ON LARGE RATIONAL SOLUTIONS OF CUBIC THUE EQUATIONS: WHAT THUE DID TO PELL

JARROD ANTHONY CUNNINGHAM, NANCY HO, KAREN LOSTRITTO, JON ANTHONY MIDDLETON, AND NIKIA TENILLE THOMAS

Abstract. It is well-known that cubic Thue equations have finitely many integer points, and once one associates these equations with elliptic curves, then there exist algorithms to determine whether they have infinitely many rational points. In the case of infinitely many rational solutions, we explain how to explicitly find "large" rational points of a cubic Thue equation.

The paper proceeds as follows. First we exhibit a map from the cubic Thue equation C having a rational point of inflection to an elliptic curve of the form $E : y^2 = x^3 - D$, then prove that a "large" rational point on C maps to a rational point of "approximate" order 3 on E. Second, following an idea of Zagier, we compute rational points of "approximate" order 3 using continued fractions of elliptic logarithms. Third, we investigate how to modify the algorithm by considering homogeneous spaces when a rational point of inflection does not exist.

1. Introduction

For centuries, mathematicians have studied various methods of finding rational solutions to Diophantine equations. Such luminaries as Brahmagupta and Fermat have made significant contributions to the study of Pell's Equation: $u^2 - d\,v^2 = 1$, while another (none other than Euler!) named it after the wrong person. If $d > 0$, then it is known that Pell's Equation has infinitely many integral solutions.

The equation $C : u^3 - d\,v^3 = 1$ is called a cubic Thue equation. In a sense, it generalizes Pell's Equation. It is known that it has only finitely many integer solutions. However, depending on the value of d, it may have infinitely many *rational* solutions. The number of rational solutions of the cubic Thue equation is not the focus of this paper; there are several computer packages, including `apecs` and `mwrank`, that determine the set of those solutions. Our goal is to find an algorithm that produces large rational points on such a cubic Thue equation.

We explain the main results and approach. We consider nonsingular rational cubic curves of the form

$$C : au^3 + bu^2v + cuv^2 + dv^3 = m. \tag{1}$$

If C has a rational point of inflection, then we have a birational equivalence between C and an elliptic curve of the form $E : y^2 = x^3 - D$ for some nonzero rational

2000 *Mathematics Subject Classification.* Primary 33E05; Secondary 14H52, 11D59.

Key words and phrases. Pell's Equation, Thue Equation, Elliptic Curves, rational points, continued fractions, points of inflection.

The authors would like to thank the Summer Undergraduate Mathematical Sciences Research Institute (SUMSRI) at Miami University for the opportunity to conduct this research, with funding provided by the National Science Foundation and the National Security Agency.

number D. (If C does not have a rational point of inflection, we find a rational map from C to an isogeneous elliptic curve $E' : Y^2 = X^3 + 27\,D$.) An increasing sequence of rational points on C tends to a point of order three on E. Therefore, we exhibit an algorithm that can generate a sequence of points that tends to a point of order three on the elliptic curve.

This is done by using elliptic logarithms, following an idea of Zagier [Zag87] explained by Guy [Guy95]. Choose one rational point $P = (x, y)$ on the elliptic curve such that its y-coordinate is positive. We then compute the quotient of the elliptic logarithm of the point over the real period of E:

$$\frac{3}{2} \cdot \int_x^\infty \frac{d\xi}{\sqrt{\xi^3 - D}} \Bigg/ \int_{\sqrt[3]{D}}^\infty \frac{d\xi}{\sqrt{\xi^3 - D}} \tag{2}$$

By using continued fractions, we obtain successive convergents p/q of this quotient as a sequence of rational approximations. Choose the denominators q of this sequence such that numerators p are not divisible by 3. Then the multiple $[q]\,P$ approximates a point of order three on the elliptic curve, and by using the birational equivalence between C and E, we can translate each point calculated on the elliptic curve back onto the cubic Thue equation. Then we will have our desired sequence of large rational points.

2. Pell's Equation

In order to motivate our discussion of a generalization of Pell's equation, we first analyze the structure of the standard Pell's equation $u^2 - dv^2 = 1$.

2.1. **Algebraic Integers.** Fix a nonsquare $d \in \mathbb{Z}$. Then

$$u^2 - dv^2 = \left(u + v\sqrt{d}\right)\left(u - v\sqrt{d}\right). \tag{3}$$

Consider the ring of algebraic integers

$$\mathbb{Z}\big[\sqrt{d}\big] = \{a = u + v\sqrt{d}\;\big|\, u, v \in \mathbb{Z}\}. \tag{4}$$

Since we are interested in $u^2 - dv^2 = 1$, we want those elements a from the ring that are units. Denote $\bar{a} = u - v\sqrt{d}$ as the *conjugate of* a; and denote $\mathbb{N}(a) = a\bar{a} = u^2 - dv^2$ as the *norm of* a.

Lemma 2.1.1. *If d is not a square, then both the conjugate and the norm of a are well-defined.*

Proof. Let $a = u + v\sqrt{d}$ and $b = w + z\sqrt{d}$. Now, let $a = b$ but say either $u \neq w$ or $v \neq z$. We have

$$\begin{aligned} 0 &= a - b \\ 0 &= (u - w) + (v - z)\sqrt{d} \\ -(u - w) &= (v - z)\sqrt{d} \\ (u - w)^2 &= d(v - z)^2 \end{aligned} \tag{5}$$

Since d is not a perfect square, $d \neq 0$. For the equation to hold, it must be true that both $u \neq w$ and $v \neq z$. This implies that

$$d = \left(\frac{u - w}{v - z}\right)^2. \tag{6}$$

Here, d is a perfect square, but this contradicts our statement. We must have $u = w$ and $v = z$, which completes the proof. □

Example. Let $d = 1$. Then

$$\begin{aligned} a &= 4 + 0\sqrt{d} = 4 \\ b &= 3 + 1\sqrt{d} = 4 \end{aligned} \qquad \text{which implies that} \qquad \begin{aligned} \bar{a} &= 4 - 0\sqrt{d} = 4 \\ \bar{b} &= 3 - 1\sqrt{d} = 2. \end{aligned} \tag{7}$$

Hence the conjugate of a is not well-defined.

Consider the set

$$G = \left\{ a \in \mathbb{Z}\big[\sqrt{d}\big] \;\middle|\; \mathbb{N}(a) = 1 \right\} \subseteq \mathbb{C}^{\times}, \tag{8}$$

as contained in the set of nonzero complex numbers. It follows that if $a = u + v\sqrt{d} \in G$, then $u^2 - dv^2 = 1$. Note that G is an abelian group under multiplication: Since G is a subset of the complex numbers, the operation is both associative and commutative. Given two elements $a, b \in G$, we have

$$\mathbb{N}(a \cdot b) = \mathbb{N}(a) \cdot \mathbb{N}(b) = 1 \cdot 1 = 1, \tag{9}$$

so G is closed. The identity element of G is 1, and the inverse of any $a \in G$ is $\bar{a}$. Note that as a corollary, if we are given just one solution to Pell's equation, we can find other solutions by raising the given solution to some arbitrary integral power i.e. if $\mathbb{N}(a) = 1$ then $\mathbb{N}(a^n) = 1$ as well.

2.2. **The Fundamental Solution.**

Proposition 2.2.1. *Fix d and G as above, and assume d is positive. There exists a unique $\delta = u_1 + v_1\sqrt{d} \in G$, with $\delta > 1$, such that for each element $a = u + v\sqrt{d} \in G$ there exists $n \in \mathbb{Z}$ such that $a = \pm\delta^n$.*

Such a δ is called *the fundamental solution* of $u^2 - dv^2 = 1$.

