^3$$

and

$$(-32x + 7y)A_2^*(x,y) - (-32x + 15y)B_2^*(x,y) = 80xy^2.$$

Therefore, by (3.26) we have

$$80(v)^2 \subset (-10v^3, 80uv^2) \subset (A_2^*(u,v), B_2^*(u,v)) \subset \mathfrak{r}_2.$$

Since $B_2^*(0,1) = 7$, we have

$$80^4 \times 7^4(\xi_1^4 - \eta_1^4)^9 \subset 80^4 \times 7^4 p(\xi_1^4 - \eta_1^4)^8 = 80^4 p^9 v^8 B_2^*(0,1)^4 \subset \mathfrak{I}'_2.$$

When $r = 3$, we have

$$B_2^*(x,y)A_3^*(x,y) - A_2^*(x,y)B_3^*(x,y) = -210y^5$$

and

$$(1616x^2 - 1078xy + 77y^2)A_3^*(x,y) - (1616x^2 - 1482xy + 195y^2)B_3^*(x,y) = -16800x^2y^3.$$

Substituting 77 for $B_3^*(0,1)$, we conclude

$$16800^4 \times 77^4 (\xi_1^4 - \eta_1^4)^{13} \subset 16800^4 \times 77^4 p(\xi_1^4 - \eta_1^4)^{12} = 16800^4 p^{13} v^{12} B_3^*(0,1)^4 \subset \mathfrak{I}_3'.$$

For $r = 4$, setting

$$G_4(x,y) = 14178304x^3 - 15889280x^2y + 4071760xy^2 - 162393y^3,$$
$$H_4(x,y) = 14178304x^3 - 19433856x^2y + 6714864xy^2 - 466089y^3,$$

we may verify that

$$B_3^*(x,y)A_4^*(x,y) - A_3^*(x,y)B_4^*(x,y) = -6006y^7$$

and

$$G_4(x,y)A_4^*(x,y) - H_4(x,y)B_4^*(x,y) = -150678528y^4x^3.$$

This implies that

$$150678528^4 \times 231^4 (\xi_1^4 - \eta_1^4)^{17} \subset 150678528^4 \times 231^4 p(\xi_1^4 - \eta_1^4)^{16}.$$

Since this latter quantity is equal to $150678528^4 p^{17} v^{16} B_4^*(0,1)^4$, it follows that

$$150678528^4 \times 231^4 (\xi_1^4 - \eta_1^4)^{17} \subset \mathfrak{I}_4'.$$

Finally, for $r = 5$, we have

$$B_4^*(x,y)A_5^*(x,y) - A_4^*(x,y)B_5^*(x,y) = -14586y^7$$

and

$$G_5(x,y)A_5^*(x,y) - H_5(x,y)B_5^*(x,y) = -134424576y^5x^4,$$

where

$$G_5(x,y) =$$
$$43706368x^4 - 69346048x^3y + 32767856x^2y^2 - 4764782xy^3 + 123519y^4,$$
$$H_5(x,y) =$$
$$43706368x^4 - 80272640x^3y + 46006896x^2y^2 - 8845746xy^3 + 391833y^4.$$

This implies that

$$134424576^4 \times 209^4 (\xi_1^4 - \eta_1^4)^{21} \subset 134424576^4 \times 209^4 p(\xi_1^4 - \eta_1^4)^{20}$$

whereby

$$134424576^4 \times 209^4 (\xi_1^4 - \eta_1^4)^{21} \subset 134424576^4 p^{21} v^{20} B_5^*(0,1)^4 \subset \mathfrak{I}_5'.$$

From the preceding arguments, we are thus able to deduce the following series of inequalities :

$$N(\mathfrak{I}_1)^{1/2}|\xi_1^4 - \eta_1^4|^{-5} \leq 1296,$$

$$N(\mathfrak{I}_2)^{1/2}|\xi_1^4 - \eta_1^4|^{-9} \leq 560^4,$$

$$N(\mathfrak{I}_3)^{1/2}|\xi_1^4 - \eta_1^4|^{-13} \leq (77 \times 16800)^4,$$

$$N(\mathfrak{I}_4)^{1/2}|\xi_1^4 - \eta_1^4|^{-17} \leq (231 \times 150678528)^4$$

and

$$N(\mathfrak{I}_5)^{1/2}|\xi_1^4 - \eta_1^4|^{-21} \leq (209 \times 134424576)^4.$$

These will enable us to contradict inequality (3.25) for $r \leq 5$, provided we can find a suitably strong lower bound for $|\xi_1|$. Since

$$\xi_i^4 = 4(\sqrt{-t}+1)(x_i - \sqrt{-t}y_i)^4$$

and $x_1 y_1 > 64t^3$, via calculus we have that

$$|\xi_1|^4 > 2^{16}\, t^{15/2}, \tag{3.27}$$

whence (3.25) and the assumption that $P(x,y) \leq t^2$ imply

$$2^{26r-3} t^{11r-2} < N(\mathfrak{I}_r)^{1/2} \left|\xi_1^4 - \eta_1^4\right|^{-4r-1} |F_r(z_1)|^{-1}. \tag{3.28}$$

From (3.27), we have

$$|z_1| = \left|\frac{8P(x,y)}{\xi_1^4}\right| < \left(2^{13}\, t^{11/2}\right)^{-1} < 0.001,$$

and consequently,

$$F_1(z_1) > 10^2,\ F_2(z_1) > 10^4,\ F_3(z_1) > 10^{10},\ F_4(z_1) > 10^{13} \text{ and } F_5(z_1) > 10^{14}.$$

In case $r = 1$, inequality (3.28) thus implies that

$$2^{23} t^9 < 6635.52 \times t^6,$$

a contradiction for all t. Arguing similarly for $r = 2, 3, 4$ and 5, and noting that $t > 204$, completes the proof of Lemma 3.6.3. □

3.7 The Proof Of Theorem 3.1.1

Assume that there are two distinct coprime solutions (x_1, y_1) and (x_2, y_2) to inequality (3.7) with $|\xi_2| > |\xi_1|$. We will show that $|\xi_2|$ is arbitrary large in relation to $|\xi_1|$. In particular, we will demonstrate via induction that

$$|\xi_2| > \frac{\sqrt{r}}{5\,t^{4r+7/4}} \left(\frac{4}{81}\right)^r |\xi_1|^{4r+3}, \tag{3.29}$$

for each positive integer r. Since inequality (3.27) thus implies that

$$|\xi_2| > t^{7r/2+31/8},$$

for arbitrary r, we deduce an immediate contradiction.

We first prove inequality (3.29) for $r = 1$. By (3.12) and (3.27),

$$c_1(1,0)\,|\xi_1|^5|\xi_2|^{-3} < 2^{-13}\pi^{-1/2}t^{-5/2} < 0.1,$$

and hence, since $\Sigma_{1,0} \neq 0$, Lemma 3.6.1 yields

$$c_2(1,0)|\xi_1|^{-7}|\xi_2| > 0.9,$$

which, after a little work, implies (3.29).

We now proceed by induction. Suppose that (3.29) holds for some $r \geq 1$. Then

$$c_1(r+1,0)|\xi_1|^{4r+5}|\xi_2|^{-3} < \frac{2000}{\sqrt{\pi}r^2}\, t^{12r+13/2} \left(\frac{3^{12}}{2^4}\right)^r |\xi_1|^{-8r-4},$$

and hence, from (3.27),

$$c_1(r+1,0)|\xi_1|^{4r+5}|\xi_2|^{-3} < \frac{125}{2^{12}\sqrt{\pi}r^2}\, t^{-3r-1} \left(\frac{3^{12}}{2^{36}}\right)^r < 0.1.$$

If $\Sigma_{r+1,0} \neq 0$, then by Lemma 3.6.1,

$$c_2(r+1,0)|\xi_1|^{-4(r+1)-3}|\xi_2| > 0.9,$$

which leads to inequality (3.29) with r replaced by $r+1$. If, however, $\Sigma_{r+1,0} = 0$ then by Lemmas 3.6.2 and 3.6.3, both $\Sigma_{r+1,1}$ and $\Sigma_{r+2,1}$ are nonzero, and $r \geq 5$. Using the induction hypothesis, we find as previously that

$$c_1(r+1,1)|\xi_1|^{4r+4}|\xi_2|^{-3} < 0.1$$

and thus by Lemma 3.6.1 conclude that

$$c_2(r+1,1)|\xi_1|^{-4r-4}|\xi_2| > 0.9.$$

It follows that

$$|\xi_2| > 0.08 \times \frac{\sqrt{r+1}}{t^{4r+29/8}} \left(\frac{4}{81}\right)^r |\xi_1|^{4r+4}.$$

Consequently,

$$c_1(r+2,1)|\xi_1|^{4r+8}|\xi_2|^{-3} < \frac{24000}{(r+1)^2} \left(\frac{3^{12}}{2^4}\right)^r t^{12r+25/2}\,|\xi_1|^{-8r-4},$$

whereby, from (3.27) and the fact that $r \geq 5$,

$$c_1(r+2,1)|\xi_1|^{4r+8}|\xi_2|^{-3} < \frac{1}{2(r+1)^2} \left(\frac{3^{12}}{2^{36}}\right)^r t^{5-3r} < 0.1.$$

Lemma 3.6.1 thus implies the inequality

$$c_2(r+2,1)|\xi_1|^{-4r-8}|\xi_2| > 0.9$$

and so

$$|\xi_2| > 0.08\,\sqrt{r+1} \left(\frac{4}{81}\right)^{r+1} t^{-4r-61/8}|\xi_1|^{4r+8}.$$

From (3.27), it follows that

$$|\xi_2| > \frac{\sqrt{r+1}}{5t^{4r+4+7/4}} \left(\frac{4}{81}\right)^{r+1} |\xi_1|^{4r+7},$$

as desired. This completes the proof of inequality (3.29) and hence we conclude that there is at most one solution to (3.7) related to each fourth root of unity.

To finish the proof of Theorem 3.1.1, it is enough to show that three of the roots of unity under consideration do not have solutions to (3.7) associated to them. We recall that the polynomial

$$P(x,1) = x^4 + 4tx^3 - 6tx^2 - 4t^2x + t^2$$

has 4 real roots β_1, β_2, β_3, β_4, say, where

$$\sqrt{t} + \frac{1}{2} + \frac{1}{8\sqrt{t}} - \frac{2}{8t} < \beta_1 < \sqrt{t} + \frac{1}{2} + \frac{1}{8\sqrt{t}} - \frac{1}{8t}$$

$$-\sqrt{t} + \frac{1}{2} - \frac{1}{8\sqrt{t}} - \frac{1}{8t} < \beta_2 < -\sqrt{t} + \frac{1}{2} - \frac{1}{8\sqrt{t}}$$

$$\frac{1}{4} - \frac{5}{64t} + \frac{22}{512t^2} < \beta_3 < \frac{1}{4} - \frac{5}{64t} + \frac{23}{512t^2}$$

$$-4t - \frac{5}{4} + \frac{21}{64t} - \frac{87}{512t^2} < \beta_4 < -4t - \frac{5}{4} + \frac{21}{64t} - \frac{84}{512t^2}.$$

(since $t \geq 18$, the polynomial $P(x,1)$ changes sign between the given bounds). Since

$$P(\beta_i, 1) = \frac{1}{8}(\xi^4(\beta_i,1) - \eta^4(\beta_i,1)) = 0,$$

it follows that, for each $1 \leq i \leq 4$, $\frac{\eta(\beta_i,1)}{\xi(\beta_i,1)}$ is a fourth root of unity. Noting that

$$\frac{\eta(\beta_i,1)}{\xi(\beta_i,1)} - \frac{\eta(\beta_j,1)}{\xi(\beta_j,1)} = \left(\frac{\sqrt{-t}-1}{\sqrt{-t}+1}\right)^{1/4} \frac{2\sqrt{-t}(\beta_j - \beta_i)}{(\beta_i - \sqrt{-t})(\beta_j - \sqrt{-t})},$$

they are in fact distinct. We now proceed to show that solutions to (3.7) necessarily correspond to fourth roots of unity related to β_2.

In [22], it is shown that for $\{V_{2n+1}\}$ defined in Section 3.2, the equation $z^2 = V_{4n+1}$ has no solution. Supposing that $z^2 = V_{4n+3}$, as in the proof of Proposition 3.3.1, there exist integers t_1, t_2, G and H, so that the integers x, y arising from Proposition 3.3.1 satisfy $x = -t_1 G$ and $y = H$. We have

$$\begin{aligned} \frac{x}{y} = \frac{-t_1 G}{H} = \frac{-2t_1 G^2}{2GH} &= -\frac{\sqrt{V_{4n+3}} - V_{2n+1}}{U_{n+1}} \\ &= -\frac{\sqrt{V_{2n+2}^2 + V_{2n+1}^2} - V_{2n+1}}{\frac{V_{2n+2}}{\sqrt{t}}} \\ &= -\sqrt{t}\left(\sqrt{1 + \frac{V_{2n+1}^2}{V_{2n+2}^2}} - \frac{V_{2n+1}}{V_{2n+2}}\right), \end{aligned}$$

using the fact that $V_{2n+2} = \sqrt{t}\,U_{n+1}$. Thus

$$\left|\frac{x}{y} + \sqrt{t}\right| = \sqrt{t}\left|\sqrt{1 + \frac{V_{2n+1}^2}{V_{2n+2}^2}} - \frac{V_{2n+1}}{V_{2n+2}} - 1\right|.$$

A crude application of the Mean Value Theorem therefore implies that

$$\left|\frac{x}{y} + \sqrt{t}\right| < \sqrt{t}$$

and consequently, $x/y \in (-2\sqrt{t}, 0)$, whereby the inequalities for β_i yield

$$\left|\frac{x}{y} - \beta_1\right| \geq \left|\sqrt{t} + \beta_1\right| - \left|\frac{x}{y} + \sqrt{t}\right| > 2\sqrt{t} - \sqrt{t} = \sqrt{t},$$

$$\left|\frac{x}{y} - \beta_3\right| \geq \left|\sqrt{t} + \beta_3\right| - \left|\frac{x}{y} + \sqrt{t}\right| > \sqrt{t} + \frac{1}{5} - \sqrt{t} = \frac{1}{5}$$

and

$$\left|\frac{x}{y} - \beta_4\right| \geq \left|\sqrt{t} + \beta_4\right| - \left|\frac{x}{y} + \sqrt{t}\right| > 3t - \sqrt{t} > 2t.$$

Let $\beta \in \{\beta_1, \beta_3, \beta_4\}$. We have just shown that if (x, y) is a solution to inequality (3.7), then

$$\left|\frac{x}{y} - \beta\right| > \frac{1}{5}.$$

If we suppose that $\omega = \frac{\eta(\beta,1)}{\xi(\beta,1)}$, then

$$\left|\omega - \frac{\xi(x,y)}{\eta(x,y)}\right| = \left|\frac{\eta(\beta,1)}{\xi(\beta,1)} - \frac{\eta(\frac{x}{y},1)}{\xi(\frac{x}{y},1)}\right| = \left|\frac{2\sqrt{-t}(\frac{x}{y} - \beta)}{(\beta - \sqrt{-t})(\frac{x}{y} - \sqrt{-t})}\right|,$$

whence the inequalities

$$|\beta - \sqrt{-t}| < \sqrt{16t^2 + 17t}$$

and

$$\left|\frac{x}{y} - \sqrt{-t}\right| < \sqrt{5t}$$

(recall that $|x/y| < 2\sqrt{t}$) imply

$$\left|\omega - \frac{\xi(x,y)}{\eta(x,y)}\right| > \frac{2}{5\sqrt{80t^2 + 85t}}.$$

Since

$$|z| = \frac{8P(x,y)}{|\xi^4(x,y)|} \leq \frac{8t^2}{|\xi^4(x,y)|},$$

this, together with (3.27), contradicts Lemma 3.3.2.

This shows that there is no solution related to three of the fourth roots of unity (those corresponding to β_1, β_3 and β_4). Therefore, there is at most a single solution to inequality (3.7). Together with Propositions 3.2.2 and 3.3.1, this completes the proof of Theorem 3.1.1.

Bibliography

[1] M.A. Bennett. On the representation of unity by binary cubic forms. Trans. Amer. Math. Soc. 353 (2001), 1507–1534.

[2] M.A. Bennett and P.G. Walsh, The Diophantine equation $b^2X^4 - dY^2 = 1$, Proc. A.M.S. 127 (1999) 3481–3491.

[3] M.A. Bennett, A. Togbe, P.G. Walsh, A generalization of a theorem of Bumby on quartic Diophantine equations, International J. Number Theory 2 (2006), 195–206.

[4] A. Bremner and N. Tzanakis, On squares in Lucas sequences, to appear in J. Number Theory.

[5] J.H. Chen, P.M. Voutier, A complete solution of the Diophantine equation $x^2 + 1 = dy^4$ and a related family of quartic Thue equations, J. Number Theory 62 (1997), 71–99.

[6] G.V. Chudnovsky, On the method of Thue-Siegel, Ann. of Math. II Ser. 117 (1983), 325–382.

[7] J.H.E. Cohn, The Diophantine equation $x^4 - Dy^2 = 1$ II, Acta Arith. 78 (1997) 401–403.

[8] J.H. Evertse, On the representation of integers by binary cubic forms of positive discriminant. Invent. Math. 73 (1983), 117–138.

[9] C. Heuberger, On general families of parametrized Thue equations. Algebraic number theory and Diophantine analysis (Graz, 1998), 215–238, de Gruyter, Berlin, 2000.

[10] V. Krechmar, On the superior bound of the number of representation of an integer by binary forms of the fourth degree (Russian). Bull. Acad. Sci. URSS, Ser. Math. (1939), 289–302

[11] W. Ljunggren, Über die Gleichung $x^4 - Dy^2 = 1$. (German) Arch. Math. Naturvid. 45, (1942). no. 5, 61–70.

[12] W. Ljunggren, Ein Satz Über die diophantische Gleichung $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$. (German) Tolfte Skandinaviska Matematikerkongressen, Lund, 1953, pp. 188–194. Lunds Universitets Matematiska Inst., Lund, (1954).

[13] W. Ljunggren, Some remarks on the diophantine equations $x^2 - Dy^4 = 1$ and $x^4 - Dy^2 = 1$. J. London Math. Soc. 41 1966 542–544.

[14] W. Ljunggren, On the diophantine equation $Ax^4 - By^2 = C\,(C = 1,\, 4)$. Math. Scand. 21 1967 149–158 (1969)

[15] W. Ljunggren, A remark concerning the paper "On the diophantine equation $Ax^4 - By^2 = C(C = 1,\, 4)$". Math. Scand. 22 1968 282 (1969).

[16] A. Rotkiewicz, Application of Jacobi's symbol to Lehmer's numbers, Acta Arith. 42 (1983), 163–187.

[17] C.L. Siegel, Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Wiss. 1 (1929).

[18] K. Stromberg, An Introduction to Classical Real Analysis. Wadsworth international mathematical series, 1981.

[19] A. Thue, Bemerkungen Über gewisse Näherungsbrüche algebraischer Zahlen, Kra. Vidensk. Selsk. Skrifter. I. mat. nat. Kl. (1908), no 3, Kra, 1908.

[20] A. Thue, Über rationale Annaherungswerte der reellen Wüzel der ganzen Funktion dritten Grades $x^3 - ax - b$. Kra. Vidensk. Selsk. Skrifter. I. Mat. Nat. Kl. (1908), no. 6, Kra, 1908.

[21] A. Thue, Ein Fundamental Theorem zur Bestimmung vou Annäherungs-Werten aller Würzeln gewisser ganzer Funktionen. J. Reine Angew. Mat. 138 (1910), 96–108.

[22] A. Togbe, P.M. Voutier, P.G. Walsh, Solving a family of Thue equations with an application to the equation $x^2 - Dy^4 = 1$. Acta Arith. 120.1 (2005), 39–58.

[23] I. Wakabayashi, On a family of quartic Thue inequalities. I. J. Number Theory 66 (1997), no. 1, 70–84.

[24] I. Wakabayashi, Cubic Thue inequalities with negative discriminant. J. Number Theory 97 (2002), no. 2, 222–251.

[25] D.T. Walker, On the Diophantine equation $mX^2 - nY^2 = \pm 1$, Amer. Math. Monthly 74 (1967), 504–513.

[26] P.G. Walsh, Diophantine equations of the form $aX^4 - bY^2 = \pm 1$, in Algebraic Number Theory and Diophantine Analysis, Proceeding of International Conference in Graz 1998 (Walter de Gruyter, Berlin 2000), pp. 531–554.

Chapter 4

The Diophantine Equation $aX^4 - bY^2 = 2$ [3]

4.1 Introduction

The problem of determining upper bounds for the number of integer points on elliptic curves has received considerable attention, and is notoriously difficult. In a series of papers [11],[12],[13],[14],[15], Ljunggren proved absolute upper bounds for the number of positive integer solutions to equations of the form

$$aX^4 - bY^2 = c \quad c \in \{\pm 1, -2, \pm 4\}.$$

In the case $c = 1$, Ljunggren [12] proved that the equation $X^4 - bY^2 = 1$ has at most two solutions in positive integers X, Y. This result was extended by Bennett and the third author in [3], wherein it was proved that all equations of the form $a^2X^4 - bY^2 = 1$, with $a > 1$, have at most one solution in positive integers. In [5], Chen and Voutier proved that the equation $aX^4 - Y^2 = 1$ $(a > 2)$ has at most one solution in positive integers. These results have recently been extended by the first author [1], wherein it was proved that any equation of the form $aX^4 - bY^2 = 1$ has at most two solutions in positive integers. A key fact in proving this result is that one needs only to prove the result for the subfamily of equations $(t + 1)X^4 - tY^2 = 1$.

Noticeably absent from the above list of values for c is the particular value $c = 2$. The third author [19] has recently proved, under stringent conditions on a, b, that the equation $aX^4 - bY^2 = 2$ has at most one solution in positive integers. Proving a similar result for the general equation $aX^4 - bY^2 = 2$ remains elusive. However, the methods of [1] can be employed for the particular subfamily of equations $(t + 2)X^4 - tY^2 = 2$. The purpose of the present paper is to prove an upper bound in the case that $c = 2$. In particular, we prove

[3] A version of this chapter has been accepted for publication. Akhtari. S, Togbe. A, and Walsh. P.G. On the equation $aX^4 - bY^2 = 2$. Acta Arith. 131 (2008), 145-169.

Theorem 4.1.1. *For all odd positive integers $t > 40,000$, the equation*

$$(t+2)X^4 - tY^2 = 2 \tag{4.1}$$

has at most two solutions in positive integers X, Y. For the remaining odd positive integers t, equation (4.1) has at most three solutions in positive integers X, Y.

Theorem 4.1.1 is likely not best possible. We conjecture that the only positive integer solution to equation (4.1) is $(X, Y) = (1, 1)$, and more generally, that any equation of the form $aX^4 - bY^2 = 2$, with a and b odd, has at most one solution in positive integers, and that such a solution must arise from the fundamental solution to the quadratic equation $aX^2 - bY^2 = 2$. This conjecture was verified for (4.1) in the range $1 \le t < 1200$.

The organization of the paper is as follows. In Section 4.2 we reduce the solution of (4.1) to the problem of determining all squares in certain linear recurrences, yielding equations of the form $X^2 = V_{2k+1}(t)$. In Section 4.3, the problem is further reduced to a family of Thue equations with the property that the roots of the associated family of polynomials can be given explicitly in terms of the parameter t. We finish off the first part of the paper by proving some lower bounds in Section 4.4, which will be needed in the sequel. In Section 4.5 the family of Thue equations are shown to be written in terms of resolvent forms, and the concept of a solution being associated to a fourth root of unity is introduced. In Section 4.6 the Main Lemma is proved, which shows that for each fourth root of unity, there can be at most one associated solution to the Thue equation. The proof of this fact uses the hypergeometric method, and in particular, proves that for fixed t, there is at most one solution (k, x) to the equation $X^2 = V_{4k+3}(t)$. In Section 4.7, we use Thue's method to solve the equation $X^2 = V_{4k+1}(t)$ completely, completing the proof of Theorem 4.1.1.

4.2 Linear Recurrences

For $t \ge 1$ and odd, let $\alpha = \frac{\sqrt{t+2}+\sqrt{t}}{\sqrt{2}}$, and for $k \ge 0$, define sequences $\{V_i\}, \{U_i\}$ by

$$\alpha^{2k+1} = \frac{V_{2k+1}\sqrt{t+2} + U_{2k+1}\sqrt{t}}{\sqrt{2}},$$

$$\alpha^{2k} = V_{2k} + U_{2k}\sqrt{t(t+2)}.$$

All positive integer solutions (X, Y) to the quadratic equation

$$(t+2)X^2 - tY^2 = 2$$

are given by $(X, Y) = (V_{2k+1}, U_{2k+1})$.

Thus, a positive integer solution (X, Y), with $X > 1$, to equation (4.1) is equivalent to the existence of positive integers (t, k) satisfying

$$X^2 = V_{2k+1}(t).$$

Our strategy to prove Theorem 4.1.1 is to first prove that for fixed t, the equations

$$X^2 = V_{4k+1}(t) \tag{4.2}$$

and

$$X^2 = V_{4k+3}(t) \tag{4.3}$$

are solvable for at most one integer $k > 0$. This results in an upper bound of three solutions for equation (4.1). We then show that for t large enough, equation (4.2) has no solution with $k > 0$.

4.3 Reduction To Thue Equations

We show here that a solution to equation (4.1) gives rise to a solution to a Thue equation.

It is easily proved by induction that the following relation holds for $\{V_n\}$

$$V_{4k+1} = V_{2k+1}^2 + 2tU_{2k}^2. \tag{4.4}$$

Therefore, if $V_{4k+1} = X^2$, then

$$X^2 = V_{2k+1}^2 + 2tU_{2k}^2,$$

and hence, $(X - V_{2k+1})(X + V_{2k+1}) = 2tU_{2k}^2$. It follows that there are positive integers r, s, A, B, with $rs = 2t$ and $U_{2k} = 2AB$, for which

$$X - V_{2k+1} = 2rA^2, X + V_{2k+1} = 2sB^2.$$

Consequently, $V_{2k+1} = sB^2 - rA^2$, and from the easily seen identity $V_{2k+1} = V_{2k} + tU_{2k}$, one has that $V_{2k} = sB^2 - rA^2 - 2tAB$. Substituting these expressions for V_{2k} and U_{2k} into the equation $V_{2k}^2 - t(t+2)U_{2k}^2 = 1$ results in the equation

$$s^2B^4 - 4tsAB^3 - 12tA^2B^2 + 4rtBA^3 + r^2A^4 = 1.$$

Multiplying this equation through by s^2, and setting

$$x = -sB, y = A \tag{4.5}$$

shows that x and y satisfy the Thue equation

$$x^4 + 4tx^3y - 12tx^2y^2 - 8t^2xy^3 + 4t^2y^4 = s^2. \tag{4.6}$$

Similar to (4.4), one has the relation

$$V_{4k+3} = V_{2k+1}^2 + 2tU_{2k+2}^2,$$

and so if $V_{4k+3} = X^2$, then

$$X^2 = V_{2k+1}^2 + 2tU_{2k+2}^2.$$

Therefore, $(X - V_{2k+1})(X + V_{2k+1}) = 2tU_{2k+2}^2$, and so there are positive integers r, s, A, B, with $rs = 2t$ and $U_{2k+2} = 2AB$, for which

$$X - V_{2k+1} = 2rA^2, X + V_{2k+1} = 2sB^2.$$

It follows that $V_{2k+1} = sB^2 - rA^2$, and from identity $V_{2k+2} = V_{2k+1} + tU_{2k+2}$, one has that $V_{2k+2} = sB^2 - rA^2 + 2tAB$. Substituting these expressions into the equation $V_{2k+2}^2 - t(t+2)U_{2k+2}^2 = 1$ gives

$$s^2B^4 + 4tsAB^3 - 12tA^2B^2 - 4rtBA^3 + r^2A^4 = 1.$$

Multiplying through by s^2 and letting

$$x = sB, y = A \tag{4.7}$$

shows that x and y satisfy equation (4.6).

