Shabnam AKHTARI

Integral points on a certain family of elliptic curves

Integral points on a certain family of elliptic curves

par Shabnam AKHTARI

RÉSUMÉ. Nous utilisons la méthode de Thue-Siegel pour obtenir une borne supérieure du nombre de solutions entières primitives d'une famille d'inégalités quartic de Thue. Cela permet de donner une borne supérieure du nombre de points entiers pour une famille de courbes elliptiques d'invariant j égal à 1728.

ABSTRACT. The Thue-Siegel method is used to obtain an upper bound for the number of primitive integral solutions to a family of quartic Thue's inequalities. This will provide an upper bound for the number of integer points on a family of elliptic curves with j-invariant equal to 1728.

1. Introduction and statements of the main results

A well-known theorem of Siegel, in its simplest form, is the fact that a nonsingular elliptic curve contains only finitely many integer points. Let

$$E : y^2 = x^3 + Ax + B$$

and

$$H = \max\{|A|, |B|\}.$$

Schmidt in [12] established some upper bounds for the number and the size of integer points on plane curves of genus 1. His work implies, for given $\epsilon > 0$, the upper bound

$$c(\epsilon)H^{2+\epsilon}$$

upon the number of integral points on $y^2 = x^3 + Ax + B$, where the constant $c(\epsilon)$ is effectively computable. Schmidt conjectured that for every $\epsilon > 0$, there exists a constant $c(\epsilon)$ such that the number of integral points on $y^2 = x^3 + Ax + B$ is bounded above by $c(\epsilon)H^\epsilon$. Evertse and Silverman in [6] gave an upper bound for the number of integer points on elliptic curves

$$(1.1) \qquad y^2 = f(x) = x^3 + bx^2 + cx + d,$$

which depends on the class number of the splitting field of $x^3 + bx^2 + cx + d$. They showed that for any $\epsilon > 0$, the number of integer solution to an equation of the form (1.1), with $b, c, d \in \mathbb{Z}$ and non-zero discriminant $\Delta(f)$, is bounded by $c(\epsilon)|\Delta(f)|^{1/2+\epsilon}$ for some effectively computable $c(\epsilon) > 0$. Also Helfgott and Venkatesh in [7] provided some nice upper bounds on the number of integer points (and S-integer points) on elliptic curves. Their work implies an upper bound in terms of the rank of the elliptic curves. Moreover, they showed, among other things, that the number of integral points on any given elliptic curve E is $\ll |\Delta|^{\theta+\epsilon}$ for every sufficiently small ϵ, where Δ is the discriminant of E and $\theta = 0.20070\ldots$.

In this manuscript we will consider a certain family of elliptic curves with j-invariant 1728 and use different tools to provide an upper bound for the number of integer points on such curves. We will improve upon some results obtained by Walsh in [16]. The results presented here are substantially more restrictive than those in [6], [7] and [12]. However our results and techniques are quite different and improve upon the previous results in certain cases.

Elliptic curves with j-invariant 1728 are one of the important families in the arithmetic theory of elliptic curves. Every such curve has an equation of the form $Y^2 = X^3 \pm NX$, where N is a 4th-power-free positive integer (see [13], for example). Here we will consider the problem of counting the number of integral points on curves of this form, though our focus is mainly on the cubic equation

$$(1.2) \qquad\qquad Y^2 = X^3 - NX,$$

where N is a square-free positive integer. In Section 7 we briefly discuss the problem of counting the integral points on the curve $Y^2 = X^3 + NX$ and explain how this problem is different from our main problem. It turns out that the integral points on the equation (1.2) can be seen as integral points on a finite number of curves given by quartic equations of the form

$$(1.3) \qquad\qquad X^2 - DY^4 = k,$$

where $D > 1$ is a square-free integer and $k < 0$ is a negative integer relatively prime to D. To study the integral solutions of (1.3), we can look at the integral solutions of the quadratic equation

$$\mathfrak{X}^2 - D\mathfrak{Y}^2 = k$$

and detect those with $\mathfrak{Y}$ a perfect square. For the positive non-square integer D, let

$$\epsilon_D = T + U\sqrt{D},$$

with T, U positive integers, denote the minimal unit greater than 1 in the ring $\mathbb{Z}[\sqrt{D}]$. Notice that $\mathbb{Z}[\sqrt{D}]$ is an order in the ring of integers of the number field $\mathbb{Q}(\sqrt{D})$, and since we are looking for integer points on various

curves, we prefer to work with $\mathbb{Z}[\sqrt{D}]$ instead of the ring of integers of $\mathbb{Q}(\sqrt{D})$.

Theorem 1.1. *Let k be a negative integer. The quartic equation* (1.3) *has at most*

$$384.\, 2^{\omega(k)} \epsilon_D^{3/2} \sqrt{|k|/2D}$$

solutions in positive integers X and Y, where $\omega(k)$ denotes the number of prime factors of the integer k.

Theorem 1.2. *Let k be a negative integer satisfying*

$$|k| \geq \frac{\pi}{2^{14} 3^{11/2}} \frac{\epsilon_D^{12}}{D^{13/2}}.$$

The quartic equation (1.3) *has at most*

$$40.2^{\omega(k)}$$

solutions in positive integers X and Y, where $\omega(k)$ denotes the number of prime factors of the integer k.

The unit ϵ_D is bounded from above. In fact, we have

(1.4) $$\epsilon_D < \exp\left(D^{1/2}\left(\log(4D) + 2\right)\right)$$

(see [8]). Therefore, in the statement of Theorem 1.2, one can replace the given lower bound on $|k|$ with an explicit function of D:

$$|k| \geq \frac{\pi}{2^{14} 3^{11/2}} \frac{\exp\left(12\, D^{1/2}\left(\log(4D) + 2\right)\right)}{D^{13/2}}.$$

Theorem 1.3. *Let N be a positive square-free integer. The equation* (1.2) *has at most*

$$384\sqrt{N/2} \sum_{D|N} \frac{2^{\omega(N/D)} \epsilon_D^{3/2}}{D}$$

solutions in integers X, Y.