Proof. We are motivated by LeVeque [LeV77]. Let $a = u + v\sqrt{d} \in G$. Consider the following identities:

$$\pm a = \pm\left(u + v\sqrt{d}\right) \text{ and } a^{\pm 1} = u \pm v\sqrt{d}. \tag{10}$$

It follows that we may assume u and v are nonnegative integers. If $a = 1$ we are done, so assume $a \neq 1$. Since the elements of G are real, let $\delta \in G$ be the smallest element such that $\delta > 1$. Then $1 < \delta \leq a$. Choose $n \in \mathbb{Z}$ in terms of the floor function as $n = \left\lfloor \frac{\log a}{\log \delta} \right\rfloor \geq 1$. This implies $\delta^n \leq a < \delta^{n+1}$. We multiply through by δ^{-n} and get $1 \leq a\,\delta^{-n} < \delta$. Denote $b = a\,\delta^{-n}$. Note that since G is a group, $b \in G$. Now by the minimality of δ, we must have $b = 1$. Thus $a = \delta^n$. □

Example. For $d = 2$, the fundamental solution to $u^2 - dv^2 = 1$ is $\delta = 3 + 2\sqrt{2}$ where $(u_1, v_1) = (3, 2)$. Some other fundamental solutions are listed below.

d	(u_1, v_1)	δ
3	$(2, 1)$	$2 + \sqrt{3}$
5	$(9, 4)$	$9 + 4\sqrt{5}$
6	$(5, 2)$	$5 + 2\sqrt{6}$

2.3. **Continued Fractions.** The fundamental solution of $u^2 - dv^2 = 1$ can be found using continued fractions. Again, we are motivated by the exposition in LeVeque [LeV77]. Given a real number x, define the sequence $x_{k+1} = 1/\left(x_k - \lfloor x_k \rfloor\right)$ in terms of the floor function, and beginning with $x_0 = x$. We define the continued fraction of x by

$$\lfloor x_0 \rfloor + \cfrac{1}{\lfloor x_1 \rfloor + \cfrac{1}{\lfloor x_2 \rfloor + \cfrac{1}{\lfloor x_3 \rfloor + \cdots}}}. \tag{11}$$

Denote $a_k = \lfloor x_k \rfloor$ as integers. We use the notation

$$\{a_0; a_1, a_2, a_3, \dots\} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} = a_0 + \frac{1}{a_1+}\,\frac{1}{a_2+}\,\frac{1}{a_3+}\cdots \tag{12}$$

to denote the continued fraction. For each nonnegative integer n, the quantity obtained by including n terms of the continued fraction

$$\{a_0; a_1, a_2, a_3, \dots, a_n\} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}} \tag{13}$$

is called the *nth convergent.* This is some rational number which we denote in lowest terms by u_n/v_n. Each convergent is an approximation of x, and the greater the number of terms that are included, the better the approximation.

It is well-known that the continued fraction of the square root of a squarefree integer is of the form

$$\sqrt{d} = \{a_0; \overline{a_1, a_2, ..., a_{h-1}, 2a_0}\} \tag{14}$$

where the bar means the sequence of terms repeats indefinitely. Let h denote the number of terms that repeat indefinitely. Consider the hth convergent:

$$\{a_0; a_1, a_2, ..., a_{h-1}\} = \frac{u_h}{v_h} \implies u_h^2 - dv_h^2 = (-1)^h. \tag{15}$$

We can use this to find the fundamental solution δ. The process in case h is odd is slightly different than if h is even. If h is even we have $u_h^2 - dv_h^2 = +1$, and so $\delta = u_h + v_h\sqrt{d}$. If h is odd we have $u_h^2 - dv_h^2 = -1$, and so $\delta = u_{2h} + v_{2h}\sqrt{d} = \left(u_h + v_h\sqrt{d}\right)^2$.

Examples. It is easy to compute that $\sqrt{6} = \{2;\ 2,\ 4,\ 2,\ 4, \dots\}$, so $h = 2$ is even. Then $\frac{u_2}{v_2} = \{2; 2\} = \frac{5}{2}$ so that $\delta = 5 + 2\sqrt{6}$. Also,

$$\sqrt{61} = \left\{7; \overline{1,\ 4,\ 3,\ 1,\ 2,\ 2,\ 1,\ 3,\ 4,\ 1,\ 14}\right\}. \tag{16}$$

where here $h = 11$ is odd. We have the convergent

$$\frac{u_{11}}{v_{11}} = \{7; 1, 4, 3, 1, 2, 2, 1, 3, 4, 1\} = \frac{29718}{3805}. \tag{17}$$

This satisfies $u_{11}^2 - 61\,v_{11}^2 = -1$, which is the wrong sign. On the other hand,

$$\frac{u_{22}}{v_{22}} = \{7; 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1\} = \frac{1766319049}{226153980}. \tag{18}$$

Hence the fundamental solution for $u^2 - 61\,v^2 = 1$ is

$$\delta = 1766319049 + 226153980\sqrt{61} = \left(29718 + 3805\sqrt{61}\right)^2. \tag{19}$$

Proposition 2.3.1. *Say $\delta = u_1 + v_1\sqrt{d}$ is a fundamental solution to $u^2 - dv^2 = 1$. Denote $\delta^n = u_n + v_n\sqrt{d}$ for $n = 0, 1, 2, \ldots$ As $n \longrightarrow \infty$ the sequences $u_n \longrightarrow \infty$ and $v_n \longrightarrow \infty$. Moreover, the ratio $\frac{u_n}{v_n} \longrightarrow \sqrt{d}$ as $n \longrightarrow \infty$.*

Proof. Since $\delta^n = u_n + v_n\sqrt{d}$ we have $\delta^{-n} = u_n - v_n\sqrt{d}$. By forming $\delta^n \pm \delta^{-n}$ we derive:

$$u_n = \frac{\delta^n + \delta^{-n}}{2} \qquad \text{and} \qquad v_n = \frac{\delta^n - \delta^{-n}}{2\sqrt{d}}. \tag{20}$$

Note that $\delta > 1$, but $0 < \delta^{-1} < 1$, so $\delta^n \longrightarrow \infty$ and $\delta^{-n} \longrightarrow 0$ as $n \longrightarrow \infty$. Hence $u_n, v_n \longrightarrow \infty$.

Since δ is the fundamental solution, we have $u_n^2 - dv_n^2 = 1$. Divide through by v_n^2 to find $\left(\frac{u_n}{v_n}\right)^2 - d = \frac{1}{v_n^2}$. As u_n and $v_n \longrightarrow \infty$ we have $\left(\frac{u_n}{v_n}\right)^2 - d \longrightarrow 0$. Thus $\frac{u_n}{v_n} \longrightarrow \sqrt{d}$. □

Example. Let $x = \sqrt{5} = 2.236067978$. We define a sequence of real numbers recursively by $x_0 = x$ and $x_{k+1} = 1/\left(x_k - \lfloor x_k \rfloor\right)$. Similarly, define a sequence of integers by $a_k = \lfloor x_k \rfloor$. We have

$$\begin{array}{lll} x_0 = 2.23607 & a_0 = 2 & \{a_0\} = 2 \\ x_1 = 4.23607 & a_1 = 4 & \{a_0; a_1\} = 9/4 = 2.25 \\ x_2 = 4.23607 & a_2 = 4 & \{a_0; a_1, a_2\} = 38/17 = 2.23529 \\ x_3 = 4.23607 & a_3 = 4 & \{a_0; a_1, a_2, a_3\} = 161/72 = 2.23611 \end{array} \tag{21}$$

Hence $\sqrt{5} = \{2;\, 4,\, 4,\, 4, \ldots\}$.

3. Cubic Thue Equations with Rational Points of Inflection

3.1. **Definitions.** In 1909, Axel Thue considered the equation

$$a_N u^N + a_{N-1} u^{N-1} v + a_{N-2} u^{N-2} v^2 + \ldots.. + a_0 v^N = m \tag{22}$$

in terms of integers $N \geq 3$, a_i, $m \neq 0$. He proved that this equation has only finitely many integer solutions whenever the homogeneous polynomial in u and v has no repeated (complex) roots; see Silverman and Tate [ST92] for the proof. We will consider $N = 3$; i.e. we study the following cubic equation:

$$C : \ au^3 + bu^2v + cuv^2 + dv^3 = m, \tag{23}$$

such that the discriminant

$$\text{Disc} = b^2c^2 - 4ac^3 - 4b^3d + 18abcd - 27a^2d^2 \tag{24}$$

is nonzero. In order to study rational solutions to this cubic equation, we will first focus on curves C that have a rational point of inflection. A *point of inflection* is a point (u_0, v_0) that satisfies the following two equations

$$\begin{aligned} a u_0^3 + b u_0^2 v_0 + c u_0 v_0^2 + d v_0^3 &= m \\ (b^2 - 3ac) u_0^2 + (bc - 9ad) u_0 v_0 + (c^2 - 3bd) v_0^2 &= 0 \end{aligned} \tag{25}$$

The cubic equation guarantees the point will be on the curve, and the quadratic equation guarantees the determinant of Hessian matrix of the cubic polynomial will vanish. We remark that as the quadratic equation has a rational root, the quantity $\sqrt{-3\,\mathrm{Disc}}$ will be an integer.

