Cubic Thue equations

By SHABNAM AKHTARI (Bonn)

Abstract. We revisit a work by R. Okazaki and prove that for every cubic binary form $F(x, y)$ with large enough discriminant, the Thue equation $|F(x, y)| = 1$ has at most 7 solutions in integers x and y.

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

$$|F(x, y)| = 1 \tag{1}$$

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 (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 (1) 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, respectively. In the first case there are 6 solutions and in the second case there are 9 solutions to (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 (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 if discriminant of F is greater than 5.65×10^{65} then equation (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 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.

Theorem 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.*

Despite the numerical improvement, the bounds remain out of reach of computers. The main purpose of this paper, is to look at some beautiful geometric ideas of OKAZAKI [15] from Classical Analysis point of view.

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 $n = 1$ ([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 (1) has more than 5 solutions, have discriminant less than 362.

The following conjecture is essentially due to Nagell and refined by Pethő and Lippok.

Conjecture. If F is a binary cubic form with positive discriminant D_F, then the number of solutions of equation (1) is less than 6, if $D_F > 361$.

2. The covariants of binary cubic forms

Suppose
$$F = ax^3 + bx^2 y + cxy^2 + dy^3$$
with discriminant
$$D_F = 18abcd + b^2 c^2 - 27a^2 d^2 - 4ac^3 - 4b^3 d = a^4 \prod_{i,j} (\alpha_i - \alpha_j)^2$$

where α_1, α_2 and α_3 are the roots of polynomial $F(x,1)$. Let us define, for the form F, an associated quadratic form, the Hessian $H = H_F$, and a cubic form $G = G_F$, by

$$H(x,y) = -\frac{1}{4}\left(\frac{\delta^2 F}{\delta x^2} \frac{\delta^2 F}{\delta y^2} - \left(\frac{\delta^2 F}{\delta x \delta y} \right)^2 \right) = Ax^2 + Bxy + Cy^2$$

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.

$$H_{F \circ \gamma} = H_F \circ \gamma \quad \text{and} \quad G_{F \circ \gamma} = G_F \circ \gamma$$

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

$$F_1(a_1 x + a_2 y, a_3 x + a_4 y) = F_2(x,y)$$

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 (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).

For $F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ with discriminant D, it follows by routine calculation that

$$A = b^2 - 3ac, \quad B = bc - 9ad, \quad C = c^2 - 3bd$$

and

$$B^2 - 4AC = -3D.$$

Further, these forms are related to $F(x,y)$ via the identity

$$4H(x,y)^3 = G(x,y)^2 + 27DF(x,y)^2 \tag{2}$$

Binary cubic form F is called *reduced* if the Hessian

$$H(x,y) = Ax^2 + Bxy + Cy^2$$

of F, 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 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

$$H(x,y) = Ax^2 + Bxy + Cy^2 \geq Cy^2 \geq C \geq \frac{1}{2}\sqrt{3D}.$$

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. $\qquad \square$

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 (1) if and only if F is monic.

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 (2), we may write

$$H(x,y)^3 = U(x,y)V(x,y)$$

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

$$\xi(x,y)^3 - \eta(x,y)^3 = 3\sqrt{-3D}F(x,y), \quad \xi(x,y)^3 + \eta(x,y)^3 = G(x,y),$$
$$\xi(x,y)\eta(x,y) = H(x,y). \tag{3}$$

and

$$\frac{\xi(x,y)}{\xi(1,0)} \quad \text{and} \quad \frac{\eta(x,y)}{\eta(1,0)} \in M.$$

The reason for the last identity is that for any pair of rational integers x_0, y_0,

$$\xi(x_0, y_0) \quad \text{and} \quad \eta(x_0, y_0)$$

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 forms, 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 a pair of resolvent forms if

$$\left| 1 - \frac{\eta(x,y)}{\xi(x,y)} \right| = \min_{0 \le k \le 2} \left| \omega^k - \frac{\eta(x,y)}{\xi(x,y)} \right| \tag{4}$$

Following a discussion of DELONE and FADDEEV in [1], we call the roots ρ_1, ρ_1', ρ_1'' of the equation $F(x, a) = 0$ the left roots of the form F, while the roots ρ_2, ρ_2', ρ_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 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

$$\xi = \xi_1 x + \xi_2 y, \qquad\qquad \eta = \eta_1 x + \eta_2 y,$$

$$\xi_1 = \rho_1 + \omega\rho_1' + \omega^2\rho_1'', \qquad \eta_1 = \rho_1 + \omega^2\rho_1' + \omega\rho_1'',$$

$$\xi_2 = \rho_2 + \omega\rho_2' + \omega^2\rho_2'', \qquad \eta_2 = \rho_2 + \omega^2\rho_2' + \omega\rho_2''$$

and $\omega = e^{\frac{2\pi i}{3}}$.