Asymptotically, the roots of the polynomial

$$p_t(x) = x^4 + 4tx^3 - 12tx^2 - 8t^2x + 4t^2 \tag{4.8}$$

are given as follows. We adopt the L-notation defined in [8], pages 1151-1152, that we recall here. Let c be a real number, assume $f(x), g(x)$, and $h(x)$ are real functions and $h(x) > 0$ for $x > c$. We will write

$$f(x) = g(x) + L_c(h(x))$$

if

$$g(x) - h(x) \leq f(x) \leq g(x) + h(x), \text{ for } x > c.$$

Therefore we obtain

$$\begin{aligned}
\beta^{(1)} &= \sqrt{2t} + 1 + \tfrac{1}{2\sqrt{2t}} - \tfrac{1}{2t} - \tfrac{9}{16t\sqrt{2t}} + L_6\left(\tfrac{0.59}{t^2}\right) \\
\beta^{(2)} &= -\sqrt{2t} + 1 - \tfrac{1}{2\sqrt{2t}} - \tfrac{1}{2t} + \tfrac{9}{16t\sqrt{2t}} + L_{792}\left(\tfrac{0.48}{t^2}\right) \\
\beta^{(3)} &= \tfrac{1}{2} - \tfrac{5}{16t} + \tfrac{23}{64t^2} + L_{105}\left(\tfrac{0.49}{t^3}\right) \\
\beta^{(4)} &= -4t - \tfrac{5}{2} + \tfrac{21}{16t} - \tfrac{84}{64t^2} + L_5\left(\tfrac{1.349}{t^3}\right).
\end{aligned}$$

Carefully analyzing the construction of the Thue equation (4.6), it is not difficult to verify that if $X^2 = V_{4k+1}$, with $k > 0$, then the corresponding positive integer solution (x, y), given by (4.5), to equation (4.6), satisfies the property that the closest root to x/y is $\beta^{(4)}$, whereas if $X^2 = V_{4k+3}$, then the corresponding positive integer solution (x, y), given by (3.4), to equation (4.6), satisfies the property that the closest root to $\frac{x}{y}$ is $\beta^{(1)}$. We make this comment more concrete in the following.

Lemma 4.3.1. *If $X^2 = V_{4k+1}$ is solvable with X an integer and $k > 0$, and if (x, y), given by (4.5), is the corresponding solution to the Thue equation (4.6), then*

$$|x/y - \beta^{(4)}| < \frac{1}{16t|y|^4}.$$

If $X^2 = V_{4k+3}$ is solvable with X an integer and $k > 0$, and if (x, y), given by (4.7), is the corresponding solution to the Thue equation (4.6), then

$$|x/y - \beta^{(1)}| < \frac{1}{4t|y|^4}.$$

Proof. We will prove the result for the equation $X^2 = V_{4k+1}$, as the proof for the second case is essentially identical. We will use the fact that V_{2k}/U_{2k} is a close approximation to $\sqrt{t(t+2)}$. The definition of (x, y) gives

$$\frac{x}{y} = \frac{-sB}{A} = \frac{-2sB^2}{2AB} = -\frac{X + V_{2k+1}}{U_{2k}} = -\frac{\sqrt{V_{4k+1}} + V_{2k+1}}{U_{2k}}.$$

Using the relations $V_{4k+1} = V_{2k+1}^2 + 2tU_{2k}^2$ and $V_{2k+1} = V_{2k} + tU_{2k}$, we find that

$$x/y = -(\sqrt{(V_{2k}/U_{2k})^2 + 2t(V_{2k}/U_{2k}) + (t^2+t)} + (V_{2k}/U_{2k}) + t).$$

Using the fact that V_{2k}/U_{2k} is a close approximation to $\sqrt{t(t+2)}$, we see that the above expression is closely approximated by $-4t-5/2$, which shows that the closest root to x/y is $\beta^{(4)}$. As

$$|p_t(x,y)| = |y|^4 \prod_{i=1}^{4} |x/y - \beta^{(i)}| \leq 4t^2,$$

we see that

$$|x/y - \beta^{(4)}| \leq \frac{4t^2}{|y|^4 \prod_{i \neq 4} |x/y - \beta^{(i)}|}.$$

Using the crude estimate $4t$ for each factor $|x/y - \beta^{(i)}|$, we see that

$$|x/y - \beta^{(4)}| \leq \frac{1}{16t|y|^4}.$$

□

4.4 Lower Bounds For k, t And $|y|$

In order to prove Theorem 4.1.1, we first need to verify that equation (4.1) has only the positive integer solution $(X,Y) = (1,1)$ for all t up to a certain bound. Two independent computations, using PARI and MAGMA, were run in order to verify that equation (4.1) has no positive integer solutions other than $(X,Y) = (1,1)$ for all $1 \leq t \leq 1200$. This was achieved by computing all integer solutions to each Thue equation of the form $p_t(x,y) = s^2$, where $p_t(x,y)$ is given in (4.8), and s is a divisor of $2t$.

We will also need a lower bound for k. The polynomial $V_{4k+1}(t)$ is monic and of even degree. Therefore, Runge's method can be applied directly to equation (4.2). Fortunately, Runge's method has been implemented in MAGMA by Beukers and Tengely (see [4]). This rather short MAGMA computation verified that no positive integer solutions (X,t) to equation (4.2) exist for each $1 \leq k \leq 24$.

We now describe how to obtain the lower bound $k > 6$ in the case of solving $X^2 = V_{4k+3}$. Firstly, it is trivial to see that $V_{4k+3} \equiv 3 \pmod 4$ for k even. To see this, first note that from the definition of V_k,

$$V_{2k+1} = (t+1)V_{2k-1} + tU_{2k+1},$$

and as $(t+1+\sqrt{t(t+2)})^{-1} = t+1-\sqrt{t(t+2)}$, we also have the relation

$$V_{2k-3} = (t+1)V_{2k-1} - tU_{2k+1}.$$

Combining these two equations gives the second order linear recurrence

$$V_{2k+1} = (2t+2)V_{2k-1} - V_{2k-3}.$$

Since t is odd, 4 divides $2t+2$, and so for each k,

$$V_{2k+1} \equiv -V_{2k-3} \pmod 4.$$

As $V_1 = 1$ and $V_3 = 2t+1 \equiv 3 \pmod 4$, it follows that

$$V_{2k+1} \equiv 1 \pmod 4$$

for $2k+1 \equiv 1, 7 \pmod 8$, and

$$V_{2k+1} \equiv 3 \pmod 4$$

for $2k+1 \equiv 3, 5 \pmod 8$.

If $k = 1$, then the equation is simply $X^2 = 8t^3 + 20t^2 + 12t + 1$, which is easily seen to have no solutions in positive integers X, t using MAGMA. For the case $k = 3$, the equation $V_{15} = X^2$ implies that $V_5 = 4t^2 + 6t + 1$ is either a square or three times a square by elementary divisibility properties of terms in the sequence $\{V_n\}$ (see [9] for details). Evidently, neither of these possibilities is possible. Finally, if $k = 5$, we use the fact that for each $i \geq 0$, the Jacobi symbol $(V_{16i+7}/V_{16i+5}) = -1$, which is easily proved by induction, however we provide the details for the reader. The proof uses the above linear recurrence equation for $\{V_{2k+1}\}$, the above congruences (mod 4) for V_{2k+1}, along with basic manipulation of Jacobi symbols. First,

$$\begin{aligned}(V_7/V_5) &= (((2t+2)V_5 - V_3)/V_3) \\ = (-V_3/V_5) &= -(V_3/V_5) \\ = (V_5/V_3) &= (-V_1/V_3) \\ = (-1/V_3) &= -1.\end{aligned}$$

Thus, the result holds for $i = 1$. We next show that

$$(V_{8j+7}/V_{8j+5}) = -(V_{8j-1}/V_{8j-3}),$$

for all $j \geq 0$, which upon putting $j = 2i$ and $j = 2i - 1$ gives the desired result.

$$\begin{aligned}
(V_{8j+7}/V_{8j+5}) &= (-V_{8j+3}/V_{8j+5}) \\
= -(V_{8j+3}/V_{8j+5}) &= (V_{8j+5}/V_{8j+3}) \\
= (-V_{8j+1}/V_{8j+3}) &= -(V_{8j+1}/V_{8j+3}) \\
= -(V_{8j+3}/V_{8j+1}) &= -(V_{8j-1}/V_{8j+1}) \\
= -(V_{8j+1}/V_{8j-1}) &= -(V_{8j-3}/V_{8j-1}) \\
= -(V_{8j-1}/V_{8j-3}).
\end{aligned}$$

We use the above lower bounds for k to obtain lower bounds for $|y|$, where (x, y) is a solution to the Thue equation (4.6) arising from a solution to equation (4.1). In the case of a solution to (4.1) with $X^2 = V_{4k+3}$, we see from the above construction that

$$2ry^2 = \sqrt{V_{4k+3}} - V_{2k+1} = \sqrt{V_{2k+1}^2 + 2tU_{2k+2}^2} - V_{2k+1}.$$

It follows that

$$2ry^2 = \frac{2tU_{2k+2}^2}{\sqrt{V_{2k+1}^2 + 2tU_{2k+2}^2} + V_{2k+1}}.$$

Dividing the numerator and denominator of this equation by $\sqrt{t}U_{2k+2}$ gives

$$2ry^2 = \frac{2\sqrt{t}U_{2k+2}}{\sqrt{(V_{2k+1}^2/tU_{2k+2}^2) + 2} + (V_{2k+1}/\sqrt{t}U_{2k+2})}.$$

Using the fact that $V_{2k+1} < U_{2k+2}$, it follows that

$$2ry^2 > \sqrt{t}U_{2k+2},$$

and from the lower bound

$$U_{2k+2} > (2t)^k > (2t)^6,$$

it follows that

$$|y| > 2\sqrt{2}t^{9/4}.$$

In the case of a solution to $X^2 = V_{4k+1}$, with $k > 0$, we obtain a much larger lower bound since the equation $X^2 = V_{4k+1}$ was solved using Runge's method for $1 \le k \le 24$. In this case, an analysis similar to the one given above shows that $|y| > 2^{10}t^{11}$.

4.5 Associated Fourth Roots Of Unity

Let
$$p_t(x,y) = x^4 + 4tx^3y - 12tx^2y^2 - 8t^2xy^3 + 4t^2y^4$$
and t be a positive integer. Our goal is to find, for fixed t, an upper bound upon the number of coprime nonzero integer solutions to the inequality
$$0 < p_t(x,y) \leq 4t^2. \tag{4.9}$$
To proceed, let $\xi = \xi(x,y)$ and $\eta = \eta(x,y)$ be linear functions of (x,y) so that
$$\xi^4 = 4\,(-\sqrt{-\frac{t}{2}} + 1)\left(x + \sqrt{-2t}y\right)^4$$
and
$$\eta^4 = 4\,(-\sqrt{-\frac{t}{2}} - 1)\left(x - \sqrt{-2t}y\right)^4.$$
We refer to (ξ, η) as a pair of *resolvent forms.* Note that $\xi^4 = -\bar{\eta}^4$ and that
$$p_t(x,y) = \frac{1}{8}(\xi^4 - \eta^4)$$
and if (ξ, η) is a pair of resolvent forms then there are precisely three others with distinct ratios, say $(-\xi, \eta)$, $(i\xi, \eta)$ and $(-i\xi, \eta)$. Let ω be a fourth root of unity, (ξ, η) a fixed pair of resolvent forms and set
$$z = 1 - \left(\frac{\eta(x,y)}{\xi(x,y)}\right)^4.$$
We say that the integer pair (x,y) is *related* to ω if
$$\left|\omega - \frac{\eta(x,y)}{\xi(x,y)}\right| < \frac{\pi}{12}|z|.$$
It turns out that each nontrivial solution (x,y) to (3.3) is related to a fourth root of unity :

Lemma 4.5.1. *Suppose that (x,y) is a positive integral solution to (4.9), with*
$$\left|\omega_j - \frac{\eta(x,y)}{\xi(x,y)}\right| = \min_{0\leq k\leq 3}\left|e^{k\pi i/2} - \frac{\eta(x,y)}{\xi(x,y)}\right|.$$
Then
$$|\omega_j - \frac{\eta(x,y)}{\xi(x,y)}| < \frac{\pi}{12}|z(x,y)|. \tag{4.10}$$

Proof. We begin by noting that

$$|z| = \left|\frac{\xi^4 - \eta^4}{\xi^4}\right| = \frac{8\,p_t(x,y)}{|\xi^4|},$$

and, from $xy \neq 0$,

$$|\xi^4(x,y)| \geq 8\sqrt{2}(\sqrt{t})^5,$$

whereby

$$|z| \leq \frac{4t^2}{\sqrt{2}(\sqrt{t})^5} < 1.$$

Since $\eta = -\bar{\xi}$, it follows that

$$\left|\frac{\eta}{\xi}\right| = 1, \quad |1 - z| = 1.$$

Now let $4\theta = \arg\left(\frac{\eta(x,y)^4}{\xi(x,y)^4}\right)$. We have

$$\sqrt{2 - 2\cos(4\theta)} = |z| < 1,$$

and so $|\theta| < \frac{\pi}{12}$. Since

$$\left|\omega_j - \frac{\eta(x,y)}{\xi(x,y)}\right| \leq |\theta|,$$

it follows that

$$\left|\omega_j - \frac{\eta(x,y)}{\xi(x,y)}\right| \leq \frac{1}{4}\frac{|4\theta|}{\sqrt{2 - 2\cos(4\theta)}}\left|1 - \frac{\eta(x,y)^4}{\xi(x,y)^4}\right|.$$

From the fact that $\frac{|4\theta|}{\sqrt{2-2\cos(4\theta)}} < \pi/3$ whenever $0 < |\theta| < \frac{\pi}{12}$, we obtain the desired inequality. □

We now put $\omega_i = \frac{\eta(\beta^{(i)},1)}{\xi(\beta^{(i)},1)}$ for $1 \leq i \leq 4$. The ω_i are the distinct fourth roots of unity. The following lemma represents a key step towards the proof of Theorem 4.1.1.

Lemma 4.5.2. *If $X^2 = V_{4k+1}$ is solvable, with X an integer and $k > 0$, and if (x,y), given by (4.5), is the corresponding solution to the Thue equation (4.6), then (x,y) is associated to ω_4.*
If $X^2 = V_{4k+3}$ is solvable, with X an integer and $k > 0$, and if (x,y), given by (4.7), is the corresponding solution to the Thue equation (4.6), then (x,y) is associated to ω_1.

Proof. Assume that $X^2 = V_{4k+3}$, as the other case is proved in the same way. The goal is to prove that

$$\left|\frac{\eta(\beta^{(1)},1)}{\xi(\beta^{(1)},1)} - \frac{\eta(x,y)}{\xi(x,y)}\right| < \frac{\pi}{12}\left|1 - \left(\frac{\eta(x,y)}{\xi(x,y)}\right)^4\right|.$$

Obtaining a common divisor for the left side, expanding and simplifying, shows that the above inequality is the same as

$$\frac{|2\sqrt{-2t}||x - \beta^{(1)}y|}{|\beta^{(1)} + \sqrt{-2t}||x + y\sqrt{-2t}|} < \frac{|2P_t(x,y)|}{|\xi(x,y)^4|}.$$

Cross multiplying the above and dividing through by $|y|^4$, we reduce the problem to proving the inequality

$$\frac{|2\sqrt{-2t}||2 - \sqrt{-2t}||x/y + \sqrt{-2t}|^3}{|\beta^{(1)} + \sqrt{-2t}|} \tag{4.11}$$

$$< \quad |x/y - \beta^{(2)}||x/y - \beta^{(3)}||x/y - \beta^{(4)}|. \tag{4.12}$$

Lemma 4.3.1 shows that x/y is very close to $\beta^{(1)}$. Indeed, Lemma 4.3.1, together with the lower bound for $|y|$ determined in section 4.4, show that $|x/y - \beta^{(1)}| < 1/(2^8 t^{10})$. This difference is sufficiently small that we will replace x/y in (4.11) by $\beta^{(1)}$, which entails that we need to prove the inequality

$$|2\sqrt{-2t}||2-\sqrt{-2t}||\beta^{(1)}+\sqrt{-2t}|^2 < |\beta^{(1)}-\beta^{(2)}||\beta^{(1)}-\beta^{(3)}||\beta^{(1)}-\beta^{(4)}|. \tag{4.13}$$

Expanding the left hand side of (4.13) gives an estimate with leading terms $16t^2+20t$, while that for the right hand side has leading terms $16t^2+24t$. □

4.6 The Main Lemma

The following represents the most crucial lemma of this paper, as it provides for an absolute bound for the number of integer solutions to equation (4.1).

Lemma 4.6.1. *There is at most one solution of (4.9) related to each fourth root of unity.*

Because of the lower bound for k obtained in section 4.4, we may assume that $k > 6$. Furthermore, since $\xi_i^4 = 4(-\sqrt{-\frac{t}{2}} + 1)(x_i + \sqrt{-2t}y_i)^4$, via calculus one may conclude that

$$|\xi_1|^4 > t^{23/2}. \tag{4.14}$$

4.6.1 Approximating Polynomials

The following Lemma gives a family of dense approximations to ξ/η from rational function approximations to the binomial function $(1-z)^{1/4}$.

Lemma 4.6.2. *Let r be a positive integer and $g \in \{0,1\}$. Put*

$$\begin{aligned} A_{r,g}(z) &= \sum_{m=0}^{r} \binom{r-g+\frac{1}{4}}{m} \binom{2r-g-m}{r-g} (-z)^m, \\ B_{r,g}(z) &= \sum_{m=0}^{r-g} \binom{r-\frac{1}{4}}{m} \binom{2r-g-m}{r} (-z)^m. \end{aligned}$$

(i) There exists a power series $F_{r,g}(z)$ such that for all complex numbers z with $|z| < 1$

$$A_{r,g}(z) - (1-z)^{1/4} B_{r,g}(z) = z^{2r+1-g} F_{r,g}(z) \tag{4.15}$$

and

$$|F_{r,g}(z)| \le \frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}} (1-|z|)^{-\frac{1}{2}(2r+1-g)}. \tag{4.16}$$

(ii) For all complex numbers z with $|1-z| \le 1$ we have

$$|A_{r,g}(z)| \le \binom{2r-g}{r}. \tag{4.17}$$

(iii) For all complex numbers $z \ne 0$ and for $h \in \{1,0\}$ we have

$$A_{r,0}(z) B_{r+h,1,1}(z) \ne A_{r+h,1}(z) B_{r,0}(z). \tag{4.18}$$

Proof. See the proof of Lemma 4.1 of [1]. □

Combining the polynomials of Lemma 4.6.2 with the resolvent forms $\xi(x,y)$ and $\eta(x,y)$, we will consider the complex sequences $\Sigma_{r,g}$ given by

$$\Sigma_{r,g} = \frac{\eta_2}{\xi_2} A_{r,g}(z_1) - (-1)^r \frac{\eta_1}{\xi_1} B_{r,g}(z_1)$$

where $z_1 = 1 - \eta_1^4/\xi_1^4$. Define

$$\Lambda_{r,g} = \frac{\xi_1^{4r+1-g}\xi_2}{(-\frac{t}{2}-1)^{1/4}} \Sigma_{r,g}. \tag{4.19}$$

Let $\mathbf{O_K}$ be the ring of integers of the number field $\mathbf{K} = \mathbb{Q}(\sqrt{-2t})$. Put

$$\mathbf{O} = \{\frac{m + n\sqrt{-2t}}{2} \in \mathbf{O_K} \quad | \quad m, n \in \mathbb{Z}\}.$$

It is easy to check that $\mathbf{O}$ is a subring of $\mathbf{O_K}$. Let d be the largest square-free divisor of $2t$. From the well-known characterization of algebraic integers in quadratic fields, we have

$$\mathbf{O_K} = \{a + b\,\frac{1+\sqrt{-d}}{2} \quad | \quad a, b \in \mathbb{Z}\} \qquad \text{if} \qquad d \equiv 1 \mod 4$$

and

$$\mathbf{O_K} = \{a + b\sqrt{-d} \quad | \quad a, b \in \mathbb{Z}\} \qquad \text{if} \qquad d \equiv 2, 3 \mod 4.$$

Therefore,

$$\theta \in \mathbf{O} \qquad \text{if and only if} \qquad \theta \in \mathbf{O_K}, \quad \theta - \bar{\theta} \in \mathbb{Z}(\sqrt{-2t}), \tag{4.20}$$

where $\bar{\theta}$ is the complex conjugate of θ. This implies that

$$|\theta| \geq |\text{ Im } \theta| \geq \frac{1}{2}(\sqrt{-2t}). \tag{4.21}$$

We will show that $\Lambda_{r,g}$ is either in $\mathbf{O}$ or a fourth root of such an algebraic integer. If $\Lambda_{r,g} \neq 0$, this provides a lower bound upon $|\Lambda_{r,g}|$. In conjunction with the inequalities derived in Lemma 4.6.2, this will induce a strong "gap principle".

Lemma 4.6.3. *If (x_1, y_1) and (x_2, y_2) are two pairs of rational integers then*

$$\frac{\xi(x_1, y_1)\eta(x_2, y_2)}{(-\frac{t}{2} - 1)^{1/4}}, \quad \xi(x_1, y_1)^3\xi(x_2, y_2) \quad \textit{and} \quad \eta(x_1, y_1)^3\eta(x_2, y_2)$$

are contained in $\mathbf{O}$.

Proof. This is an immediate consequence of the definition of resolvent forms. □

For a polynomial $P(z)$ of degree n, we will denote by $P^*(x, y) = x^n P(y/x)$ an associated binary form. Let $A_{r,g}$ and $B_{r,g}$ be as in Lemma 6.2, and set

$$C_{r,g}(z) = A_{r,g}(1 - z) \ \text{ and } \ D_{r,g}(z) = B_{r,g}(1 - z).$$

For $z \neq 0$, we have $D_{r,0}(z) = z^r C_{r,0}(z^{-1})$, hence

$$\begin{aligned} A^*_{r,0}(z, z+\bar{z}) &= z^r A_{r,0}\left(1 + \frac{\bar{z}}{z}\right) = z^r C_{r,0}\left(\frac{-\bar{z}}{z}\right) \\ &= (-1)^r \bar{z}^r D_{r,0}\left(\frac{-z}{\bar{z}}\right) = (-1)^r \bar{z}^r B_{r,0}\left(1 + \frac{z}{\bar{z}}\right) \\ &= (-1)^r B^*_{r,0}(\bar{z}, \bar{z}+z) = (-1)^r \bar{B}^*_{r,0}(z, z+\bar{z}). \end{aligned}$$

Lemma 4.6.4. *For any pair of integers (x, y), both*

$$A^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$$

and

$$B^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$$

belong to **O**.

Proof. It is clear that $A^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$ and $B^*_{r,g}(\xi^4(x,y), \xi^4(x,y) - \eta^4(x,y))$ belong to $\mathbb{Q}(\sqrt{-2t})$; we need only show that they belong to **O**. From the definitions of $A^*_{r,g}(x,y)$, $B^*_{r,g}(x,y)$, $\xi(x,y)$ and $\eta(x,y)$ (in particular, since $\xi^4(x,y) - \eta^4(x,y) = 8p_t(x,y)$), this is an immediate consequence of Lemma 4.1 of [6], which, in this case, implies that

$$\binom{a/4}{n} 8^n$$

is, for fixed nonnegative integers a and n, a rational integer. □

Proposition 4.6.5. *Let $\Lambda_{r,g}$ be the complex number defined in (4.19). Then $\Lambda_{r,0}$ belongs to $\mathbb{Z}.\sqrt{-2t}$ and $\Lambda_{r,1}$ is a fourth root of an algebraic integer in* **O**.

Proof. We have

$$\Lambda_{r,g} = \frac{\xi_1^{1-g}\eta_2}{(-\frac{t}{2}-1)^{1/4}} A^*_{r,g}(\xi_1^4, \xi_1^4 - \eta_1^4) - \frac{(-1)^r \xi_1^{2g}\xi_2\eta_1}{(-\frac{t}{2}-1)^{1/4}} B^*_{r,g}(\xi_1^4, \xi_1^4 - \eta_1^4).$$

By Lemmas 4.6.3 and (4.6.4), $\Lambda_{r,0} \in \mathbb{Z}\sqrt{-2t}$. Similarly, Lemmas 4.6.3 and 4.6.4 imply that $\Lambda^4_{r,1}$ is in **O**. We claim that it is not a rational integer. To see this, let us start by noting that

$$\begin{aligned} \frac{\Sigma_{r,g}}{(-\frac{t}{2}-1)^{1/4}} &= \frac{\eta_2}{\xi_2} A_{r,g}(z_1) - (-1)^r \frac{\eta_1}{\xi_1} B_{r,g}(z_1) \\ &= \frac{\eta}{\xi}\left(\frac{\eta_2/\eta}{\xi_2/\xi} A_{r,g}(z_1) - (-1)^r \frac{\eta_1/\eta}{\xi_1/\xi} B_{r,g}(z_1)\right), \end{aligned}$$

where $\eta = (\sqrt{-\frac{t}{2}} - 1)^{1/4}$ and $\xi = (\sqrt{-\frac{t}{2}} + 1)^{1/4}$. By Lemma 4.6.4,

$$\frac{\eta_2/\eta}{\xi_2/\xi} A_{r,g}(z_1) - (-1)^r \frac{\eta_1/\eta}{\xi_1/\xi} B_{r,g}(z_1) \in \mathbb{Q}(\sqrt{-2t})$$

and so

$$\begin{aligned} \mathfrak{f} = \mathbb{Q}(\sqrt{-2t}, \Sigma_{r,g}) &= \mathbb{Q}(\sqrt{-2t}, (-\frac{t}{2} - 1)^{1/4} \frac{\eta}{\xi}) \\ &= \mathbb{Q}(\sqrt{-2t}, (-\frac{t}{2} + 1 - \sqrt{-2t})^{1/4}). \end{aligned}$$

If we choose a complex number X so that $\xi(X,1) = \eta(X,1)$ then $X \in \mathfrak{f}$ and

$$p_t(X,1) = \frac{1}{8}(\xi^4(X,1) - \eta^4(X,1)) = 0.$$

Since p_t is irreducible, X and $\Sigma_{r,g}$ both have degree 4 over $\mathbb{Q}(\sqrt{-2t})$.