Example. Let $a = m = -1$ and $b = c = 0$. Then we have the system

$$u_0^3 - d\, v_0^3 = 1 \qquad \text{and} \qquad 9\, d\, u_0\, v_0 = 0, \tag{26}$$

so that we choose $(u_0, v_0) = (1, 0)$ as the point of inflection.

We will eventually show that if a curve C has a rational point of inflection, then it will be birationally equivalent to an elliptic curve. This equivalence will allow us to study the rational points on C.

3.2. **Elliptic Curves.** An elliptic curve is a projective variety associated to a cubic equation of the form

$$E : \, y^2 = x^3 + ax + b, \tag{27}$$

such that the discriminant $4a^3 + 27b^2$ is nonzero. More precisely,

$$E = \left\{ (X : Y : Z) \in \mathbb{P}^2 \;\middle|\; Y^2 Z = X^3 + aXZ^2 + bZ^3 \right\}, \tag{28}$$

where $x = X/Z$ and $y = Y/Z$ as expressed in projective coordinates. If a and b are integers, the collection $E(\mathbb{Q})$ of rational points (x, y) on an elliptic curve form a finitely generated abelian group, called the Mordell-Weil group. We explain how to define the group operation $\oplus$ on elliptic curves: Given two rational points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, we find the intersection of the cubic curve and the line defined by these two points. Denote this point as $P * Q$. Reflecting $P * Q$ over the x-axis will yield a point which we define as $P \oplus Q$. We can define the identity as $\mathcal{O} = (0 : 1 : 0)$, the "point at infinity." We also define the inverse of a point $P = (x, y)$ as $[-1]P = (x, -y)$. (Note that the line through P and $[-1]P$ will be vertical and can be said to intersect the curve at the "point at infinity" which is our identity.) Doubling a point involves drawing the tangent line to the point and then reflecting the point of intersection of this tangent line with the curve over the x-axis. The *torsion* subgroup $E(\mathbb{Q})_{tors}$ of an elliptic curve is the collection of points of finite order, and the *rank* of an elliptic curve is defined as the number of generators for the quotient $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$ (since it is a finitely generated free group). For more information, see Silverman and Tate [ST92]. (For more advanced reading, see Silverman [Sil86] and [Sil94].)

Proposition 3.2.1. *Assume that the cubic Thue equation C has a rational point of inflection (u_0, v_0). Define the rational substitution*

$$\begin{aligned} x &= 4m \frac{v_0(u-u_0) - u_0(v-v_0)}{(3au_0+bv_0)(u-u_0)+(bu_0+cv_0)(v-v_0)} w_0 \\ y &= 4m \frac{(3au_0+bv_0)(u+u_0)+(bu_0+cv_0)(v+v_0)}{(3au_0+bv_0)(u-u_0)+(bu_0+cv_0)(v-v_0)} \sqrt{-3\,Disc} \end{aligned} \tag{29}$$

where w_0 is a nonzero rational number satisfying $v_0 w_0 = b^2 - 3ac$. This substitution gives a birational transformation from C to $E : y^2 = x^3 - D$, where $D = -16m^2\,Disc$. Moreover, this transformation sends $(u_0, v_0) \mapsto \mathcal{O}$ on E.

Proof. This can be verified with the aid of a symbolic computer package. □

It is also important to note that the inverse transformation from E to C is

$$\begin{aligned} u &= u_0\,\frac{y+4\,m\sqrt{-3\,\mathrm{Disc}}}{y-4\,m\sqrt{-3\,\mathrm{Disc}}} + \frac{b\,u_0+c\,v_0}{w_0}\,\frac{2\sqrt{-3\,\mathrm{Disc}}\,x}{y-4\,m\sqrt{-3\,\mathrm{Disc}}} \\ v &= v_0\,\frac{y+4\,m\sqrt{-3\,\mathrm{Disc}}}{y-4\,m\sqrt{-3\,\mathrm{Disc}}} - \frac{3\,a\,u_0+b\,v_0}{w_0}\,\frac{2\sqrt{-3\,\mathrm{Disc}}\,x}{y-4\,m\sqrt{-3\,\mathrm{Disc}}} \end{aligned} \tag{30}$$

Example. We consider the curve $u^3 - dv^3 = 1$. Using the formula above, this curve transforms to the elliptic curve $E : y^2 = x^3 - 432d^2$. The equations for the transformation between (u, v) and (x, y) reduce to

$$\begin{aligned} u &= \frac{y+36d}{y-36d} \\ v &= \frac{6x}{y-36d} \end{aligned} \qquad \longleftrightarrow \qquad \begin{aligned} x &= 12d\,\frac{v}{u-1} \\ y &= 36d\,\frac{u+1}{u-1} \end{aligned} \tag{31}$$

Theorem 3.2.2. *Say the cubic Thue equation C has a rational point of inflection. Assume we have a sequence of rational points $\{(u_n, v_n)\}$ on C such that $|u_n|, |v_n| \longrightarrow \infty$ as $n \longrightarrow \infty$. This corresponds to a sequence of rational points $\{(x_n, y_n)\}$ on E such that*

$$(x_n, y_n) \longrightarrow \left(-4m \left(\frac{Disc}{m} \right)^{\frac{1}{3}}, 4m\sqrt{-3\,Disc} \right) \qquad as \qquad n \longrightarrow \infty. \tag{32}$$

Moreover, this limit is a point of order 3 on E.

Proof. According to (29) we have:

$$\begin{aligned} \frac{y_n}{4m\sqrt{-3\mathrm{Disc}}} &= \frac{(3\,a\,u_0+b\,v_0)\,(u_n+u_0)+(b\,u_0+c\,v_0)\,(v_n+v_0)}{(3\,a\,u_0+b\,v_0)\,(u_n-u_0)+(b\,u_0+c\,v_0)\,(v_n-v_0)} \\ &= \frac{(3\,a\,u_0+b\,v_0)\left(\frac{u_n}{v_n}+\frac{u_0}{v_n}\right)+(b\,u_0+c\,v_0)\left(1+\frac{v_0}{v_n}\right)}{(3\,a\,u_0+b\,v_0)\left(\frac{u_n}{v_n}+\frac{u_0}{v_n}\right)+(b\,u_0+c\,v_0)\left(1+\frac{v_0}{v_n}\right)} \end{aligned} \tag{33}$$

Dividing both sides of the Thue equation by v_n^3 gives us

$$a\left(\frac{u_n}{v_n}\right)^3 + b\left(\frac{u_n}{v_n}\right)^2 + c\left(\frac{u_n}{v_n}\right) + d = \frac{m}{v_n^3} \tag{34}$$

As $n \to \infty, |v_n| \to \infty$, so $\frac{u_n}{v_n}$ approaches a constant, say z. Therefore we see that:

$$\frac{y_n}{4m\sqrt{-3\mathrm{Disc}}} \longrightarrow \frac{(3\,a\,u_0 + b\,v_0)z + (b\,u_0 + c\,v_0)}{(3\,a\,u_0 + b\,v_0)z + (b\,u_0 + c\,v_0)} = 1, \tag{35}$$

and so $y_n \longrightarrow 4m\sqrt{-3\mathrm{Disc}}$. Plugging $4m\sqrt{-3\mathrm{Disc}}$ into the Weierstrass equation, with $D = -16m^2\,\mathrm{Disc}$, gives us the following:

$$\begin{aligned}(4m\sqrt{-3\mathrm{Disc}})^2 &= x^3 + 16m^2\mathrm{Disc}\\ x^3 &= 16m^2(-3\mathrm{Disc}) - 16m^2 Disc\\ x^3 &= -64m^2\mathrm{Disc}\\ x &= -4m^{\frac{2}{3}}\,(\mathrm{Disc})^{\frac{1}{3}}\\ x &= -4\frac{m}{m^{\frac{1}{3}}}\,(\mathrm{Disc})^{\frac{1}{3}}\\ x &= -4m\left(\frac{\mathrm{Disc}}{m}\right)^{\frac{1}{3}}.\end{aligned} \tag{36}$$

Therefore, as $n \to \infty$, the numbers $x_n \longrightarrow -4m\left(\frac{\mathrm{Disc}}{m}\right)^{\frac{1}{3}}$ and $y_n \longrightarrow 4m\sqrt{-3\,\mathrm{Disc}}$.