PROOF. One can find the complete proof of Lemma 3.1 in [1]. □

We continue with the following definitions of p, q and u_i:

$$p = \frac{\eta + \xi}{\sqrt{2}}, \quad q = \frac{\sqrt{-1}(\eta - \xi)}{\sqrt{2}},$$

$$u_1 = D^{-1/6}\left(\frac{q}{\sqrt{6}} + \frac{p}{\sqrt{2}}\right), \quad u_2 = D^{-1/6}\left(\frac{q}{\sqrt{6}} - \frac{p}{\sqrt{2}}\right), \quad u_3 = D^{-1/6}\frac{2}{\sqrt{6}}q. \quad (5)$$

Since η and ξ are linear functions of x and y, so are p, q and u_i. The reason for 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 (1). In other words, these functions allow us to recast the resolvent forms ξ and η in a geometric setting.

By Lemma 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

$$\frac{q}{\sqrt{6}} = -\frac{(\rho_1' - \rho_1'')x + (\rho_2' - \rho_2'')y}{2}. \quad (6)$$

Further

$$\frac{p}{\sqrt{2}} = \frac{\left(2\rho_1 + \omega(\rho_1' + \rho_1'') + \omega^2(\rho_1' + \rho_1'')\right)x + \left(2\rho_2 + \omega(\rho_2' + \rho_2'') + \omega^2(\rho_2' + \rho_2'')\right)y}{2}.$$

Since ω is a primitive third root of unity, $\omega + \omega^2 = -1$. Hence

$$\frac{p}{\sqrt{2}} = \frac{2(\rho_1 x + \rho_2 y) - (\rho_1' + \rho_1'')x - (\rho_2' + \rho_2'')y}{2} \quad (7)$$

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:

$$u_1 = D^{-1/6}(\rho_1 - \rho_1'')(x - \rho_1' y/a), \quad (8)$$

$$u_2 = D^{-1/6}(\rho_1' - \rho_1)(x - \rho_1'' y/a), \quad (9)$$

$$u_3 = D^{-1/6}(\rho_1' - \rho_1'')(x - \rho_1 y/a), \quad (10)$$

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 (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,

$$u_1 u_2 u_3 = D^{-1/2}(\rho_1 - \rho_1'')(\rho_1' - \rho_1)(\rho_1' - \rho_1'')F(x, y) = \pm F(x, y).$$

Suppose that (x, y) is a solution to $F(x, y) = 1$. Since

$$\log|u_1| - \log|u_2| = \log\left|\frac{\rho_1 - \rho_1''}{\rho_1' - \rho_1}\right| + \log\left|\frac{x - \rho_1' y}{x - \rho_1'' y}\right|$$

and $|\frac{x - \rho_1' y}{x - \rho_1'' y}|$ is a unit, we can write

$$\log|u_1| - \log|u_2| = \log\lambda_1 + m\log\lambda_2 + n\log\lambda_3, \tag{11}$$

where $\lambda_1 = |\frac{\rho_1 - \rho_1''}{\rho_1' - \rho_1}|$, 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

$$\left|1 - \frac{\eta_i}{\xi_i}\right| = \left|1 - \frac{p_i - \sqrt{-1}q_i}{p_i + \sqrt{-1}q_i}\right| = \frac{2|q_i|}{|\xi_i|}.$$