Suppose that $\Lambda_{r,1}^4 \in \mathbb{Z}$. Then we have for some $\rho, \rho_1 \in \{\pm 1, \pm i\}$, that $\Lambda_{r,1} = \rho \bar{\Lambda}_{r,1}$ and $(-\frac{t}{2} - 1)^{1/4} = \rho_1 \overline{(-\frac{t}{2} - 1)^{1/4}}$), whence, from Lemma 4.6.3,

$$\begin{aligned} \Sigma_{r,1} &= (-\frac{t}{2} - 1)^{1/4} \xi_1^{-4r} \xi_2^{-1} \rho \bar{\Lambda}_{r,1} \\ &= \xi_1^{-4r} \xi_2^{-1} \eta_1^{4r} \eta_2 \rho \rho_1 \left(\frac{\xi_2}{\eta_2} A_{r,1} \left(1 - \frac{\xi^4}{\eta^4}\right) - (-1)^r \frac{\xi_1}{\eta_1} B_{r,1} \left(1 - \frac{\xi^4}{\eta^4}\right)\right) \\ &= \rho \rho_1 \frac{\eta_1^{4r}}{\xi_1^{4r}} \left(A_{r,1} \left(1 - \frac{\xi_1^4}{\eta_1^4}\right) - (-1)^r \frac{\xi_1 \eta_2}{\xi_2 \eta_1} B_{r,1} \left(1 - \frac{\xi_1^4}{\eta_1^4}\right)\right). \end{aligned}$$

This together with Lemmas 4.6.3 and 4.6.4 imply that $\Sigma_{r,1} \in \mathbb{Q}(\sqrt{-2t}, \rho\rho_1)$, which contradicts the fact that $\Sigma_{r,1}$ has degree 4 over $\mathbb{Q}(\sqrt{-2t})$. We conclude that $\Lambda_{r,1}$ can not be a rational integer. □

By (4.21), we may conclude that, if $\Lambda_{r,g} \neq 0$, $g \in \{0,1\}$, then

$$|\Lambda_{r,g}| \geq 2^{\frac{-g}{4}} (2t)^{\frac{1}{2} - \frac{3g}{8}}. \tag{4.22}$$

4.6.2 Gap Principles

Lemma (4.9) shows that each integer pair (x,y) is related to precisely one fourth root of unity. Let us fix such a fourth root, say ω, and suppose that we have distinct coprime positive solutions (x_1,y_1) and (x_2,y_2) to inequality (4.9), each related to ω. We will assume that $|\xi(x_2,y_2)| \geq |\xi(x_1,y_1)|$. Let us write $\eta_i = \eta(x_i, y_i)$ and $\xi_i = \xi(x_i, y_i)$. We will use the following results to prove that (x_1, y_1) and (x_2, y_2) are far apart in height.

Since

$$|z| = \frac{8p_t(x,y)}{|\xi|^4} \leq \frac{32t^2}{|\xi|^4}, \tag{4.23}$$

it follows from (4.10) that

$$\begin{aligned} |\xi_1\eta_2 - \xi_2\eta_1| &= |\xi_1(\eta_2 - \omega\xi_2) - \xi_2(\eta_1 - \omega\xi_1)| \quad (4.24) \\ \leq \frac{8\,\pi t^2}{3}\left(\frac{|\xi_1|}{|\xi_2^3|} + \frac{|\xi_2|}{|\xi_1^3|}\right) &\leq \frac{16\,\pi t^2\,|\xi_2|}{3|\xi_1^3|}. \end{aligned}$$

On the other hand, choosing our fourth root appropriately, we have

$$\begin{pmatrix} \sqrt{2}(-\sqrt{-\frac{t}{2}}+1)^{1/4} & \sqrt{2}(-\sqrt{-\frac{t}{2}}+1)^{1/4}\sqrt{-2t} \\ \sqrt{2}(-\sqrt{-\frac{t}{2}}-1)^{1/4} & -\sqrt{2}(-\sqrt{-\frac{t}{2}}-1)^{1/4}\sqrt{-2t} \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$$
$$= \begin{pmatrix} \xi_1 & \xi_2 \\ \eta_1 & \eta_2 \end{pmatrix}$$

and so

$$|\xi_1\eta_2 - \xi_2\eta_1| = \left|4(\frac{t}{2}+1)^{1/4}\sqrt{2t}\,(x_1y_2 - x_2y_1)\right|.$$

Since $x_1y_2 - x_2y_1$ is a nonzero integer (recall that we assumed $\gcd(x_i, y_i) = 1$), we have

$$|\xi_1\eta_2 - \xi_2\eta_1| \geq 4\sqrt{2t}(\frac{t}{2}+1)^{1/4}, \tag{4.25}$$

and thus, combining (4.24) and (4.25), we conclude that if (x_1, y_1) and (x_2, y_2) are distinct solutions to (4.9), related to ω, with

$$|\xi(x_2, y_2)| \geq |\xi(x_1, y_1)|$$

then

$$|\xi_2| > \frac{3\,t^{-5/4}}{4\pi}\,|\xi_1|^3. \tag{4.26}$$

We will now combine inequality (4.22) with upper bounds from Lemma 4.6.2 to show that solutions to (4.9) are widely spaced:

Lemma 4.6.6. *If $\Sigma_{r,g} \neq 0$, then*

$$c_1(r,g)\,|\xi_1|^{4r+1-g}|\xi_2|^{-3} + c_2(r,g)\,|\xi_1|^{-4r-3(1-g)}|\xi_2| > 1,$$

where we may take

$$c_1(r,g) = \frac{\sqrt{\pi}2^{2r+11/4+5g/8}}{3\sqrt{r}}\, t^{5/4+3g/8}$$

and

$$c_2(r,g) = \frac{2^{1/4+5g/8-2r}33^{2r+1-g}}{\pi\sqrt{r}} t^{4r+5/4-13g/8}.$$

Proof. By (4.15), we can write

$$\left|(\frac{t}{2}+1)^{1/4}\,\Lambda_{r,g}\right| = |\xi_1|^{4r+1-g}|\xi_2|\ \left|\left(\frac{\eta_2}{\xi_2}-\omega\right)A_{r,g}(z_1)+\omega z_1^{2r+1-g}F_{r,g}(z_1)\right|.$$

Since $|1-z_1| = 1$ and $|z_1| \le 1$, from (4.10), (4.23), (4.16), (4.17), and the inequality

$$|\xi_1|^4 > 8\sqrt{2}\,(t)^{5/2},$$

we have

$$\left|(\frac{t}{2}+1)^{1/4}\,\Lambda_{r,g}\right| \le$$

$$|\xi_1|^{4r+1-g}|\xi_2| \left(\binom{2r-g}{r}\frac{2\pi t^2}{3|\xi_2^4|} + \frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}}\left(\frac{9t^2}{|\xi_1^4|}\right)^{2r+1-g}\right).$$

Comparing this with (4.22), we obtain

$$c_1(r,g)\,|\xi_1|^{4r+1-g}|\xi_2|^{-3} + c_2(r,g)\,|\xi_1|^{-4r-3(1-g)}|\xi_2| > 1,$$

where we may take c_1 and c_2 so that

$$c_1(r,g) \ge \frac{2^{11/4+5g/8}\,t^{5/4+3g/8}\pi}{3}\binom{2r}{r}$$

and

$$c_2(r,g) \ge 2^{5g/8-1/4}\,33^{2r+1-g}\,t^{4r+5/4-13g/8}\,\frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}}.$$

Applying the following version of Stirling's formula (see Theorem (5.44) of [16])

$$\frac{1}{2\sqrt{k}}4^k \le \binom{2k}{k} < \frac{1}{\sqrt{\pi k}}4^k,$$

(valid for $k \in \mathbb{N}$) leads immediately to the stated choice of c_1. One can also show via Stirling's formula that for $r \in \mathbb{N}$ and $g \in \{0,1\}$, we have

$$\frac{\binom{r-g+1/4}{r+1-g}\binom{r-1/4}{r}}{\binom{2r+1-g}{r}} < \frac{\sqrt{2}}{\sqrt{r}\pi 4^r}$$

(see the proof of Lemma 6.1 of [1] for more details). This gives the desired value for $c_2(r,g)$. □

4.6.3 The Proof of Lemma 4.6.1

We will start this section with the statements of two Lemmas from [1]. These Lemmas allow us to apply the strong gap principle provided by Lemma 4.6.5. We note here that although $\xi(x,y)$ and $\eta(x,y)$ are defined differently in [1], those properties of ξ and η used in the proofs of Lemmas 6.2 and 6.3 of [1], hold for our choice of ξ and η in the present paper.

Lemma 4.6.7. *If $r \in \mathbb{N}$ and $h \in \{0,1\}$, then at most one of $\{\Sigma_{r,0}, \Sigma_{r+h,1}\}$ can vanish.*

Lemma 4.6.8. *Suppose that $t > 1200$. For $r \in \{1,2,3,4,5\}$, we have $\Sigma_{r,0} \neq 0$.*

Assume that there are two distinct coprime solutions (x_1,y_1) and (x_2,y_2) to inequality (4.9) with $|\xi_2| > |\xi_1|$. We will show that $|\xi_2|$ is arbitrary large in relation to $|\xi_1|$. In particular, we will demonstrate via induction that

$$|\xi_2| > \frac{\sqrt{r}}{t^{4r+7/4}}\left(\frac{4}{33^2}\right)^r |\xi_1|^{4r+3}, \tag{4.27}$$

for each positive integer r. So by (4.14),

$$|\xi_2| > t^{7r}$$

for arbitrary r, a contradiction.
To prove inequality (4.27) for $r = 1$, we use (4.26) and (4.14) to get

$$c_1(1,0)|\xi_1|^5|\xi_2|^{-3} < \frac{2^{43/4}\sqrt{\pi}}{3}\, t^5\, |\xi_1|^{-4} < 0.01,$$

and hence, since $\Sigma_{1,0} \neq 0$, Lemma 4.6.6 yields

$$c_2(1,0)|\xi_1|^{-7}|\xi_2| > 0.09,$$

which, immediately, implies (4.27). We now proceed by induction. Suppose that (4.27) holds for some $r \geq 1$. Then

$$c_1(r+1,0)|\xi_1|^{4r+5}|\xi_2|^{-3} < \frac{\sqrt{\pi}}{\sqrt{3}r^2}\, t^{12r+26/4} \left(\frac{33^6}{2^6}\right)^r |\xi_1|^{-8r-4},$$

and hence, from (6.1), and the fact that $t \geq 1200$,

$$c_1(r+1,0)|\xi_1|^{4r+5}|\xi_2|^{-3} < 0.1.$$

If $\Sigma_{r+1,0} \neq 0$, then by Lemma 4.6.6,

$$c_2(r+1,0)|\xi_1|^{-4(r+1)-3}|\xi_2| > 0.9,$$

which again leads to (4.27). If, however, $\Sigma_{r+1,0} = 0$, then by Lemmas 4.6.7 and 4.6.8, both $\Sigma_{r+1,1}$ and $\Sigma_{r+2,1}$ are nonzero, and $r \geq 2$. Using the induction hypothesis, we find as previously that

$$c_1(r+1,1)|\xi_1|^{4r+4}|\xi_2|^{-3} < 0.001,$$

and thus by Lemma 4.6.6 conclude that

$$c_2(r+1,1)|\xi_1|^{-4r-4}|\xi_2| > 0.999.$$

It follows that

$$|\xi_2| > \frac{\sqrt{r+1}}{2^{7/8}\, t^{4r+29/8}} \left(\frac{4}{33^2}\right)^{r+1} |\xi_1|^{4r+4}.$$

Consequently, from (4.14), $r \geq 6$ and $t > 1200$,

$$c_1(r+2,1)|\xi_1|^{4r+8}|\xi_2|^{-3} < 0.001.$$

Therefore Lemma 6.5 implies that

$$c_2(r+2,1)|\xi_1|^{-4r-8}|\xi_2| > 0.999,$$

and so

$$|\xi_2| > \frac{\pi}{2^{7/8}} \sqrt{r+2} \left(\frac{4}{33^2}\right)^{r+2} t^{-4r-61/8}|\xi_1|^{4r+8}.$$

From (4.14), it follows that

$$|\xi_2| > \frac{\sqrt{r+1}}{t^{4r+4+7/4}} \left(\frac{4}{33^2}\right)^{r+1} |\xi_1|^{4r+7},$$

as desired. This completes the proof of inequality (4.27), and hence we conclude that there is at most one solution to (4.9) related to each fourth root of unity.

We conclude from the above, in conjunction with Lemma 4.5.2, that there are at most three solutions in positive integers to equation (4.1). In particular, there is the solution $(X, Y) = (1, 1)$, and for both $i = 1$ and $i = 3$, at most one integer k for which $X^2 = V_{4k+i}$ is solvable. We now proceed to the proof that for t large enough, the equation $X^2 = V_{4k+1}$ is not solvable for all $k > 0$.

4.7 An Effective Measure Of Approximation

In this section we will apply the hypergeometric method to obtain effective measures of approximation to the two roots $\beta^{(3)}$ and $\beta^{(4)}$. Because of the relation $\beta^{(3)}\beta^{(4)} = -2t$, we will only need to deal with one of the roots, say $\beta^{(3)}$.

Our first lemma is Thue's "Fundamentaltheorem" [17] together with its relation to the hypergeometric function, as discovered by Siegel. The reader is also referred to Proposition 1 in [10], or Lemma 3.1 in [18].

Lemma 4.7.1. *Let α_1, α_2, c_1 and c_2 be complex numbers with $\alpha_1 \neq \alpha_2$. For $n \geq 2$, we define the following polynomials*

$$\begin{aligned}
a(X) &= \frac{n^2-1}{6}(\alpha_1 - \alpha_2)(X - \alpha_2), \\
c(X) &= \frac{n^2-1}{6}\alpha_1(\alpha_1 - \alpha_2)(X - \alpha_2), \\
b(X) &= \frac{n^2-1}{6}(\alpha_2 - \alpha_1)(X - \alpha_1), \\
d(X) &= \frac{n^2-1}{6}\alpha_2(\alpha_2 - \alpha_1)(X - \alpha_1), \\
u(X) &= -c_2(X - \alpha_2)^n, \\
z(X) &= c_1(X - \alpha_1)^n.
\end{aligned}$$

Putting

$$\lambda = (\alpha_1 - \alpha_2)^2/4,$$

for any positive integer r, we define

$$\begin{aligned}(\sqrt{\lambda})^r A_r(X) &= a(X)X^*_{n,r}(z,u) + b(X)X^*_{n,r}(u,z) \text{ and} \\ (\sqrt{\lambda})^r B_r(X) &= c(X)X^*_{n,r}(z,u) + d(X)X^*_{n,r}(u,z).\end{aligned}$$

Then, for any root β of $P(X) = z(X) - u(X)$, the polynomial

$$C_r(X) = \beta A_r(X) - B_r(X)$$

is divisible by $(X - \beta)^{2r+1}$.

Proof. This is a simplified version Lemma 2.1 from [5], obtained by noting that if $P(X)$ satisfies the differential equation given there, with $U(X) = (X - \alpha_1)(x - \alpha_2)$, then $P(X)$ must be of the form given here, which allows us to determine the above expressions. □

Lemma 4.7.2. *With the above notation, put $w(x) = z(x)/u(x)$ and write $w(x) = \mu e^{i\varphi}$ with $\mu \geq 0$ and $-\pi < \varphi \leq \pi$. Put $w(x)^{1/n} = \mu^{1/n} e^{i\varphi/n}$.*
(i) *For any $x \in \mathbf{C}$ such that $w = w(x)$ is not a negative real number or zero,*

$$\begin{aligned}&\left(\sqrt{\lambda}\right)^r C_r(x) = \\ &\left\{\beta\left(a(x)w(x)^{1/n} + b(x)\right) - \left(c(x)w(x)^{1/n} + d(x)\right)\right\} X_{n,r}(u,z) \\ &- (\beta a(x) - c(x))\, u(x)^r R_{n,r}(w),\end{aligned}$$

with

$$R_{n,r}(w) = \frac{\Gamma(r+1+1/n)}{r!\Gamma(1/n)} \int_1^w ((1-t)(t-w))^r\, t^{1/n-r-1}\, dt,$$

where the integration path is the straight line from 1 to w.
(ii) *Let $w = e^{i\varphi}, 0 < \varphi < \pi$ and put $\sqrt{w} = e^{i\varphi/2}$. Then*

$$|R_{n,r}(w)| \leq \frac{n\Gamma(r+1+1/n)}{r!\Gamma(1/n)} \varphi \left|1 - \sqrt{w}\right|^{2r}.$$

Proof. This is Lemma 2.5 of [5]. □

Lemma 4.7.3. *Let u, w and z be as above. Then*

$$\left|X^*_{n,r}(u,z)\right| \leq 4|u|^r \frac{\Gamma(1-1/n)r!}{\Gamma(r+1-1/n)} \left|1 + \sqrt{w}\right|^{2r-2}.$$

Proof. This is Lemma 2.6 of [5]. □

Lemma 4.7.4. *Let $N_{4,r}$ be the greatest common divisor of the numerators of the coefficients of $X_{4,r}(1-2x)$ and let $D_{4,r}$ be the least common multiple of the denominators of the coefficients of $X_{4,r}(x)$. Then the polynomial $(D_{4,r}/N_{4,r})\, X_{4,r}(1-2x)$ has integral coefficients.*
Moreover, $N_{4,r} = 2^r$ and

$$D_{4,r}\frac{\Gamma(3/4)r!}{\Gamma(r+3/4)} < 0.8397{\cdot}5.342^r \qquad \textit{and} \qquad D_{4,r}\frac{\Gamma(r+5/4)}{\Gamma(1/4)r!} < 0.1924{\cdot}5.342^r.$$

Proof. Using the so-called Kummer transformation, we can write

$$X_{4,r}(1-2x) = {}_2F_1\left(-r, -r-1/4; -2r; 2x\right).$$

Expanding the right-hand side, we find that

$$X_{4,r}(1-2x) = \sum_{i=0}^{r}(-1)^i \frac{(r+1)\cdots(2r-i)}{3\cdot 7\cdots(4r-1)}\binom{r}{i}(4r-4i+1)\cdots(4r+1)2^{2r-i}x^i.$$

Therefore, 2^r divides $N_{4,r}$ and by examining the coefficient of x^r, we see that $N_{4,r} = 2^r$. We know turn to the inequalities.

From the arguments in the proof of Proposition 2(c) from [10], we obtain

$$D_{4,r} < \exp\left(1.6708r + 3.43\sqrt[3]{r}\right) < 5.341227^r$$

for $r \geq 20\,000$. Since $\exp(0.000073r) > \exp(1.46) > 2$ for such values of r, the upper bound for $D_{4,r}$ holds for $r \geq 20\,000$.

For $r \geq 2$,

$$\begin{aligned}\frac{\Gamma(r+5/4)}{\Gamma(1/4)r!} &= \frac{5}{16}\prod_{i=2}^{r}\frac{i+1/4}{i} < \frac{5}{16}\exp\left(\int_1^r \log\left(\frac{x+1/4}{x}\right)dx\right)\\ &< \frac{5}{16}\exp\left(\int_1^r \frac{dx}{4x}\right) \leq \frac{5}{16}r^{1/4}.\end{aligned}$$

As a consequence, the inequalities in the statement of the lemma hold for $r \geq 20\,000$. A computation, similar to those described in the proof of Proposition 2 from [10], shows that the same inequalities holds for all smaller values of r. □

Lemma 4.7.5. *Let $\alpha_1, \alpha_2, A_r(X), B_r(X)$ and $P(X)$ be defined as in Lemma 3.1 and let a, b, c and d be complex numbers satisfying $ad - bc \neq 0$. Define*

$$K_r(X) = aA_r(X) + bB_r(X) \quad \text{and} \quad L_r(X) = cA_r(X) + dB_r(X).$$

If $(x - \alpha_1)(x - \alpha_2)P(x) \neq 0$, then

$$K_{r+1}(x)L_r(x) \neq K_r(x)L_{r+1}(x),$$

for all $r \geq 0$.

Proof. This is Lemma 2.7 of [5]. □

Lemma 4.7.6. *Let $\theta \in \mathbf{R}$. Suppose that there exist $k_0, l_0 > 0$ and $E, Q > 1$ such that for all $r \in \mathbf{N}$, there are rational integers p_r and q_r with $|q_r| < k_0 Q^r$ and $|q_r\theta - p_r| \leq l_0 E^{-r}$ satisfying $p_r q_{r+1} \neq p_{r+1} q_r$. Then for any rational integers p and q with $|q| \geq 1/(2l_0)$, we have*

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{c|q|^{\kappa+1}}, \text{ where } c = 2k_0 Q(2l_0 E)^{\kappa} \text{ and } \kappa = \frac{\log Q}{\log E}.$$

Proof. This is Lemma 2.8 from [5]. □

For the remainder of this section, we shall assume that t is a fixed integer greater than 37. We shall also simplify our notation here to reflect the fact that we have $n = 4$. We shall use R_r and X_r instead of $R_{4,r}$ and $X_{4,r}$.

We now determine the quantities defined in the Lemma 4.7.1. Put

$$\alpha_1 = \sqrt{-2t}, \ \ \alpha_2 = -\sqrt{-2t}, \ \ c_1 = \left(1 + \sqrt{-t/2}\right)/2, \ \ c_2 = \left(1 - \sqrt{-t/2}\right)/2,$$

then

$$p_t(X) = X^4 + 4tX^3 - 12tX^2 - 8t^2X + 4t^2.$$

We define

$$\tau = \frac{\sqrt{t} + \sqrt{t+2}}{\sqrt{2}} \quad \text{and} \quad \rho = \sqrt{\tau^2 + 1} = \sqrt{t + 2 + \sqrt{t^2 + 2t}}.$$

for any positive integer t.

The preliminary results above will now be used in order to obtain an effective measure of approximation to $\beta^{(3)}$. By Lemma 4.7.2, we want to choose x so that

$$\beta^{(3)} = \frac{c(x)w(x)^{1/4} + d(x)}{a(x)w(x)^{1/4} + b(x)},$$

and for this purpose we will select $x = 0$. We have

$$w = w\left(0\right) = \frac{2+\sqrt{-2t}}{-2+\sqrt{-2t}},$$

$$\left(\frac{\tau - i}{\tau + i}\right)^2 = w, \ \left(\frac{\tau - i}{\rho}\right)^2 = \frac{\tau - i}{\tau + i},$$

and so

$$w^{1/4} = \frac{\tau - i}{\rho}.$$

Using the fact that $\rho^2 = \tau^2 + 1$, one can check that

$$\frac{-i\tau - 1 + i\rho}{-\tau + i - \rho} = -\tau + \rho,$$

and since

$$a(0) = -10t, \quad b(0) = -10t, \quad c(0) = -10t\sqrt{-2t} \quad \text{and} \quad d(0) = 10t\sqrt{-2t},$$

it follows that

$$\beta^{(3)} = \frac{c(0)w^{1/4} + d(0)}{a(0)w^{1/4} + b(0)}.$$

Therefore, the first term in the expression for $(-2t)^{r/2}C_r(0)$ in Lemma 4.7.2 disappears.

We now construct our sequence of rational approximations to $\beta^{(3)}$. By Lemma 4.7.1, Lemma 4.7.2, we have that $\lambda = -2t$, and moreover

$$\begin{aligned}
(-2t)^{r/2}A_r(0) &= a(0)X_r^*(z(0), u(0)) + b(0)X_r^*(u(0), z(0)), \\
(-2t)^{r/2}B_r(0) &= c(0)X_r^*(z(0), u(0)) + d(0)X_r^*(u(0), z(0)), \\
(-2t)^{r/2}C_r(0) &= -\left(\beta^{(3)}a(0) - c(0)\right)u(0)^r R_r(w).
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
(-2t)^{r/2}A_r(0) &= -10t\ \left[X_r^*(z(0), u(0)) + X_r^*(u(0), z(0))\right], \\
(-2t)^{r/2}B_r(0) &= 5(-2t)^{3/2}\ \left[X_r^*(z(0), u(0)) - X_r^*(u(0), z(0))\right], \\
(-2t)^{r/2}C_r(0) &= 10t^{2r+1}\ \left[\beta^{(3)} - \sqrt{-2t}\right]\left(-2+\sqrt{-2t}\right)^r R_r(w).
\end{aligned}$$

These quantities will form the basis for our approximations. We first eliminate some common factors. We can write $u(0) = t^2\left(-2+\sqrt{-2t}\right)$ and

$z(0) = t^2\left(2+\sqrt{-2t}\right)$. Using Lemma 4.7.2, Lemma 4.7.3, and triangular inequality, we obtain

$$|A_r(0)| \le 80t^{(3r+2)/2}\,(2+t)^{r/2}\,\frac{\Gamma(3/4)r!}{\Gamma(r+3/4)}\left|1+\sqrt{w}\right|^{2r-2};$$

$$|B_r(0)| \le 80\sqrt{2}\,t^{(3r+3)/2}\,(2+t)^{r/2}\,\frac{\Gamma(3/4)r!}{\Gamma(r+3/4)}\,\left|1+\sqrt{w}\right|^{2r-2};$$

and

$$|C_r(0)| \le 40\,t^{(3r+2)/2}\,\varphi\left|\beta^{(3)}-\sqrt{-2t}\right|(2+t)^{r/2}\frac{\Gamma(r+5/4)}{r!\Gamma(1/4)}\,\left|1-\sqrt{w}\right|^{2r}.$$

In the other hand, after some routine manipulations, we find that

$$(-2t)^{r/2}A_r(0) = \frac{-10t^{2r+1}\,N_{4,r}}{D_{4,r}}\left\{\frac{D_{4,r}}{N_{4,r}}\left[\left(2+\sqrt{-2t}\right)^r X_r\left(1-2\eta\right)+\left(-2+\sqrt{-2t}\right)^r X_r\left(1-2\bar{\eta}\right)\right]\right\}$$

and

$$(-2t)^{r/2}B_r(0) = \frac{5(-2)^{3/2}\,t^{2r+3/2}N_{4,r}}{D_{4,r}}\left\{\frac{D_{4,r}}{N_{4,r}}\left[\left(-2+\sqrt{-2t}\right)^r X_r\left(1-2\bar{\eta}\right)-\left(2+\sqrt{-2t}\right)^r X_r\left(1-2\eta\right)\right]\right\};$$

where $\eta = \frac{2}{2+\sqrt{-2t}}$.
By Lemma 4.7.4, the quantities inside the braces can be expressed as

$$(-1)^r(e-f\sqrt{-2t}) \pm (e-f\sqrt{-2t}),$$

where e and f are rational integers, and recalling from Lemma 4.7.4 that $N_{4,r} = 2^r$, considering the cases of r being even or odd separately, we find that

$$P_r = \frac{D_{4,r}B_r(0)}{20\cdot t^{[(3r+3)/2]}} \quad \text{and} \quad Q_r = \frac{D_{4,r}A_r(0)}{20\cdot t^{[(3r+3)/2]}} \tag{4.28}$$

are rational integers. We note for future reference that if r is even, then P_r will be divisible by t. The numbers P_r/Q_r are those that will be used as the rational approximations to $\beta^{(3)}$. We have

$$Q_r\beta^{(3)} - P_r = S_r,$$

where

$$S_r = \frac{D_{4,r}C_r(0)}{20\cdot t^{[(3r+3)/2]}}.$$

We wish to show that these are good approximations. This will be done by estimating $|P_r|, |Q_r|$ and $|S_r|$ from above. It is readily verified that

$$|1+\sqrt{w(0)}| = \frac{2\tau}{\sqrt{\tau^2+1}} = 2 - \frac{1}{2t} + O\left(\frac{11}{16t^2}\right);$$

and in particular we have that

$$|1+\sqrt{w(0)}| < 2.$$

Therefore, we have, for $t \geq 37$, that

$$|Q_r| \leq 3.36\ (22\ \sqrt{t})^r.$$

Similarly, one obtains for $t \geq 37$ that

$$|P_r| \leq 4.75\sqrt{t}\ (22\ \sqrt{t})^r.$$

Also we have

$$\left|1-\sqrt{w(0)}\right|^2 = \frac{4}{\tau^2+1} \leq \frac{2}{t}.$$

With ϕ as in Lemma 4.7.2, it can be shown that $2\varphi/\pi \leq \sin\varphi$ and

$$\sin\varphi = \text{Im}\ w(0) = -2\sqrt{2t}/(t+2) \geq -2\sqrt{2/t}.$$

From the estimates for the roots of $p_t(X)$ given in section 3, we know that $0 < \beta^{(3)} < 0.5$, and so

$$\varphi\left|\beta^{(3)} - \sqrt{-2t}\right| \leq \pi\left(2+\frac{1}{\sqrt{2t}}\right) \leq \pi\left(2+\frac{1}{\sqrt{2}}\right).$$

Combining these inequalities with Lemma 4.7.4, we obtain

$$|S_r| < 3.3\ \left(\frac{11}{\sqrt{t}}\right)^r;$$

for $t \geq 37$. Note also that since $\beta^{(3)}\beta^{(4)} = -2t$, we have

$$2tQ_r + \beta^{(4)}P_r = -\beta^{(4)}S_r.$$

With these estimates, Lemma 4.7.6 gives the following.