We will now show that this point is a point of order 3 on the elliptic curve. This point (x, y) has order 3 if x is a zero of the 3-division polynomial, i.e. $3x^4 + 6ax^2 + 12bx - a^2 = 0$. In our case, $a = 0$ and $b = 16m^2\,\mathrm{Disc}$. So we can see that $x = -4m\left(\frac{\mathrm{Disc}}{m}\right)^{\frac{1}{3}}$ is a root of the 3 division polynomial as follows:

$$\begin{aligned}&3x^4 + 6ax^2 + 12bx - a^2\\ &= 3\left[-4m\left(\frac{\mathrm{Disc}}{m}\right)^{\frac{1}{3}}\right]^4 + 12\cdot 16m^2\mathrm{Disc}\cdot\left[-4m\left(\frac{\mathrm{Disc}}{m}\right)^{\frac{1}{3}}\right]\\ &= 3\cdot 256\cdot m^4\cdot\frac{\mathrm{Disc}^{\frac{4}{3}}}{m^{\frac{4}{3}}} - 768m^3\cdot\frac{\mathrm{Disc}^{\frac{4}{3}}}{m^{\frac{1}{3}}}\\ &= 768m^{\frac{8}{3}}\,\mathrm{Disc}^{\frac{4}{3}} - 768m^{\frac{8}{3}}\,\mathrm{Disc}^{\frac{4}{3}}\\ &= 0.\end{aligned} \tag{37}$$

Therefore, the point $(x_\infty, y_\infty) = \left(-4m(\frac{\mathrm{Disc}}{m})^{\frac{1}{3}}, 4m\sqrt{-3\mathrm{Disc}}\right)$ is a point of order 3 on E. □

3.3. **Finding Large Rational Solutions.** The following is a special case of the result in Silverman [Sil94, Corollary 2.3.1, pg. 420]. We give the proof since it will be relevant to our algorithm.

Theorem 3.3.1. *Assume that we have the elliptic curve $E : y^2 = x^3 - D$, for some nonzero $D \in \mathbb{Z}$. There exists a group isomorphism $\Psi : E(\mathbb{R}) \longrightarrow \mathbb{R}/\mathbb{Z}$ defined by*

$$(x, y) \mapsto \pm\cdot\frac{1}{2\Omega_E}\int_x^\infty \frac{d\xi}{\sqrt{\xi^3 - D}} \pmod{\mathbb{Z}} \tag{38}$$

with the ± 1 sign chosen so that $y = \pm|y|$. Here,

$$\Omega_E = \int_{\sqrt[3]{D}}^\infty \frac{d\xi}{\sqrt{\xi^3 - D}} \tag{39}$$

is the real period of the elliptic curve.

Proof. Denote the roots of $\xi^3 - D = 0$ by e_1, e_2, and e_3; and define the complex numbers

$$\omega_1 = 2 \int_{e_1}^{\infty} \frac{d\xi}{\sqrt{\xi^3 - D}} \quad \text{and} \quad \omega_2 = 2 \int_{e_2}^{e_3} \frac{d\xi}{\sqrt{\xi^3 - D}}. \tag{40}$$

We consider $\Lambda_E = \{m\,\omega_1 + n\,\omega_2 \,|\, m,\, n \in \mathbb{Z}\}$ as a lattice in $\mathbb{C}$. It is well-known that the map $E(\mathbb{C}) \to \mathbb{C}/\Lambda_E$ defined by

$$(x, y) \mapsto \varepsilon \int_{x}^{\infty} \frac{d\xi}{\sqrt{\xi^3 - D}} \pmod{\Lambda_E} \tag{41}$$

is an isomorphism of Lie groups, where $\varepsilon \in \mathbb{C}^\times$ is chosen such that $y = \varepsilon\,|y|$. (If $y = 0$ we may choose $\varepsilon = 1$.) Hence we have an isomorphism $E(\mathbb{R}) \to \mathbb{R}/\left(\Lambda_E \cap \mathbb{R}\right)$. If we denote $e_1 = \sqrt[3]{D}$ as the real root, then $\omega_1 = 2\,\Omega_E \in \mathbb{R}$ while ω_2 is purely imaginary, so that $\Lambda_E \cap \mathbb{R} = 2\,\Omega_E\,\mathbb{Z}$. Hence the composition $\Psi : E(\mathbb{R}) \to \mathbb{R}/2\,\Omega_E\,\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ is an isomorphism of Lie groups. □

Corollary 3.3.2. *Assume C is a cubic Thue equation which has a rational point of inflection, so that C is (birationally equivalent to) an elliptic curve. If C has positive rank, then there exists a sequence of rational points $\{(u_n, v_n)\}$ such that $|u_n|, |v_n| \longrightarrow \infty$ as $n \longrightarrow \infty$.*

Proof. We use an idea following Guy [Guy95], which in turn is motivated by a paper of Zagier [Zag87]. Assume C has positive rank, and let $P = (x_1, y_1)$ be a point of infinite order. Define

$$\gamma = \frac{1}{\Omega_E} \int_{x_1}^{\infty} \frac{d\xi}{\sqrt{\xi^3 - D}}, \qquad \text{with} \qquad D = -16m^2 \text{Disc}. \tag{42}$$

Using continued fractions, find a sequence of convergents

$$\frac{p_n}{q_n} \approx \frac{3}{2}\gamma \quad \text{for} \quad n = 1, 2, 3... \tag{43}$$

Define $(x_n, y_n) = [q_n](x_1, y_1)$. This point has "approximate" order 3:

$$\begin{aligned} \psi([3](x_n, y_n)) &= \psi([3q_n](x_1, y_1)) = 3q_n\,\psi(x_1, y_1) \\ &\equiv \text{sign}(y) \cdot 3q_n \cdot \frac{\gamma}{2} \pmod{\mathbb{Z}} \\ &\approx \pm p_n \pmod{\mathbb{Z}} \\ &\equiv 0 \pmod{\mathbb{Z}} \end{aligned} \tag{44}$$

Hence, since ψ is an isomorphism, (x_n, y_n) is "approximately" a point of order 3 on E, so the corresponding point (u_n, v_n) on C has large rational coefficients. □

Example. We start with the Thue equation where $a = m = -1$, $b = c = 0$, and $d = 7$, which gives us $u^3 - 7\,v^3 = 1$. We wish to transform this curve to an elliptic curve. We find $D = -16 \cdot 1^2 \cdot \text{Disc} = 21168$ so the corresponding elliptic curve is $y^2 = x^3 - 21168$. We now implement the algorithm explained above to find a point of order 3 on this elliptic curve, which transforms to a large rational point on the cubic. Using a program such as `mwrank`, we determine that this elliptic curve has rank 1 with the generator $(84, 756)$. We compute $\frac{3}{2}\gamma = 0.7106994116$, find the convergents $\frac{p}{q}$ of the corresponding continued fraction, and multiply the generator by q – assuming that p is not divisible by three. Finally we use the transformation given above in (30) to find large rational points (u, v) satisfying $u^3 - 7\,v^3 = 1$. We construct the following table:

$[q]$	$[q]\,(x, y)$	(u, v)	$\frac{u}{v}$
3	$(57, -405)$	$(4.2941, 2.2353)$	1.921052631
7	$(42.0481, -230.5966)$	$(-22.5476, -11.7873)$	1.912875562
121	$(43.4989, -247.2625)$	$(-105.3857, -55.0912)$	1.912930638
159	$(44.0055, -253.0765)$	$(469.1832, 245.2693)$	1.912931189

Our sequence on the elliptic curve should approach the point of order 3, namely the point $\left(-4m(\frac{\text{Disc}}{m})^{\frac{1}{3}}, 4m\sqrt{-3\text{Disc}}\right)$, where Disc$= -1323$ and $m = -1$. This point has the numerical value $(4\cdot(1323^{\frac{1}{3}}),\ -252) = (43.91166852,\ -252)$, and we see that as q gets larger, we obtain a better approximation for this point. We also see that $|u|$, $|v|$ are also getting larger as q gets larger, and that the ratio $\frac{u}{v}$ approximates $\sqrt[3]{7} = 1.912931183$.