By identities in (3) and Lemma 3.1, $|\eta_i| = |\xi_i|$ and $|\xi_i(x, y)| = \sqrt{H(x, y)}$. Hence,

$$\left|1 - \frac{\eta_i}{\xi_i}\right| = \frac{2|q_i|}{\sqrt{H}}.$$

Suppose that (x, y) is a solution to (1) and related to resolvent form (ξ_i, η_i). Since

$$\left|1 - \frac{\eta_i}{\xi_i}\right| = \min_{k=1,2,3}\left|1 - \frac{\eta_k}{\xi_k}\right|,$$

we conclude that

$$|q_i| = \min_{k=1,2,3} |q_k|.$$

On the other hand,

$$\prod_{k=1}^{3} |q_i| = \frac{|\eta - \xi|\,|\omega\eta - \omega^2\xi|\,|\omega^2\eta - \omega\xi|}{2\sqrt{2}} = \frac{|\eta^3 - \xi^3|}{2\sqrt{2}} = \frac{3\sqrt{3}}{2\sqrt{2}}\sqrt{D},$$

where the last equality comes from the equation (3).

If the solution (x, y) is related to (ξ_i, η_i), then

$$|u_3| = |D^{-1/6}\frac{2}{\sqrt{6}}q_i| < 1. \tag{12}$$

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,

$$\log|u_1| + \log|u_2| + \log|u_3| = 0 \qquad \text{and} \qquad \log|u_1u_2| > 0.$$

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 $F(x, 1) = 0$.

Since we assumed that F has positive discriminant, the algebraic number field $\mathbb{Q}(\rho_1)$ is real and has two fundamental units, say λ_2 and λ_3. By Dirichlet's unit theorem, we have a sequence of mappings

$$U \longmapsto V - \{0\} \subset \mathbb{R}^3$$

and

$$\log : V - \{0\} \longmapsto \Lambda - \{0\},$$

where Λ is a 2-dimensional lattice, $U \longmapsto V - \{0\}$ is the obvious restriction of the embedding of K in $\mathbb{R}^3$, and $\log$ is defined as follows: For $(x_1, x_2, x_3) \in V - \{0\}$,

$$\log(x_1, x_2, x_3) = (\log|x_1|, \log|x_2|, \log|x_3|).$$

We define τ to be the embedding from the unit group U to the lattice Λ:

$$\tau : U \longmapsto \Lambda - \{0\}.$$

By identities (8), (9) and (10), the vector

$$\vec{u} = (\log |u_1|, \log |u_3|, \log |u_3|)$$

can be considered as

$$\vec{v} + (\log |x - \rho_1' y|, \log |x - \rho_1'' y|, \log |x - \rho_1 y|), \tag{13}$$

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 (13) is a permutation of the vector $\vec{u}(1, 0)$.

If (x, y) is a solution 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 solution to $F(x, y) = 1$ and define functions t and s of x and y as follows

$$t = \frac{-\sqrt{6}}{2} \log |u_3|, \quad s = \frac{\log |u_1| - \log |u_2|}{\sqrt{2}}.$$

Then we have

$$\log |u_1| = s/\sqrt{2} + t/\sqrt{6}$$

$$\log |u_2| = -s/\sqrt{2} + t/\sqrt{6}$$

$$\log |u_3| = -2t/\sqrt{6}. \tag{14}$$

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 (14,) we get

$$\left\| \left(\log \left| \frac{u_1}{u_2} \right|, log \left| \frac{u_2}{u_3} \right|, \log \left| \frac{u_3}{u_1} \right| \right) \right\| = \sqrt{3}s\vec{\alpha'} + \sqrt{3}t\vec{\beta'},$$

where

$$\vec{\alpha'} = \frac{1}{\sqrt{3}} \left(\sqrt{2}, \frac{-1}{\sqrt{2}}, \frac{-1}{\sqrt{2}} \right)$$

and

$$\vec{\beta'} = \frac{1}{\sqrt{3}} \left(0, \frac{3}{\sqrt{6}}, \frac{-3}{\sqrt{6}} \right).$$

Since $\vec{\alpha'}$ and $\vec{\beta'}$ are orthonormal vectors in $\mathbb{R}^3$, we get

$$\left\| \left(\log \left| \frac{u_1}{u_2} \right|, \log \left| \frac{u_2}{u_3} \right|, \log \left| \frac{u_3}{u_1} \right| \right) \right\| = \sqrt{3}\sqrt{s^2 + t^2} = \sqrt{3}\|\vec{u}\|. \tag{15}$$

Remark. Since $\log|u_3| < 0$, the function t is a positive-valued function.