Lemma 4.7.7. *Suppose that* $t \geq 37$. *Define*

$$\kappa = \frac{\log\left(22\sqrt{t}\right)}{\log\left(\sqrt{t}/11\right)}.$$

For $j = 3, 4$ *and any rational integers* p *and* q, *we have*

$$\left|p - \beta^{(j)}q\right| > \frac{1}{c_j|q|^\kappa}$$

for $|q| \geq 1$, *where*

$$c_3 = 147.84\sqrt{t}\left(.6\sqrt{t}\right)^\kappa \quad \text{and} \quad c_4 = 4598\sqrt{t}\,(.44t)^\kappa.$$

Proof. In each case we will apply Lemma 4.7.5 and Lemma 4.7.6. First notice that $P_rQ_{r+1} - P_{r+1}Q_r$ is a non-zero multiple of $A_{r+1}(0)B_r(0) - A_r(0)B_{r+1}(0)$. Applying Lemma 4.7.5, with $a = d = 1, b = c = 0$ and $x = 0$, we see that $P_rQ_{r+1} \neq P_{r+1}Q_r$. For $\beta^{(3)}$, we put $p_r = P_r$ and $q_r = Q_r$, and apply Lemma 7.6 with $k_0 = 3.36$, $l_0 = 3.3$, $E = \sqrt{t}/11$ and $Q = 22\sqrt{t}$. For $\beta^{(4)}$, we take advantage of the fact that P_{2r} is divisible by t. In this case, we set $p_r = -2Q_{2r}$, $q_r = P_{2r}/t$, $s_r = S_{2r}\beta^{(4)}/t$, and apply Lemma 7.6 accordingly. Since $-4t - 2 < \beta^{(4)} < -4t$, we can put $k_0 = 4.75/\sqrt{t}, l_0 = 13.2, E = t/11^2 = (\sqrt{t}/11)^2$, and $Q = 484t = (22\sqrt{t})^2$. We see therefore that the value of κ in this case is the same as in the case of $\beta^{(3)}$. □

4.8 Completion Of The Proof Of Theorem 4.1.1

The goal now is to solve equation (4.2) for all $t > 40,000$. We remark that the analysis here will use the fact that, by not restricting that a solution (x, y) have the property that x/y is close to $\beta^{(4)}$, as asserted in Lemma 4.3.1, we can restrict to the case that s in equation (4.6) satisfies the inequality $s < \sqrt{2t}$. The can be seen by considering once again the equation

$$s^2B^4 - 4tsAB^3 - 12tA^2B^2 + 4rtBA^3 + r^2A^4 = 1$$

appearing in section 3. Since $rs = 2t$, we define $s_0 = \min(r, s)$, and multiply the above equation through by s_0^2. By defining $(x, y) = (-sB, A)$ if $s_0 = s$ and $(x, y) = (rA, B)$ if $s_0 = r$, one obtains the Thue equation

$$x^4 + 4tx^3y - 12tx^2y^2 - 8t^2xy^3 + 4t^2y^4 = s_0^2,$$

where, as discussed above, s_0 divides $2t$, and also, $s_0 \le \sqrt{2t}$. It is not difficult to verify that if $s_0 = s$, then the closest root of $p_t(X)$ to x/y is $\beta^{(4)}$, while if $s_0 = r$, then the closest root of $p_t(X)$ to x/y is $\beta^{(3)}$. The consequence of this remark is that one then needs only to solve the Thue inequality

$$|p_t(x,y)| \le 2t,$$

as opposed to having $4t^2$ on the right hand side.

We first obtain a lower bound for $|y|$ for any solution to the Thue inequality.

We will assume, in the construction of p_t, given in section 3, that $r < \sqrt{2t}$, as the case $s < \sqrt{2t}$ actually gives a larger lower bound for $|y|$. Recall that $y = A$, where

$$X - V_{2k+1} = \sqrt{V_{4k+1}} - V_{2k+1} = 2rA^2.$$

Recall also that $r < 2t$. We make use of the inequality $U_{2k} > (2t)^{k-1}$, which is easily proved by induction. We note that because of the relation $V_{4k+1} = V_{2k+1}^2 + 2tU_{2k}^2$, we can deduce the following expression

$$\sqrt{V_{4k+1}} - V_{2k+1} = \frac{\sqrt{2t}U_{2k}}{\sqrt{V_{2k+1}/\sqrt{2t}U_{2k} + 1} + V_{2k+1}/\sqrt{2t}U_{2k}}.$$

Therefore,

$$y^2 = A^2 > \frac{\sqrt{2t}U_{2k}}{4t} > (\sqrt{2t})^{2k-1}.$$

By the fact that $k > 24$, we deduce that

$$|y| > (2t)^{47/4}.$$

As remarked earlier, the assumption $s < \sqrt{2t}$ implies that x/y is closest to $\beta^{(3)}$. In other words, $|x - \beta^{(3)}y| = \min_{i=1,2,3,4} |x - \beta^{(i)}y|$, and since $|P_t(x,y)| \le 2t$, it follows that $|x - \beta^{(3)}y| < (2t)^{1/4}$. Therefore, as $y > 4$, $x/y > \beta^{(3)} - (2t)^{1/4}/4$, and so

$$|x/y - \beta^{(4)}| > \beta^{(3)} - (2t)^{1/4}/4 - \beta^{(4)} > 4t - (2t)^{1/4}/4 + 3 - 21/(16t) \ldots.$$

Similarly for $i = 1, 2$,

$$|x/y - \beta^{(i)}| > \sqrt{2t} - (2t)^{1/4}/4 - 1/2 \ldots.$$

Therefore, because $t > 40,000$, it is readily deduced that

$$|x/y - \beta^{(3)}| < \frac{1}{15.9ty^4}.$$

A similar argument for $\beta^{(4)}$ gives

$$|x/y - \beta^{(4)}| < \frac{1}{31.9t^2y^4}.$$

Combining the above upper bound for $|x/y - \beta^{(3)}|$ with the lower bound proved in Lemma 4.7.7, it follows that

$$|y|^{3-\kappa} < \frac{c_3(t)}{15.9t}.$$

For $t > 40,000$, $\kappa < 2.9$, and we conclude that

$$3t^2 > \frac{147.84\sqrt{t}(.6\sqrt{t})^3}{15.9t} > \frac{147.84\sqrt{t}(.6\sqrt{t})^\kappa}{15.9t} > |y|^{.1} > (2^{21}t^{23})^{.1} > 4t^2,$$

which is not possible.

Similarly for $\beta^{(4)}$, combining the upper and lower bounds for $|x/y - \beta^{(4)}|$ gives

$$|y|^{3-\kappa} < \frac{c_3(t)}{31.9t^2}.$$

Again since $t > 40000$, we have that $\kappa < 2.9$, and we therefore conclude that

$$13t^{1.5} > \frac{4598\sqrt{t}(.44t)^3}{31.9t^2} > \frac{4598\sqrt{t}(.44t)^\kappa}{31.9t^2} > |y|^{.1} > (2^{21}t^{23})^{.1} > 4t^2,$$

which is not possible for $t > 10$.

Bibliography

[1] S. Akhtari, The equation $aX^4 - bY^2 = 1$. To Appear in J. Reine Angew. Math.

[2] M.A. Bennett. On the representation of unity by binary cubic forms, Trans. Amer. Math. Soc. **353** (2001), 1507-1534.

[3] M.A. Bennett and P.G. Walsh, The Diophantine equation $b^2X^4 - dY^2 = 1$. Proc. A.M.S. **127** (1999), 3481-3491.

[4] F. Beukers and S. Tengely, An implementation of Runge's method for Diophantine equations. preprint, 2005.

[5] J.H. Chen and P.M. Voutier. A complete solution of the Diophantine equation $x^2 + 1 = dy^4$ and a related family of quartic Thue equations. J. Number Theory **62** (1997), 71-99.

[6] G.V. Chudnovsky, On the method of Thue-Siegel, Ann. of Math. II Ser. **117** (1983), 325-382.

[7] J.H. Evertse. On the representation of positive integers by binary cubic forms of positive discriminant, Invent. Math. **73** (1983), 117-138.

[8] C. Heuberger, A. Togbé, and V. Ziegler. Automatic solutions of families of Thue equations and an example of degree 8, J. Symbolic Comput. **38** (2004), 1145-1163.

[9] D.H. Lehmer. An extended theory of Lucas functions. Ann. Math. **31** (1930), 419-448.

[10] G. Lettl, A. Pethö and P.M. Voutier. Simple families of Thue inequalities. Trans. Amer. Math. Soc. **351** (1999), 1871-1894.

[11] W. Ljunggren. Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. Avh. Norsk. Vid. Akad. Oslo (1942), 1-27.

[12] W. Ljunggren. Über die Gleichung $x^4 - Dy^2 = 1$. Arch. Math. Naturv. **45** (1942) no.5.

[13] W. Ljunggren. Einige Eigenschaften der Einheiten reeller quadratischer und reinbiquadratischer Zahl-Körper usw. Oslo Vid.-Akad. Skrifter (1936), nr. 12.

[14] W. Ljunggren. Ein Satz über die Diophantische Gleichung $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$ Tolfte Skand. Matemheikerkongressen, Lund, 1953, 188-194, (1954).

[15] W. Ljunggren. On the Diophantine equation $Ax^4 - By^2 = C(C = 1, 4)$. Math. Scand. **21** (1967), 149-158.

[16] K. Stromberg. *An Introduction to Classical Real Analysis,* Wadsworth International Mathematical Series, 1981.

[17] A. Thue. Ein Fundamentaltheorem zur Bestimmung von Annäherungswerten aller Wurzeln gewisser ganzer Funktionen, J. Reine Angew. Math. **138** (1910), 96-108.

[18] A. Togbe, P.M. Voutier, and P.G. Walsh. Solving a family of Thue equations with an application to the equation $x^2 - Dy^4 = 1$, Acta Arith. **120** (2005), 39-58.

[19] P.G. Walsh. On a family of quartic equations and a Diophantine problem of Martin Gardner. Glasnik Matematiki **41** (2006), 217-221.

Chapter 5

Addendum on the equation $aX^4 - bY^2 = 2$ [4]

In a recent paper [2], the authors proved that for $t > 40,000$, the Diophantine equation $(t+2)X^4 - tY^2 = 2$ has at most two solutions in positive integers X, Y. In this addendum, we provide a simple argument due to Ljunggren [3] which shows that the above result implies that any equation of the form $aX^4 - bY^2 = 2$ has at most two solutions in positive integers X, Y.

We necessarily restrict our attention to pairs of odd integers a, b for which the quadratic equation $ax^2 - by^2 = 2$ is solvable in odd integers x, y. Given such a pair of integers a, b, let $(x, y) = (u_1, v_1)$ denote the smallest solution in positive integers to $ax^2 - by^2 = 2$, and define

$$\tau = \tau_{a,b} = \frac{u_1\sqrt{a} + v_1\sqrt{b}}{\sqrt{2}}.$$

For $i \geq 1$ odd, define sequences $\{u_i\}, \{v_i\}$ by

$$\tau^i = \frac{u_i\sqrt{a} + v_i\sqrt{b}}{\sqrt{2}}.$$

Then all positive integer solutions (x, y) to the quadratic equation $ax^2 - by^2 = 2$ are given by $(x, y) = (u_i, v_i)$.

Theorem 5.0.1. *If a, b are odd positive integers with $\tau = \tau_{a,b} > 280$, then the equation*

$$aX^4 - bY^2 = 2 \tag{1.1}$$

[4] A version of this chapter has been submitted for publication. Akhtari. S, Togbe. A, and Walsh. P.G. Addendum On the equation $aX^4 - bY^2 = 2$.

has at most two solutions in positive integers X, Y. For the remaining finite set of pairs of positive integers a, b, equation (1.1) *has at most three solutions in positive integers X, Y.*

Theorem 1.1 is likely not best possible. We conjecture that any equation of the form $aX^4 - bY^2 = 2$, with a and b odd, has at most one solution in positive integers, and that such a solution must arise from the fundamental solution to the quadratic equation $aX^2 - bY^2 = 2$. This conjectured was verified for $(a, b) = (t + 2, t)$, with t in the range $1 \leq t < 1200$.

Proof

We will assume that a, b are odd positive integers for which there is at least one solution in odd integers (X, Y) to the equation $aX^4 - bY^2 = 2$. Thus, there is at least one odd positive integer k with the property that u_k is a square, and we assume that k represents the smallest such integer. We therefore define the positive integer X specifically by $u_k = X^2$. Write $u_1 = l_1 s_1^2$ with l_1 squarefree. Then by elementary divisibility properties of terms in the sequence $\{u_i\}$, it follows that l_1 divides k. If $l_1 > 1$, write $u_{l_1} = l_2 s_2^2$ with l_2 squarefree. By the same reasoning as before, $l_1 l_2$ must divide k. If $l_2 > 1$, then we write $u_{l_1 l_2} = l_3 s_3^2$ with l_3 squarefree, and again it follows that $l_1 l_2 l_3$ must divide k. Since k is finite, this process must stop, and so there are squarefree integers $l_1, l_2, \ldots, l_j$ such that $k = l_1 l_2 \cdots l_j$. Furthermore, arguing as above, if k_1 is any odd positive integer for which u_{k_1} is a square, then $k = l_1 l_2 \cdots l_j$ must be a divisor of k_1.

Thus, we define $t = au_k^2 - 2 = aX^4 - 2$, and put

$$\gamma = \frac{\sqrt{t+2} + \sqrt{t}}{\sqrt{2}}.$$

For $i \geq 1$ odd, we define new sequences $\{U_i\}, \{V_i\}$ by

$$\gamma^i = \frac{U_i\sqrt{t+2} + V_i\sqrt{t}}{\sqrt{2}}.$$

It follows that for each odd $i \geq 1$,

$$U_i X^2 = u_{ki},$$

and so u_{ki} is a square precisely when U_i is a square. Since the set of squares in the sequence $\{u_i\}$ are contained in the subsequence $\{u_{ki}\}$, we see that there is a one to one correspondence between the set of squares in $\{u_i\}$, and the set of squares in $\{U_i\}$.

Finally, if $\tau_{a,b} \geq 280$, then it is easily verified that $t = aX^4 - 2 > 40,000$, and so we may deduce that there are at most two squares in the sequence $\{u_i\}$.

Bibliography

[1] S. Akhtari, The Diophantine equation $aX^4 - bY^2 = 1$. To Appear in J. Reine Angew. Math.

[2] S. Akhtari, A. Togbe, P.G. Walsh, On the equation $aX^4 - bY^2 = 2$. Acta Arith. 131 (2008), 145-169.

[3] W. Ljunggren, Über die Gleichung $x^4 - Dy^2 = 1$. Arch. Math. Naturv. 45 (1942) no.5.

Chapter 6

Geometry Of Quartic Thue Equations [5]

6.1 Introduction

In this paper, we will consider irreducible binary quartic forms with integer coefficients; i.e. polynomials of the shape

$$F(x,y) = a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4.$$

The discriminant D of F is given by

$$D = a_0^6(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_1 - \alpha_4)^2(\alpha_2 - \alpha_3)^2(\alpha_2 - \alpha_4)^2(\alpha_3 - \alpha_4)^2,$$

where α_1 , α_2, α_3 and α_4 are the roots of

$$F(x,1) = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4.$$

The invariants of F form a ring, generated by two invariants of weights 4 and 6, namely

$$I = I_F = a_2^2 - 3a_1a_3 + 12a_0a_4$$

and

$$J = J_F = 2a_2^3 - 9a_1a_2a_3 + 27a_1^2a_4 - 72a_0a_2a_4 + 27a_0a_3^2.$$

These are algebraically independent and every invariant is a polynomial in I and J. For the invariant D, we have

$$27D = 4I^3 - J^2.$$

In [1], we show that if $J_F = 0$ and F splits in $\mathbb{R}$ then the equation

$$|F(x,y)| = 1 \tag{6.1}$$

[5] A version of this chapter will be submitted for publication. Akhtari. S. Geometry of quartic Thue equations.

has at most 12 solutions in integers x, y. In this paper we will give upper bounds for the number of integral solutions to (6.1) with large discriminant and no restriction on J.

We will use some ideas of Stewart [16] to prove

Theorem 6.1.1. *Let $F(x, y)$ be an irreducible binary form with integral coefficients and degree 4. The Diophantine equation (6.1) has at most 61 solutions in integers x and y (with (x, y) and $(-x, -y)$ regarded as the same), provided that the discriminant of F is greater than 10^{500}.*

We also combine some analytic methods from [16] with some geometric methods from [13] to show that

Theorem 6.1.2. *Let $F(x, y)$ be an irreducible binary form with integral coefficients and degree 4 that splits in $\mathbb{R}$. Then the Diophantine equation (6.1) has at most 37 solutions in integers x and y (with (x, y) and $(-x, -y)$ regarded as the same), provided that the discriminant of F is greater than 10^{500}.*

Note that If (x, y) is a solution to (6.1) then $(-x, -y)$ is also a solution to (6.1). So here we will only count the solutions with $y \geq 0$. Let

$$F(x, y) = a_0(x - \alpha_1 y)(x - \alpha_2 y)(x - \alpha_3 y)(x - \alpha_4 y).$$

We call forms F_1 and F_2 equivalent if they are equivalent under $GL_2(\mathbb{Z})$-action; i.e. if there exist integers a_1 , a_2 , a_3 and a_4 such that

$$F_1(a_1 x + a_2 y, a_3 x + a_4 y) = F_2(x, y)$$

for all x, y, where $a_1 a_4 - a_2 a_3 = \pm 1$. We denote by N_F the number of solutions in integers x and y of the Diophantine equation (6.1). If F_1 and F_2 are equivalent then $N_{F_1} = N_{F_2}$ and $D_{F_1} = D_{F_2}$.

Suppose there is a solution (x_0, y_0) to the equation (6.1). Since

$$\gcd(x_0, y_0) = 1,$$

there exist integers x_1, $y_1 \in \mathbb{Z}$ with

$$x_0 y_1 - x_1 y_0 = 1.$$

Then

$$F^*(1, 0) = 1,$$

where,

$$F^*(x,y) = F(x_0x + x_1y, y_0x + y_1y).$$

Therefore, F^* is a monic form equivalent to F. From now on we will assume F is monic.

In this paper we give an upper bound for the number of integral solutions to $F(x,y) = \pm 1$. For the equation

$$F(x,y) = h$$

of degree 4, one may use an argument of Bombieri and Schmidt [2] to prove that if N is a given bound in the special case $h = 1$, then $N4^{\nu}$ is a corresponding bound in the general case, where ν is the number of distinct prime factors of h.

6.2 Quartic Forms And Elliptic Curves

Let us define, for a quartic form F, a quartic covariant, the Hessian G, by

$$G(x,y) = \frac{d^2F}{dx^2}\frac{d^2F}{dy^2} - \left(\frac{d^2F}{dxdy}\right)^2.$$

Then

$$G(x,y) = A_0x^4 + A_1x^3y + A_2x^2y^2 + A_3xy^3 + A_4y^4,$$

where

$$\begin{aligned} A_0 &= 3(8a_0a_2 - 3a_1^2), \\ A_1 &= 12(6a_0a_3 - a_1a_2), \\ A_2 &= 6(3a_1a_3 + 24a_0a_4 - 2a_2^2), \\ A_3 &= 12(6a_1a_4 - a_2a_3), \\ A_4 &= 3(8a_2a_4 - 3a_3^2). \end{aligned} \tag{6.2}$$

For the binary form $F(x,y)$ with Hessian $G(x,y)$, the sextic covariant $Q(x,y)$ is defined by

$$Q(x,y) = \frac{\delta F}{\delta x}.\frac{\delta G}{\delta y} - \frac{\delta F}{\delta y}.\frac{\delta G}{\delta x}.$$

We have the following syzygy between the covariants: (see [4] for a proof)

$$27Q^2 = -G^3 + 48IF^2G + 64JF^3. \tag{6.3}$$

Theorem 6.2.1. *[Hermite] The binary forms with integer coefficients, with given invariants, can be arranged in a finite number of equivalent classes.*

The proof to this theorem can be found in chapter 18 of [12].

Suppose that

$$F_1(x,y) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4, \tag{6.4}$$

where a, b, c, d, e are integers. Let us define, for the quartic form F_1 in (6.4), the invariants

$$g_2 = \frac{I}{12}, \quad g_3 = \frac{J}{432},$$

where I and J are the invariants of F_1. Observe that $g_2, g_3 \in \mathbb{Z}$ and for covariants G and Q of F_1 we have

$$\frac{G}{144}, \frac{Q}{8} \in \mathbb{Z}[x,y].$$

By (6.3),

$$\left(\frac{Q}{8}\right)^2 = -4\left(\frac{G}{144}\right)^3 + g_2F_1^2G + g_3F_1^3. \tag{6.5}$$

We can now find the integer solutions of the equation

$$Z^2 = X^3 - G_2XY^2 - G_3Y^3, \tag{6.6}$$

where G_2, G_3 are given integers and the right-hand side has no square linear factor.

Let $F_1(x,y) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4$ be a binary quartic form with invariants $g_2 = 4G_2$, $g_3 = 4G_3$. Then from (6.5), a solution to (6.6) is given by

$$X = \frac{G}{144}(p,q), \ Y = F(p,q), \ 2Z = \frac{Q}{8}, \tag{6.7}$$

and, further, the X, Y and Z are all integers, provided p, q are integers. We may assume that $\gcd(p,q) = 1$, because the 4th power of $\gcd(p,q)$ will divide X, Y and its 6th power will divide Z. In chapter 25 of [12], an elementary proof is given to show that all the integer solutions (X,Y,Z) to (6.6) with $\gcd(X,Y) = 1$ are included in the formulae (6.7).

6.3 Heights

For any algebraic number α, we define the (naive) height of α, denoted by $H(\alpha)$, by

$$H(\alpha) = \max\left(|a_n|, |a_{n-1}|, \ldots, |a_0|\right)$$

where $f(x) = a_n x^n + \ldots + a_1 x + a_0$ is the minimal polynomial of α. Suppose that over $\mathbb{C}$,

$$f(x) = a_n(x - \alpha_1)\ldots(x - \alpha_n).$$

We put

$$M(\alpha) = |a_n| \prod_{i=1}^{n} \max(1, |\alpha_i|).$$

$M(\alpha)$ is known as the Mahler measure of α. We have the following result of Landau:

Lemma 6.3.1. *Let α be an algebraic number of degree n. then*

$$M(\alpha) \leq (n+1)^{1/2} H(\alpha).$$

For any polynomial G in $\mathbb{C}[z_1, \ldots, z_n]$ that is not identically zero the Mahler measure $M(G)$ is defined by

$$M(G) = \exp \int_0^1 dt_1 \ldots \int_0^1 dt_n \log\left|G(e^{2\pi i t_1}, \ldots, e^{2\pi i t_n})\right|.$$

Thus if $n = 1$ and $G(z) = a_n(z - \alpha_1)\ldots(z - \alpha_n)$ with $a_n \neq 0$, by Jensen's theorem,

$$M(G) = |a_n| \prod_{i=1}^{n} \max(1, |a_i|).$$

In [9], Mahler showed that

$$M(F) \geq \left(\frac{D_F}{4^4}\right)^{\frac{1}{6}}. \tag{6.8}$$

Following Matveev [10, 11], we will define the absolute logarithmic height of an algebraic number. Let $\mathbb{Q}(\alpha_1)^\sigma$ be the embeddings of the real number field $\mathbb{Q}(\alpha_1)$ in $\mathbb{R}$, $1 \leq \sigma \leq n$, where $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ are roots of $F(x, 1) = 0$. We respectively have n Archimedean valuations of $\mathbb{Q}(\alpha_1)$:

$$|\rho|_\sigma = \left|\rho^{(\sigma)}\right|, \quad 1 \leq \sigma \leq n.$$

We enumerate simple ideals of $\mathbb{Q}(\alpha)$ by indices $\sigma > n$ and define non-Archimedean valuation of $\mathbb{Q}(\alpha)$ by the formulas

$$|\rho|_\sigma = (\text{Norm } \mathfrak{p})^{-k},$$

Where

$$k = \text{ord}_{\mathfrak{p}}(\alpha), \ \mathfrak{p} = \mathfrak{p}_\sigma, \ \sigma > n,$$

for any $\rho \in \mathbb{Q}^*(\alpha)$. Then we have the *product formula* :

$$\prod_1^\infty |\rho|_\sigma = 1, \ \rho \in \mathbb{Q}(\alpha).$$

Note that $|\rho|_\sigma \neq 1$ for only finitely many ρ. We should also remark that if $\sigma_2 = \bar{\sigma_1}$, i.e.,

$$\sigma_2(x) = \sigma_1\bar{(}x) \qquad \text{for} \qquad x \in \mathbb{Q}(\alpha),$$

then the valuations $|\,.\,|_{\sigma_1}$ and $|\,.\,|_{\sigma_2}$ are equal. We define the *absolute logarithmic height* of ρ as

$$h(\rho) = \frac{1}{2n} \sum_{\sigma=1}^{\infty} |\log |\rho|_\sigma| \,.$$

Lemma 6.3.2. *Suppose α is an algebraic number of degree n over $\mathbb{Q}$. Then*

$$h(\alpha) = \frac{1}{n} \log M(\alpha).$$

Proof. It is well-known that

$$\prod_\sigma \max(1, |\alpha|_\sigma) = M(\alpha).$$

Since

$$h(\rho) = \frac{1}{2n} \sum_{\sigma=1}^{\infty} |\log |\rho|_\sigma| \,,$$

by the product formula,

$$h(\alpha) = \frac{2}{2n} \log \prod_\sigma \max(1, |\alpha|_\sigma).$$

Therefore,

$$h(\alpha) = \frac{1}{n} \log M(\alpha).$$

□

Let α and β be two algebraic numbers. Then the following inequalities hold (see [3]):

$$h(\alpha+\beta) \leq \log 2 + h(\alpha) + h(\beta) \tag{6.9}$$

and

$$h(\alpha\beta) \leq h(\alpha) + h(\beta). \tag{6.10}$$

Two algebraic integers α and α' are called equivalent if their minimal polynomials are equivalent.

Proposition 6.3.3. *(Győry [8]) Suppose that α is an algebraic integer with discriminant $D(\alpha)$ and $|D| \geq 3$. Then there is an algebraic number α' equivalent to α for which we have*

$$H(\alpha') \leq \exp\exp\left[2(\log D)^{13}\right].$$

This allows us to assume $H(\alpha) \leq \exp\exp\left[2(\log D)^{13}\right]$, where need be.