In order for this algorithm to work, it is imperative that the rank of the elliptic curve is positive since a positive rank implies that we can find an infinite sequence of points on the elliptic curve and a corresponding sequence on the cubic. For d from 1 to 1000, it was found that the rank of the curve $y^2 = x^3 - 432d^2$ was positive for about 63% of the curves. See the appendix for the empirical evidence.

4. Cubic Thue Equations without Rational Points of Inflection

4.1. **Homogeneous Spaces and Isogeneous Curves.**

Given a cubic Thue equation

$$C:\ au^3 + bu^2v + cuv^2 + dv^3 = m \tag{45}$$

with arbitrary integers a, b, c, d, it is usually the case that C does not have a rational point of inflection. This is so if $\sqrt{-3\,\text{Disc}}$ is not an integer. (In fact, if a cubic C with a nonzero discriminant is chosen "at random" it seems that there is a mere 0.16% chance of the cubic having a rational point of inflection. See appendix for some empirical evidence.) In general, one does not expect C to be birationally equivalent to an elliptic curve. However, we demonstrate the relation between C and E.

Theorem 4.1.1. *Let C be a cubic Thue equation. Then there exists a rational map $C \to E'$ to the elliptic curve*

$$E':\ Y^2 = X^3 - D', \qquad \textit{where} \quad D' = -27D \tag{46}$$

such that E' is 3-isogeneous to the elliptic curve

$$E:\ y^2 = x^3 - D, \qquad \textit{where} \quad D = -16m^2\,\textit{Disc.} \tag{47}$$

Proof. Given a rational point (u, v) on C, denote

$$\begin{aligned} X &= 4\left[\left(b^2 - 3\,a\,c\right)u^2 + \left(b\,c - 9\,a\,d\right)u\,v + \left(c^2 - 3\,b\,d\right)v^2\right] \\ Y &= 4\left[\left(2\,b^3 - 9\,a\,b\,c + 27\,a^2\,d\right)u^3 + 3\left(b^2\,c - 6\,a\,c^2 + 9\,a\,b\,d\right)u^2\,v\right. \\ &\qquad \left. -3\left(b\,c^2 - 6\,b^2\,d + 9\,a\,c\,d\right)u\,v^2 - \left(2\,c^3 - 9\,b\,c\,d + 27\,a\,d^2\right)v^3\right]. \end{aligned} \tag{48}$$

One checks that $Y^2 = X^3 - D'$ where

$$D' = 432\,m^2\,\text{Disc} = -27\,(-16\,m^2\,\text{Disc}) = -27D. \tag{49}$$

These formulas may be found in Silverman [Sil82].

We have a map from $E : y^2 = x^3 - D$ to $E' : Y^2 = X^3 - D'$ defined by

$$\left.\begin{aligned} X &= \frac{x^3 - 4\,D}{x^2} \\ Y &= \frac{x^3 + 8\,D}{x^3}\,y \end{aligned}\right\} \quad \text{with dual map} \quad \left\{\begin{aligned} x &= \frac{1}{9}\,\frac{X^3 - 4\,D'}{X^3} \\ y &= \frac{1}{27}\,\frac{X^3 + 8\,D'}{X^3}\,Y \end{aligned}\right. \tag{50}$$

These are not linear substitutions. The composition of the map $\psi : E \to E'$ and its dual map $\widehat{\psi} : E' \to E$ yields $\widehat{\psi} \circ \psi = [3]$ as the "multiplication-by-3" map on E. We see that E and E' are isogeneous elliptic curves and ψ is an isogeny of degree 3. □

Examples. Consider the Thue equation $2\,u^3 + 9\,u^2\,v + 13\,u\,v^2 + 6\,v^3 = 2$. Here, a trivial solution is $(1, 0)$. Since Disc $= 1$, this implies that $\sqrt{-3\,\text{Disc}}$ is not rational. Therefore, this Thue equation has no rational points of inflection. However, the equation is "isogenous" to the elliptic curve $E' : Y^2 = X^3 - D'$ where $D' = 432\,m^2 = 1728$. In this case, the group of rational points on E' consists of 2-torsion, with generator $(X, Y) = (12, 0)$:

$$E'(\mathbb{Q}) = \{(12, 0),\, \mathcal{O}\} \simeq \mathbb{Z}/2\,\mathbb{Z}. \tag{51}$$

The isogenous curve is $E : y^2 = x^3 - D$ where $D = -16\,m^2 = -64$. The group of rational points on this curve consists of 6-torsion, with all six rational points generated by $(x, y) = (8, 24)$:

$$E(\mathbb{Q}) = \left\{ [n]\,(8, 24) \,\middle|\, n \in \mathbb{Z} \right\} \simeq \mathbb{Z}/6\mathbb{Z}\,. \tag{52}$$

From the above map ψ of our isogeny, $(8, 24)$ on E maps to $(12, 0)$ on E'. Under the dual map $\widehat{\psi}$, the torsion point $(12, 0)$ maps to $(-4, 0) = [3]\,(8, 24)$. Since $E : y^2 = x^3 + 64$ has finitely many rational points, $C : 2\,u^3 + 9\,u^2\,v + 13\,u\,v^2 + 6\,v^3 = 2$ will have finitely many as well. Therefore, we are unable to construct a sequence of rational points tending to $\mathcal{O}$.

We will now consider the curve $C : 2u^3 + 9u^2v + 13uv^2 + 6v^3 = 6$. Again, this curve does not have a rational point of inflection so it is not birationally equivalent to an elliptic curve. However, it will be "isogenous" to the elliptic curve

$$E' : Y^2 = X^3 - D', \qquad \text{where} \quad D' = 432m^2\,\text{Disc} = 15552. \tag{53}$$

Using `mwrank`, we determine that E' has rank 1 with generator $(X, Y) = (28, 80)$. Our goal is to use E' to find rational points on C. The transformation from C to E' given above will simplify to the following transformation when $a = 2, b = 9, c = 13, d = 6, m = 6$:

$$X = 4(3u^2 + 9uv + 7v^2), \qquad Y = -4v(3u + 4v)(3u + 5v). \tag{54}$$

Substituting $X = 28$ and $Y = 80$ into the transformations, we can use `Maple` to solve for points (u, v) which satisfy these equations and are on the curve C. We obtain the set $\{(-8, 5),\, (3, -1),\, (5, -4)\}$.

We explain the relationship between the rational maps above and points of inflection on the cubic Thue equation.

Corollary 4.1.2. *Say C has a rational point of inflection (u_0, v_0). Under the rational map above, this corresponds to a point $(0, 12m\sqrt{-3Disc})$ on E', and this point in turn is in the kernel of the dual isogeny $\widehat{\psi} : E' \to E$.*

Proof. First we prove that a rational point of inflection on C will correspond to $(0, 12m\sqrt{-3\text{Disc}})$ on E'. We substitute the x-coordinate of the point of inflection (u_0, v_0) into our X transformation to yield:

$$X = 4[(b^2 - 3ac)u_0^2 + (bc - 9ad)u_0v_0 + (c^2 - 3bd)v_0^2] = 0. \tag{55}$$

We now substitute $X = 0$ into $E' : Y^2 = X^3 - 432m^2\text{Disc}$ and solve for Y:

$$Y^2 = -432m^2\text{Disc} \implies Y = \sqrt{-432m^2\text{Disc}} = 12m\sqrt{-3\text{Disc}}. \tag{56}$$

So our point of inflection on C maps to $(0, 12m\sqrt{-3\text{Disc}})$.

To say the point $\left(0, 12m\sqrt{-3\text{Disc}}\right)$ is in the kernel of the dual isogeny from E' to E means that this point is mapped to the “point at infinity.” Using the formulas in equation (50) we see that $X = 0$ maps to $\mathcal{O}$ on E. Hence $\left(0, 12m\sqrt{-3\,\text{Disc}}\right)$ is in the kernel of the dual isogeny as desired. □

4.2. **Finding Large Rational Solutions.** Continue the notation as above. We explain how to compute a sequence of large rational points on a cubic Thue equation which does not necessarily have a rational point of inflection.