Lemma 4.1. *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 (5), the definition of u_i, we have $u_1 + u_2 + u_3 = 0$. Assume that $s > 0$. From (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. $\qquad\square$

Let us define

$$g(t) := \sqrt{2}\sinh^{-1}\left(\frac{\exp(-\sqrt{6}t/2)}{2} \right).$$

Then $s = \pm g(t)$.

In the following theorem, we summarize the properties of function g, which will be used later.

Theorem 4.2. *Let $g(t) = \sqrt{2}\sinh^{-1}\left(\frac{\exp(-\sqrt{6}t/2)}{2} \right)$. 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
$$A'(t) = e^{at}\left(g'(t) + ag(t)\right).$$

For $a \leq 0$, $A' < 0$ since $g' < 0$. For positive a, by part (i) and (ii), we have
$$A'(t) \leq \exp at - \sqrt{6}t/2\left(\frac{-\sqrt{3}}{2\cosh(g/\sqrt{2})} + \frac{a}{\sqrt{2}}\right).$$

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

$$a \leq \frac{\sqrt{6}}{\sqrt{5}}. \qquad \Box$$

Lemma 4.3. *Let (x, y) and (x', y') be two distinct solutions to equation* (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

$$|pq' - p'q| = \left| \frac{\eta + \xi}{\sqrt{2}} \frac{\sqrt{-1}(\eta' - \xi')}{\sqrt{2}} - \frac{\eta' + \xi'}{\sqrt{2}} \frac{\sqrt{-1}(\eta - \xi)}{\sqrt{2}} \right| = |\eta\xi' - \eta'\xi|.$$

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. $\qquad \Box$

Lemma 4.4. *Let (x, y) and (x', y') be two distinct solutions to equation* (1), *related to (ξ, η). Assume that $t(x', y') \geq t(x, y)$. Then we have*

$$t(x', y') \geq 2t(x, y) + \frac{\sqrt{6}}{6} \log D - \sqrt{6} \log\left(2 + \frac{1}{\sqrt{2}}\right).$$

PROOF. Put

$$p = p(x, y), \quad p' = p(x', y'),$$
$$q = q(x, y), \quad q' = q(x', y'),$$
$$s = s(x, y), \quad s' = s(x', y'),$$
$$t = t(x, y), \quad t' = t(x', y')$$

and

$$u_i = u_i(x, y), \qquad u'_i = u_i(x', y').$$

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:

$$|p| = \frac{1}{\sqrt{2}} |\sqrt{2} p| \leq \frac{1}{\sqrt{2}} \left(\left| (p/\sqrt{2}) + (q/\sqrt{6}) \right| + \left| (q/\sqrt{6}) - (p/\sqrt{2}) \right| \right)$$
$$= \frac{1}{\sqrt{2}} \frac{|(q/\sqrt{6}) + (p/\sqrt{2})|^{1/2}}{|(q/\sqrt{6}) - (p/\sqrt{2})|^{1/2}} \left(\left| (q/\sqrt{6}) + (p/\sqrt{2}) \right|^{1/2} \left| (q/\sqrt{6}) - (p/\sqrt{2}) \right|^{1/2} \right)$$
$$+ \frac{1}{\sqrt{2}} \frac{|(q/\sqrt{6}) - (p/\sqrt{2})|^{1/2}}{|(q/\sqrt{6}) + (p/\sqrt{2})|^{1/2}} \left(\left| (q/\sqrt{6}) + (p/\sqrt{2}) \right|^{1/2} \left| (q/\sqrt{6}) - (p/\sqrt{2}) \right|^{1/2} \right).$$

By (14) and (23), we have

$$\left| (q/\sqrt{6}) + (p/\sqrt{2}) \right|^{1/2} \left| (q/\sqrt{6}) - (p/\sqrt{2}) \right|^{1/2} = D^{1/6} u_1^{1/2} u_2^{1/2} = D^{1/6} \exp(t/\sqrt{6}).$$