Lemma 6.3.4. *(Mahler [9]) If a and b are distinct zeros of polynomial $P(x)$ with degree n, then we have*

$$|a-b| \geq \sqrt{3}(n+1)^{-n}M(P)^{-n+1},$$

where $M(P)$ is the Mahler measure of P.

Since $M(P) \leq (n+1)^{1/2}H(P)$, we have

$$|a-b| \geq \sqrt{3}(n+1)^{-(2n+1)/2}H(P)^{-n+1}.$$

6.4 The Thue-Siegel Principle

Let α be an algebraic number of degree n and f be its minimal polynomial over the integers. Let t and τ be positive numbers such that $t < \sqrt{2/n}$ and $\sqrt{2-nt^2} < \tau < t$, and put $\lambda = \frac{2}{t-\tau}$ and

$$A_1 = \frac{t^2}{2-nt^2}\left(\log M(\alpha) + \frac{n}{2}\right).$$

Suppose that $\lambda < n$. A rational number $\frac{x}{y}$ is said to be a very good approximation to α if

$$|\alpha - x/y| < \left(4\,e^{A_1}\max(|x|,|y|)\right)^{-\lambda}.$$

The following result of Bombieri and Schmidt is based on a classical work of Thue and Siegel.

Proposition 6.4.1. *(Thue-Siegel principle) If α is of degree $n \geq 3$ and x/y and x'/y' are two very good approximations to α then*

$$\log\left(4e^{A_1}\right) + \log\left(\max(|x'|, |y'|)\right) \leq \gamma^{-1}\left(\log\left(4e^{A_1}\right) + \log\left(\max(|x|, |y|)\right)\right),$$

where $\gamma = \frac{nt^2+\tau^2-2}{n-1}$.

We also need the following refinement of an inequality of Lewis and Mahler :

Lemma 6.4.2. *Let F be a binary form of degree $n \geq 3$ with integer coefficients and nonzero discriminant D. For every pair of integers (x, y) with $y \neq 0$*

$$\min_{\alpha}\left|\alpha - \frac{x}{y}\right| \leq \frac{2^{n-1}n^{n-1/2}\left(M(F)\right)^{n-2}|F(x,y)|}{|D(F)|^{1/2}|y|^n},$$

where the minimum is taken over the zeros α of $F(z, 1)$.

Proof. This is Lemma 3 of [16]. □

6.5 Large Solutions

We will now estimate the number of solutions (x, y) of (6.1) with $y > M(F)^2$. Suppose that (x, y) is an integral solution to (6.1). Then we have

$$(x - \alpha_1 y)(x - \alpha_2 y)(x - \alpha_3 y)(x - \alpha_4 y) = \pm 1.$$

Therefore, for some $1 \leq i \leq 4$,

$$|x - \alpha_i y| < 1.$$

Definition. We say the pair of solution (x, y) is *r*elated to α_i if

$$|x - \alpha_i y| = \min_{1 \leq j \leq 4}|x - \alpha_j y|.$$

Suppose (x_1, y_1), (x_2, y_2), ... are the solutions to (6.1) which are related to α_i with $y_j > M(F)^2$, for $j = 1, 2, \ldots$, ordered so that $y_1 \leq y_2 \leq \ldots$. By Lemma 6.4.2,

$$\left|\alpha_i - \frac{x_j}{y_j}\right| \leq \frac{2^{10}M(F)^2}{|D(F)|^{1/2}y_j^4} \tag{6.11}$$

for $j = 1, 2, \ldots$. Therefore,

$$\left|\frac{x_{j+1}}{y_{j+1}} - \frac{x_j}{y_j}\right| \leq \frac{2^{11}M(F)^2}{|D(F)|^{1/2}y_j^4}$$

Since $|x_{j+1}y_j - x_jy_{j+1}| \geq 1$ and $D > 2^{22}$, we have

$$\frac{y_j^3}{M(F)^2} \leq y_{j+1}. \tag{6.12}$$

To each solution (x_j, y_j), we associate a real number $\delta_j > 1$ by

$$y_j = M(F)^{1+\delta_j}. \tag{6.13}$$

From (6.12), we have

$$3\delta_j \leq \delta_{j+1}.$$

Therefore,

$$3^{j-1} \leq \delta_j. \tag{6.14}$$

Moreover, if the pairs of solutions (x_k, y_k) and (x_{k+l}, y_{k+l}) are both related to α_i then

$$3^l\delta_k \leq \delta_{k+l}. \tag{6.15}$$

Let us now apply the Thue-Siegel principle (Lemma 6.4.1) with

$$t = \sqrt{\frac{2}{4.01}}$$

and

$$\tau = 1.2\sqrt{2-4t^2} = 0.12\, t.$$

Then

$$\lambda = \frac{2}{t-\tau} = \frac{2}{0.88t} < 3.22,$$
$$A_1 = 100\left(\log(M(F)) + 2\right)$$

and

$$\gamma^{-1} < 1368, \tag{6.16}$$

where, $\gamma = \frac{4t^2+\tau^2-2}{3}$. Since we have assumed $\left|\alpha_i - \frac{x_j}{y_j}\right| < 1$,

$$|x_j| < |y_j|(|\alpha_i| + 1) \leq 2M(F)y_j.$$

Whereby

$$H(x_j, y_j) < 2M(F)y_j.$$

By (6.8) and since $D > 10^{500}$, we have

$$8e^{A_1} = 8e^{200}M(F)^{100} < M(F)^{102}. \tag{6.17}$$

So by (6.13),

$$(4e^{A_1}H(x_j, y_j))^{\lambda} < M(F)^{(103+\delta_j)\lambda}. \tag{6.18}$$

From (6.11),

$$\left|\alpha_i - \frac{x_j}{y_j}\right| < M(F)^{-4\delta_j}.$$

Hence, $\frac{x_j}{y_j}$ is a very good approximation to α_i whenever

$$4\delta_j \geq (103 + \delta_j)\lambda.$$

Since $\lambda \leq 3.22$, if $\delta_j > 414$ then $\frac{x_j}{y_j}$ is a very good approximation to α_i. So by (6.14), whenever

$$k > 1 + \frac{\log 415}{\log 3},$$

then $\frac{x_k}{y_k}$ is a very good approximation to α_i. This means there are at most 6 large solutions $(x_1,y_1),\ldots, (x_6, y_6)$ to (6.1) which are related to α_i for which $\frac{x_1}{y_1},\ldots, \frac{x_6}{y_6}$ are not good approximations to α_i. Suppose that there are l pairs of solutions (x_7, y_7), $\ldots$, (x_{6+l}, y_{6+l}) $(l > 1)$ which are both related to α_i, and for which $\frac{x_j}{y_j}$ are good approximations to α_i. Then by the Thue-Siegel principle (Lemma (6.4.1)) and (6.16),

$$\log\left(4e^{A_1}\right) + \log y_{7+l} \leq 1368\left(\log\left(4e^{A_1}\right) + \log(2M(F)y_8)\right),$$

and so, by (6.17),

$$\log y_{7+l} \leq 1368\,(103 \log M(F) + \log(y_8)) - 102 \log M(F) + \log(2).$$

Since $\delta_8 > 414$, by (6.13) and (6.15),

$$3^{l-1}\delta_8 \leq \delta_{7+l} < 1368\,\delta_8 + 139435 < 336\,\delta_8.$$

Thus,

$$l \leq \frac{\log 336}{\log 3} + 1 \leq 6.30.$$

This means there are at most 12 large solution related to each root of $F(x, 1)$.

6.6 Small Solutions

Here we will count the number of solutions to (6.1) with $1 \leq y \leq M(F)^2$. We will follow Stewart's[16] results for Thue inequalities with arbitrary degree and sharpen them for quartic Thue equations. Suppose that Y_0 is a fixed positive number. For each root α_i of $F(x,1)$, let $(x^{(i)}, y^{(i)})$ be the solution to (6.1) related to α_i with the largest value of y among those with $1 \leq y \leq Y_0$. Let $\mathfrak{X}$ be the set of solutions of (6.1) with $1 \leq y \leq Y_0$ minus the elements $(x^{(1)}, y^{(1)})$, $(x^{(2)}, y^{(2)})$, $(x^{(3)}, y^{(3)})$, $(x^{(4)}, y^{(4)})$. From inequality (60) of [16], we have

$$\left(\left(\frac{2}{7}\right)^4 M(F)\right)^{|\mathfrak{X}|} \leq Y_0^4, \tag{6.19}$$

where $|\mathfrak{X}|$ denotes the cardinality of $\mathfrak{X}$. By (6.8), when $D > 10^{500}$, we have

$$\left(\frac{2}{7}\right)^4 M(F) \geq M(F)^{64/65}.$$

By (6.19),

$$|\mathfrak{X}| < 4\frac{65 \log Y_0}{64 \log M(F)}. \tag{6.20}$$

So when $Y_0 = M(F)^2$, we have $|\mathfrak{X}| \leq 8$. Therefore the number of small solutions does not exceed 12.

We have seen that there are at most 48 large solutions and 12 small ones to (6.1), when the discriminant is large. Since we assumed the quartic form $F(x,y)$ is monic, $(1,0)$ is also a solution to (6.1). Thus, the proof of Theorem 6.1.1 is complete.

In the next section, we will consider quartic forms $F(x,y)$ for which all roots of $F(x,1)$ are real. There we will call a solution (x,y) a large solution if $y > M(F)^6$.

Lemma 6.6.1. *There are at most* 14 *solutions to (6.1) with* $y \leq M(F)^6$.

Proof. Choose $\theta > 0$ such that

$$\frac{65}{16}\left(\frac{8}{3} + \theta\right) < 11.$$

From (6.19), we conclude that (6.1) has at most 10 solutions with $1 \leq y < M(f)^{\frac{8}{3}+\theta}$. Further, by (6.12), equation (6.1) has at most 4 solutions with $M(f)^{\frac{8}{3}+\theta} \leq y < M(f)^6$. So altogether (6.1) has at most 14 solutions with $1 \leq y < M(f)^6$.

□

6.7 Forms With Real Roots

In this section, we will assume α_i, the roots of $F(x,1)$, are real.

Define

$$\phi_m(x,y) = \log\left|\frac{D^{\frac{1}{12}}(x - y\alpha_m)}{|f'(\alpha_m)|^{\frac{1}{3}}}\right| \tag{6.21}$$

and

$$\phi(x,y) = (\phi_1(x,y), \phi_2(x,y), \phi_3(x,y), \phi_4(x,y)).$$

Let

$$\|\phi(x,y)\|$$

be the L_2 norm of the vector $\phi(x,y)$.

Lemma 6.7.1. *Suppose that (x,y) is a solution to the equation $F(x,y) = 1$ for the binary form F in Theorem 6.1.2. If*

$$|x - \alpha_i y| = \min_{1\leq j\leq 4} |x - \alpha_j y|$$

Then

$$\|\phi(x,y)\| \leq 6\ \log\frac{1}{|x-\alpha_i y|} + 4\log\left(\frac{D^{\frac{1}{12}}(5)^4 M(F)^3}{\sqrt{3}}\right).$$

Proof. Let us assume that

$$\left|x - \alpha_{s_j} y\right| < 1, \qquad \text{for } 1 \leq j \leq p$$

and

$$|x - \alpha_{b_k} y| \geq 1, \qquad \text{for } 1 \leq k \leq 4-p,$$

where $1 \leq p, s_j, b_k \leq 4$. We have

$$\prod_k |x - \alpha_{b_k} y| = \frac{1}{\prod_j \left|x - \alpha_{s_j} y\right|}.$$

Therefore, for any $1 \leq k \leq 4-p$, we have

$$\log|x - \alpha_{b_k} y| \leq p\log\frac{1}{|x - \alpha_i y|}.$$

Since

$$|x - \alpha_i y| = \min_{1\leq j\leq 4} |x - \alpha_j y|,$$

we also have

$$\left|\log\left|x-\alpha_{s_j}y\right|\right| \leq \left|\log\left|x-\alpha_i y\right|\right|.$$

From here, we conclude that

$$\begin{aligned}\|\phi(x,y)\| &\leq \sum_{m=1}^{4}\log\left|\frac{D^{\frac{1}{12}}}{|f'(\alpha_m)|^{\frac{1}{3}}}\right| + (4-p)p\left|\phi_i(x,y)\right| + p\left|\phi_i(x,y)\right| \\ &= \sum_{m=1}^{4}\log\left|\frac{D^{\frac{1}{12}}}{|f'(\alpha_m)|^{\frac{1}{3}}}\right| + (5p-p^2)\left|\phi_i(x,y)\right|.\end{aligned}$$

The function $f(p) = 5p - p^2$ gets its maximum value 6 over $p \in \{1,2,3,4\}$. Our proof is complete by recalling the fact that if a and b are distinct zeros of $f(x) = F(x,1)$, then by Lemma 6.3.4, we have

$$|a-b| \geq \frac{\sqrt{3}}{5^4}M(f)^{-3}. \tag{6.22}$$

□

6.7.1 Exponential Gap Principle

Here, our goal is to show

Theorem 6.7.2. *Suppose that (x_1,y_1), (x_2,y_2) and (x_3,y_3) are three pairs of non-trivial solutions to (6.1) with*

$$|x_j - \alpha_4 y_j| < 1,$$

for $j \in \{1,2,3\}$. If $r_1 \leq r_2 \leq r_3$ then

$$r_3 > \exp\left(\frac{r_1}{6}\right) 2\sqrt{3}\log^4\frac{1+\sqrt{5}}{2},$$

where $r_j = \|\phi(x_j,y_j)\|$.

We note that for three pairs of solutions in Theorem 6.7.2, the three points $\phi_1 = \phi(x_1,y_1)$, $\phi_2 = \phi(x_2,y_2)$ and $\phi_3 = \phi(x_3,y_3)$ form a triangle Δ. To establish Theorem 6.7.2, we will find a lower bound and an upper bound for the area of Δ. Then comparing these bounds, Theorem 6.7.2 will be proven. The length of each side of Δ is less than $2r_3$. Lemma 6.7.3 gives an upper bound for the height of Δ. Suppose that $(x,y) \neq (1,0)$ is a solution to (6.1) and let $t = \frac{x}{y}$. We have

$$\phi(x,y) = \phi(t) = \sum_{i=1}^{4}\log\frac{|t-\alpha_i|}{|f'(\alpha_i)|^{\frac{1}{3}}}\mathbf{b_i},$$

where,

$$\mathbf{b_1} = \frac{1}{4}(3,-1,-1,-1), \qquad \mathbf{b_2} = \frac{1}{4}(-1,3,-1,-1),$$
$$\mathbf{b_3} = \frac{1}{4}(-1,-1,3,-1), \qquad \mathbf{b_4} = \frac{1}{4}(-1,-1,-1,3),$$

Without loss of generality, we will suppose that for the pair of solution (x, y) we have

$$|x - \alpha_4 y| < 1.$$

We may write

$$\phi(x,y) = \phi(t) = \sum_{i=1}^{3} \log \frac{|t-\alpha_i|}{|f'(\alpha_i)|^{\frac{1}{3}}} \mathbf{c_i} + E_4 \mathbf{b_4}, \tag{6.23}$$

where, for $1 \leq i \leq 3$,

$$\mathbf{c_i} = \mathbf{b_i} + \frac{1}{3}\mathbf{b_4}, \quad E_4 = \log \frac{|t-\alpha_4|}{|f'(\alpha_4)|^{\frac{1}{3}}} - \frac{1}{3}\sum_{i=1}^{3} \log \frac{|t-\alpha_i|}{|f'(\alpha_i)|^{\frac{1}{3}}}$$

One can easily observe that

$$\mathbf{c_i} \perp \mathbf{b_4}, \text{ for } 1 \leq i \leq 4.$$

Lemma 6.7.3. *Let*

$$\mathbf{L_4} = \sum_{i=1}^{3} \log \frac{|\alpha_4 - \alpha_i|}{|f'(\alpha_i)|^{\frac{1}{3}}} \mathbf{c_i} + z\mathbf{b_4}, \quad z \in \mathbb{R}.$$

Suppose that $(x, y) \neq (1, 0)$ *is a pair of solution to (6.1) with*

$$|x - \alpha_4 y| = \min_{1 \leq j \leq 4} |x - \alpha_j y|$$

and $y \geq M(F)^6$. *Then the distance between* $\phi(x, y)$ *and the line* $\mathbf{L_4}$ *is less than*

$$\exp\left(\frac{-r}{6}\right),$$

where $r = \|\phi(x, y)\|$.

Proof. The distance between $\phi(x, y)$ and $\mathbf{L_4}$ is equal to

$$\left\| \sum_{i=1}^{3} \log \frac{|t-\alpha_i|}{|\alpha_4 - \alpha_i|} \mathbf{c_i} \right\|,$$

where $t = \frac{x}{y}$. If $|t - \alpha_i| > |\alpha_4 - \alpha_i|$, then

$$\left|\log \frac{|t-\alpha_i|}{|\alpha_4 - \alpha_i|}\right| = \log \frac{|t-\alpha_i|}{|\alpha_4 - \alpha_i|} \leq \log\left(\frac{|t-\alpha_4|}{|\alpha_4 - \alpha_i|} + 1\right) < \frac{|t-\alpha_4|}{|\alpha_i - \alpha_4|}.$$

If $|t - \alpha_i| < |\alpha_4 - \alpha_i|$, then

$$\left|\log \frac{|t-\alpha_i|}{|\alpha_4 - \alpha_i|}\right| = \log \frac{|\alpha_4-\alpha_i|}{|t - \alpha_i|} \leq \log\left(\frac{|t-\alpha_4|}{|t - \alpha_i|} + 1\right) < \frac{|t-\alpha_4|}{|\alpha_i - t|}.$$

Note that when $i \neq 3$, either

$$|t - \alpha_i| > |\alpha_4 - \alpha_i|$$

or

$$|t - \alpha_i| > |\alpha_3 - \alpha_i|.$$

Therefore, for $i \neq 3$,

$$\left|\log \frac{|t-\alpha_i|}{|\alpha_4 - \alpha_i|}\right| < \frac{|t-\alpha_4|}{m},$$

where $m = \min_{i\neq j}\{|\alpha_j - \alpha_i|\}$. Moreover, since we assumed t is closer to α_4,

$$|t - \alpha_3| \geq \frac{|\alpha_4 - \alpha_3|}{2}.$$

Consequently,

$$\left|\log \frac{|t-\alpha_3|}{|\alpha_4 - \alpha_3|}\right| < \frac{2|t-\alpha_4|}{m}.$$

Therefore

$$\left\|\sum_{i=1}^{3} \log \frac{|t-\alpha_i|}{|\alpha_4 - \alpha_i|}\mathbf{c_i}\right\| < 4\sqrt{\frac{2}{3}}\frac{|u|}{m}, \tag{6.24}$$

where $u = t - \alpha_4$. On the other hand, by Lemma 6.7.1

$$r - 4\log\left(\frac{D^{\frac{1}{12}}5^4 M(F)^3}{\sqrt{3}}\right) \leq 6\log\frac{1}{|x - \alpha_4 y|},$$

which implies

$$\log|yu| < \frac{-r}{6} + \frac{16}{25}\log\left(\frac{D^{\frac{1}{12}}5^4 M(F)^3}{\sqrt{3}}\right).$$

Therefore,

$$|u| < \exp\left(\frac{-r}{6}\right) \frac{\exp\left(\frac{16}{25}\log\left(\frac{D^{\frac{1}{12}} 5^4 M(F)^3}{\sqrt{3}}\right)\right)}{|y|}$$

Comparing this with(6.24), since $|y| > M(F)^6$ and (by (6.8)) we have

$$D^{1/12} < 4^{1/3} M(F)^{1/12},$$

our proof is complete (note that by (6.3.4), $m \geq \frac{\sqrt{3}}{5^4 M(f)^3}$). □

Lemma 6.7.3 shows that the height of Δ is at most

$$2\exp\left(\frac{-r_1}{6}\right).$$

Therefore, the area of Δ is less than

$$2r_3 \exp\left(\frac{-r_1}{6}\right). \tag{6.25}$$

To estimate the area of Δ from below, we appeal to Pohst's lower bound for units. Since

$$F(x,y) = (x-\alpha_1 y)(x-\alpha_2 y)(x-\alpha_3 y)(x-\alpha_4 y) = \pm 1,$$

we conclude that $x - \alpha_i y$ is a unit in $\mathbb{Q}(\alpha_i)$ when (x,y) is a pair of solution to (6.1). Suppose that (x_1,y_1) and (x_2,y_2) are two pairs of non-trivial solutions to (6.1). Then

$$\phi(x_1,y_1) - \phi(x_2,y_2) = \left(\log\frac{x_1-\alpha_1 y}{x_2-\alpha_1 y_2}, \ldots, \log\frac{x_1-\alpha_4 y_1}{x_2-\alpha_4 y_2}\right) = \vec{e}.$$

Since $\frac{x_1-\alpha_i y}{x_2-\alpha_i y_2}$ is a unit in $\mathbb{Q}(\alpha_i)$, we have

$$\|\vec{e}\| \geq 4\log^2\frac{1+\sqrt{5}}{2}$$

(see exercise 2 on page 367 of [14]). Now we can estimate each side of Δ from below to conclude that the area of the triangle Δ is greater than

$$16\,\frac{\sqrt{3}}{4}\log^4\frac{1+\sqrt{5}}{2}.$$

Comparing this with (6.25) we conclude that

$$2\,r_3\exp\left(\frac{-r_1}{6}\right) > 16\,\frac{\sqrt{3}}{4}\log^4\frac{1+\sqrt{5}}{2}.$$

Theorem 6.7.2 is immediate from here.

6.7.2 Geometry Of The Curve $\phi(t)$

In order to study the curve $\phi(t)$, we will consider some well-known geometric properties of the unit group U of $\mathbb{Q}(\alpha)$, where α is a root of $F(x, 1) = 0$.

Theorem 6.7.4 (Dirichlet's Unit Theorem)**.** *Let K be an algebraic number field of degree n. Let r be the number of real conjugate fields of K and $2s$ the number of complex conjugate fields of K. Then the ring of integers O_K contains $r + s - 1$ fundamental units $\epsilon_1, \ldots, \epsilon_{r+s-1}$ such that each unit of O_K can be expressed uniquely in the form $u\epsilon_1^{n_1} \ldots \epsilon_{r+s-1}^{n_{r+s-1}}$, where u is a root of unity in O_K and $n_1, \ldots, n_{r+s-1}$ are integers.*

For a real algebraic number field $\mathbb{Q}(\alpha)$ of degree 4, in Dirichlet's Unit Theorem we have $r = 4$ and $s = 0$. By Dirichlet's unit theorem, we have a sequence of mappings

$$\tau : U \longmapsto V \subset \mathbb{R}^4 \tag{6.26}$$

and

$$\log : V \longmapsto \Lambda, \tag{6.27}$$

where V is the image of the map τ, Λ is a 3-dimensional lattice, τ is the obvious restriction of the embedding of $\mathbb{Q}(\alpha)$ in $\mathbb{R}^4$, and the mapping log is defined as follows:
For $(x_1, x_2, x_3, x_4) \in V$,

$$\log(x_1, x_2, x_3, x_4) = (\log|x_1|, \log|x_2|, \log|x_3|, \log|x_4|).$$

If (x, y) is a pair of solutions to (6.1) then

$$(x - \alpha_j y)$$

is a unit in $\mathbb{Q}(\alpha_i)$. Suppose that

$$\lambda_2, \lambda_3, \lambda_4$$

are fundamental units of $\mathbb{Q}(\alpha_i)$ and are chosen so that

$$\log(\tau(\lambda_2)), \log(\tau(\lambda_3)), \log(\tau(\lambda_4))$$

form a *reduced* basis for the lattice Λ. Let us assume that

$$\|\log(\tau(\lambda_2))\| \leq \|\log(\tau(\lambda_3))\| \leq \|\log(\tau(\lambda_4))\|.$$

$$\phi(x, y) = \phi(1, 0) + \sum_{k=2}^{4} m_k \log(\tau(\lambda_k))\ m_k \in \mathbb{Z} \tag{6.28}$$

Lemma 6.7.5. *For every fixed integer m, there are at most 6 solutions (x, y) to (6.1) for which in (6.28), $m_4 = m$.*

Proof. Let S be the 3-dimensional space of all points $\phi(1,0)+\sum_{i=2}^{4}\mu_i \log(\tau(\lambda_i))$ ($\mu_4 \in \mathbb{R}$). Let $\mu_4 = m$. Then the points

$$\phi(1,0) + \sum_{i=2}^{3} \mu_i \log(\tau(\lambda_i)) + m \log(\tau(\lambda_4))$$

form a linear subvariety S_1 of S. Let

$$\vec{N} = (N_1, \ldots, N_4) \in S$$

be the normal vector of S_1. Then the number of times that the curve $\phi(t)$ intersects S_1 equals the number of solutions in t to

$$\vec{N}.\phi(t) = 0, \tag{6.29}$$

where $\vec{N}.\phi(t)$ is the inner product of two vectors $\vec{N}$ and $\phi(t)$. We have

$$\frac{d}{dt}\left(\vec{N}.\phi(t)\right) = \frac{P(t)}{F(t)},$$

where

$$F(t) = (t - \alpha_1)\ldots(t - \alpha_4)$$

and $P(t)$ is a polynomial of degree 3. Therefore, since

$$\lim_{t\to\alpha_i^+} \log|t - \alpha_i| = -\infty$$

and

$$\lim_{t\to\alpha_i^-} \log|t - \alpha_i| - \infty,$$

the derivative has at most 3 zeros and consequently, the equation (6.29) can not have more than 6 solutions. ☐

Definition of the set $\mathfrak{A}$. Assume that equation (6.1) has more than 6 solutions. Then we can list 6 solutions (x_i, y_i) $(1 \leq i \leq 6)$, so that $r_i = \|\phi(x_i, y_i)\|$ are the smallest among all $\|\phi(x, y)\|$, where (x, y) varies over all non-trivial pairs of solutions. We call the set of all these 6 solutions $\mathfrak{A}$.