Corollary 4.2.1. *If C is a sequence of rational points (u_n, v_n) that tend to infinity, then this sequence maps to a sequence of points (X_n, Y_n) that tend to infinity on E'.*

Proof. First we prove that as $|u_n|$, $|v_n|$ go to infinity, $|X_n|$ also goes to infinity:

$$\begin{aligned} X_n &= 4\left[(b^2 - 3ac)u_n^2 + (bc - 9ad)u_nv_n + (c^2 - 3bd)v_n^2\right] \\ \frac{X_n}{v_n^2} &= 4\left[(b^2 - 3ac)(\frac{u_n}{v_n})^2 + (bc - 9ad)\frac{u_n}{v_n} + (c^2 - 3bd)\right]. \end{aligned} \tag{57}$$

As $n \longrightarrow \infty$, $\frac{u_n}{v_n}$ approaches a constant. (Recall the proof of Corollary 3.2.2.) Therefore, looking at the above equation $\frac{X_n}{v_n^2}$ must also approach a constant. Because $|v_n| \to \infty$, $|X_n| \to \infty$ as well. We will now do a similar proof to show that as $|u_n|$, $|v_n| \to \infty$, the number $|Y_n| \to \infty$:

$$\begin{aligned} \frac{Y_n}{v_n^3} = 4\Bigg[&(2b^3 - 9abc + 27a^2d)(\frac{u_n}{v_n})^3 + 3(b^2c - 6ac^2 + 9abd)(\frac{u_n}{v_n})^2 \\ &-3(bc^2 - 6b^2d + 9acd)(\frac{u_n}{v_n}) - (2c^3 - 9bcd + 27ad^2)\Bigg] \end{aligned} \tag{58}$$

Hence $|Y_n| \to \infty$ as well. □

Example. We will now use the cubic curve

$$C : 2u^3 + 9u^2v + 13uv^2 + 6v^3 = 6. \tag{59}$$

As we stated above, this curve is isogenous to the curve $Y^2 = X^3 - 15552$ which has rank 1 and generator $(28, 80)$. We will use E' to find large rational points on C. Looking at the transformations given above, we see that a large rational point (X, Y) will be the image of a large rational point (u, v). Looking at the transformations, we see that a large point (u, v) will map to a large (X, Y). We can therefore use our algorithm given above to find large rational points on E' and then find the corresponding points on C. As explained above in the proof of Theorem 3.3.2, we calculate $\frac{3}{2}\gamma$ and find the continued fraction, convergents, and q such that

p is not divisible by three. We know, from example above, that multiplying our generator by $q = 4$ will give an approximate point of order 3. Therefore to find a large rational point, we multiply our generator by $q = 12$ to obtain

$$\begin{aligned} X &\approx 7215.4351885546712061806 29850, \\ Y &\approx 612905.8775557362715732618242. \end{aligned} \tag{60}$$

Substituting these values into the transformations, we find the following set (u, v) which also satisfy the cubic equation:

$$\{(42.48017, -42.47684), \quad (-127.41723, 84.94371), \quad (84.93706, -42.46686)\}. \tag{61}$$

5. Appendix

5.1. **Table of Ranks and Torsion Subgroups.** We consider the Mordell-Weil group of the elliptic curve $y^2 = x^3 - 432d^2$. The tables below contain $1 \le d \le 1000$. The rank was computed using `mwrank`, and the torsion subgroup was computed using `Maple`. We place an asterisk (*) next to the number where the rank listed is only the lower bound as determined by `mwrank`. Note that 32.4% have rank 0; 47.3% have rank 1; 14.9% have rank 2; and 0.9% have rank 3. (We could not determine the exact value of the ranks for 4.6% of the curves below, only bounds.)

Table 1. Ranks of $y^2 = x^3 - 432d^2$

Rank	Torsion	d
0	$\{\mathcal{O}\}$	3, 4, 5, 10, 11, 14, 16, 21, 23, 24, 25, 29, 32, 36, 38, 39, 40, 41*, 44, 45, 46, 47, 52, 55, 57, 59*, 60, 66, 73, 74, 76, 77, 80, 81, 82, 83, 88, 93, 95, 99, 100, 101*, 102, 108, 109, 111, 112, 113, 116*, 118, 119, 121, 122*, 129*, 131*, 135, 137*, 138, 144, 145, 146, 147, 148, 149, 150, 154, 155, 158*, 165, 167, 168, 173, 174, 175, 181, 184, 185*, 188, 190, 191, 192, 194, 196, 199, 200, 204, 207*, 220, 221, 225, 226*, 227, 230, 232, 234, 235*, 237, 239, 242*, 245, 249*, 252, 253, 255, 256, 257, 260, 261, 262*, 263*, 266, 268, 270, 276, 281, 288, 290, 291, 292, 293, 297, 298*, 299, 300, 302*, 304, 307, 311*, 312, 315, 317, 318, 320, 326*, 327, 328*, 329, 332*, 334, 338, 340, 346*, 347*, 350, 352, 353*, 354, 360, 361, 362, 364, 365, 368, 369, 371, 374, 375, 376, 378, 381*, 382*, 383*, 389*, 393*, 398, 401*, 404, 406, 410, 412, 415, 416, 417*, 419, 423*, 426, 434, 437*, 440, 442, 443*, 445*, 451, 454*, 455, 456, 461, 470, 471, 472*, 473, 475, 476, 478, 479, 480, 482, 486, 487, 489*, 491*, 492, 500, 505, 507*, 508, 509*, 514, 515*, 517*, 518, 527, 528, 529*, 531, 533, 534, 541, 542, 543*, 545*, 551, 556*, 558, 561, 563*, 564, 567, 569*, 570,

Rank	Torsion	d
		575, 577, 580, 584, 585, 586*, 587, 591*, 592, 595, 597, 599, 606*, 608, 613, 616, 617*, 620, 621, 622, 623, 625, 626, 633, 634*, 636, 640, 641*, 642, 648, 649, 652, 653, 656, 659, 661*, 662*, 664, 666, 667, 669, 675, 677*, 678, 684, 685, 687, 689, 692*, 693, 694*, 695, 697*, 698, 703, 704, 705, 707, 708, 722, 723, 724*, 725*, 726, 731, 734, 739*, 741, 743, 744, 747, 749, 757, 758, 759, 760, 761, 764, 766*, 767, 770, 772, 774, 777, 778*, 779, 780, 783, 785, 788*, 792, 795*, 796*, 797, 800, 801, 802, 803, 806, 807*, 808*, 811, 815, 816, 821, 822, 830, 831, 833*, 836, 838, 839*, 841*, 842*, 844*, 849, 850*, 852, 857*, 858, 864, 865, 868, 869, 872, 878, 879*, 882, 887, 888, 893, 894, 895*, 896, 902, 904, 908, 909*, 910, 911, 913*, 914, 921, 923, 925, 928*, 929, 938, 939*, 941*, 944, 947, 948*, 952, 955*, 959, 963, 965, 968, 972, 974*, 976*, 977*, 980, 982, 983*, 985*, 986, 990, 991*, 993, 996
0	$\mathbb{Z}/2\mathbb{Z}$	2, 16, 54, 128, 250, 432, 686
0	$\mathbb{Z}/3\mathbb{Z}$	1, 8, 27, 64, 125, 216, 343, 512, 729, 1000
1	$\{\mathcal{O}\}$	6, 7, 9, 12, 13, 15, 17, 20, 22, 26, 28, 31, 33, 34, 35, 42, 43, 48, 49, 50, 51, 53, 56, 58, 61, 62, 63, 67, 68, 69, 70, 71, 72, 75, 78, 79, 84, 85, 87, 89, 90, 92, 94, 96, 97, 98, 103, 104, 105, 106, 107, 114, 115, 117, 120, 123, 130, 133, 134, 136, 139, 140, 141, 142, 143, 151, 156, 157, 158, 160, 161, 162, 164, 166, 169, 170, 171, 172, 176, 177, 178, 179, 180, 186, 187, 189, 193, 195, 197, 198, 202, 205, 206, 208, 211, 212, 213, 214, 215, 222, 223, 224, 228, 229, 231, 233, 236, 238, 241, 243, 244, 247, 248, 251, 258, 259, 264, 265, 267, 269, 272, 274, 275, 277, 278, 279, 280, 283, 284, 285, 286, 287, 289, 294, 295, 301, 303, 305, 306, 308, 310, 313, 314, 316, 319, 321, 322, 323, 324, 325, 330, 331, 333, 336, 337, 339*, 341, 344, 349, 351, 355, 356, 357, 358, 359, 363, 366, 367, 372, 373, 377, 380, 384, 385, 386, 387, 388, 391, 392, 394, 395, 396, 400, 402, 403, 405, 408, 409, 411, 413, 414, 418, 421, 422, 424, 425, 427, 428*, 429, 430, 431*, 438, 439, 441, 444, 447*,448, 449, 450, 452, 457, 458, 459, 460, 463, 464, 465, 466, 467, 474, 481, 483, 484, 485, 488, 490, 493, 494, 495, 496,