The above theorems improve the results in [16]. Walsh in [16] proved that there are at most $48.2^{\omega(k)}$ integer solutions to (1.3) with

$$|Y| > \frac{2^{5/4}|k|^{39/4}\epsilon_D^{45/4}}{D^{13/4}}.$$

Then he concluded that, if N is a positive square-free integer, there are at most $48\sum_{D|N} 2^{\omega(D)}$ integer solutions to (1.2) with

$$|X| > \max_{D|N, D>1} \frac{2^{5/2}|N/D|^{39/2}\epsilon_D^{45/2}}{D^{11/2}}.$$

In order to count the number of integral points on the above cubic and quartic curves, we will reduce them to a family of quartic Thue equations $F(x, y) = m$, where $m \in \mathbb{Z}$. Let

$$F(x, y) = a_0 x^4 + a_1 x^3 y + a_2 x^2 y^2 + a_3 x y^3 + a_4 y^4$$

be a binary quartic form with integer coefficients. The discriminant Δ of F is given by

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

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

$$F(x, 1) = a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4.$$

The ring of invariants of F is generated by two invariants

$$I = I_F = a_2^2 - 3a_1 a_3 + 12 a_0 a_4,$$

and

$$J = J_F = 2a_2^3 - 9a_1 a_2 a_3 + 27 a_1^2 a_4 - 72 a_0 a_2 a_4 + 27 a_0 a_3^2,$$

of weights 4 and 6, respectively. Every invariant of F is a polynomial in I and J. In particular, for the discriminant Δ, we have

$$27\Delta = 4I^3 - J^2.$$

In this manuscript we will consider the forms F for which the invariant $J = 0$, so that we have

$$27\Delta = 4I^3.$$

We will show

Theorem 1.4. *Let $F(x, y)$ be an irreducible binary quartic form with $I > 0$ and $J = 0$. Suppose that all four roots of $F(X, 1)$ are real and h is an integer satisfying $h = \frac{\sqrt{3}\, I^{1/2 - \epsilon}}{\pi}$, with $0 < \epsilon < \frac{1}{2}$. Then the Thue inequality*

$$(1.5) \qquad\qquad |F(x, y)| \leq h$$

has at most

$$4 \left[\frac{\log \left(\frac{1}{2\epsilon} - \frac{1}{2} \right)}{\log 3} \right] + 16$$

solutions in coprime integers x and y with $y \neq 0$, where $[.]$ denotes the greatest integer function and (x, y) and $(-x, -y)$ are counted as one solution.

The upper bound given in the statement of Theorem 1.4 depends on ϵ and therefore, on the integer h. Setting $\epsilon > \frac{1}{4}$, for example, in Theorem 1.4 yields the following.

Corollary 1.1. *Let $F(x,y)$ be an irreducible binary quartic form with $I > 0$ and $J = 0$. Suppose that all roots of polynomial $F(x,1)$ are real and h is an integer satisfying $h < \frac{\sqrt{3}\,I^{5/14}}{\pi}$. Then the inequality*

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

has at most 16 *solutions in coprime integers x and y, with $y \neq 0$. Here (x,y) and $(-x,-y)$ are counted as one solution.*

Let $G(x,y) \in \mathbb{Z}[x,y]$ be a form of degree n that is irreducible over $\mathbb{Q}$ and let $h \in \mathbb{Z}$. Bombieri and Schmidt [3] showed that the number of solutions of $G(x,y) = h$ in co-prime integers x and y is at most

$$C_2\, n^{1+\omega(h)},$$

where C_2 is an absolute constant. In [2] the author obtained an upper bound for the number of integer solutions to the Thue inequality $|G(x,y)| \leq h$, where G is a binary form of degree $n \geq 3$ and with non-zero discriminant Δ, and h is an integer smaller than $|\Delta|^{\frac{1}{4(n-1)}}$. One may apply that upper bound to the quartic Thue inequalities appearing in this manuscript. Using properties specific to this family, we obtain better upper bounds here. In particular, the hypergeometric method of Thue and Siegel will be applied to the specific family of inequalities we are dealing with here. The method of Thue-Siegel cannot be used in more general cases. We refer the reader to [4] for an overall study of the Thue-Siegel method. In [1], we showed that the Thue-Siegel method may be applied to a quartic Thue equation $F(x,y) = h$, only if $J_F = 0$.

2. Quartic Thue inequalities and Proof of Theorem 1.4

In this section we will consider Thue inequalities of the shape

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

where $F(x,y)$ is a quartic binary form. We will provide an upper bound for the number of co-prime integer solutions (or *primitive* solutions) to such inequalities under the assumptions in Theorem 1.4.

We call binary forms F_1 and F_2 equivalent if they are equivalent under $GL_2(\mathbb{Z})$-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 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 $J_{F_1} = J_{F_2}$, where I and J are the invariants defined in the Introduction.

Let

$$H(x, y) = \frac{d^2 F}{dx^2} \frac{d^2 F}{dy^2} - \left(\frac{d^2 F}{dxdy} \right)^2$$

denote the Hessian associated to the quartic form $F(x, y)$. Then

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

with

(2.1)
$$
\begin{aligned}
A_0 &= 3(8a_0 a_2 - 3a_1^2), \\
A_1 &= 12(6a_0 a_3 - a_1 a_2), \\
A_2 &= 6(3a_1 a_3 + 24a_0 a_4 - 2a_2^2), \\
A_3 &= 12(6a_1 a_4 - a_2 a_3), \\
A_4 &= 3(8a_2 a_4 - 3a_3^2).
\end{aligned}
$$

Lemma 2.1. *Suppose $F(x, y)$ is a quartic form with invariants I and J and Hessian $H(x, y)$. Let ϕ be a root of $X^3 - 3IX + J$. Then*

$$-\frac{1}{9} H(x, y) + \frac{4}{3} \phi F(x, y) = \mathbf{m}(x, y)^2,$$

where $\mathbf{m}(x, y)$ is a quadratic covariant of $F(x, y)$.

Proof. See part (vi) of Proposition 6 of [5]. $\qquad\qquad\qquad\square$

Lemma 2.2. *Let $F(x, y)$ be a quartic form with real coefficients and leading coefficient a_0. Suppose that $F(Z, 1) = 0$ has 4 real roots. Let ϕ_1, ϕ_2 and ϕ_3 be the roots of $X^3 - 3IX + J$, with $4a_0\phi_1 > 4a_0\phi_2 > 4a_0\phi_3$. Set $\phi = \phi_2$. Then $\mathbf{m}(x, y)$ is a positive definite quadratic form with real coefficients, where $\mathbf{m}(x, y)$ is the covariant of $F(x, y)$ defined in Lemma 2.1.*

Proof. This is part (ii) of Proposition 8 of [5]. Also see Lemma 3.4 of [1]. $\quad\square$

A real quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is called *reduced* if

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

It is well-known that every positive definite quadratic form is equivalent to a reduced one. Following Definition 4 of [5], we say that the quartic form $F(x, y) = a_0 x^4 + a_1 x^3 y + a_2 x^2 y^2 + a_3 x y^3 + a_4 y^4$ with positive discriminant is *reduced* if and only if the positive definite quadratic form $\mathbf{m}(x, y)$ is reduced.