Corollary 6.7.6. *Let* $(x,y) \notin \mathfrak{A}$ *be a solution to (6.1). Then*

$$\|\log(\tau(\lambda_2))\| \leq \|\log(\tau(\lambda_3))\| \leq \|\log(\tau(\lambda_4))\| \leq 2\,\|\phi(x,y)\|\,.$$

Proof. Since we have assumed that $\|\log(\tau(\lambda_2))\| \leq \|\log(\tau(\lambda_3))\| \leq \|\log(\tau(\lambda_4))\|$, it is enough to show that $\|\log(\tau(\lambda_4))\| \leq \|\phi(x,y)\|$. By Lemma 6.7.5, there is at least one solution $(x_0,y_0) \in \mathfrak{A}$ so that

$$\phi(x,y) - \phi(x_0,y_0) = \sum_{i=2}^{4} k_i \log(\tau(\lambda_i))\,,$$

with $k_4 \neq 0$. Since $\{\log(\tau(\lambda_i))\}$ is a reduced basis for the lattice Λ in (6.27), we conclude that

$$\begin{aligned}\|\log(\tau(\lambda_4))\| &< \|\phi(x,y) - \phi(x_0,y_0)\| \\ &\leq 2\,\|\phi(x,y)\|\,.\end{aligned}$$

□

Lemma 6.7.7. *Suppose* $(x,y) \notin \mathfrak{A}$. *Then for* $r(x,y) = \|\phi(x,y)\|$, *we have*

$$r(x,y) \geq \frac{1}{2}\log\left(\frac{|D|^{1/12}}{2}\right).$$

Proof. Let $(x',y') \in \mathfrak{A}$ be a pair of solutions to equation (6.1) and α_i and α_j be two distict roots of quartic polynomial $F(x,1)$. We have

$$\begin{aligned}\left|e^{\phi_i(x',y')-\phi_i(x,y)} - e^{\phi_j(x',y')-\phi_j(x,y)}\right| &= \left|\frac{x'-y'\alpha_i}{x-y\alpha_i} - \frac{x'-y'\alpha_j}{x-y\alpha_j}\right| \\ &= \frac{|\alpha_i-\alpha_j|\,|xy'-yx'|}{|x-y\alpha_i||x-y\alpha_j|} \\ &\geq \frac{|\alpha_i-\alpha_j|}{|x-y\alpha_i||x-y\alpha_j|}.\end{aligned}$$

The last inequality follows from the fact that $|xy'-yx'|$ is a non-zero integer. Since $|\phi_i| < \|\phi\| = r$ and $r(x',y') < r(x,y)$, we may conclude

$$\left(2e^{2r(x,y)}\right)^6 \geq \prod_{1\leq i<j\leq 4}\left|\frac{x'-y'\alpha_i}{x-y\alpha_i} - \frac{x'-y'\alpha_j}{x-y\alpha_j}\right| \geq \sqrt{D}.$$

□

Let us define $T_{i,j}(t) := \log\left|\frac{(t-\alpha_i)(\alpha_4-\alpha_j)}{(t-\alpha_j)(\alpha_4-\alpha_i)}\right|$, so that for a pair of solutions $(x, y) \neq (1, 0)$,

$$\begin{aligned} T_{i,j}(x,y) = T_{i,j}(t) &= \log\left|\frac{\alpha_4-\alpha_i}{\alpha_4-\alpha_j}\right| + \log\left|\frac{t-\alpha_j}{t-\alpha_i}\right| \\ &= \log\left|\frac{\alpha_4-\alpha_i}{\alpha_4-\alpha_j}\right| + \log\left|\frac{x-\alpha_j y}{x-\alpha_i y}\right| \\ &= \log|\lambda_{i,j}| + \sum_{k=2}^{4} m_i \log\frac{|\lambda_k|}{|\lambda'_k|}, \end{aligned} \tag{6.30}$$

where $t = \frac{x}{y}$,

$$\lambda_{i,j} = \log\left|\frac{\alpha_4-\alpha_i}{\alpha_4-\alpha_j}\right|$$

and λ_k and λ'_k are fundamental units in $\mathbb{Q}(\alpha_j)$ and $\mathbb{Q}(\alpha_i)$, respectively. Note that the $m_k \in \mathbb{Z}$ in (6.28) and (6.30) are the same integers. We will end this section by giving an upper bound for $|T|$ and will estimate $|T|$ from below in the next section.

Lemma 6.7.8. *Let (x, y) be a pair of solution to (6.1) with $|y| > M(F)^6$. Then there exists a pair (i, j) for which*

$$|T_{i,j}(x,y)| < \exp\left(\frac{-r}{6}\right),$$

where $r = \|\phi(t)\|$.

Proof. Let us define

$$\beta_i = \begin{cases} \alpha_i & \text{if } i \leq 3 \\ \beta_{i-3} & \text{if } i \geq 4. \end{cases}$$

Note that

$$\sum_{k=1}^{2}\sum_{i=1}^{3}\log^2\left|\frac{(t-\beta_i)(\alpha_4-\beta_{i+k})}{(\alpha_4-\beta_i)(t-\beta_{i+k})}\right| =$$

$$4\sum_{i=1}^{3}\log^2\left|\frac{(t-\alpha_i)}{(\alpha_4-\alpha_i)}\right| - 4\sum_{i\neq j}\log\left|\frac{(t-\alpha_i)}{(\alpha_4-\alpha_i)}\right|\log\left|\frac{(t-\alpha_j)}{(\alpha_4-\alpha_j)}\right| =$$

$$4\sum_{i=1}^{3}\log^2\left|\frac{(t-\alpha_i)}{(\alpha_4-\alpha_i)}\right| - 2\sum_{i=1}^{3}\log\left|\frac{(t-\alpha_i)}{(\alpha_4-\alpha_i)}\right|\sum_{j\neq i}\log\left|\frac{(t-\alpha_j)}{(\alpha_4-\alpha_j)}\right| =$$

$$4\sum_{i=1}^{3}\log^2\left|\frac{(t-\alpha_i)}{(\alpha_4-\alpha_i)}\right| - 2\sum_{i=1}^{3}\log\left|\frac{(t-\alpha_i)}{(\alpha_4-\alpha_i)}\right|\log\left|\frac{(\alpha_4-\alpha_i)}{y^4f'(\alpha_4)(t-\alpha_4)(t-\alpha_i)}\right| =$$

$$6\sum_{i=1}^{3}\log^2\left|\frac{(t-\alpha_i)}{(\alpha_4-\alpha_i)}\right| - 2\log\left|\frac{1}{y^nf'(\alpha_4)(t-\alpha_n)}\right|\sum_{i=1}^{3}\log\left|\frac{(t-\alpha_i)}{(\alpha_4-\alpha_i)}\right| =$$

$$6\sum_{i=1}^{3}\log^2\left|\frac{(t-\alpha_i)}{(\alpha_4-\alpha_i)}\right| - 2\log^2\left|\frac{1}{y^4f'(\alpha_4)(t-\alpha_4)}\right|$$

On the other hand, from the proof of Lemma 6.7.3 the distance between $\phi(x,y)$ and the line $\mathbf{L_4} = \sum_{i=1}^{3}\log\frac{|\alpha_4-\alpha_i|}{|f'(\alpha_i)|^{\frac{1}{3}}}\mathbf{c_i} + z\mathbf{b_4}, \quad z\in\mathbb{R}$. is equal to $\left\|\sum_{i=1}^{3}\log\frac{|t-\alpha_i|}{|\alpha_4-\alpha_i|}\mathbf{c_i}\right\|$ and by the definition of $\mathbf{c_i}$ in section 6.7.1, we have

$$\begin{aligned}
&\left\|\sum_{i=1}^{3}\log\frac{|t-\alpha_i|}{|\alpha_4-\alpha_i|}\mathbf{c_i}\right\|^2\\
=\ &\left\|\sum_{i=1}^{3}\log\left(\frac{|t-\alpha_i|}{|\alpha_4-\alpha_i|}-\frac{1}{3}\left|\log\frac{1}{y^4f'(\alpha_4)(t-\alpha_4)}\right|\right)\mathbf{e_i}\right\|^2\\
=\ &\sum_{i=1}^{3}\log^2\left(\frac{|t-\alpha_i|}{|\alpha_4-\alpha_i|}-\frac{1}{3}\left|\log\frac{1}{y^4f'(\alpha_4)(t-\alpha_4)}\right|\right)\\
=\ &\sum_{i=1}^{3}\log^2\left|\frac{(t-\alpha_i)}{(\alpha_4-\alpha_i)}\right|-\frac{1}{3}\log\left|\frac{1}{y^4f'(\alpha_4)(t-\alpha_4)}\right|\sum_{i=1}^{3}\log\left|\frac{(t-\alpha_i)}{(\alpha_4-\alpha_i)}\right|
\end{aligned}$$

where $\{e_i\}$ is the standard basis for $\mathbb{R}^3$. So, there must be a pair of (i,j), for which

$$\begin{aligned} &\log^2\left|\frac{(t-\alpha_i)(\alpha_4-\alpha_j)}{(t-\alpha_j)(\alpha_4-\alpha_i)}\right| \\ < \; & \frac{1}{6}\sum_{k=1}^{2}\sum_{i=1}^{3}\log^2\left|\frac{(t-\beta_i)(\alpha_4-\beta_{i+k})}{(\alpha_4-\beta_i)(t-\beta_{i+k})}\right| = \\ = \; & \left\|\sum_{i=1}^{3}\log\frac{|t-\alpha_i|}{|\alpha_4-\alpha_i|}\mathbf{c_i}\right\|^2 . \end{aligned}$$

Therefore, by Lemma 6.7.3

$$|T_{i,j}(x,y)| = \left|\log\left|\frac{(t-\alpha_i)(\alpha_4-\alpha_j)}{(t-\alpha_j)(\alpha_4-\alpha_i)}\right|\right| < \exp\left(\frac{-r}{6}\right).$$

□

6.7.3 Linear Forms In Logarithms

Theorem 6.7.9 (Matveev)**.** *Suppose that $\mathbb{K}$ is a real algebraic number field of degree d. We are given numbers $\alpha_1, \ldots \alpha_n \in \mathbb{K}^*$ with absolute logarithm heights $h(\alpha_j)$. Let $\log\alpha_1$, ... , $\log\alpha_n$ be arbitrary fixed non-zero values of the logarithms. Suppose that*

$$A_j \geq \max\{dh(\alpha_j), |\log\alpha_j|\}, \quad 1 \leq j \leq n.$$

Now consider the linear form

$$L = b_1\log\alpha_1 + \ldots + b_n\log\alpha_n,$$

with $b_1, \ldots, b_n \in \mathbb{Z}$ and with the parameter $B = max\{1, \max\{b_jA_j/A_n : \; 1 \leq j \leq n\}\}$. Put

$$\Omega = A_1 \ldots A_n,$$

$$C(n) = \frac{16}{n!}e^n(2n+2)(n+2)(4n+4)^{n+1}(\frac{1}{2}en),$$

$$C_0 = \log(e^{4.4n+7}n^{5.5}d^2\log(en)),$$

$$W_0 = \log(1.5eBd\log(ed)).$$

If $b_n \neq 0$, then

$$\log|L| > -C(n)C_0W_0d^2\Omega.$$

Proof. See [11] for proof. □

Let index σ be the isomorphism from $\mathbb{Q}(\alpha_i)$ to $\mathbb{Q}(\alpha_j)$ such that $\sigma(\alpha_i) = \alpha_j$. We may assume that $\sigma(\lambda_i) = \lambda'_i$ for $i = 2, 3, 4$. Let (x_1, y_1) , (x_2, y_2) , (x_3, y_3),(x_4, y_4),(x_5, y_5) be five distinct " large" solutions to (6.1) with $(x_k, y_k) \notin \mathfrak{A}$,

$$y_k > M(F)^6$$

and

$$|x_k - \alpha_4 y_k| = \min_{1 \leq i \leq 4} |x_k - \alpha_i y_k| \quad k \in \{1, 2, 3, 4, 5\}$$

and $r_1 \leq r_2 \leq r_3 \leq r_4 \leq r_5$ where $r_k = \|\phi(x_k, y_k)\|$. We will apply Matveev's lower bound to

$$T_{i,j}(x_5, y_5) = \log |\lambda_{i,j}| + \sum_{k=2}^{4} m_k \log \frac{|\lambda_k|}{|\lambda'_k|},$$

where (i, j) is chosen so that Lemma 6.7.8 is satisfied and $m_k \in \mathbb{Z}$. In the above representation, λ_k are multiplicatively dependent if and only if $\lambda_{i,j}$ is a unit. If $\lambda_{i,j}$ is a unit then we can write $T_{i,j}(x, y)$ as a linear form in 3 logarithms. Since theorem 6.7.9 gives a better lower bound for linear forms in 3 logarithms, we will assume that $\lambda_{i,j}$, λ_2, λ_3 and λ_4 are multiplicatively independent and $T_{i,j}(x, y)$ is a linear form in 4 logarithms.

Suppose that λ is a unit in the number field and λ' is its algebraic conjugate. We have

$$h(\lambda') = h(\lambda) = \frac{1}{8} \left|\log\left(\tau(\lambda)\right)\right|_1,$$

where h is the logarithmic height and $| \ |_1$ is the L_1 norm on $\mathbb{R}^4$ and the mappings τ and log are defined in (6.26) and (6.27) . So we have

$$h(\lambda) = \frac{1}{8} \left|\log\left(\tau(\lambda)\right)\right|_1 \leq \frac{\sqrt{4}}{8} \left\|\log\left(\tau(\lambda)\right)\right\|,$$

where $\|\|$ is the L_2 norm on $\mathbb{R}^4$. Since α_4, α_i and α_j have degree 4 over $\mathbb{Q}$, the number field $\mathbb{Q}(\alpha_4, \alpha_i, \alpha_j)$ has degree $d \leq 24$ over $\mathbb{Q}$. So when λ is a unit

$$\max\{dh(\frac{\lambda}{\lambda'}), \left|\log(\left|\frac{\lambda}{\lambda'}\right|)\right|\} \leq \max\{24h(\frac{\lambda}{\lambda'}), |\log(\left|\frac{\lambda}{\lambda'}\right|)|\} \leq 12 \left\|\log\left(\tau(\lambda)\right)\right\|. \tag{6.31}$$

Therefore, to apply Theorem 6.7.9 to $T_{i,j}(x, y)$, by Lemma 6.7.6, we may take

$$A_i = 24r_1, \text{ for } 2 \leq i \leq 4.$$

By Lemma 6.3.2, Proposition 6.3.3, (6.9) and (6.10), we may take

$$\frac{A_1}{24} = 2\log 2 + 4\exp\left[2(\log D)^{13}\right],$$

(note that α_1, α_i , α_j are algebraic conjugates). To estimate B, we note that since λ_i $(2 \le i \le 4)$ form a reduced basis for the lattice Λ, we have

$$\begin{aligned} m_i \|\log \tau(\lambda_i)\| &\le \|\phi(x_5, y_5)\| + \|\phi(1,0)\| \\ &\le r_5 + 2\log D^{1/12} + 2\log\frac{5^4 M(F)^3}{\sqrt{3}} \\ &\le r_5 + 2\log D^{1/12} + 2\log\frac{5^{11/2} H(F)^3}{\sqrt{3}}, \end{aligned}$$

where the inequalities are from Lemmas 6.3.1 and (6.22). Therefore, by Proposition 6.3.3,

$$B = \max\{1, \max\{b_j A_j/A_1 : \ 1 \le j \le n\}\} < r_5.$$

Theorem 6.7.9 implies that for a constant number K,

$$\log T_{i,j}(x_5, y_5) > -K\ \exp\left[2(\log D)^{13}\right] r_1^3 \log r_5.$$

Comparing this with Lemma 6.7.8, we have

$$\left(\frac{-r_5}{6}\right) > -K\ \exp\left[2(\log D)^{13}\right] r_1^3 \log r_5.$$

Thus we may compute the constant number K_1, so that

$$r_5 < K_1\ \exp\left[2(\log D)^{13}\right] r_1^3 \log r_1,$$

This contradicts Lemma 6.7.2 when $D > 10^{500}$, for by Lemma 6.7.7,

$$r_1 \ge \frac{1}{2}\log\left(\frac{|D|^{\frac{1}{12}}}{2}\right).$$

Thus, there are at most 16 solutions $(x, y) \notin \mathfrak{A}$ with $y > M(F)^6$. By Lemma 6.6.1 and since $|\mathfrak{A}| = 6$, counting the solution $(1, 0)$, Theorem 6.1.2 is proven.

Bibliography

[1] S. Akhtari, The method of Thue-Siegel for binary quartic forms, submitted (2007).

[2] E. Bombieri, W. M. Schmidt, On Thue's equation, Invent. Math. 88 (1987), 69-81.

[3] Y. Bugeaud, Bornes effectives pour les solutions des équations en S-units et des équations de Thue-Mahler, J. Number Theory 71(1998), 227-244.

[4] J.E. Cremona. Reduction of binary cubic and quartic forms. LMS JMC 2 (1999), 62-92.

[5] B.N. Delone and D.K. Fadeev. The Theory of Irrationalities of the Third Degree. Translation of Math. Monographs, AMS 10 (1964).

[6] J.H. Evertse and K. Gyory, Effective finiteness results for binary forms with given discriminant, Compositio Math. 79(1991), 169-204.

[7] K. Győry, Polynomials and binary forms of given discriminant, Publ. Math. Debrecen 69 (2006), 473-499.

[8] K. Győry, Sur les polynomial a coefficients entiers et the discriminant donne II, Pub. Math. Debrecen 21 (1974), 125-144.

[9] K. Mahler, An inequality for the discriminant of a polynomial, Michigan Math. J. 11 (1964), 257-262.

[10] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, Izv. Ross. Akad. Nauk Ser. Mat. 62 (1998), 81-136, translation in Izv. Math. 62 (1998), 723-772.

[11] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, Izv. Ross. Akad. Nauk

Ser. Mat. 64 (2000), 125-180, translation in Izv. Math. 64 (2000), 1217-1269.

[12] L.J. Mordell, Diophantine Equations, Academic Press, London and New York (1969).

[13] R. Okazaki. Geometry of a cubic Thue equation, Publ. Math. Debrecen. 61 (2002),267-314.

[14] M. Pohst and H. Zassenhause. Algorithmic Algebraic Number Theory, Cambridge University Press (1989).

[15] W.M. Schmidt, Diophantine approximations and Diophantine equations, Lecture Notes in Mathematics, Springer Verlag (2000).

[16] C. L. Stewart, On the number of solutions of polynomial congruences and Thue equations, Journal of American Math. Soc., 4 (1991), 793-838.

Chapter 7

Geometry of Binary Cubic Forms [6]

7.1 Introduction

Let $F(x, y)$ be an irreducible binary cubic form with integral coefficients and negative discriminant. More than 80 years ago, Delone and Nagell established independently that the equation

$$F(x, y) = 1 \tag{7.1}$$

has at most five solutions in integers x, y. This result is proved by considering units in the algebraic number field $\mathbb{Q}(\rho)$, where ρ is the real root of $F(x, 1) = 0$. In their proofs the fact that the group of units in the ring of integers of $\mathbb{Q}(\rho)$ is generated by one fundamental unit is essential.

The situation where the discriminant of $F(x, y)$ is positive is complicated by the fact that the number field $\mathbb{Q}(\rho)$ (where ρ is any real root of $F(x, 1) = 0$) has a ring of integers generated by a pair of fundamental units. However, it is possible to reduce (7.1) to a set of exponential equations to which a local method of Skolem can be applied. In this way, Ljunggren [14] and Baulin [4], solved (7.1) respectively for $F(x, y) = x^3 - 3xy^2 + y^3$ of discriminant 81 and $F(x, y) = x^3 + x^2y - 2xy^2 - y^3$ of discriminant 49. In the first case there are 6 solutions and in the second case there are 9 solutions to (7.1).

In 1929, Siegel [16] used the theory of Padé approximation to binomial functions (via the hypergeometric functions), to show for F cubic of positive discriminant, that equation (7.1) has at most 18 solutions in integers x and y. Refining these techniques, Evertse [5] reduced this upper bound to 12. Later, Bennett [2] showed that if $F(x, 1)$ has at least two distinct complex roots, then the equation $F(x, y) = 1$ possesses at most 10 solutions in integers x and y. In 2003, by studying the geometry of numbers in the "logarithmic space", Okazaki [15] proved that when discriminant of F is greater than 5.65×10^{65},

[6] A version of this chapter will be submitted for publication. Akhtari. S. Geometry of binary cubic forms

equation (7.1) has at most 7 solutions. Okazaki's method is essentially different from Evertse's. In this paper, we will relate some geometric ideas of Okazaki [15] to the method of Thue-Siegel as refined by Evertse [5], in conjunction with lower bounds for linear forms in logarithms of algebraic numbers. The following are the main results of this paper:

Theorem 7.1.1. *If $F(x,y)$ is a binary cubic form with discriminant $D > 1.4 \times 10^{57}$, then the equation*

$$F(x,y) = 1$$

possesses at most 7 solutions in integers x and y.

We will define the reduced forms in Section 7.2. It is well-known that every cubic form of positive discriminant is equivalent to a reduced form $F(x,y)$.

Theorem 7.1.2. *Let $F(x,y)$ be a cubic form with discriminant $D > 9 \times 10^{58}$. If $F(x,y)$ is equivalent to a reduced form which is not monic, then the equation $F(x,y) = 1$ posses at most 6 solutions in integers x and y.*

In 1990, using the fact that the underlying number fields are the so-called "simplest cubics", Thomas [17] showed that the equations

$$G_{1,n}(x,y) = x^3 + nx^2y - (n+3)xy^2 + y^3 = 1$$

have only the solutions $(1,0)$, $(0,1)$ and $(-1,-1)$ in integers, provided $n \geq 1.365 \times 10^7$. This restriction was later removed by Mignotte [11] except for the equation with

$$n \in \{-1, 0, 2\}.$$

It is known that $G_{1,n}(x,y) = 1$ has 9 solutions for $n = -1$ ([4]), 6 solutions for $n = 0$ ([14]) and 6 solutions for $n = 2$ ([6]) .

Define $F_m(x,y)$ by

$$F_m(x,y) = x^3 - (m+1)x^2y + mxy^2 + y^3$$

for $m \in \mathbb{Z}$. Provided $m \neq -2$, -1 or 1 , the equation $F_m(x,y) = 1$ has the five distinct integral solutions $(x,y) = (1,0)$, $(1,1)$, $(1,-m-1)$, $(0,1)$ and $(m,1)$. That this list is complete was proven, independently, by Lee [7] and Mignotte and Tzanakis [13], for m suitably large and later, by Mignotte [12], for $m > 2$. The cases $m = 0$ and $m = 1$ correspond to discriminant -23 and -31, respectively.

All known irreducible cubic forms $F(x,y)$, for which the equation (7.1) has more than 5 solutions, have discriminant less than 362.

The following conjecture is essentially due to Nagell and refined by Pethö and Lippok.

Conjecture If F is a binary cubic form with positive discriminant $D_F > 361$, then the number of solutions of equation (7.1) is less than 6.

7.2 The Covariants of Binary Cubic Forms

Let us define, for a cubic form F with discriminant D, an associated quadratic form, the Hessian $H = H_F$, and a cubic form $G = G_F$, by

$$\begin{aligned} H(x,y) &= -\frac{1}{4}\left(\frac{\delta^2 F}{\delta x^2}\frac{\delta^2 F}{\delta y^2} - \left(\frac{\delta^2 F}{\delta x \delta y}\right)^2\right) = \\ & Ax^2 + Bxy + Cy^2 \end{aligned}$$

and

$$G(x,y) = \frac{\delta F}{\delta x}\frac{\delta H}{\delta y} - \frac{\delta F}{\delta y}\frac{\delta H}{\delta x}.$$

These forms satisfy a covariance property; i.e.

$$H_{F\circ\gamma} = H_F \circ \gamma \qquad \text{and} \qquad G_{F\circ\gamma} = G_F \circ \gamma$$

for all $\gamma \in GL_2(\mathbb{Z})$.

We call forms F_1 and F_2 equivalent if they are equivalent under $GL_2(\mathbb{Z})$-action; i.e. if there exist integers a_1 , a_2 , a_3 and a_4 such that

$$F_1(a_1x + a_2y, a_3x + a_4y) = F_2(x,y)$$

for all x, y , where $a_1a_4 - a_2a_3 = \pm 1$.

We denote by N_F the number of solutions in integers x and y of the diophantine equation (7.1). If F_1 and F_2 are equivalent, then $N_{F_1} = N_{F_2}$ and $D_{F_1} = D_{F_2}$. Therefore, we can assume that F is monic (the coefficient of x^3 in $F(x,y)$ is 1). The discriminant D of such a form is given by

$$D = 18abcd + b^2c^2 - 27a^2d^2 - 4ac^3 - 4b^3d = a^4 \prod_{i,j}(\alpha_i - \alpha_j)^2$$

where α_1, α_2 and α_3 are the roots of polynomial $F(x,1)$.

For $F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, it follows by routine calculation that

$$A = b^2 - 3ac,\ B = bc - 9ad,\ C = c^2 - 3bd$$

and

$$B^2 - 4AC = -3D.$$

Further, these forms are related to $F(x, y)$ via the identity

$$4H(x,y)^3 = G(x,y)^2 + 27DF(x,y)^2 \tag{7.2}$$

Binary cubic form F is called *reduced* if the Hessian of F, $H(x, y) = Ax^2 + Bxy + Cy^2$, satisfies

$$C \geq A \geq |B|$$

It is a basic fact (see [1]) that every cubic form of positive discriminant is equivalent to a reduced form $F(x, y)$. The reader is directed to [1] (chapter III and supplement I) for more details on reduction. We will later use the following lemma to bound the discriminant D from above.

Lemma 7.2.1. *Let F be an irreducible binary cubic form with positive discriminant D and Hessian H. For all integer solutions (x_1, y_1) to equation $F(x, y) = 1$, except possibly one solution, we have $H(x_1, y_1) \geq \frac{1}{2}\sqrt{3D}$.*

Proof. If F_1 is an equivalent reduced form to F and

$$F_1(a_1x + a_2y, a_3x + a_4y) = F(x, y),$$

then

$$H_1(a_1x + a_2y, a_3x + a_4y) = H(x, y),$$

where H and H_1 are the Hessians of F and F_1 respectively. This means the set of values of the Hessian at solutions is fixed under $GL_2(\mathbb{Z})$-action. So we may assume that F is reduced. Now following the proof of lemma 5.1. of [2], we suppose (x, y) is a solution to $F(x, y) = 1$ with $y \neq 0$. If $|y| \leq |x|$, then, since $A > |B|$ and $B^2 - 4AC = -3D$, we have that

$$H(x,y) \geq Cy^2 \geq C \geq \frac{1}{2}\sqrt{3D}.$$

If, on the other hand, $|y| \geq |x| + 1$, then

$$H(x,y) \geq (C - |B|)y^2 + |B||y| + Ax^2.$$

Since this is an increasing function of $|y|$ and $y \neq 0$, we have

$$H(x,y) \geq C + Ax^2 \geq C \geq \frac{1}{2}\sqrt{3D}.$$

Therefore, if $H(x, y) < \frac{1}{2}\sqrt{3D}$, then $y = 0$ and so $x = \pm 1$ accordingly . □

Remark. The above proof shows the only possibility for the Hessian $H(x, y)$ to assume a value less than $\frac{1}{2}\sqrt{3D}$, at a pair of solutions (x, y), is when the equivalent reduced form is monic. This is because $(1, 0)$ is a solution to (7.1) if and only if F is monic.

7.3 Some Functions In The Number Field $\mathbb{Q}(\sqrt{-3D})$

Let $\sqrt{-3D}$ be a fixed choice of the square-root of $-3D$. we will work in the number field $M = \mathbb{Q}(\sqrt{-3D})$. It is well-known that if F has positive discriminant then H is positive definite. By (7.2), we can write $H^3(x, y) = U(x, y)V(x, y)$ where

$$U(x, y) = \frac{G(x, y) + 3\sqrt{-3D}F(x, y)}{2},$$

$$V(x, y) = \frac{G(x, y) - 3\sqrt{-3D}F(x, y)}{2}.$$

Then U and V are cubic forms with coefficients belonging to M such that corresponding coefficients of U and V are complex conjugates. Since F must be also irreducible over M, U and V do not have factors in common. It follows that $U(x, y)$ and $V(x, y)$ are cubes of linear forms over M, say $\xi(x, y)$ and $\eta(x, y)$.

Note that $\xi(x, y)\eta(x, y)$ must be a quadratic form which is cube root of $H(x, y)^3$ and for which the coefficient of x^3 is a positive real number. Hence we have

$$\xi(x, y)^3 - \eta(x, y)^3 = 3\sqrt{-3D}F(x, y),$$

$$\xi(x, y)^3 + \eta(x, y)^3 = G(x, y), \tag{7.3}$$

$$\xi(x, y)\eta(x, y) = H(x, y).$$

and for $x, y \in \mathbb{Z}$,

$$\frac{\xi(x, y)}{\xi(1, 0)} \text{ and } \frac{\eta(x, y)}{\eta(1, 0)} \in M.$$

The reason for the last identity is that for any pair of rational integers x_0 , y_0,

$$\xi(x_0, y_0) \,\text{and}\, \eta(x_0, y_0)$$

are complex conjugates and the discriminant of H is $-3D$.