Equations (14) and (23) also give us the following identities:

$$\left(\frac{|(q/\sqrt{6}) + (p/\sqrt{2})|^{1/2}}{|(q/\sqrt{6}) - (p/\sqrt{2})|^{1/2}} + \frac{|(q/\sqrt{6}) - (p/\sqrt{2})|^{1/2}}{|(q/\sqrt{6}) + (p/\sqrt{2})|^{1/2}} \right)$$
$$= e^{\frac{(\log |u_1| - \log |u_2|)}{2}} + e^{-\frac{(\log |u_1| - \log |u_2|)}{2}} = 2 \cosh\left(\frac{s}{\sqrt{2}} \right)$$

and

$$|q| = (\sqrt{6}/2) D^{1/6} e^{-2t/\sqrt{6}}.$$

Using Lemma 4.3, we get

$$D^{1/6} \leq e^{(t' - 2t)/\sqrt{6}} \cosh\left(|s'|/\sqrt{2} \right) + e^{(t - 2t')/\sqrt{6}} \cosh\left(|s|/\sqrt{2} \right).$$

One can express the above equation in terms of sinh instead of cosh by substituting $\cosh(|s|/\sqrt{2})$ with

$$\sinh\left(\frac{|s|}{\sqrt{2s}}\right) + e^{-|s|/\sqrt{2}}.$$

Now we use the assumption that $t' \geq t$ and the fact that $e^{-|s|/\sqrt{2}} \leq 1$. By Lemma 4.1, we get

$$D^{1/6} \leq e^{(t'-2t)/\sqrt{6}}\left(1 + e^{-3(t'-t)/\sqrt{6}}\right)\left(1 + \frac{e^{-\sqrt{6}t/2}}{2}\right).$$

Note that by Theorem (4.2), $t \geq \log(2)/\sqrt{6}$, whereby taking the logarithm of both sides of the above equality, yields

$$t' - 2t \geq \sqrt{6}/6\log(D) - \sqrt{6}\log\left(\left(1 + e^{-3(t'-t)/\sqrt{6}}\right)\left(1 + \frac{1}{2\sqrt{2}}\right)\right).$$

Therefore,

$$t' - 2t \geq \sqrt{6}/6\log(D) - \sqrt{6}\log\left(2 + \frac{1}{\sqrt{2}}\right). \qquad \square$$

Lemma 4.5. *Suppose that (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 4.4, 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). $\qquad \square$

Suppose that (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 4.2 shows that

$$|s'| < |s| e^{\frac{-\sqrt{6}(t' - t)}{\sqrt{5}}},$$

Therefore,

$$\mathrm{Vol}(\Lambda) = \mathrm{Vol}(\Lambda_1) \leq (t'' - t)|s| \left(1 + e^{\frac{-\sqrt{6}(t' - t)}{\sqrt{5}}}\right).$$

Using Theorem 4.2 again, we get the following gap principle of this paper which is essentially Theorem 5.5 of [15]:

Theorem 4.6. *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

$$t'' \geq \frac{\sqrt{2}\,\mathrm{Vol}(\Lambda) \exp(\sqrt{6}t/2)}{1 + \exp(-\sqrt{6}(t' - t)/\sqrt{5}\,)},$$

where $\mathrm{Vol}(\Lambda)$ is the volume of fundamental parallelepiped of lattice Λ.

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 2. By Lemma 4.2, 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 5.1 (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 logarithmic heights $h(\alpha_j)$. Let $\log \alpha_1, \ldots, \log \alpha_n$ 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

$$L = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n,$$

with $b_1, \ldots, b_n \in \mathbb{Z}$ and with the parameter $B = \max\{1, \max\{b_j A_j / A_n : 1 \leq j \leq n\}\}$. Put

$$\Omega = A_1 \ldots A_n,$$

$$C(n) = \frac{16}{n!} e^n (2n+2)(n+2)(4n+4)^{n+1} \left(\frac{1}{2} en\right),$$

$$C_0 = \log(e^{4.4n+7} n^{5.5} d^2 \log(en)),$$

$$W_0 = \log(1.5eBd \log(ed)).$$

If $b_n \neq 0$, then

$$\log |L| > -C(n) C_0 W_0 d^2 \Omega.$$

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 simple ideals of $\mathbb{Q}(\rho)$ by indices $\sigma > 3$ and define non-Archimedean valuation of $\mathbb{Q}(\rho)$ by the formulas