Suppose that the quartic form $F(x, y)$ is reduced, $J_F = 0$ and $I_F > 0$. Then in Lemma 2.2, we have $\phi_1, \phi_3 \in \{\sqrt{3I_F}, -\sqrt{3I_F}\}$ and $\phi_2 = 0$. Taking $\phi = 0$ in Lemma 2.1, we know that the algebraic covariant $\frac{-1}{9} H(x, y)$ is the square of a quadratic form, say

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

Using the fact that $\mathbf{m}(Z) = \mathbf{m}(Z, 1)$ assumes a minimum equal to $\frac{4AC - B^2}{4A}$ at $Z = \frac{-B}{2A}$, we showed in [1] that when $\theta_1, \theta_2 \in \mathbb{R}$ and $\theta_2 \neq 0$, we have

$$(2.2) \qquad \mathbf{m}(\theta_1, \theta_2) \geq 2\sqrt{I}\theta_2^2.$$

The following results from [1] provide an upper bound for the number of "large" primitive solutions to quartic Thue inequalities of the shape $|F(x, y)| \leq h$. After stating these results, we will obtain an upper bound for the number of "small" primitive solutions, when $h < \frac{\sqrt{3I}}{\pi}$. We call a primitive solution (x, y) small if $|H(x, y)| < 4h^3\sqrt{|3IA_4|}$, and large if $|H(x, y)| \geq 4h^3\sqrt{|3IA_4|}$.

Lemma 2.3. *Let $F(x, y) \in \mathbb{Z}[x, y]$ be a quartic form with $J = 0$. If F is reduced then for every $(x_1, y_1) \in \mathbb{Z}^2$ we have*

$$|H(x_1, y_1)| \geq 36\, I y_1^4,$$

where $H(x, y)$ is the Hessian of $F(x, y)$.

Proof. This is Lemma 3.5 of [1]. $\qquad\square$

Proposition 2.1. *Let $F(x, y) \in \mathbb{Z}[x, y]$ be a quartic form with $J = 0$ that is irreducible over $\mathbb{Q}$. Then*

$$F(x, y) = \frac{1}{8\sqrt{3I|A_4|}} \left(\xi^4(x, y) - \eta^4(x, y) \right),$$

where $\xi(x, y)$ and $\eta(x, y)$ are linear forms in x and y, with

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

Moreover, if all roots of the polynomial $F(Z, 1)$ are real then $I > 0$, $A_0 < 0$, and $\xi(x, y)$ and $\eta(x, y)$ are complex conjugate linear forms.

Proof. This is Lemma 5.1 of [1]. $\qquad\square$

The linear forms $\xi(x, y)$ and $\eta(x, y)$ in Proposition 2.1 are called a pair of *resolvent forms*. In what follows we will often write ξ and η for $\xi(x, y)$ and $\eta(x, y)$ at a particular point (x, y) when that point is understood. Note that if (ξ, η) is one pair of resolvent forms then there are precisely three others, given by $(i\xi, -i\eta)$, $(-\xi, -\eta)$ and $(-i\xi, i\eta)$, where $i = \sqrt{-1}$. For the fixed pair of resolvent forms (ξ, η), we have equation (22) of [1]:

$$(2.3) \qquad |\xi(x, y)\eta(x, y)| = \frac{(H(x, y)^2|A_4|)^{1/4}}{\sqrt{3}}.$$

Also as a direct consequence of the definition of ξ and η, it is shown in [1] (equation (25)) that if $x_1, y_1, x_2, y_2 \in \mathbb{Z}$, with $x_1 y_2 - x_2 y_1 \neq 0$, then

$$(2.4) \qquad |\xi(x_1, y_1)\eta(x_2, y_2) - \xi(x_2, y_2)\eta(x_1, y_1)| \geq 2\sqrt{I}\,|A_4|^{1/4}.$$

From now on, we fix a pair of resolvent forms. Let ω be a fourth root of unity. We say that the integer pair (x, y) is *related* to ω if

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

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 the complex number $1 - z$). We have

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

Note that when $F(x, y)$ is irreducible then $|z| \ne 2$. Because if $|z| = 2$ then $\eta^4 = -\xi^4$, so $F(x, y) = \frac{1}{4\sqrt{3IA_4}} \xi^4(x, y)$. This implies that $F(x, y)$ has one root with multiplicity 4 and therefore the discriminant of $F(x, y)$ is 0. This contradicts the assumption that $F(x, y)$ is irreducible over $\mathbb{Q}$.

Lemma 2.4. *Let ω be a fourth root of unity and $(x, y) \in \mathbb{Z}^2$ satisfy $F(x, y) = \frac{1}{8\sqrt{3IA_4}} (\xi^4(x, y) - \eta^4(x, y)) = 1$, with*

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

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

$$(2.5) \qquad\qquad\qquad \left| \omega - \frac{\eta(x,y)}{\xi(x,y)} \right| \le \frac{\pi}{8} |z|.$$

If $|z| < 1$ then

$$(2.6) \qquad\qquad\qquad \left| \omega - \frac{\eta(x,y)}{\xi(x,y)} \right| < \frac{\pi}{12} |z|.$$

Proof. This is Lemma 6.1 of [1]. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Lemma 2.5. *Let $F(x, y) \in \mathbb{Z}[x, y]$ be a reduced quartic form satisfying the conditions in Proposition 2.1. If all roots of the polynomial $F(Z, 1)$ are real then the inequality $|F(x, y)| \le h$ has at most 12 primitive solutions (x, y) with*

$$|\xi(x, y)|^4 \ge 4h^3 \sqrt{|3IA_4|}.$$

Proof. This was shown in [1] (see, in particular, equation (29) through equation (30)). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Note that in the above lemma, and generally in [1], no restriction is assumed on the value of h. Instead, the upper bounds are given for the number of those solutions that are large in terms of h.

Using a standard gap argument, we will establish an upper bound for the number of solutions (x, y) to (1.5) that satisfy

$$|\xi(x, y)|^4 < 4h^3 \sqrt{|3IA_4|},$$

when

$$h \leq \frac{\sqrt{3}\, I^{1/2-\epsilon}}{\pi}, \text{ with } 0 < \epsilon < \frac{1}{2}.$$

Suppose there are distinct solutions to $|F(x, y)| \leq h$ indexed by i, say (x_i, y_i), that are related to a fixed fourth root of unity ω with

$$|\xi(x_{i+1}, y_{i+1})| \geq |\xi(x_i, y_i)|.$$

Let

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

with $|h_i|, |h_{i+1}| \leq h$. Set

$$\eta_i = \eta(x_i, y_i) \quad \text{and} \quad \xi_i = \xi(x_i, y_i).$$

By Lemma 2.3 and (2.3), for every index i, we have

(2.7) $$|\xi_i| \geq 12^{1/4} I^{1/4} |A_4|^{1/8},$$

provided that $y_i \neq 0$. Using the definition of z_i above, then Proposition 2.1 and the assumption that $|h_i| \leq h < \frac{\sqrt{3} I^{1/2}}{\pi}$, we get

$$
\begin{aligned}
|z_i| &= \left| 1 - \frac{\eta^4(x, y)}{\xi^4(x, y)} \right| \\
&= \left| \frac{8h_i \sqrt{|3I\, A_4|}}{\xi_i^4} \right| \\
&\leq \frac{3I \sqrt{|A_4|}\, 8}{\pi |\xi^4(x, y)|} \\
&\leq \frac{3I \sqrt{|A_4|}\, 8}{\pi 12 I \sqrt{|A_4|}} \\
&= 2/\pi < 1.
\end{aligned}
$$