We call a pair of forms ξ and η satisfying the above properties a pair of *resolvent* forms. Note that there are exactly three pairs of resolvent form, given by

$$(\xi, \eta),\ (\omega\xi, \omega^2\eta),\ (\omega^2\xi, \omega\xi),$$

where ω is a primitive cube root of unity.

We say that a pair of rational integers (x, y) is related to the pair of resolvent forms (ξ, η) if

$$|1 - \frac{\eta(x,y)}{\xi(x,y)}| = \min_{0\le k\le 2} |\omega^k - \frac{\eta(x,y)}{\xi(x,y)}| \tag{7.4}$$

Following a discussion of Delone and Faddeev in [1], we call the roots $\rho_1, \rho_1', \rho_1''$ of the equation $F(x, a) = 0$ the left roots of the form F, while the roots $\rho_2, \rho_2', \rho_2''$ of $F(d, -y)$ are called the right roots of the form F. If t_1 is a left root, then it is easily seen that $t_2 = -ad/t_1$ is a right root of F. Two such roots of F will be called corresponding roots and we will assume that ρ_1 and ρ_2 , ρ_1' and ρ_2', ρ_1'' and ρ_2'' correspond in pairs.

The following lemma is a statement of Lagrange's method for solution of cubic equations by means of the resolvent adapted to the case of binary cubic forms.

Lemma 7.3.1. *For the cubic form $F(x, y)$ the following identity holds*

$$F(x,y) = \frac{1}{3\sqrt{-3D}}(\xi^3 - \eta^3),$$

where

$$\xi = \xi_1 x + \xi_2 y,$$

$$\eta = \eta_1 x + \eta_2 y,$$

$$\xi_1 = \rho_1 + \omega\rho_1' + \omega^2\rho_1'',$$

$$\eta_1 = \rho_1 + \omega^2\rho_1' + \omega\rho_1'',$$

$$\xi_2 = \rho_2 + \omega\rho_2' + \omega^2\rho_2'',$$

$$\eta_2 = \rho_2 + \omega^2\rho_2' + \omega\rho_2''$$

and $\omega = e^{\frac{2\pi i}{3}}$.

Proof. One can find the complete proof of Lemma 7.3.1 in [1]. □

We continue with the following definitions of p, q and u_i :

$$p = \frac{\eta + \xi}{\sqrt{2}} \ , \ q = \frac{\sqrt{-1}(\eta - \xi)}{\sqrt{2}},$$

$$u_1 = D^{-1/6}(\frac{q}{\sqrt{6}} + \frac{p}{\sqrt{2}}) \ , \ u_2 = D^{-1/6}(\frac{q}{\sqrt{6}} - \frac{p}{\sqrt{2}}) \ , \ u_3 = D^{-1/6}\frac{2}{\sqrt{6}}q. \quad (7.5)$$

Since η and ξ are functions of x and y, so are p, q and u_i

The reason of our interest in the new functions $p(x, y)$, $q(x, y)$ and $u_i(x, y)$, despite their apparent complication, is that they explain the relation between the method of Evertse [5] and the method of Okazaki [15] for finding an upper bound for the number of integral solutions of (7.1). In other words, these functions allow us to recast the resolvent forms ξ and η in a geometric setting.

By Lemma 7.3.1, we have

$$\frac{q}{\sqrt{6}} = \frac{\sqrt{-1}(\eta - \xi)}{2\sqrt{3}} = \sqrt{-1}\,\frac{\omega^2 - \omega}{2\sqrt{3}}[(\rho'_1 - \rho''_1)x - (\rho'_2 - \rho''_2)y].$$

We also have

$$\omega^2 - \omega = \cos(4\pi/3) + \sqrt{-1}\sin(4\pi/3) - (\cos(2\pi/3) + \sqrt{-1}\sin(2\pi/3)) = \sqrt{-3}.$$

so we get

$$\frac{q}{\sqrt{6}} = -\frac{(\rho'_1 - \rho''_1)x + (\rho'_2 - \rho''_2)y}{2}. \quad (7.6)$$

Further

$$\frac{p}{\sqrt{2}} = \frac{(2\rho_1 + \omega(\rho'_1 + \rho''_1) + \omega^2(\rho'_1 + \rho''_1))x + (2\rho_2 + \omega(\rho'_2 + \rho''_2) + \omega^2(\rho'_2 + \rho''_2))y}{2}.$$

Since ω is a primitive third root of unity, $\omega + \omega^2 = -1$. Hence

$$\frac{p}{\sqrt{2}} = \frac{2(\rho_1 x + \rho_2 y) - (\rho'_1 + \rho''_1)x - (\rho'_2 + \rho''_2)y}{2} \quad (7.7)$$

Substituting $-ad/\rho_1$, $-ad/\rho'_1$ and $-ad/\rho''_1$ for ρ_2, ρ'_2 and ρ''_2 respectively, and noting that $\rho_1\rho'_1\rho''_1 = -a^2 d$, we obtain the following identities:

$$u_1 = D^{-1/6}(\rho_1 - \rho''_1)(x - \rho'_1 y/a), \quad (7.8)$$

$$u_2 = D^{-1/6}(\rho_1' - \rho_1)(x - \rho_1'' y/a), \tag{7.9}$$

$$u_3 = D^{-1/6}(\rho_1' - \rho_1'')(x - \rho_1 y/a), \tag{7.10}$$

where ρ_1, ρ_1' and ρ_1'' are left roots of F. Here we note that if we start with another choice of resolvent forms, only the order of u_i changes. In other words, all three resolvent forms can be indexed so that

$$q_i = \frac{\sqrt{-1}(\eta_i - \xi_i)}{\sqrt{2}}$$

Let us assume that F is monic, as we may. Therefore

$$(x - \rho_1 y)(x - \rho_1' y)(x - \rho_1'' y) = F(x, y).$$

If the pair (x_0, y_0) is a solution to (7.1), we conclude that $(x_0 - \rho_1 y_0)$, $(x_0 - \rho_1' y_0)$ and $(x_0 - \rho_1'' y_0)$ are units in $\mathbb{Q}(\rho_1)$. Moreover,

$$u_1 u_2 u_3 = D^{-1/2}(\rho_1 - \rho_1'')(\rho_1' - \rho_1)(\rho_1' - \rho_1'')F(x, y) = \pm F(x, y).$$

When (x, y) is a solution to $F(x, y) = 1$, since

$$\log|u_1| - \log|u_2| = \log|\frac{\rho_1 - \rho_1''}{\rho_1' - \rho_1}| + \log|\frac{x - \rho_1' y}{x - \rho_1'' y}|$$

and $\frac{x - \rho_1' y}{x - \rho_1'' y}$ is a unit, we can write

$$\log|u_1| - \log|u_2| = \log|\lambda_1| + m\log|\lambda_2| + n\log|\lambda_3|, \tag{7.11}$$

where $\lambda_1 = \frac{\rho_1 - \rho_1''}{\rho_1' - \rho_1}$ and where λ_2 and λ_3 are fundamental units in the ring of integers of $\mathbb{Q}(\rho_1)$ (when $D_F > 0$, the number field $\mathbb{Q}(\rho_1)$ is real and has a ring of integer generated by a pair of fundamental units).

Let us fix a resolvent forms (ξ_i, η_i) and corresponding p_i and q_i. We get

$$|1 - \frac{\eta_i}{\xi_i}| = |1 - \frac{p_i - \sqrt{-1}q_i}{p_i + \sqrt{-1}q_i}| = 2|q_i|/|\xi_i|.$$

Since $|\eta_i| = |\xi_i|$, by (7.3), $|\xi_i| = \sqrt{H}$. Hence,

$$|1 - \frac{\eta_i}{\xi_i}| = 2|q_i|/\sqrt{H}.$$

Suppose that (x, y) is a solution to (7.1) and related to resolvent form (ξ_i, η_i). Since

$$|1 - \frac{\eta_i}{\xi_i}| = \min_{k=1,2,3} \left|1 - \frac{\eta_k}{\xi_k}\right|,$$

we conclude that

$$|q_i| = \min_{k=1,2,3} |q_k|.$$

On the other hand,

$$\begin{aligned} \prod_{k=1}^{3} |q_i| &= \frac{|\eta - \xi||\omega\eta - \omega^2\xi||\omega^2\eta - \omega\xi|}{2\sqrt{2}} \\ &= \frac{|\eta^3 - \xi^3|}{2\sqrt{2}} = \frac{3\sqrt{3}}{2\sqrt{2}}\sqrt{D}, \end{aligned}$$

where the last equality comes from the equation (7.3).

If the solution (x, y) is related to (ξ_i, η_i), then

$$|u_3| = |D^{-1/6} \frac{2}{\sqrt{6}} q_i| < 1. \tag{7.12}$$

So we have

$$\log |u_3| < 0.$$

The identity

$$|u_1(x, y)u_2(x, y)u_3(x, y)| = 1$$

holds when (x, y) is a pair of solution to $|F(x, y)| = 1$. Therefore,

$$\log |u_1| + \log |u_2| + \log |u_3| = 0$$

and

$$\log |u_1 u_2| > 0.$$

7.4 Geometric Gap Principles

We will study the geometric properties of the functions u_i defined in section 2, by considering the well-known geometric properties of the unit group U of $\mathbb{Q}(\rho_1)$, where ρ_1 is a root of $F(x, 1) = 0$.

Theorem 7.4.1 (Dirichlet's unit theorem)**.** *Let K be an algebraic number field of degree n. Let r be the number of real conjugate fields of K and $2s$ the number of complex conjugate fields of K. Then the ring of integers O_K contains $r+s-1$ fundamental units $\epsilon_1, \ldots, \epsilon_{r+s-1}$ such that each unit of O_K can be expressed uniquely in the form $u\epsilon_1^{n_1} \ldots \epsilon_{r+s-1}^{n_{r+s-1}}$, where u is a root of unity in O_K and $n_1, \ldots, n_{r+s-1}$ are integers.*

Since F has positive discriminant, for the algebraic number field $\mathbb{Q}(\rho_1)$, in the notation of Dirichlet's unit theorem, we have $r = 3$ and $s = 0$. Suppose that λ_2 and λ_3 are fundamental units of $\mathbb{Q}(\rho_1)$. By Dirichlet's unit theorem, we have a sequence of mappings

$$\tau : U \longmapsto V \subset \mathbb{R}^3$$

and

$$\log : V \longmapsto \Lambda,$$

where Λ is a 2-dimensional lattice, τ is the obvious restriction of the embedding of K in $\mathbb{R}^3$, V is the image of mapping τ on U and log is defined as follows:
For $(x_1, x_2, x_3) \in V$,

$$\log(x_1, x_2, x_3) = (\log|x_1|, \log|x_2|, \log|x_3|).$$

We define τ to be the embedding from the unit group U to the lattice Λ:

$$\tau : U \longmapsto \Lambda - \{0\}.$$

By identities (7.8), (7.9) and (7.10), the vector

$$\vec{u} = (\log|u_1|, \log|u_3|, \log|u_3|)$$

can be considered as

$$\vec{v} + (\log|x - \rho_1' y|, \log|x - \rho_1'' y|, \log|x - \rho_1 y|), \tag{7.13}$$

where

$$\vec{v} = (\log|D^{-1/6}(\rho_1 - \rho_1'')|, \log|D^{-1/6}(\rho_1' - \rho_1)|, \log|D^{-1/6}(\rho_1'' - \rho_1')|.$$

We have assumed that $F(x, y)$ is monic, so we can suppose that $(1, 0)$ is a pair of integer solutions to $F(x, y) = 1$. Note that the vector $\vec{v}$ in (7.13) is a permutation of the vector $\vec{u}(1, 0)$.

If (x, y) is a pair of solutions to $|F(x, y)| = 1$, then

$$\vec{u} \in \vec{v} + \Lambda = \Lambda_1.$$

Note that $\mathrm{Vol}(\Lambda) = \mathrm{Vol}(\Lambda_1)$, where $\mathrm{Vol}(\Lambda)$ is the volume of fundamental parallelepiped of lattice Λ. Since $\vec{u}$ belongs to a 2-dimensional lattice, we can find a 2-dimensional representation for $\vec{u}$, say (t, s). Specifically, let (x, y) be a pair of solution to $F(x, y) = 1$ and define functions t and s of x and y as follows

$$t = \frac{-\sqrt{6}}{2} \log |u_3| \quad , \quad s = \frac{\log |u_1| - \log |u_2|}{\sqrt{2}}.$$

Then we have

$$\begin{aligned} \log |u_1| &= s/\sqrt{2} + t/\sqrt{6} \\ \log |u_2| &= -s/\sqrt{2} + t/\sqrt{6} \\ \log |u_3| &= -2t/\sqrt{6}. \end{aligned} \tag{7.14}$$

Therefore, it can be easily verified that

$$\vec{u} = (\log |u_1|, \log |u_2|, \log |u_3|) = s\vec{\alpha} + t\vec{\beta},$$

where $\vec{\alpha} = \frac{1}{\sqrt{2}}(1, -1, 0)$ and $\vec{\beta} = \frac{1}{\sqrt{6}}(1, 1, -2)$ are two orthonormal vectors in $\mathbb{R}^3$. Hence, we can write $\vec{u} = (t, s)$ and $\|\vec{u}\| = \sqrt{s^2 + t^2}$, where $\| \ \|$ is the L_2 norm. By (7.14,) we get

$$\left\| (\log |\frac{u_1}{u_2}|, \log |\frac{u_2}{u_3}|, \log |\frac{u_3}{u_1}|) \right\| = \sqrt{3}s\vec{\alpha'} + \sqrt{3}t\vec{\beta'},$$

where

$$\vec{\alpha'} = \frac{1}{\sqrt{3}}(\sqrt{2}, \frac{-1}{\sqrt{2}}, \frac{-1}{\sqrt{2}})$$

and

$$\vec{\beta'} = \frac{1}{\sqrt{3}}(0, \frac{3}{\sqrt{6}}, \frac{-3}{\sqrt{6}}).$$

Since $\vec{\alpha'}$ and $\vec{\beta'}$ are orthonormal vectors in $\mathbb{R}^3$, we get

$$\left\| (\log |\frac{u_1}{u_2}|, \log |\frac{u_2}{u_3}|, \log |\frac{u_3}{u_1}|) \right\| = \sqrt{3}\sqrt{s^2 + t^2} = \sqrt{3}|\vec{u}|_2. \tag{7.15}$$

Remark. Since $\log |u_3| < 0$, the function t is a positive-valued function.

Lemma 7.4.2. *If* $s \geq 0$ *then* $\log|u_1| \geq \log|u_2|$ *and*

$$2\sinh(s/\sqrt{2}) = \exp(-\sqrt{6}t/2),$$

and if $s < 0$ *then* $\log|u_1| < \log|u_2|$ *and*

$$2\sinh(-s/\sqrt{2}) = \exp(-\sqrt{6}t/2).$$

Proof. From (7.5), the definition of u_i, we have $u_1+u_2+u_3 = 0$. Assume that $s > 0$. From (7.14), since s and t are both nonnegative, we get $|u_1| \geq |u_2|$ and $|u_1| \geq |u_3|$. Therefore,

$$e^{s/\sqrt{2}+t/\sqrt{6}} - e^{-s/\sqrt{2}+t/\sqrt{6}} - e^{-2t/\sqrt{6}} = |u_1| - |u_2| - |u_3| = 0,$$

and

$$e^{t/\sqrt{6}}(e^{s/\sqrt{2}} - e^{-s/\sqrt{2}}) = e^{-2t/\sqrt{6}}.$$

Noting that $e^{s/\sqrt{2}} - e^{-s/\sqrt{2}} = 2\sinh(s/\sqrt{2})$, will complete the proof. One can give a similar proof for negative s . □

Let us define

$$g(t) := \sqrt{2}\sinh^{-1}(\frac{\exp(-\sqrt{6}t/2)}{2}).$$

Then $s = \pm g(t)$.

In the following theorem, we summarize the properties of function g, which will be used later.

Theorem 7.4.3. *Let* $g(t) = \sqrt{2}\sinh^{-1}(\frac{\exp(-\sqrt{6}t/2)}{2})$. *We have:*

(i) g *is decreasing .*

(ii) For any $t > 0$,

$$|s| = g(t) < e^{-\sqrt{6}t/2}/\sqrt{2}.$$

(iii) The function $g(t)e^{at}$ *is decreasing when* $a \leq \frac{\sqrt{6}}{\sqrt{5}}$.

Proof. (i) Since

$$\sinh(g/\sqrt{2}) = \exp(-\sqrt{6}t/2)/2,$$

we have the following implicit differentiation:

$$\frac{dg}{dt}\cosh(g/\sqrt{2}) = \frac{-\sqrt{3}}{2}\exp(-\sqrt{6}t/2).$$

Since $\cosh(g/\sqrt{2})$ and $\exp(-\sqrt{6}t/2)/2)$ are both positive,

$$\frac{dg}{dt} < 0$$

(ii) Define the function

$$f(x) = \sqrt{2}\sinh(x/\sqrt{2}) - x.$$

The first derivative test shows that f is an increasing function and for positive x, $f(x) > f(0) = 0$. So

$$\sqrt{2}\sinh(x/\sqrt{2}) > x,$$

when $x > 0$. Put $x = |s|$ to get

$$|s| = g(t) < \sqrt{2}\sinh(|s|/\sqrt{2}).$$

(iii) Set

$$A(t) = g(t)e^{at},$$

then

$$A'(t) = e^{at}(g'(t) + ag(t).$$

For $a \leq 0$, $A' < 0$ since $g' < 0$. For positive a, by part (i) and (ii), we have

$$A'(t) \leq e^{at}e^{-\sqrt{6}t/2}(\frac{-\sqrt{3}}{2\cosh(g/\sqrt{2})} + \frac{a}{\sqrt{2}}).$$

Since g is a decreasing and positive-valued function, $\cosh(g(t)/\sqrt{2})$ is a decreasing function of t. So we have

$$\cosh(g(t)/\sqrt{2}) < \cosh(g(0)/\sqrt{2}).$$

An easy way to evaluate $\cosh(g(0)/\sqrt{2})$ is to recall that $\sinh(g(0)/\sqrt{2}) = \exp(0)/2 = 1/2$. Therefore,

$$\cosh(g(0)/\sqrt{2}) = \sqrt{1 + \frac{1}{4}} = \sqrt{5}/2.$$

We conclude that A' is negative if

$$-\sqrt{3}/\sqrt{5} + a/\sqrt{2} \leq 0.$$

This means

$$a \leq \frac{\sqrt{6}}{\sqrt{5}}.$$

□

Lemma 7.4.4. *Let (x, y) and (x', y') be two distinct solutions to equation (7.1), related to (η, ξ). Put $p = p(x, y)$, $p' = p(x', y')$, $q = q(x, y)$, $q' = q(x', y')$. We have*

$$|pq' - p'q| \geq \sqrt{3D}.$$

Proof. By definition

$$\begin{aligned} |pq' - p'q| &= |\frac{\eta + \xi}{\sqrt{2}} \frac{\sqrt{-1}(\eta' - \xi')}{\sqrt{2}} - \frac{\eta' + \xi'}{\sqrt{2}} \frac{\sqrt{-1}(\eta - \xi)}{\sqrt{2}}| \\ &= |\eta\xi' - \eta'\xi|. \end{aligned}$$

Since $\xi(x, y)\eta(x, y) = H(x, y)$ is a quadratic form of discriminant $-3D$, it follows that

$$\eta\xi' - \eta'\xi = \pm\sqrt{-3D}(xy' - x'y).$$

Since (x, y) and (x', y') are distinct solutions to $F(x, y)$, $xy' - x'y$ is a nonzero integer. □

Lemma 7.4.5. *Let (x, y) and (x', y') be two distinct solutions to equation (7.1), related to (ξ, η). Assume that $t(x', y') \geq t(x, y)$. Then we have*

$$t(x', y') \geq 2t(x, y) + \frac{\sqrt{6}}{6} \log D - \sqrt{6} \log(2 + \frac{1}{\sqrt{2}}).$$

Proof. Put

$$\begin{aligned} p = p(x, y)\, p' &= p(x', y'), \\ q = q(x, y)\, q' &= q(x', y'), \\ s = s(x, y)\, s' &= s(x', y'), \\ t = t(x, y)\, t' &= t(x', y') \end{aligned}$$

and

$$u_i = u_i(x, y), u_i' = u_i(x', y').$$

First we show that

$$|p| \leq \sqrt{2} D^{1/6} e^{t/\sqrt{6}} \cosh(s/\sqrt{2}).$$

By the triangle inequality we have:

$$
\begin{aligned}
& |p| = \frac{1}{\sqrt{2}}|\sqrt{2}p| \leq \\
& \frac{1}{\sqrt{2}}(|(p/\sqrt{2})+(q/\sqrt{6})|)+|(q/\sqrt{6})-(p/\sqrt{2})|) = \\
& \frac{1}{\sqrt{2}}\frac{|(q/\sqrt{6})+(p/\sqrt{2})|^{1/2}}{|(q/\sqrt{6})-(p/\sqrt{2})|^{1/2}}(|(q/\sqrt{6})+(p/\sqrt{2})|^{1/2}|(q/\sqrt{6})-(p/\sqrt{2})|^{1/2}) \\
+ \quad & \frac{1}{\sqrt{2}}\frac{|(q/\sqrt{6})-(p/\sqrt{2})|^{1/2}}{|(q/\sqrt{6})+(p/\sqrt{2})|^{1/2}}(|(q/\sqrt{6})+(p/\sqrt{2})|^{1/2}|(q/\sqrt{6})-(p/\sqrt{2})|^{1/2}).
\end{aligned}
$$

By (7.14) and (7.5), we have

$$|(q/\sqrt{6})+(p/\sqrt{2})|^{1/2}|(q/\sqrt{6})-(p/\sqrt{2})|^{1/2} = D^{1/6}u_1^{1/2}u_2^{1/2} = D^{1/6}\exp(t/\sqrt{6}).$$

Equations (7.14) and (7.5) also give us the following identities:

$$
\begin{aligned}
& (\frac{|(q/\sqrt{6})+(p/\sqrt{2})|^{1/2}}{|(q/\sqrt{6})-(p/\sqrt{2})|^{1/2}} + \frac{|(q/\sqrt{6})-(p/\sqrt{2})|^{1/2}}{|(q/\sqrt{6})+(p/\sqrt{2})|^{1/2}}) \\
= \quad & e^{\frac{(\log|u_1|-\log|u_2|)}{2}} + e^{-\frac{(\log|u_1|-\log|u_2|)}{2}} \\
= \quad & 2\cosh(\frac{s}{\sqrt{2}})
\end{aligned}
$$

and

$$|q| = (\sqrt{6}/2)D^{1/6}e^{-2t/\sqrt{6}}.$$

Using Lemma 7.4.4, we get

$$D^{1/6} \leq e^{(t'-2t)/\sqrt{6}}\cosh(|s'|/\sqrt{2}) + e^{(t-2t')/\sqrt{6}}\cosh(|s|/\sqrt{2}).$$

One can express the above equation in terms of sinh instead of cosh by substituting $\cosh(|s|/\sqrt{2})$ with

$$\sinh\left(\frac{|s|}{\sqrt{2}}\right) + e^{-|s|/\sqrt{2}}.$$

Now we use the assumption that $t' \geq t$ and the fact that $e^{-|s|/\sqrt{2}} \leq 1$. By Lemma 7.4.2, we get

$$D^{1/6} \leq e^{(t'-2t)/\sqrt{6}}(1+e^{-3(t'-t)/\sqrt{6}})(1+\frac{e^{-\sqrt{6}t/2}}{2}) \ .$$

Note that by Theorem (7.4.3), $t \geq \log(2)/\sqrt{6}$, whereby taking the logarithm of both sides of the above equality yields

$$t' - 2t \geq \frac{\sqrt{6}}{6} \log(D) - \sqrt{6} \log((1 + e^{-3(t'-t)/\sqrt{6}})(1 + \frac{1}{2\sqrt{2}}))$$

So we have

$$t' - 2t \geq \frac{\sqrt{6}}{6} \log(D) - \sqrt{6} \log(2 + \frac{1}{\sqrt{2}}).$$

□

Lemma 7.4.6. *Suppose that (7.1) has three distinct solutions related to* (ξ, η)*. Then three distinct corresponding points* (t, s) , (t', s') *and* (t'', s'') *form a triangle.*

Proof. Suppose (t, s) , (t', s') and (t'', s'') are collinear and $t \leq t' \leq t''$. Then

$$\frac{s' - s}{t' - t} = \frac{s'' - s'}{t'' - t'}.$$

Assume, without loss of generality, $s' > 0$. Since $g(t) = |s|$ is a decreasing function of t, we have

$$s'' - s' < 0$$

and consequently, $s' - s < 0$. Therefore,

$$s > 0.$$

Since we assumed (t, s) , (t', s') and (t'', s'') to be collinear,

$$\frac{s'' - s}{t'' - t} = \frac{s' - s}{t' - t}$$

By Lemma 7.4.5, and since $|s| \geq |s'| \geq |s''| > 0$, we get

$$\frac{s' - s}{t' - t} < \frac{-s'}{t} < \frac{-2s'}{t'} < \frac{s'' - s'}{t'' - t'} < 0.$$

This contradiction shows that (t, s) , (t', s') and (t'', s'') are not collinear (note that any vertical or horizontal line intersects the graph of g and g' at most in two points). □

Suppose that (7.1) has three distinct solutions related to (ξ, η) and A is the area of the triangle formed by three distinct corresponding points (t, s), (t', s') and (t'', s''). Then vectors $(t - t', s - s')$ and $(t - t'', s - s'')$ generate a sub-lattice of Λ_1 with the volume of fundamental parallelepiped equal to $2A$. Therefore,

$$2A \geq \mathrm{Vol}(\Lambda_1).$$

Now let us estimate $2A$, the area of rectangle which has (t, s) , (t', s') and (t'', s'') as three of its edges. Recall that $s(x, y) = \pm g(t(x, y))$ and g is a decreasing function. Suppose that $t \leq t' \leq t''$. Then $g(t'') \leq g(t') \leq g(t)$ and we have

$$2A \leq (t'' - t)(g(t) + g(t')) = (t'' - t)(|s| + |s'|).$$

Part (iii) of Theorem 7.4.3 shows that

$$|s'| < |s|e^{\frac{-\sqrt{6}(t'-t)}{\sqrt{5}}},$$

Therefore,

$$\mathrm{Vol}(\Lambda) = \mathrm{Vol}(\Lambda_1) \leq (t'' - t)|s|(1 + e^{\frac{-\sqrt{6}(t'-t)}{\sqrt{5}}}).$$

Using Theorem 7.4.3 again, we get the following gap principle of this paper which is essentially Theorem 5.5 of [15]:

Theorem 7.4.7. *Suppose that $F(x, y)$ has three distinct solutions (x, y), (x', y') and (x'', y''), all related to (ξ, η). Assume that $t = t(x, y) \leq t' = t(x', y') \leq t'' = t(x'', y'')$, where t is the function defined in the begining of this section. We have*

$$t'' \geq \frac{\sqrt{2}\, Vol(\Lambda) exp(\sqrt{6}t/2)}{1 + \exp(-\sqrt{6}(t' - t)/\sqrt{5})},$$

where $Vol(\Lambda)$ is the volume of fundamental parallelepiped of lattice Λ.