Rank	Torsion	d
		499, 501, 502, 503, 504, 510, 511, 516, 519, 521, 522, 524, 525, 526, 530, 532, 535, 536, 537, 538, 539, 540, 544, 546, 547*, 549, 550, 552, 553, 555, 557, 560, 562, 565, 566, 568, 571, 572, 573*, 574, 576, 578, 582, 583, 588, 589, 593, 594, 596, 598, 600, 601, 602, 603, 604, 605, 607, 609, 610, 611, 612, 618, 619, 624, 627, 629, 630, 632, 637, 638, 643, 644, 645, 646, 647, 650, 654, 655, 660, 663, 665, 668, 670, 672, 673, 674, 676, 679, 680, 681, 682, 683, 690, 691, 696, 699, 700, 701, 702, 706, 709, 710, 711, 712, 715, 716, 717, 718*, 719, 720, 727, 732, 733, 735, 736, 737, 738, 740, 742, 745, 746, 748, 750, 751, 752, 753*, 754, 755, 756, 762, 763, 765, 768, 769, 771, 773, 775, 776, 781, 782, 784, 787, 789, 790, 791, 798, 799, 804, 805, 809, 812, 814, 817, 818, 819, 820, 823, 824, 826, 827, 828, 832, 834, 835, 837, 840, 845, 846, 847, 848, 853, 856, 859, 860, 861, 862, 863, 867, 870, 871, 873, 875, 876, 877*, 881, 884, 886*, 889, 890, 891, 892, 897, 898, 899, 900, 906, 907, 912, 915, 917, 918, 920, 922, 926, 927, 931, 932, 933*, 936, 942, 943, 945, 949, 950, 951, 953, 954, 956, 958, 960, 961, 962, 964, 967, 969, 970, 971, 975, 978, 979, 981, 984, 987, 989, 994, 997, 998
2	$\{\mathcal{O}\}$	19, 30, 37, 65, 86, 91, 110, 124, 126, 127, 132, 152, 153, 163, 182, 183, 201, 203, 209, 210, 217, 218, 219, 240, 246, 254, 271, 273, 282, 296, 309, 335, 342, 345, 348, 370, 379, 390, 397, 399, 407, 420, 433, 435, 436, 446, 453, 462, 468, 469, 477, 497, 498, 506, 513, 520, 523, 554, 559, 579, 581, 590, 614, 615, 628, 631, 635, 639, 651, 658, 671, 688, 713, 714, 721, 728, 730, 786, 793, 794, 810, 813, 825, 829, 851, 855, 866, 874, 880, 883, 885, 901, 903, 905, 916, 919, 924, 930, 937, 940, 946, 957, 966, 973, 988, 992, 995, 999
3	$\{\mathcal{O}\}$	657, 854

5.2. **Cubic Thue Equations with Rational Points of Inflection.** We consider a list of integers a, b, c, and d such that $|a|$, $|b|$, $|c|$, $|d| \leq 5$, $gcd(a,b,c,d) = 1$, and $\text{Disc} = b^2c^2 - 4ac^3 - 4b^3d + 18abcd - 27a^2d^2 \neq 0$. We express the projective cubic curve

$$a\,U^3 + b\,U^2\,V + c\,U\,V^2 + d\,V^3 = m\,W^3. \tag{62}$$

in the form $(a, b, c, d; m)$. (The curves in the list below may be birationally equivalent to others in the list.) We use Maple and apecs to compute the rank and the generators; such points are expressed projectively as $(U : V : W)$.

Note that 3.76% of such integers a, b, c, d appear in the table below i.e. in the range $|a|$, $|b|$, $|c|$, $|d| \leq 5$, there is a 3.76% chance that $\sqrt{-3\,\mathrm{Disc}}$ is an integer. However, if we increase the range to $|a|$, $|b|$, $|c|$, $|d| \leq 50$, there is a 0.16% chance that $\sqrt{-3\,\mathrm{Disc}}$ is an integer. This larger table is not included.

Table 2. Ranks of $a\,u^3 + b\,u^2\,v + c\,u\,v^2 + d\,v^3 = m$

Rank	Curve	Inflect'n Pt	Generators
1	$(-5,-2,-4,2;-54)$	$(2:1:1)$	$(0:3:-1)$
	$(-5,0,0,-3;-5)$	$(1:0:1)$	$(11951:18030:17351)$
	$(-5,0,0,-2;-5)$	$(1:0:1)$	$(11267:30555:23417)$
	$(-5,0,0,2;-5)$	$(1:0:1)$	$(-11267:30555:-23417)$
	$(-5,0,0,3;-5)$	$(1:0:1)$	$(-11951:18030:-17351)$
	$(-5,2,-4,-2;-189)$	$(1:4:1)$	$(-7891703:5228653:-2691683)$
	$(-5,3,3,-2;-3)$	$(1:2:1)$	$(2:1:2)$
	$(-4,-3,-3,-1;-3)$	$(1:-1:1)$	$(-1:4:2)$
	$(-4,0,0,-3;-4)$	$(1:0:1)$	$(-17:42:37)$
	$(-4,0,0,3;-4)$	$(1:0:1)$	$(17:42:-37)$
	$(-4,3,-3,1;-3)$	$(1:1:1)$	$(1:4:-2)$
	$(-3,-3,-1,-4;-3)$	$(1:0:1)$	$(-1:1:1)$
	$(-3,-3,-1,-3;-3)$	$(1:0:1)$	$(0:1:1)$
	$(-3,-3,-1,-2;-3)$	$(1:0:1)$	$(-2:7:6)$
	$(-3,-3,-1,3;-3)$	$(1:0:1)$	$(0:1:-1)$
	$(-3,-1,3,-3;-84)$	$(3:1:1)$	$(-855201:7891703:2691683)$
	$(-3,0,0,-1;-3)$	$(1:0:1)$	$(-1:3:2)$
	$(-3,0,0,1;-3)$	$(1:0:1)$	$(1:3:-2)$
	$(-3,1,3,3;84)$	$(-3:1:1)$	$(-8075049:-5485087:-285067)$
	$(-3,3,-1,-3;-3)$	$(1:0:1)$	$(0:1:1)$
	$(-3,3,-1,2;-3)$	$(1:0:1)$	$(2:7:-6)$
	$(-3,3,-1,3;-3)$	$(1:0:1)$	$(0:1:-1)$
	$(-3,3,-1,4;-3)$	$(1:0:1)$	$(1:1:-1)$
	$(-2,-4,2,-5;-54)$	$(-1:2:1)$	$(3:0:1)$
	$(-2,-3,3,-1;-3)$	$(1:1:1)$	$(-1:2:2)$
	$(-2,-3,3,5;3)$	$(-2:1:1)$	$(-1:-1:-1)$
	$(-2,-1,-3,-3;-51)$	$(3:-1:1)$	$(-270:617:199)$
	$(-2,0,0,-5;-2)$	$(1:0:1)$	$(-1:14:19)$
	$(-2,0,0,-3;-2)$	$(1:0:1)$	$(-19:78:89)$
	$(-2,0,0,3;-2)$	$(1:0:1)$	$(19:78:-89)$
	$(-2,0,0,5;-2)$	$(1:0:1)$	$(1:14:-19)$
	$(-2,1,-3,3;-51)$	$(3:1:1)$	$(270:617:-199)$
	$(-2,3,3,1;3)$	$(-1:1:1)$	$(-2:-1:-1)$
	$(-2,4,2,5;189)$	$(-4:1:1)$	$(-14855117:-5485087:-285067)$
	$(-1,-5,1,-1;-21)$	$(-1:2:1)$	$(4373452:3518251:2691683)$
	$(-1,-3,-3,5;-1)$	$(1:0:1)$	$(-4:21:-37)$
	$(-1,-1,-5,1;-21)$	$(2:1:1)$	$(-3518251:4373452:-2691683)$