We have

$$
\begin{aligned}
&\ |\xi_i \eta_{i+1} - \xi_{i+1} \eta_i| \\
=&\ |\xi_i(\eta_{i+1} - \omega\xi_{i+1}) - \xi_{i+1}(\eta_i - \omega\xi_i)| \\
\leq&\ \left| \xi_i \xi_{i+1} \left(\frac{\eta_{i+1}}{\xi_{i+1}} - \omega \right) \right| + \left| \xi_i \xi_{i+1} \left(\frac{\eta_i}{\xi_i} - \omega \right) \right| \text{ (by the triangle inequality)} \\
\leq&\ \frac{\pi}{12} \left(|\xi_i \xi_{i+1} z_{i+1}| + |\xi_i \xi_{i+1} z_i| \right) \text{ (from (2.6))} \\
=&\ \frac{\pi}{12} \left(|\xi_i \xi_{i+1} \frac{\eta_{i+1}^4 - \xi_{i+1}^4}{\xi_{i+1}^4}| + |\xi_i \xi_{i+1} \frac{\eta_i^4 - \xi_i^4}{\xi_i^4}| \right) \\
\leq&\ \frac{2\pi}{3} h \sqrt{|3I\, A_4|} \left(\frac{|\xi_i|}{|\xi_{i+1}^3|} + \frac{|\xi_{i+1}|}{|\xi_i^3|} \right) \text{ (by Proposition 2.1).}
\end{aligned}
$$

Since we have assumed $|\xi_i| \le |\xi_{i+1}|$, we get

$$|\xi_i \eta_{i+1} - \xi_{i+1}\eta_i| \le \frac{4\pi}{3} h \sqrt{|3I\,A_4|} \left(\frac{|\xi_{i+1}|}{|\xi_i^3|} \right).$$

Combining this with (2.4), we conclude

$$(2.8) \qquad\qquad |\xi_{i+1}| \ge \frac{\sqrt{3}}{2\pi h\,|A_4|^{1/4}} |\xi_i|^3.$$

By (2.8) and (2.7), we get

$$|\xi_2| \ge \frac{\sqrt{3}}{2\pi h\,|A_4|^{1/4}} 12^{3/4} I^{3/4} |A_4|^{3/8}.$$

Since $h = \frac{3I^{1/2-\epsilon}}{2} \ge \frac{3I^{1/2-\epsilon}}{\pi}$, we obtain

$$|\xi_2| \ge \frac{\sqrt{3}\pi}{6\pi I^{1/2-\epsilon}\,|A_4|^{1/4}} 12^{3/4} I^{3/4} |A_4|^{3/8} = 12^{1/4} I^{1/4+\epsilon} |A_4|^{1/8}.$$

Repeating this, we get

$$|\xi_k| \ge 12^{1/4} I^{1/4 + \left(\frac{3^{k-1}-1}{2} \right)\epsilon} |A_4|^{1/8}.$$

In order to have

$$|\xi_k| < \sqrt{2} h^{3/4} |3IA_4|^{1/8},$$

the integer k must satisfy

$$12^{1/4} I^{1/4 + \left(\frac{3^{k-1}-1}{2} \right)\epsilon} |A_4|^{1/8} < \sqrt{2} h^{3/4} |3IA_4|^{1/8}.$$

Substituting $h = \frac{\sqrt{3} I^{1/2-\epsilon}}{2}$ in the above inequality, we get

$$\left(\frac{8}{3} \right)^{1/4} I^{\left(\frac{3^{k-1}-1}{2} + \frac{3}{4} \right)\epsilon} < I^{1/4}.$$

Therefore, since $\left(\frac{8}{3} \right)^{1/4} > 1$, we obtain

$$k - 1 < \frac{\log \left(\frac{1}{2\epsilon} - \frac{3}{2} + 1 \right)}{\log 3}.$$

We conclude that the number of solutions (x, y) related to a fixed fourth root of unity with

$$|\xi(x, y)|^4 < 4h^3 \sqrt{|3IA_4|},$$

does not exceed

$$\left[\frac{\log \left(\frac{1}{2\epsilon} - \frac{1}{2} \right)}{\log 3} \right] + 1.$$

This, together with Lemma 2.5, completes the proof of Theorem 1.4.

3. The elliptic curve $Y^2 = X^3 - NX$

let N be a positive square-free integer. An integer solution to the equation

$$(3.1) \qquad Y^2 = X^3 - NX = X(X^2 - N)$$

gives rise to a positive integer solution (x, y) to the equation $x^2 - Dy^4 = \frac{-N}{D}$, by taking

$$X = Dy^2, \text{ and } X^2 - N = Dx^2.$$

In the above change of variables D is the square-free part of X and $D \mid N$. From now on, we will focus on the quartic equation

$$(3.2) \qquad X^2 - DY^4 = k,$$

where $D > 1$ is a square-free integer, N is a positive integer, and k is a negative integer. Since we assumed that N is square-free, the integer k is also square-free and is relatively prime to D. We conclude that the summation

$$(3.3) \qquad \sum_{D \mid N} U_D,$$

wherein U_D is an upper bound for the number of solutions to (3.2), will provide an upper bound for the number of integral solutions to (3.1).

Assume that $(x_0, y_0) \in \mathbb{Z}^2$ with $x_0 y_0 \neq 0$ is a point on the curve

$$(3.4) \qquad \mathfrak{X}^2 - D\mathfrak{Y}^2 = k.$$

Let

$$\alpha = x_0 + y_0 \sqrt{D},$$

and for $i \in \mathbb{Z}$, define $x_i, y_i \in \mathbb{Z}$ as follows:

$$(3.5) \qquad x_i + y_i \sqrt{D} = \alpha \epsilon_D^i,$$

where ϵ_D denotes the minimal unit of $\mathbb{Z}[\sqrt{D}]$ and is defined in the Introduction. Then each pair $(x_i, y_i) \in \mathbb{Z}^2$ is a solution to (3.4). We refer to the set of all such solutions as the *class of solutions* to (3.4) associated to (x_0, y_0). Assume that $(x, y) \in \mathbb{Z}^2$ is a solution of (3.4). Sometimes for simplicity, we call $x + \sqrt{D}y$ a solution of (3.4). It is known [11] that two points (u_1, v_1) and (u_2, v_2) on the curve (3.4) are associated if and only if the numbers

$$\frac{u_1 u_2 - v_1 v_2 D}{k} \qquad \text{and} \qquad \frac{v_1 u_2 - v_2 u_1}{k}$$

are both integers.