$$|\alpha|_\sigma = (\mathrm{Norm}\,\mathfrak{p})^{-k},$$

where

$$k = \mathrm{ord}_\mathfrak{p}(\alpha), \quad \mathfrak{p} = \mathfrak{p}_\sigma, \quad \sigma > d,$$

for any $\alpha \in \mathbb{Q}^*(\rho)$. Then we have the *product formula*:

$$\prod_1^\infty |\alpha|_\sigma = 1, \quad \alpha \in \mathbb{Q}(\rho).$$

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 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

$$h(\lambda) = \frac{1}{6} \left(|\log |\lambda|| + |\log |\lambda'|| + |\log |\lambda''|| \right) = \frac{1}{6} |\tau(\lambda)|_1 ,$$

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

$$\max\{3h(\lambda), |\log(|\lambda|)|\} \leq \|\tau(\lambda)\|, \tag{16}$$

since $|\log(\lambda)| \leq \sqrt{\log^2 |\lambda| + \log^2 |\lambda'| + \log^2 |\lambda''|} = \|\tau(\lambda)\|$.

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 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) $\|\vec{b_1}\| \leq \|\vec{v}\|$ for every vector $\vec{v} \in \Lambda - \{\vec{0}\}$;

(ii) $\|\vec{b_2}\| \leq \|\vec{v}\|$ 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 pair of 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

$$\|\tau(\lambda_2)\| \, \|\tau(\lambda_3)\| \leq \frac{2}{\sqrt{3}} \operatorname{Vol}(\Lambda).$$

Hence, in our case,

$$A_2 A_3 \leq \frac{2}{\sqrt{3}} \operatorname{Vol}(\Lambda).$$

By (15), we have

$$\left\| \left(\log \frac{|u_1|}{|u_2|}, \log \frac{|u_2|}{|u_3|}, \log \frac{|u_3|}{|u_1|} \right) \right\| = \sqrt{3}\|\vec{u}\|.$$

The well-known inequality $\frac{a+b+c}{3} \leq [\frac{a^2+b^2+c^2}{3}]^{1/2}$ shows that

$$|\vec{v}|_1 \leq \sqrt{3}\|\vec{v}\| \tag{17}$$

for every vector $\vec{v} \in \mathbb{R}^3$. Therefore,

$$|\log |(\rho - \rho'')(x - \rho'y)|| + |\log |(\rho' - \rho)(x - \rho''y)|| + |\log |(\rho' - \rho'')(x - \rho y)||$$

$$\leq 3 \|\vec{u}(x_0, y_0)\| .$$

Now, we note that

$$\sum_{\sigma>3}\left|\log\left|\frac{(\rho-\rho'')(x-\rho'y)}{(\rho'-\rho)(x-\rho''y)}\right|_{\sigma}\right|$$

$$\leq \sum_{\sigma>3}|\log|(\rho-\rho'')(x-\rho'y)|_{\sigma}| + \sum_{\sigma>3}|\log|(\rho'-\rho)(x-\rho''y)|_{\sigma}|.$$

We know that Archimedean valuations of $|(\rho-\rho'')(x-\rho'y)|$ are itself, $|(\rho'-\rho'')(x-\rho y)|$ and $|\rho'-\rho(x-\rho'y)|$. So by the product formula, since (x,y) is a solution to (1), the product of all non-Archimedean valuations equals $D^{-1/2}$. Therefore,

$$\left|\sum_{\sigma>3}\log|(\rho-\rho'')(x-\rho'y)|_{\sigma}\right| = \frac{1}{2}\log D,$$

and similarly

$$\left|\sum_{\sigma>3}\log|(\rho'-\rho)(x-\rho''y)|_{\sigma}\right| = \frac{1}{2}\log D.$$

Since $(\rho'-\rho)(x-\rho''y)$ and $(\rho-\rho'')(x-\rho'y)$ are algebraic integers, we get

$$h(\lambda_1) \leq \frac{1}{6}\left(3\|\vec{u}(x_0,y_0)\| + \log D\right). \tag{18}$$

This gives an estimate for A_1.