Rank	Curve	Inflect'n Pt	Generators
	$(-1,1,-5,-1;-6)$	$(1:1:1)$	$(-1:1:-1)$
	$(-1,3,-3,-5;-1)$	$(1:0:1)$	$(4:21:37)$
	$(-1,5,1,1;6)$	$(-1:1:1)$	$(-5:-1:-1)$
	$(1,-5,-1,-1;-6)$	$(-1:1:1)$	$(1:1:1)$
	$(1,-3,3,5;1)$	$(1:0:1)$	$(16:-21:-17)$
	$(1,-1,5,1;6)$	$(1:1:1)$	$(1:-5:1)$
	$(1,1,5,-1;21)$	$(2:1:1)$	$(-1294981:-6780068:285067)$
	$(1,3,3,-5;1)$	$(1:0:1)$	$(-16:-21:17)$
	$(1,5,-1,1;21)$	$(-1:2:1)$	$(-6780068:1294981:-285067)$
	$(2,-4,-2,-5;-189)$	$(-4:1:1)$	$(5228653:7891703:2691683)$
	$(2,-3,-3,-1;-3)$	$(-1:1:1)$	$(1:2:2)$
	$(2,-1,3,-3;51)$	$(3:1:1)$	$(-199:-242:30)$
	$(2,0,0,-5;2)$	$(1:0:1)$	$(-19:-14:1)$
	$(2,0,0,-3;2)$	$(1:0:1)$	$(-89:-78:19)$
	$(2,0,0,3;2)$	$(1:0:1)$	$(89:-78:-19)$
	$(2,0,0,5;2)$	$(1:0:1)$	$(19:-14:-1)$
	$(2,1,3,3;51)$	$(3:-1:1)$	$(199:-242:-30)$
	$(2,3,-3,-5;-3)$	$(-2:1:1)$	$(-1:2:2)$
	$(2,3,-3,1;3)$	$(1:1:1)$	$(2:-1:-1)$
	$(2,4,-2,5;54)$	$(-1:2:1)$	$(-11:4:-1)$
	$(3,-3,1,-4;3)$	$(1:0:1)$	$(-4:-3:2)$
	$(3,-3,1,-3;3)$	$(1:0:1)$	$(-4:-3:-1)$
	$(3,-3,1,-2;3)$	$(1:0:1)$	$(-25:-21:-1)$
	$(3,-3,1,3;3)$	$(1:0:1)$	$(2:-3:-1)$
	$(3,-1,-3,-3;-84)$	$(-3:1:1)$	$(855201:7891703:2691683)$
	$(3,0,0,-1;3)$	$(1:0:1)$	$(-2:-3:1)$
	$(3,0,0,1;3)$	$(1:0:1)$	$(2:-3:-1)$
	$(3,1,-3,3;84)$	$(3:1:1)$	$(8075049:-5485087:-285067)$
	$(3,3,1,-3;3)$	$(1:0:1)$	$(-2:-3:1)$
	$(3,3,1,2;3)$	$(1:0:1)$	$(25:-21:1)$
	$(3,3,1,3;3)$	$(1:0:1)$	$(4:-3:1)$
	$(3,3,1,4;3)$	$(1:0:1)$	$(4:-3:-2)$
	$(4,-3,3,-1;3)$	$(1:1:1)$	$(-2:-5:1)$
	$(4,0,0,-3;4)$	$(1:0:1)$	$(-37:-42:17)$
	$(4,0,0,3;4)$	$(1:0:1)$	$(37:-42:-17)$
	$(4,3,3,1;3)$	$(1:-1:1)$	$(2:-5:-1)$
	$(5,-3,-3,2;3)$	$(1:2:1)$	$(-1:1:-1)$
	$(5,-2,4,2;189)$	$(1:4:1)$	$(5485087:-14855117:285067)$
	$(5,0,0,-3;5)$	$(1:0:1)$	$(-17351:-18030:-11951)$
	$(5,0,0,-2;5)$	$(1:0:1)$	$(-23417:-30555:-11267)$
	$(5,0,0,2;5)$	$(1:0:1)$	$(23417:-30555:11267)$
	$(5,0,0,3;5)$	$(1:0:1)$	$(17351:-18030:11951)$
	$(5,2,4,-2;54)$	$(2:1:1)$	$(-4:-11:1)$

Rank	Curve	Inflect'n Pt	Generators
2	$(-5, 1, 5, 2; 3)$	$(-1 : 1 : 1)$	$(-5 : -4 : -1)$, $(-23 : -16 : 17)$
	$(-3, -3, -1, 2; -3)$	$(1 : 0 : 1)$	$(-2 : 9 : -8)$, $(-10 : 13 : -12)$
	$(-3, -3, -1, 4; -3)$	$(1 : 0 : 1)$	$(-4 : 9 : -10)$, $(11 : 21 : -19)$
	$(-3, 3, -1, -4; -3)$	$(1 : 0 : 1)$	$(4 : 9 : 10)$, $(-11 : 21 : 19)$
	$(-3, 3, -1, -2; -3)$	$(1 : 0 : 1)$	$(2 : 9 : 8)$, $(10 : 13 : 12)$
	$(-2, 5, -1, -5; -3)$	$(1 : 1 : 1)$	$(11 : 2 : 8)$, $(23 : 10 : 12)$
	$(2, -5, 1, 5; 3)$	$(1 : 1 : 1)$	$(-4 : 5 : -1)$, $(-16 : 23 : 17)$
	$(3, -3, 1, 2; 3)$	$(1 : 0 : 1)$	$(5 : -9 : -1)$, $(23 : -39 : 17)$
	$(3, -3, 1, 4; 3)$	$(1 : 0 : 1)$	$(7 : -9 : 1)$, $(4 : -7 : -6)$
	$(3, 3, 1, -4; 3)$	$(1 : 0 : 1)$	$(-7 : -9 : -1)$, $(-4 : -7 : 6)$
	$(3, 3, 1, -2; 3)$	$(1 : 0 : 1)$	$(-5 : -9 : 1)$, $(-23 : -39 : -17)$
	$(5, -1, -5, -2; -3)$	$(-1 : 1 : 1)$	$(-2 : 11 : 8)$, $(-10 : 23 : 12)$

References

[Guy95] Richard K. Guy. My favorite elliptic curve: a tale of two types of triangles. *Amer. Math. Monthly*, 102(9):771–781, 1995.

[LeV77] William J. LeVeque. *Fundamentals of number theory*. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1977.

[Sil82] Joseph H. Silverman. Integer points and the rank of Thue elliptic curves. *Invent. Math.*, 66(3):395–404, 1982.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York-Berlin, 1986.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, New York, 1994.

[ST92] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Springer-Verlag, New York, 1992.

[The04] The PARI Group, Bordeaux. *PARI/GP, version* 2.1.5, 2004. available from http://pari.math.u-bordeaux.fr/.

[Zag87] Don Zagier. Large integral points on elliptic curves. *Math. Comp.*, 48(177):425–436, 1987.

U-1971, University of South Alabama, Mobile, AL 36688
E-mail address: jarrod2001@yahoo.com

Mills College, P.O. Box 9312, Oakland, CA 94613
E-mail address: nho@mills.edu

Brown University, P.O. Box 5831, Providence, RI 02912
E-mail address: karen_lostritto@brown.edu

University at Buffalo, 204 A Dewey Hall, Buffalo, NY 14261
E-mail address: jonam@nsm.buffalo.edu

Mathematics Department, 1700 E. Coldspring Lane, Baltimore, MD 21251
E-mail address: thomas_nikia@msn.com