Among all solutions $x + y\sqrt{D}$ of (3.4) belonging to a given class, say C, we choose a solution $x^* + y^*\sqrt{D}$ in the following way. Let y^* be the least positive value of y which occurs in C and let x^* be a positive integer satisfying $x^{*2} - Dy^{*2} = k$. Then by the way y^* was chosen, at least one of

$x^* + y^*\sqrt{D}$ and $-x^* + y^*\sqrt{D}$ belongs to C and is called the *fundamental solution* of class C. Nagell in [11] showed the following.

Lemma 3.1. *Let $\epsilon_D = T + U\sqrt{D} > 1$ be the minimal unit in the ring $\mathbb{Z}[\sqrt{D}]$ and $x^* + y^*\sqrt{D}$ be the fundamental solution of the equation $x^2 - Dy^2 = k$ in a given class. We have*

$$0 < y^* < \frac{U}{\sqrt{2(T-1)}}\sqrt{|k|},$$

and

$$0 < |x^*| < \sqrt{\frac{(T-1)|k|}{2}}.$$

For a nonzero integer k, $\omega(k)$ denotes the number of distinct prime factors of k. Let $n(D, k)$ denote the number of classes of coprime solutions (x, y) to the quadratic equation $x^2 - Dy^2 = k$. Walsh in [16] showed (see Corollary 3.1 of [16]) that if k is square-free then

(3.6) $$n(D, k) \leq 2^{\omega(k)}.$$

4. Reduction to quartic Thue Equations

The idea of reducing the problem of counting integral points on elliptic curves to the problem of counting integral points of a finite number of quartic Thue equations is not new. Chapter 27 of [10] gives a complete overview of such reduction.

Throughout this section, D is a fixed positive square-free integer and k is a fixed negative integer. Let $(X, Y) \in \mathbb{Z}^2$ satisfy the equation $X^2 - DY^4 = k$, then $X + Y^2\sqrt{D}$ is a solution to equation (3.4) belonging to a certain class C of solutions. Let $x^* + y^*\sqrt{D}$ be the fundamental solution of C. Then

(4.1) $$X + Y^2\sqrt{D} = \left(x^* + y^*\sqrt{D}\right)\epsilon_D^i.$$

Set

$$s_2 + t_2\sqrt{D} = \left(x^* + y^*\sqrt{D}\right) \qquad \text{if } i \text{ is even,}$$

$$s_1 + t_1\sqrt{D} = \left(x^* + y^*\sqrt{D}\right)\epsilon_D \qquad \text{if } i \text{ is odd.}$$

Therefore, there exists a non-negative integer j, such that

(4.2) $$X + Y^2\sqrt{D} = \left(s + t\sqrt{D}\right)\epsilon_D^{2j},$$

where either $s + t\sqrt{D} = s_1 + t_1\sqrt{D}$ or $s + t\sqrt{D} = s_2 + t_2\sqrt{D}$. Let

$$m + n\sqrt{D} = \epsilon_D^j,$$

where $\epsilon_D = T + U\sqrt{D}$, with $T, U > 0$. Then we have

$$m^2 - Dn^2 = 1$$

and

$$Y^2 = tm^2 + 2smn + tDn^2.$$

Multiplying the above identity by t, completing the square, and using the fact that $s^2 - Dt^2 = k$, we obtain

(4.3) $$-(tm + sn)^2 + kn^2 + tY^2 = 0.$$

Walsh in [16] showed the following.

Lemma 4.1. *Let a, b, c be nonzero integers with $\gcd(a, b, c) = 1$, and such that the equation*

(4.4) $$ax^2 + by^2 + cz^2 = 0$$

has a solution in integers x, y and z not all zero. Then there are integers R_1, S_1, T_1, R_2, S_2, T_2, z_1, depnding only on a, b and c, satisfying the relations

$$R_1 T_2 + R_2 T_1 = 2 S_1 S_2,$$
$$S_2^2 - R_2 T_2 = -acz_1^2,$$
$$S_1^2 - R_1 T_1 = -bcz_1^2$$

and a nonzero integer δ, depending only on a, b, c, such that for every nonzero solution (x, y, z) of (4.4), there exist integers Q, u, v and a divisor P of δ, so that

$$\begin{aligned} Px &= Q(R_1 u^2 - 2 S_1 uv + T_1 v^2) \text{ and} \\ Py &= Q(R_2 u^2 - 2 S_2 uv + T_2 v^2). \end{aligned}$$

The integers R_1, R_2, T_1, T_2 satisfy $R_1 T_2 - R_2 T_1 = 0$.

Applying Lemma 4.1 to (4.3), with $a = -1$, $b = k$ and $c = t$, we conclude that there are integers R_1, S_1, T_1, R_2, S_2, T_2 and z_1, depending only on t and k, satisfying the relations

(4.5) $$S_2^2 - R_2 T_2 = tz_1^2,$$

(4.6) $$S_1^2 - R_1 T_1 = -ktz_1^2,$$

(4.7) $$R_1 T_2 + R_2 T_1 = 2 S_1 S_2.$$

and

(4.8) $$R_1 T_2 - R_2 T_1 = 0.$$

Also

(4.9) $$P(tm + sn) = Q(R_1 u^2 - 2 S_1 uv + T_1 v^2),$$
(4.10) $$Pn = Q(R_2 u^2 - 2 S_2 uv + T_2 v^2).$$

Therefore,

$$\frac{tm + sn}{n} = \frac{R_1 \left(\frac{u}{v}\right)^2 - 2S_1 \left(\frac{u}{v}\right) + T_1}{R_2 \left(\frac{u}{v}\right)^2 - 2S_2 \left(\frac{u}{v}\right) + T_2}$$

The above identity allows us to compute $\frac{u}{v}$ in terms of m and n, by solving a quadratic equation. We obtain $\frac{u}{v}$ is equal to one of the following two possible values:

$$\frac{S_1 - S_2 l \pm \sqrt{(S_1 - S_2 l)^2 - (R_1 - R_2 l)(T_1 - T_2 l)}}{R_1 - R_2 l},$$

where $l = t\frac{m}{n} + s$. The quantity under the square root in the above line can be simplified. Using (4.5), (4.6), (4.7) and (4.8), we have

$$(4.11) \qquad \frac{u}{v} = \frac{S_1 - S_2 \left(t\frac{m}{n} + s\right) \pm \sqrt{2t^2 z_1^2 \sqrt{D}(t\frac{m}{n} + s)}}{R_1 - R_2 \left(t\frac{m}{n} + s\right)}.$$