Let $B_1 = BA_3$, where B is as in Theorem 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

$$\left(\log\left|\frac{u_1}{u_2}\right|, \log\left|\frac{u_2}{u_3}\right|, \log\left|\frac{u_3}{u_1}\right|\right)$$

$$= \left(\log\frac{|(\rho-\rho'')(x-\rho'y)|}{|(\rho'-\rho)(x-\rho''y)|}, \log\frac{|(\rho'-\rho)(x-\rho''y)|}{|(\rho'-\rho'')(x-\rho y)|}, \log\frac{|(\rho'-\rho'')(x-\rho y)|}{|(\rho-\rho'')(x-\rho'y)|}\right)$$

$$+ m\vec{\lambda_1} + n\vec{\lambda_2},$$

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

$$m|\vec{\lambda_2}|_1, n|\vec{\lambda_3}|_1$$

$$\leq \left|\left(\log\frac{|(\rho-\rho'')(x-\rho'y)|}{|(\rho'-\rho)(x-\rho''y)|}, \log\frac{|(\rho'-\rho)(x-\rho''y)|}{|(\rho'-\rho'')(x-\rho y)|}, \log\frac{|(\rho'-\rho'')(x-\rho y)|}{|(\rho-\rho'')(x-\rho'y)|}\right)\right|_1$$

$$+ \left| \left(\log \left| \frac{u_1}{u_2} \right|, \log \left| \frac{u_2}{u_3} \right|, \log \left| \frac{u_3}{u_1} \right| \right) \right|_1.$$

Therefore, by (15) and (17)

$$m|\vec{\lambda_2}|_1, n|\vec{\lambda_3}|_1 \leq 3\left(\|\vec{u}\| + \|\vec{u}(x_0, y_0)\| \right). \tag{19}$$

Theorem 5.2. *Let F be a cubic binary equation with positive discriminant. For all pairs of solution (a, b) to the equation (1), except possibly one of them, we have*

$$D \leq 64e^{2\sqrt{6}t},$$

where D is the discriminant of $F(x, y)$ and $t = t(a, b)$, for the function t defined in Section 3. Moreover, when $t \geq 5$

$$D \leq \frac{1}{2}e^{2\sqrt{6}t}.$$

PROOF. By (3)

$$|H| = |\xi\eta| = \left| \frac{p + iq}{\sqrt{2}} \cdot \frac{p - iq}{\sqrt{2}} \right| = \frac{p^2 + q^2}{2}.$$

By (5),

$$q = \frac{\sqrt{6}}{2}D^{1/6}u_3$$

and

$$|p| = \left| \frac{\sqrt{2}}{2}(u_1 - u_2) \right| D^{1/6} \leq \frac{\sqrt{2}}{2}D^{1/6}(|u_1| + |u_2|).$$

Therefore, by (14)

$$|H| \leq \frac{1}{2}D^{1/3}\left(e^{2t/\sqrt{6}}(e^{2s/\sqrt{2}} + e^{-2s/\sqrt{2}} + 2)/2 + \frac{3}{2}e^{-4t/6} \right). \tag{20}$$

Therefore, by Lemma 2.1, for all solutions (a, b) to (1), except at most one of them

$$\frac{1}{2}D^{1/2}\sqrt{3} \leq \frac{1}{2}D^{1/3}\left(e^{2t/\sqrt{6}}(e^{2s/\sqrt{2}} + e^{-2s/\sqrt{2}} + 2)/2 + \frac{3}{2}e^{-4t/6} \right). \tag{21}$$

Since $t > 0$, part (ii) of Lemma 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 4.2. $\qquad\square$

Since $\vec{u} = (t, s)$ and $\|\vec{u}\| = \sqrt{t^2 + s^2}$, from Theorem 4.2, we deduce that $|\vec{u}|_2$ is an increasing function of t. So we can assume that Theorem 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 (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 (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 4.2, if we take $t \geq 5$ (Theorem 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 (18) and Theorem 5.2, we can take

$$A_1 = 1.0016(\frac{3}{2}t + \sqrt{6}t).$$

Inequality (19) suggests the value $3(1.0016)(t'' + t)$ for B_1. But by Theorem 4.4, for large discriminant D, $t'' > 4t$. So we take

$$B_1 = 3(1.0016)(t'' + t''/4). \tag{22}$$

So Matveev 's lower bound gives us:

$$\log |L| > -1.5036 \times 10^{11} A_1 A_2 A_3 \log\left(25.6708(3.0048)(1.25)t''/A_3\right),$$

where $L = \log |u_1| - \log |u_2|$. On the other hand, by Theorem 4.2, 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 $A_2 A_3 \leq 2/\sqrt{3} \operatorname{Vol}(\Lambda)$, we obtain the following upper bound for t'':

$$t'' \leq \frac{e}{e-1} 1.2276 \times 10^{11} \left(\frac{2}{\sqrt{3}}\right) \operatorname{Vol}(\Lambda) A_1 \log(1.1892 \times 10^{13} A_1 A_2). \tag{23}$$