7.5 Linear Forms In Logarithms

We have seen that $\sqrt{2}s = \log |u_1| - \log |u_2| = \log \lambda_1 + m \log \lambda_2 + n \log \lambda_3$. Where s is a function of (x, y) defined in Section 3 and u_i are also functions of (x, y) defined in Section 7.2. By Lemma 7.4.3, we have

$$\log(\sqrt{2}|s|) \leq -(\sqrt{6}/2)t.$$

Here, we will use a well-known lower bound for linear forms in logarithms of algebraic numbers, to find an upper bound for $\log(\sqrt{2}|s|)$.

Theorem 7.5.1 (Matveev)**.** *Suppose that* $\mathbb{K}$ *is a real algebraic number field of degree* d*. We are given numbers* $\alpha_1, \dots \alpha_n \in \mathbb{K}^*$ *with absolute logarithmic heights* $h(\alpha_j)$*.*
Let $\log \alpha_1, \dots, \log \alpha_n$ *be arbitrary fixed non-zero values of the logarithms. Suppose that*

$$A_j \geq \max\{dh(\alpha_j), |\log \alpha_j|\}, \quad 1 \leq j \leq n.$$

Now consider the linear form

$$L = b_1 \log \alpha_1 + \dots + b_n \log \alpha_n,$$

with $b_1, \dots, b_n \in \mathbb{Z}$ *and with the parameter* $B = max\{1, max\{b_j A_j / A_n : 1 \leq j \leq n\}\}$ *. Put*

$$\Omega = A_1 \dots A_n,$$

$$C(n) = \frac{16}{n!} e^n (2n+2)(n+2)(4n+4)^{n+1} (\frac{1}{2} en),$$

$$C_0 = \log(e^{4.4n+7} n^{5.5} d^2 \log(en)),$$

$$W_0 = \log(1.5 eBd \log(ed)).$$

If $b_n \neq 0$*, then*

$$\log |L| > -C(n) C_0 W_0 d^2 \Omega.$$

Proof. See mat26 for the proof. □

Here, we recall the definition of absolute logarithmic height from [9, 10]. Let $\mathbb{Q}(\rho)^\sigma$ be the embeddings of the real number field $\mathbb{Q}(\rho)$ in $\mathbb{R}$, $1 \leq \sigma \leq 3$, where ρ is a root of $F(x,1) = 0$. We respectively have 3 Archimedean valuations of $\mathbb{Q}(\rho)$:

$$|\alpha|_\sigma = |\alpha^{(\sigma)}|, \quad 1 \leq \sigma \leq 3.$$

We enumerate prime ideals of $\mathbb{Q}(\rho)$ by indices $\sigma > 3$ and define non-Archimedean valuation of $\mathbb{Q}(\rho)$ by the formulas

$$|\alpha|_\sigma = (\text{Norm } \mathfrak{p})^{-k},$$

where

$$k = \text{ord}_{\mathfrak{p}}(\alpha), \ \mathfrak{p} = \mathfrak{p}_\sigma, \ \sigma > d,$$

for any $\alpha \in \mathbb{Q}(\rho)^*$. Then we have the *product formula* :

$$\prod_{1}^{\infty} |\alpha|_\sigma = 1, \ \alpha \in \mathbb{Q}(\rho)^*.$$

Note that $|\alpha|_\sigma \neq 1$ for only finitely many α . We define the *absolute logarithmic height* of α as

$$h(\alpha) = \frac{1}{6} \sum_{\sigma=1}^{\infty} |\log |\alpha|_\sigma|.$$

We will apply Matveev's lower bound to

$$\log |u_1| - \log |u_2| = \log \lambda_1 + m_1 \log \lambda_2 + n_1 \log \lambda_3.$$

Suppose that

$$\|\vec{u}(x_0, y_0)\| = \min_{(x,y)\in S} \|\vec{u}(x, y)\|$$

and

$$\log |u_1(x_0, y_0)| - \log |u_2(x_0, y_0)| = \log \left| \frac{\rho - \rho''}{\rho' - \rho} \right| + a \log \lambda_1 + b \log \lambda_2$$

then for any solution (x, y), we can write

$$\log |u_1(x, y)| - \log |u_2(x, y)| = \log \lambda + m \log \lambda_1 + n \log \lambda_2,$$

where $m = m_1 - a$, $n = n_1 - a$ and

$$\lambda = \left| \frac{\rho - \rho''}{\rho' - \rho} \right| \lambda_1^a \lambda_2^b.$$

Since λ_2 and λ_3 are the fundamental units of the ring of integers of $\mathbb{Q}(\rho)$, λ_1, λ_2 and λ_3 are multiplicatively dependent if and only if λ_1 is a unit. If λ_1 is a unit then we can write $\log |u_1| - \log |u_2|$ as a linear form in two logarithms. Since Theorem 7.5.1 gives a better lower bound for linear forms in two logarithms, we can assume that λ_1, λ_2 and λ_3 are multiplicatively independent and $\log |u_1| - \log |u_2|$ is a linear form in three logarithms.

First, suppose that λ is a unit in the number field. We have

$$h(\lambda) = \frac{1}{6}(|\log(|\lambda|)| + |\log(|\lambda'|)| + |\log(|\lambda''|)|) = \frac{1}{6} |\tau(\lambda)|_1 ,$$

where λ' and λ'' are the conjugates of λ , τ is the embedding of units to the lattice Λ and $|\ |_1$ is the L_1 norm on $\mathbb{R}^3$. So we have

$$h(\lambda) = \frac{1}{6} |\tau(\lambda)|_1 \leq \frac{\sqrt{3}}{6} \|\tau(\lambda)\| ,$$

where $\| \;\|$ is the L_2 norm on $\mathbb{R}^3$. So when λ is a unit

$$\max\{3h(\lambda), |\log(|\lambda|)|\} \leq \|\tau(\lambda)\|, \tag{7.16}$$

since $|\log(\lambda)| \leq \sqrt{\log^2(|\lambda|) + \log^2(|\lambda'|) + \log^2(|\lambda''|)} = |\tau(\lambda)|_2$.

In the identity

$$\log|u_1| - \log|u_2| = \log\lambda + m_1\log\lambda_2 + n_1\log\lambda_3,$$

λ_2 and λ_3 are fundamental units of $\mathbb{Q}(\rho)$. Therefore, in Theorem 7.5.1, A_i can be taken equal to $|\tau(\lambda_i)|_2$, for $i = 2, 3$.

Bases $\vec{b_1}$ and $\vec{b_2}$ of lattice Λ are called reduced if the following conditions are satisfied :

(i) $|\vec{b_1}|_2 \leq |\vec{v}|_2$ for every vector $\vec{v} \in \Lambda - \{\vec{0}\}$;

(ii) $|\vec{b_2}|_2 \leq |\vec{v}|_2$ for every vector $\vec{v} \in \Lambda - \mathbb{Z}\vec{b_1}$.

Remark. Although the definitions of reduced basis for lattices and reduced forms are somehow related, one should note that we define them separately and they are not to be confused.

It is a fact that we can always choose a reduced basis for a two dimensional lattice. So we choose the fundamental units λ_2 and λ_3 such that the basis $\tau(\lambda_2)$ and $\tau(\lambda_3)$ are reduced basis for Λ. When $\vec{b_1}$ and $\vec{b_2}$ are the reduced basis of Λ, since $\vec{b_1}, \vec{b_2} \leq \vec{b_1} \pm \vec{b_2}$, we conclude that the angle between vectors $\vec{b_1}$ and $\vec{b_2}$ must be between $\pi/3$ and $2\pi/3$. Therefore, λ_2 and λ_3 can be chosen so that

$$|\tau(\lambda_2)|_2|\tau(\lambda_3)|_2| \leq \frac{2}{\sqrt{3}}\mathrm{Vol}(\Lambda).$$

Hence, in our case,

$$A_2A_3 \leq \frac{2}{\sqrt{3}}\mathrm{Vol}(\Lambda).$$

By (7.15), we have

$$\left\|(\log\frac{|u_1|}{|u_2|}, \log\frac{|u_2|}{|u_3|}, \log\frac{|u_3|}{|u_1|})\right\| = \sqrt{3}\|\vec{u}\|.$$

The well-known inequality $\frac{a+b+c}{3} \leq [\frac{a^2+b^2+c^2}{3}]^{1/2}$ shows that

$$|\vec{v}|_1 \leq \sqrt{3}\|\vec{v}\| \tag{7.17}$$

for every vector $\vec{v} \in \mathbb{R}^3$. Therefore,

$$\begin{aligned} & \left|\log|(\rho-\rho'')(x-\rho' y)|\right| + \left|\log|(\rho'-\rho)(x-\rho'' y)|\right| + \left|\log|(\rho'-\rho'')(x-\rho y)|\right| \\ \leq & \quad 3\left\|\vec{u}(x_0,y_0)\right\|. \end{aligned}$$

Now, we note that

$$\begin{aligned} & \sum_{\sigma>3}\left|\log\left|\frac{(\rho-\rho'')(x-\rho' y)}{(\rho'-\rho)(x-\rho'' y)}\right|\right|_{\sigma} \\ \leq & \sum_{\sigma>3}\left|\log|(\rho-\rho'')(x-\rho' y)|\right|_{\sigma} + \sum_{\sigma>3}\left|\log|(\rho'-\rho)(x-\rho'' y)|\right|_{\sigma}. \end{aligned}$$

We know that the Archimedean valuations of $\lambda := (\rho-\rho'')(x-\rho' y)$ are λ , $(\rho'-\rho'')(x-\rho y)$ and $(\rho'-\rho)(x-\rho' y)$. So by the product formula, since (x, y) is a solution to (7.1), the product of all non-Archimedean valuations of λ equals

$$D^{-1/2}.$$

Therefore,

$$\left|\sum_{\sigma>3}\log\left|(\rho-\rho'')(x-\rho' y)\right|_{\sigma}\right| = \frac{1}{2}\log D,$$

and similarly

$$\left|\sum_{\sigma>3}\log\left|(\rho'-\rho)(x-\rho'' y)\right|_{\sigma}\right| = \frac{1}{2}\log D.$$

Since $(\rho'-\rho)(x-\rho'' y)$ and $(\rho-\rho'')(x-\rho' y)$ are algebraic integers, we get

$$h(\lambda_1) \leq \frac{1}{6}\left(3\|\vec{u}(x_0,y_0)\| + \log D\right). \tag{7.18}$$

This gives an estimate for A_1.
Let $B_1 = BA_3$, where B is as in theorem 7.5.1. Then

$$B_1 = \max\{b_j A_j, \ : 1 \leq j \leq 3\}.$$

Since

$$\log\left|\frac{u_1}{u_2}\right| = \log\left|\frac{(\rho-\rho'')(x-\rho' y)}{(\rho'-\rho)(x-\rho'' y)}\right| + m\lambda_1 + n\lambda_2,$$

we can write

$$\begin{aligned} & \left(\log\left|\frac{u_1}{u_2}\right|, \log\left|\frac{u_2}{u_3}\right|, \log\left|\frac{u_3}{u_1}\right|\right) = \\ & \left(\log\frac{|(\rho-\rho'')(x-\rho' y)|}{|(\rho'-\rho)(x-\rho'' y)|}, \log\frac{|(\rho'-\rho)(x-\rho'' y)|}{|(\rho'-\rho'')(x-\rho y)|}, \log\frac{|(\rho'-\rho'')(x-\rho y)|}{|(\rho-\rho'')(x-\rho' y)|}\right) \\ + & \quad m\vec{\lambda_1} + n\vec{\lambda_2}, \end{aligned}$$

where $\vec{\lambda_i} = \tau(\lambda_i)$, for $i = 2, 3$. Since λ_2 and λ_3 have been chosen so that $\vec{\lambda_2}$ and $\vec{\lambda_3}$ form a reduced basis for the lattice Λ, we get

$$m|\vec{\lambda_2}|_1\,, n|\vec{\lambda_3}|_1 \leq \left|(\log\frac{|(\rho-\rho'')(x-\rho' y)|}{|(\rho'-\rho)(x-\rho'' y)|}, \log\frac{|(\rho'-\rho)(x-\rho'' y)|}{|(\rho'-\rho'')(x-\rho y)|}, \log\frac{|(\rho'-\rho'')(x-\rho y)|}{|(\rho-\rho'')(x-\rho y)|})\right|_1 + \left|\left(\log\left|\frac{u_1}{u_2}\right|, \log\left|\frac{u_2}{u_3}\right|, \log\left|\frac{u_3}{u_1}\right|\right)\right|_1 .$$

Therefore, by (7.15) and (7.17)

$$m|\vec{\lambda_2}|_1, n|\vec{\lambda_3}|_1 \leq 3(|\vec{u}|_2 + |\vec{u}(x_0, y_0)|_2). \tag{7.19}$$

Theorem 7.5.2. *Let F be a cubic binary equation with positive discriminant. For all pairs of solution (a, b) to the equation (7.1), except possibly one of them, we have*

$$D \leq 64 e^{2\sqrt{6}t},$$

where D is the discriminant of $F(x, y)$ and $t = t(a, b)$, for the function t defined in Section 7.3. Moreover, when $t \geq 5$

$$D \leq \frac{1}{2} e^{2\sqrt{6}t}.$$

Proof. By (7.3)

$$|H| = |\xi\eta| = |\frac{p+iq}{\sqrt{2}}.\frac{p-iq}{\sqrt{2}}| = \frac{p^2+q^2}{2}.$$

By (7.5),

$$q = \frac{\sqrt{6}}{2} D^{1/6} u_3$$

and

$$|p| = |\frac{\sqrt{2}}{2}(u_1 - u_2)|D^{1/6} \leq \frac{\sqrt{2}}{2} D^{1/6}(|u_1| + |u_2|).$$

Therefore, by (7.14)

$$|H| \leq \frac{1}{2} D^{1/3}(e^{2t/\sqrt{6}}(e^{2s/\sqrt{2}} + e^{-2s/\sqrt{2}} + 2)/2 + \frac{3}{2} e^{-4t/6}). \tag{7.20}$$

Therefore, by Lemma 7.2.1, for all solutions (a, b) to (7.1), except at most one of them

$$\frac{1}{2} D^{1/2}\sqrt{3} \leq \frac{1}{2} D^{1/3}(e^{2t/\sqrt{6}}(e^{2s/\sqrt{2}} + e^{-2s/\sqrt{2}} + 2)/2 + \frac{3}{2} e^{-4t/6}). \tag{7.21}$$

Since $t > 0$, part (ii) of Lemma 7.1 says that $|s| < e^{-\sqrt{6}t/2}/\sqrt{2}$. Hence,

$$D^{1/6} \leq 2e^{2t/\sqrt{6}},$$

which proves the theorem for general t. When $t \geq 5$, we note that $\frac{3}{2}e^{-4t/6} < 0.054$ and $|s| < 0.0016$ by Theorem 7.4.3 . □

Since $\vec{u} = (t, s)$ and $\|\vec{u}\| = \sqrt{t^2 + s^2}$, from Theorem 7.4.3, we deduce that $|\vec{u}|_2$ is an increasing function of t. So we can assume that Theorem 7.5.2 is satisfied for all solutions, except possibly (x_0, y_0), where

$$\|\vec{u}(x_0, y_0)\| = \min_{(x,y)\in S} \|\vec{u}(x, y)\|,$$

S is the set of all solutions to (7.1) and $\vec{u} = (\log|u_1|, \log|u_2|, \log|u_3|)$. Suppose that three distinct solutions (x, y), (x', y') and (x'', y'') of (7.1) are related to (ξ, η) and $t'' = t(x'', y'') > t' = t(x', y') > t = t(x, y)$. First, we recall that $\vec{u} = (t, s)$ and $|\vec{u}|_2 = \sqrt{t^2 + s^2}$. By Theorem 7.4.3, if we take $t \geq 5$ (Theorem 7.5.2 enables us to assume that t is large), we get

$$|\vec{u}|_2 = \sqrt{t^2 + e^{-\sqrt{6}t}/2} \leq 1.0016t.$$

Therefore, by (7.18) and theorem 7.5.2, we can take

$$A_1 = 1.0016(\frac{3}{2}t + \sqrt{6}t).$$

Inequality (7.19) suggests the value $3(1.0016)(t'' + t)$ for B_1. But by theorem 7.4.5, for large discriminant D, $t'' > 4t$. So we take

$$B_1 = 3(1.0016)(t'' + t''/4). \tag{7.22}$$

So Matveev 's lower bound gives us:

$$\log|L| > -1.5036 \times 10^{11} A_1 A_2 A_3 \log(25.6708(3.0048)(1.25)t''/A_3),$$

where $L = \log|u_1| - \log|u_2|$. On the other hand, by Theorem 7.4.3, we have

$$\log|L| = \log\sqrt{2}|s''| \leq -\sqrt{6}t''/2.$$

We conclude that

$$t'' \leq 1.2276 \times 10^{11} A_1 A_2 A_3 \log(96.2751t''/A_3),$$

or

$$\frac{96.2751t''/A_3}{\log(96.2751t''/A_3)} \leq 1.1892 \times 10^{13} A_1 A_2.$$

Therefore,

$$\log(96.2751t''/A_3) \leq \frac{e}{e-1} \log(1.1892 \times 10^{13} A_1 A_2).$$

Recalling that $A_2 A_3 \leq 2/\sqrt{3}\mathrm{Vol}(\Lambda)$, we obtain the following upper bound for t'':

$$t'' \leq \frac{e}{e-1} 1.2276 \times 10^{11} (\frac{2}{\sqrt{3}}) \mathrm{Vol}(\Lambda) A_1 \log(1.1892 \times 10^{13} A_1 A_2). \quad (7.23)$$

7.6 Proof Of The Main Results

Let

$$\|\vec{u}(x_0, y_0)\| = min_{(x,y)\in S} \|\vec{u}(x, y)\|.$$

Suppose that (x, y), (x', y') and (x'', y''), with none of them equal to (x_0, y_0), are three distinct solutions to (7.1), and related to a fixed choice of resolvent form. Let $t = t(x, y) < t' = t(x', y') < t'' = t(x'', y'')$. By (7.23) and Theorem 7.4.7, we get

$$\begin{aligned} &\frac{e}{e-1} 1.2276 \times 10^{11} A_1 (\frac{2}{\sqrt{3}}) \mathrm{Vol}(\Lambda) \log(1.1892 \times 10^{13} A_1 A_2) \\ &\geq \frac{\sqrt{2}\mathrm{Vol}(\Lambda) exp(\sqrt{6}t/2)}{1 + \exp(-\sqrt{6}(t'-t)/\sqrt{5})}, \end{aligned} \quad (7.24)$$

where $A_1 = (3/2 + \sqrt{6})(1.006)t$ and $A_2 = |\tau(\lambda_2)|_2$. Without loss of generality, we can assume that $|\tau(\lambda_2)|_2 \leq |\tau(\lambda_3)|_2$. Therefore,

$$\frac{\sqrt{3}}{2} |\tau(\lambda_2)|_2^2 \leq \frac{\sqrt{3}}{2} |\tau(\lambda_2)|_2 |\tau(\lambda_3)|_2 \leq \mathrm{Vol}(\Lambda).$$

We have

$$\log|u_1(x, y)| - \log|u_2(x, y)| = \log\lambda_1 + m' \log\lambda_2 + n' \log\lambda_3,$$

where m' and n' are integers. Since $(x, y) \neq (x_0, y_0)$, at least one of m' or n' is a nonzero integer. So by (7.19) we have $|\tau(\lambda_2)|_2 \leq 6.01t$. Using Theorem 7.4.5, we get

$$\frac{e}{1-e}4.8484\times 10^{11}(\frac{2}{\sqrt{3}})\mathrm{Vol}(\Lambda)t\log(2.8184\times 10^{14}t^2)$$
$$\geq \frac{\sqrt{2}\mathrm{Vol}(\Lambda)exp(\sqrt{6}t/2)}{1+\exp(-\sqrt{6}t/\sqrt{5})}.$$

Therefore, $t < 27.91$ and by equation (7.21), $D < 5.31\times 10^{59}$; i.e. we have proven that there are at most 2 pairs of solutions $(x, y) \neq (1, 0)$ and $(x', y') \neq (1, 0)$ related to a resolvent form (ξ, η) , when $D \geq 5.31\times 10^{59}$. If we suppose that $D < 5.31\times 10^{59}$, by (7.18), we can take

$$A_1 = \frac{3}{2}t + \frac{1}{2}\log(5.31\times 10^{59}).$$

By substituting this new value of A_1 in (7.23), we get

$$t \leq 27.5321,$$

and therefore, $D < 1.4\times 10^{57}$. Since we have three pairs of resolvent forms, Theorem (7.1.1) is proven.
As we mentioned in the remark after the proof of Lemma 7.2.1, the solution $(1, 0)$ needs to be treated separately, only if F is equivalent to a monic reduced form. Otherwise, $(x_0, y_0) \neq (1, 0)$ and Lemma 7.2.1 and therefore Lemma 7.5.2 will hold for all solutions without any exception.
By the analytic class number formula and Louboutin's upper bound (which can be found in [3]) :

$$\mathrm{Vol}(\Lambda) \leq \frac{\sqrt{3}}{8}\sqrt{D}\log^2 D,$$

we have that

$$A_2 \leq \frac{1}{4}D^{1/4}\log D.$$

By Theorem 7.5.2,

$$A_2 \leq \frac{1}{4}e^{\sqrt{6}t/2}(\log\frac{1}{2} + 2\sqrt{6}t).$$

Now, having appropriate values of A_1 and A_2 in hand, we solve inequality (7.24) to get $t \leq 28.38$ and consequently by (7.21), $D \leq 9\times 10^{58}$; i.e. we have proven that there are at most 2 pairs of solutions (x, y) and (x', y') related to a resolvent form (ξ, η) , when $D > 9\times 10^{58}$. Therefore, we get Theorem 7.1.2.

In [2], it is proven that if $D \geq 2400$, related to a fixed pair of resolvent form, there are at most 3 different pairs of solutions (x, y) to (7.1) with $H(x, y) \geq \frac{1}{2}\sqrt{3D}$, where H is the Hessian of F. This together with lemma 7.2.1 leads to the main theorem of [2], that is, the equation $F(x, y) = 1$ has at most 10 solutions in integer x and y .
For $0 < D < 2400$, equation $F(x, y) = 1$ is completely solved for representatives of every equivalent class of binary cubic forms. This computations show that the equation (7.1) with discriminant $0 < D < 10^6$ has at most 9 solutions in integers x and y. The complete result of these computations are tabulated in section 9 of [2].

Bibliography

[1] B.N. Delone and D.K. Fadeev. The Theory of Irrationalities of the Third Degree. Translation of math. Monographs, AMS 10 (1964).

[2] M.A. Bennett. On the representation of unity By binary Cubic Forms. Trans. Amer. Math. Soc. 353 (2001), 1507-1534.

[3] J.H.E. Cohn. The Diophantine equation $x^2 + C = y^n$, II, Acta Arith. 109.2 (2003), 205-206.

[4] V.I. Baulin. On an intermediate equation of the third degree with least positive discriminant (Russian). Tul'sk Gos.Ped.Inst. Ucen. Zap. Fiz. Math. Nauk. Vip. 7 (1960), 138-170.

[5] J.H. Evertse. On the representation of integers by binary cubic forms of positive discriminant. Invent. Math.73(1983), 117-138.

[6] I. Gall and N. Schulte. Computing all power integral of cubic fields. Math. Comp. 53 (1989), 689-696.

[7] E. Lee. Studies on Diophantine Equations. PhD thesis, Cambridge University, 1992.

[8] F. Lippok. On the representation of 1 by binary cubic forms of positive discriminant. J. Symbolic Computation 15 (1993), 297-313.

[9] E.M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, Izv. Ross. Akad. Nauk Ser. Mat. 62 (1998), 81-136, translation in Izv. Math. 62 (1998), 723-772.

[10] E.M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, Izv. Ross. Akad. Nauk Ser. Mat. 64 (2000), 125-180, translation in Izv. Math. 64 (2000), 1217-1269.

[11] M. Mignotte. Verification of a conjecture of E. Thomas . J. Number Theory 44 (1993), 172-177.

[12] M. Mignotte. Petho's cubics. Dedicated to Professor Kalman Győry on the occasion of his 60th birthday. Publ. Math. Debrecen 56 (2000), 481-505.

[13] M. Mignotte and N. Tzanakis. On a family of cubics. J. Number Theory 39(1991), 41-49.

[14] W. Ljunggren. Einige Bemerkungen uber die Darstellung ganzer zahlen durch bibare kubische formen mit positiver Diskriminante. Acta Math. 75(1942), 1-21.

[15] R. Okazaki. Geometry of a cubic Thue equation, Publ. Math. Debrecen. 61 (2002),267-314.

[16] C.L. Siegel. Uber einige Anwendungen diophanticher Approximationen. Abh.Preuss.Akad.Wiss. (1929), Nr.1.

[17] E. Thomas, Complete solutions to a family of cubic Diophantine equations, J. Number Theory 34 (1990), 235-250.

Chapter 8

Conclusion

In Chapter 2, we develop general machinery based on the Thue-Siegel Method to find an upper bound upon the number of integral solutions to a family of quartic Thue inequalities. This specific family turned out to be a very important one. In Chapters 3, 4 and 5, upper bounds are given upon the number of positive integral solutions to Diophantine equations

$$aX^4 - bY^2 = 1$$

and

$$aX^4 - bY^2 = 2$$

by reducing them to quartic Thue inequalities belonging to the family of inequalities studied in Chapter 2. We believe that there are other interesting questions we could answer using the method of Chapter 2. Particularly, we are hoping to use our method to obtain a good upper bound for the number of integer points on the curve

$$x^2 - dy^4 = k.$$

Let a and b be positive integers. In chapter 3, we show that the equation

$$aX^4 - bY^2 = 1$$

has at most two solutions in positive integers (X, Y). This result is sharp, for let m be a positive integer, then the positive integral solutions to the equation

$$(m^2 + m + 1)X^4 - (m^2 + m)Y^2 = 1$$

are given by $(X, Y) = (1, 1)$ and $(X, Y) = (2m + 1, 4m^2 + 4m + 3)$. In fact, these are the only examples known to have as many as two positive solutions. This suggest a stronger version of Theorem 3.1.1.

In Chapters 6 and 7, we study two different methods, one from Diophantine analysis and the other one from the geometry of numbers.

There is another method invented by Silverman for computing the number of solutions of Thue equations. He relates the number of these solutions to the rank of Mordell-Weil group on the Jacobian of a related genus 1 curve. Because of its different nature, Silverman's method might be applied to strengthen our results when combined with our approximations.

Bibliography

[1] S. Akhtari, The method of Thue-Siegel for binary quartic forms. submitted (2007).

[2] M.A. Bennett. On the representation of unity by binary cubic forms. Trans. Amer. Math. Soc. 353 (2001), 1507-1534.

[3] E. Bombieri and W.M. Schmidt. On Thue's equation. Invent. Math. 88 (1987), 69-81.

[4] G.V. Chudnovsky. On the method of Thue-Siegel. Ann. of Math. II Ser. 117 (1983), 325-382.

[5] W. Ljunggren. On the representation of integers by certain binary cubic and biquadratic forms. Acta. Arith. XVII (1971).

[6] L.J. Mordell. On the rational solutions of indeterminate equations of the 3rd and 4th degrees. Proc. Camb. Phil. Soc.21 (1922), 179-192.

[7] W.M. Schmidt, Diophantine Approximations and Diophantine Equations, Lecture Notes in Mathematics, Springer Verlag (2000).

[8] A. Thue. Über Annäherungenswerte algebraischen Zahlen. J. reine angew. Math. 135 (1909), 284-305.