Now solving (4.9) and (4.10) for m and n and using the equation $m^2 - Dn^2 = 1$, it follows that

$$(4.12) \qquad A_1^2(u, v) - DA_2^2(u, v) = (Pt/Q)^2,$$

where

$$A_1(u, v) = (R_1 - sR_2) u^2 - 2(S_1 - sS_2)uv + (T_1 - sT_2) v^2$$

and

$$A_2(u, v) = R_2 tu^2 - 2S_2 tuv + T_2 tv^2.$$

We define

$$(4.13) \qquad \begin{aligned} F(u, v) \quad &= \quad a_0 u^4 + a_1 u^3 v + a_2 u^2 v^2 + a_3 uv^3 + a_4 v^4 \\ &:= \quad A_1^2(u, v) - DA_2^2(u, v) = (Pt/Q)^2. \end{aligned}$$

Therefore,

$$(4.14) \qquad \begin{aligned} a_0 \quad &= \quad R_1^2 - 2sR_1 R_2 + kR_2^2, \\ a_1 \quad &= \quad -4(R_1 S_1 - sR_1 S_2 - sR_2 S_1 + kR_2 S_2), \\ a_2 \quad &= \quad 6(R_1 T_1 - sR_2 T_1 - sR_1 T_2 + kR_2 T_2), \\ a_3 \quad &= \quad -4(S_1 T_1 - sS_1 T_2 - sS_2 T_1 + kS_2 T_2), \\ a_4 \quad &= \quad T_1^2 - 2sT_1 T_2 + kT_2^2. \end{aligned}$$

Notice that since m and n are relatively prime, from (4.9) and (4.10), we have $\gcd(u, v) = 1$ and we are only interested in the primitive solutions of the Thue equations in (4.13).

We claim that the roots of polynomial $F(Z, 1)$ are real. The roots of the polynomial $F(z, 1)$ are

$$\frac{S_1 - S_2 o \pm \sqrt{(S_1 - S_2 o)^2 - (R_1 - R_2 o)(T_1 - T_2 o)}}{R_1 - R_2 o}.$$

where $o = s + t\sqrt{D}$ or $o = s - t\sqrt{D}$. After routine simplification and using identities (4.5), (4.6), (4.7) and (4.8), we have

$$4\left(S_1 - S_2(s \pm t\sqrt{D})\right)^2$$
$$- 4\left(R_1 - R_2(s \pm t\sqrt{D})\right)\left(T_1 - T_2(s \pm t\sqrt{D})\right)$$
$$= 2t^2 z_1^2 \sqrt{D}(\pm s + t\sqrt{D}).$$

Since $s^2 - Dt^2 = k < 0$, both $s + t\sqrt{D}$ and $-s + t\sqrt{D}$ are positive. Therefore, $F(z, 1)$ has 4 real roots

(4.15)
$$\frac{S_1 - S_2(s \pm t\sqrt{D}) \pm \sqrt{2t^2 z_1^2 \sqrt{D}(\pm s + t\sqrt{D})}}{R_1 - R_2(s \pm t\sqrt{D})}.$$

Let $(u, v) \in \mathbb{Z}^2$ be a solution to our Thue equation that arises from a solution to the equation $X^4 - Dy^2 = k$. By (4.11) and since m and n are positive integers with $\left(\frac{m}{n}\right)^2 = D + \frac{1}{n^2}$, we conclude that in order to give a bound upon the number of solutions to $X^4 - Dy^2 = k$, we only need to count the number of solutions to the Thue equation $F(u, v) = \left(\frac{Pt}{Q}\right)^2$ that are associated to the following two real roots:

$$\frac{S_1 - S_2(s + t\sqrt{D}) \pm \sqrt{2t^2 z_1^2 \sqrt{D}(s + t\sqrt{D})}}{R_1 - R_2(s + t\sqrt{D})}.$$

5. Quartic Thue equations, proof of Theorems 1.1 and 1.3

In Section 4, we constructed at most 2 Thue equations for each fundamental solution of the equation $X^2 - DY^4 = k$ (see (4.2) and (4.1)). Let $F(u, v)$ be the quartic binary form with coefficients given in (4.14). We showed that $F(x, y)$ splits completely over $\mathbb{R}$ (see (4.15)). It turns out that $J_F = 0$.

Lemma 5.1. *Let $F(u, v)$ be the quartic binary form with coefficients given in (4.14). Then we conclude that*

$$J_F = 0 \text{ and } I_F = 48kt^3 T_2 R_2 z_1^2 D.$$

Proof. Walsh in [16] showed that $J_F = 0$. Here we will compute the value for invariant I. Recall that

$$I_F = 12a_0 a_4 - 3a_1 a_3 + a_2^2.$$

First we compute the value of each summand in the above summation, using (4.14) and relations (4.5), (4.6) and (4.7).

$$
\begin{aligned}
12a_0a_4 &= (R_1^2 - 2sR_1R_2 + kR_2^2)(T_1^2 - 2sT_1T_2 + kT_2^2) \\
&= 12(R_1^2T_1^2 - 2sR_1^2T_1T_2 + kR_1^2T_2^2 \\
&\quad -2sR_1R_2T_1^2 + 4s^2R_1R_2T_1T_2 - 2skR_1R_2T_2^2 \\
&\quad +kR_2^2T_1^2 - 2ksR_2^2T_1T_2 + k^2R_2^2T_2^2),
\end{aligned}
$$

$$
\begin{aligned}
-3a_1a_3 &= \\
&-48(R_1S_1 - sR_1S_2 - sR_2S_1 + kR_2S_2) \times \\
\times \quad &(S_1T_1 - sS_1T_2 - sS_2T_1 + kS_2T_2) \\
= \quad &-48\Big(R_1S_1^2T_1 - sR_1S_1^2T_2 - sR_1S_1S_2T_1 + kR_1S_1S_2T_2 \\
&-sR_1S_2S_1T_1 + s^2R_1S_2S_1T_2 + s^2R_1S_2^2T_1 - skR_1S_2^2T_2 \\
&-sR_2S_1^2T_1 + s^2R_2S_1^2T_2 + s^2R_2S_1S_2T_1 - skR_2S_1S_2T_2 \\
&+kR_2S_2S_1T_1 - ksR_2S_2S_1T_2 - ksR_2S_2^2T_1 + k^2R_2S_2^2T_2\Big),
\end{aligned}
$$