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 (1), and related to a fixed choice of resolvent form. Let $t = t(x,y) < t' = t(x',y') < t'' = t(x'',y'')$. By (23) and Theorem 4.6, we get

$$\frac{e}{e-1}1.2276 \times 10^{11} A_1 \left(\frac{2}{\sqrt{3}}\right) \mathrm{Vol}(\Lambda) \log(1.1892 \times 10^{13} A_1 A_2)$$

$$\geq \frac{\sqrt{2}\,\mathrm{Vol}(\Lambda) \exp(\sqrt{6}t/2)}{1 + \exp(-\sqrt{6}(t'-t)/\sqrt{5})}, \tag{24}$$

where $A_1 = (3/2 + \sqrt{6})(1.006)t$ and $A_2 = \|\tau(\lambda_2)\|$. Without loss of generality, we can assume that $\|\tau(\lambda_2)\| \leq \|\tau(\lambda_3)\|$. Therefore,

$$\frac{\sqrt{3}}{2}|\tau(\lambda_2)|_2^2 \leq \frac{\sqrt{3}}{2}\|\tau(\lambda_2)\|\,\|\tau(\lambda_3)\| \leq \mathrm{Vol}(\Lambda).$$

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 (19), we have $\|\tau(\lambda_2)\| \leq 6.01t$. Using Theorem 4.4, we get

$$\frac{e}{1-e}4.8484 \times 10^{11} \left(\frac{2}{\sqrt{3}}\right) \mathrm{Vol}(\Lambda)t \log(2.8184 \times 10^{14}t^2) \geq \frac{\sqrt{2}\,\mathrm{Vol}(\Lambda) \exp(\sqrt{6}t/2)}{1 + \exp(-\sqrt{6}t/\sqrt{5})}.$$

Therefore, $t < 27.91$ and by equation (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 (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 (23), we get

$$t \leq 27.5321,$$

and therefore, $D < 1.4 \times 10^{57}$. Since we have three pairs of resolvent forms, Theorem (1.1) is proved.

As we mentioned in the remark after the proof of Lemma 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 2.1 and therefore Lemma 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 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 (6) to get $t \leq 28.38$ and consequently by (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 1.2.

In [2], it is proved 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 (1) with $H(x,y) \geq \frac{1}{2}\sqrt{3D}$, where H is the Hessian of F. This together with Lemma 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. These computations show that the equation (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].

References

[1] B. N. DELONE and D. K. FADEEV, The Theory of Irrationalities of the Third Degree, Translations of Mathematical Monographs, Vol. 10, *American Mathematical Society, Providence, R. I.*, 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**, no. 2 (2003), 205–206.

[4] V.I. BAULIN, On an intermediate equation of the third degree with least positive discriminant, *Tul'sk Gos. Ped.Inst. Ucen. Zap. Fiz. Math. Nauk. Vip.* **7** (1960), 138–170 (in *Russian*).

[5] J. H. EVERTSE, On the representation of integers by binary cubic forms of positive discriminant, *Invent. Math.* **73** (1983), 117–138.

[6] I. GAÁL 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, Pethő's cubics, *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 über die Darstellung ganzer Zahlen durch binäre 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.*, no. 1 (1929).

[17] E. THOMAS, Complete solutions to a family of cubic Diophantine equations, *J. Number Theory* **34** (1990), 235–250.

SHABNAM AKHTARI
MAX-PLANCK-INSTITUT FÜR MATHEMATIK
53072 BONN, P.O. BOX: 7280
GERMANY

E-mail: akhtari@mpim-bonn.mpg.de
URL: http://guests.mpim-bonn.mpg.de/akhtari