and

$$
\begin{aligned}
a_2^2 &= 36(R_1T_1 - sR_2T_1 - sR_1T_2 + kR_2T_2)^2 \\
&= 36(R_1^2T_1^2 + s^2R_2^2T_1^2 + s^2R_1^2T_2^2 + k^2R_2^2T_2^2 \\
&\quad -2sR_1R_2T_1^2 - 2sR_1^2T_1T_2 + 2kR_1R_2T_1T_2 \\
&\quad +2s^2R_1R_2T_1T_2 - 2skR_2^2T_1T_2 - 2kR_1T_2^2R_2).
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
I_F &= 96ksR_1T_2(S_2^2 - T_2R_2) + 96sR_2T_1(S_1^2 - R_1T_1) \\
&\quad -48k^2R_2T_2(S_2^2 - R_2T_2) - 48s^2R_2T_2(S_1^2 - R_1T_1) \\
&= 48kT_2(S_2^2 - R_2T_2)(2sR_1 - kR_2) \\
&\quad +48sR_2(S_1^2 - R_1T_1)(2T_1 - sT_2) \\
&= 48ktz_1^2T_2R_2(s^2 - k) \\
&= 48kt^3T_2R_2z_1^2D,
\end{aligned}
$$

where the last identity is because $s^2 - k = Dt^2$.   □

We recall some results for the number of solutions of the quartic Thue equations.

Proposition 5.1. *Let $\mathfrak{S}$ be the set of quartic forms $F(x,y) \in \mathbb{Z}[x,y]$ that are irreducible over $\mathbb{Q}$ with $I_F > 0$ and $J_F = 0$. Let $\mathfrak{N}$ be an upper bound for the number of solutions of quartic Thue equations*

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

as F varies over the elements of $\mathfrak{S}$*. Then for* $h \in \mathbb{N}$ *and* $G(x, y) \in \mathfrak{S}$*, the equation*

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

has at most

$$\mathfrak{N} \, 4^{\omega(h)}$$

primitive solutions.

Proof. This is essentially a special case of Bombieri and Schmidt's result in [3], where they showed that if N_n is an upper bound for the number of solutions to the equations $F(x, y) = 1$, as $F(x, y)$ varies over irreducible binary forms of degree n with integer coefficients then $N_n n^{\omega(h)}$ is an upper bound for the number of primitive solutions to $F(x, y) = h$. Bombieri and Schmidt proved this fact by reducing a given Thue equation $F(x, y) = h$ modulo every prime factor of the integer h. This reduction is explained in the proof of Lemma 7 of [3], where the form $F(x, y)$ of degree n is reduced to some other binary forms of degree n. These reduced forms are basically obtained through the action of 2×2 matrices with integer arrays and non-zero discriminant on the binary form $F(x, y)$. Since J is an invariant, a quartic form $G(x, y)$ with $J_F = 0$ will be reduced to some quartic forms with $J = 0$ under the action of 2×2 matrices. Also since $I_F > 0$ is an invariant of weight 4 (an even number), we will get forms with positive I under the action of 2×2 matrices with non-zero discriminant. $\square$

Proposition 5.2. *Let* $F(x, y) \in \mathbb{Z}[x, y]$ *be a quartic form with positive discriminant that is irreducible over* $\mathbb{Q}$ *and 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).*

Proof. This is Theorem 1.1 of [1]. $\square$

From Propositions 5.1 and 5.2, we conclude the following.

Corollary 5.1. *Let* $F(x, y) \in \mathbb{Z}[x, y]$ *be a quartic form with positive discriminant that is irreducible over* $\mathbb{Q}$ *and splits in* $\mathbb{R}$*. If* $J_F = 0$ *and h is a positive integer, then the Diophantine equation* $|F(x, y)| = h$ *possesses at most* $12.4^{\omega(h)}$ *primitive solutions (with* (x, y) *and* $(-x, -y)$ *regarded as the same).*

Lemma 5.1 and Corollary 5.1 imply that the Thue equation $F(u, v) = \frac{P^2 t^2}{Q^2}$, with coefficients given in (4.14), has at most $12.4^{\omega\left(\frac{P^2 t^2}{Q^2}\right)}$ primitive solutions. From the proof of Lemma 2.1 of [16] and equation (6.5) and the two unnumbered equations above (6.5) in [16], we have

$$|P| = |C|,$$

and $c_0 C^2 = t$, where C and c_0 are integers. Therefore, $P|t$ and $\omega(\frac{P^2 t^2}{Q^2}) \leq \omega(t)$. By Lemma 3.1 and the definition of t in (4.2), we have

$$(5.1) \qquad\qquad t \leq \epsilon_D^{3/2} \sqrt{|k|/2D}.$$

We have

$$\omega(\frac{P^2 t^2}{Q^2}) \leq \omega(t) < 2 + \log t / \log 4 \leq 2 + \frac{\log\left(\epsilon_D^{3/2}\sqrt{|k|/2D}\right)}{\log 4}.$$

Therefore, the Thue equation $F(u, v) = \frac{P^2 t^2}{Q^2}$, with coefficients given in (4.14), has at most $12.16.\epsilon_D^{3/2}\sqrt{|k|/2D}$ primitive solutions. This completes the proof of Theorem 1.1, as we have $2\,n(D, k)$ Thue equations $F(u, v) = \frac{P^2 t^2}{Q^2}$ (see (4.13)) associated to equation (1.3) and by (3.6), $n(D, k) \leq 2^{\omega(k)}$.

By (3.3), and since $|k| = N/D$, the following is an upper bound for the number of integer solutions of the equation (1.2):

$$\sum_{D|N} 384 . 2^{\omega(N/D)} \epsilon_D^{3/2} \sqrt{N/2D^2}$$

$$= \quad 384 \sqrt{N/2} \sum_{D|N} \frac{2^{\omega(N/D)} \epsilon_D^{3/2}}{D}.$$

This completes the proof of Theorem 1.3.

6. Proof of Theorem 1.2

In Section 4, we constructed at most 2 Thue equations for each fundamental solution of the equation $X^2 - DY^4 = k$ (see (4.2) and (4.1)).

Let $F(u, v)$ be the quartic binary form with coefficients given in (4.14). In Lemma 5.1, we showed that $J_F = 0$ and $I_F = 48kt^3 T_2 R_2 z_1^2 D$. Therefore we may apply Theorem 1.4 to the inequality $|F(u, v)| \leq \frac{P^2 t^2}{Q^2}$ by taking $\epsilon = \frac{1}{12}$. Then by Lemma 5.1, we have

$$I^{1/2-\epsilon} = I^{5/12} = 48^{5/12} k^{5/6} t^{5/4} D^{5/12} P^{5/6} y_1^{5/6} z_1^{5/6}.$$

Now we observe that

$$(6.1) \qquad h = \frac{P^2 t^2}{Q^2} \leq P^{5/6} t^{4/3} P^{7/6} t^{2/3} \leq P^{5/6} t^{4/3} t^{7/12} t^{2/3},$$

because Q is an integer. From (5.1),

$$t \leq \epsilon_D^{3/2} \sqrt{|k|/2D}.$$

We conclude that

$$h \leq P^{5/6} t^{4/3} t^{5/4} \leq P^{5/6} t^{5/4} \epsilon_D^2 (|k|/2D)^{2/3}.$$

In order to apply Theorem 1.4 to the inequality $|F(u,v)| < \frac{P^2 t^2}{Q^2}$, the following must hold.

$$h < \frac{\sqrt{3}\, I^{1/2}}{\pi}.$$

We claim that if we assume

$$|k| \geq \left(\frac{\pi}{\sqrt{3} \times 2^{2/3} 48^{5/12}}\right)^6 \frac{\epsilon_D^{12}}{D^{13/2}} = \frac{\pi}{2^{14} 3^{11/2}} \frac{\epsilon_D^{12}}{D^{13/2}}$$

then we have $h \leq \frac{\sqrt{3}\, I^{5/12}}{\pi}$. This is because under this assumption, we have

$$|k|^{1/6} \geq \epsilon_D^2 (1/2D)^{2/3} \frac{\pi}{\sqrt{3}} \frac{1}{48^{5/12} D^{5/12}},$$

which holds if

$$\epsilon_D^2 (|k|/2D)^{2/3} \leq \frac{\sqrt{3}}{\pi} 48^{5/12} k^{5/6} D^{5/12}.$$

This, together with (6.1), implies that

$$h \leq C^{5/6} t^{4/3} t^{7/12} t^{2/3} \leq \frac{\sqrt{3}\, I^{5/12}}{\pi}.$$

In (4.13), we got $2\, n(D,k)$ Thue equations $F(u,v) = \frac{P^2 t^2}{Q^2}$. The primitive solutions to these equations form a subset of the primitive solutions to the Thue inequalities $F(u,v) \leq \frac{P^2 t^2}{Q^2}$. Taking $\epsilon = \frac{1}{12}$ in Theorem 1.4, each of these inequalities has at most 20 primitive solutions. Therefore, we get at most $40\, n(D,k)$ primitive solutions. This, together with (3.6), completes the proof of Theorem 1.2.

7. The elliptic curve $Y^2 = X^3 + NX$

Let N be a square-free positive integer. An integer solution to the equation

$$Y^2 = X^3 + NX$$

gives rise to a positive integer solution (x,y) to the equation $x^2 - Dy^4 = \frac{N}{D}$, by taking

$$X = Dy^2, \text{ and } X^2 + N = Dx^2.$$

In the above change of variables D is the square-free part of X and $D \mid N$. Tzanakis in [15] showed the following.

Theorem 7.1. *Let D and k be positive integers which are not perfect squares. Then all integers solutions to the equation*

$$X^2 - Dy^4 = k$$

can be found by finding the integral solutions to a finite number of quartic Thue equations of the form

$$g(u,v) = B^2,$$

where the polynomial $g(Z,1)$ has exactly two real roots.

We remark that in Theorem 7.1, the fact that $g(Z,1)$ has exactly two real roots for every form g plays a very important role. Let g be irreducible. Then we may write

$$\text{Norm}(u - v\alpha) = B^2,$$

which is equivalent to a finite number of equations

(7.1) $$u - v\alpha = \beta u_1^m u_2^n,$$

where β runs through a finite set of algebraic integers in $\mathbb{Q}(\alpha)$ with

$$\text{Norm}(\beta) = B^2,$$

and u_1 and u_2 is a pair of fundamental units in some order of $\mathbb{Q}(\alpha)$. Equation (7.1) is an exponential equation in unknowns m and n and there are two equations relating them, which are obtained by equating the coefficients of α^2 and α^3 to 0 in $u_1^m u_2^n$. The p-adic method can be applied in this situation (see, for example, [15], [10] and [9]). One may attempt to diagonalize the binary form $g(u,v)$, so that

$$g(u,v) = \xi^4(u,v) - \eta^4(u,v).$$

As opposed to the case in which the binary form splits completely in $\mathbb{R}$, in this case, where $g(z,1)$ has 2 real roots and 2 non-real roots, both linear forms $\xi(u,v)$ and $\eta(u,v)$ have real coefficients and $\xi(u,v)$ and $\eta(u,v)$ are not complex conjugates. Therefore, results such as Lemma 2.4 and the concomitant gap principles will not work in this case and the method that we applied to count the number of integer points on $Y^2 = X^3 - NX$ cannot be used for the curve $Y^2 = X^3 + NX$.

References

[1] S. AKHTARI, *The method of Thue-Siegel for binary quartic forms*, Acta Arith. **141**, 1 (2010), 1–31.
[2] S. AKHTARI, *The representation of small integers by binary forms*, to appear.
[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*, Annals of Math. **117** (1983), 325–382.
[5] J. E. CREMONA, *Reduction of binary cubic and quartic forms*, LMS JMC **2** (1999), 62–92.
[6] J. H. EVERTSE AND J. H. SILVERMAN, *Uniform bounds for the number of solutions to $Y^n = f(x)$*, Math. Proc. Camb. Phil. Soc. **100** (1986), 237–248.
[7] H. A. HELFGOTT AND A. VENKATESH, *Integral points on elliptic curves and 3-torsion in class groups*, J. Amer. Math. Soc. **19**, 3 (2006), 527–550.
[8] H. W. LENSTRA, JR, *Solving the Pell equation*, Notices Amer. Math. Soc. **49** (2002), 182–192.
[9] D. J. LEWIS, *Diophantine equations: p-adic methods, Studies in Number Theory, M.A.A. Studies in Mathematics*, Math. Assoc. of America **6** (1969).
[10] L. J. MORDELL, *Diophantine Equations*, Academic Press, London, New York, (1969).
[11] T. NAGELL, *Introduction to Number Theory*, Chelsea, New York, (1964).
[12] W. M. SCHMIDT, *Integer points on curve on genus* 1, Compositio Math. **81** (1992), 33–59.
[13] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Springer-Verlag.

[14] A. THUE, *Berechnung aller Lösungen gewisser Gleichungen von der form $ax^r - by^r = f$*, Vid. Skrifter I Mat.-Naturv. Klasse (1918), 1–9.

[15] N. TZANAKIS, *On the Diophantine equation $x^2 - Dy^4 = k$*, Acta Arith. **46** (1986), 257–269.

[16] G. P. WALSH, *On the number of large integer points on elliptic curves*, Acta Arith. **138**, 4 (2009), 317–327.

Shabnam AKHTARI
Fenton Hall
University of Oregon
Eugene, OR 97403-1222 USA
E-mail: akhtari@uoregon.edu
URL: http://pages.uoregon.edu/akhtari