On Large Rational Solutions of Cubic Thue Equations

Jarrod A. Cunningham (University of South Alabama), Nancy Ho (Mills College), Karen Lostritto (Brown University),
Jon A. Middleton (University at Buffalo), and Nikia T. Thomas (Morgan State University)

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 poster proceeds as follows. First we exhibit a map from a cubic Thue equation C having a rational point of inflection to an elliptic curve of the form

$$E: \qquad y^2 = x^3 - D,$$

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.

Thue Equations

In 1909, Axel Thue considered the equation

$$a_N\,u^N + a_{N-1}\,u^{N-1}\,v + a_{N-2}\,u^{N-2}\,v^2 + \cdots + a_0\,v^N = m$$

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

$$C: \qquad a\,u^3 + b\,u^2\,v + c\,u\,v^2 + d\,v^3 = m,$$

such that the discriminant

$$\text{Disc} = b^2\,c^2 - 4\,a\,c^3 - 4\,b^3\,d + 18\,a\,b\,c\,d - 27\,a^2\,d^2$$

is nonzero. However, we are not interested in integer solutions, but rather rational solutions. Our goal is to associate this equation with an elliptic curve.

Elliptic Curves

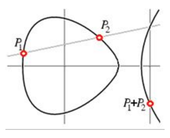
An elliptic curve is a cubic equation of the form

$$E: \qquad y^2 = x^3 + a\,x + b$$

such that the discriminant $4\,a^3 + 27\,b^2 \neq 0$.

Examples of Elliptic Curves.

If a and b are integers, the collection $E(\mathbb{Q})$ of rational points (x, y) – which we often express in projective coordinates as $(x : y : 1)$ – on an elliptic curve form a finitely generated abelian group, called the Mordell-Weil group: Given two rational points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, we find the intersection of the cubic curve and the line defined by these two points. Denote this point as $P_1 * P_2$. Reflecting $P_1 * P_2$ over the x-axis will yield a point which we define as $P_1 \oplus P_2$. 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 $[-1]P = (x, -y)$.



The Group Law on an Elliptic Curve.

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), Silverman (Sil86) or Silverman (Sil94).)

Points of Inflection

In order to study rational solutions to the cubic Thue equation, we will first focus on such curves that have a rational point of inflection i.e. a point (u_0, v_0) that satisfies

$$a\,u_0^3 + b\,u_0^2\,v_0 + c\,u_0\,v_0^2 + d\,v_0^3 = m$$
$$(b^2 - 3\,a\,c)\,u_0^2 + (b\,c - 9\,a\,d)\,u_0\,v_0 + (c^2 - 3\,b\,d)\,v_0^2 = 0$$

The cubic equation guarantees the point will be on the curve, and the quadratic equation guarantees the determinant of the Hessian matrix of the cubic polynomial will vanish.

Assume that such a point exists, define the rational substitution

$$x = 4\,m\,\frac{v_0\,(u - u_0) - u_0\,(v - v_0)}{(3\,a\,u_0 + b\,v_0)\,(u - u_0) + (b\,u_0 + c\,v_0)\,(v - v_0)}\,w_0$$

$$y = 4\,m\,\frac{(3\,a\,u_0 + b\,v_0)\,(u + u_0) + (b\,u_0 + c\,v_0)\,(v + v_0)}{(3\,a\,u_0 + b\,v_0)\,(u - u_0) + (b\,u_0 + c\,v_0)\,(v - v_0)}\,\sqrt{-3\,\text{Disc}}$$

where w_0 is a nonzero rational number satisfying $v_0\,w_0 = b^2 - 3\,a\,c$. (The existence of a rational inflection point forces $\sqrt{-3\,\text{Disc}}$ to be rational.) This is a point on the elliptic curve

$$E: \qquad y^2 = x^3 - D \qquad \text{with} \qquad D = -16\,m^2\,\text{Disc}.$$

The inverse transformation from E to C is

$$u = u_0\,\frac{y + 4\,m\sqrt{-3\,\text{Disc}}}{y - 4\,m\sqrt{-3\,\text{Disc}}} + \frac{b\,u_0 + c\,v_0}{w_0}\,\frac{2\sqrt{-3\,\text{Disc}}\,x}{y - 4\,m\sqrt{-3\,\text{Disc}}}$$

$$v = v_0\,\frac{y + 4\,m\sqrt{-3\,\text{Disc}}}{y - 4\,m\sqrt{-3\,\text{Disc}}} - \frac{3\,a\,u_0 + b\,v_0}{w_0}\,\frac{2\sqrt{-3\,\text{Disc}}\,x}{y - 4\,m\sqrt{-3\,\text{Disc}}}$$

With these transformations, our study of rational points on cubic Thue equations having a rational inflection point is reduced to the study of rational points on elliptic curves.

Large Rational Points on Thue Equations

Say the cubic Thue equation has a rational point of inflection. Assume we have a sequence of rational points $\{(u_n, v_n)\}$ on C such that

$$|u_n|\,, \quad |v_n| \longrightarrow \infty \quad \text{as} \quad n \longrightarrow \infty.$$

This corresponds to a sequence of rational points $\{(x_n, y_n)\}$ on E such that

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

This limit is a torsion point of order 3 on E.

Finding "Approximate" Points of Order 3

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 $|u_n|\,,\ |v_n| \longrightarrow \infty$.

We sketch the proof; it uses an idea following Guy (Guy95), which in turn is motivated by a paper of Zagier (Zag87). As above, consider the elliptic curve $E: y^2 = x^3 - D$, for $D = -16\,m^2\,\text{Disc}$. There is the isomorphism

$$\varphi: \quad E(\mathbb{R}) \to \mathbb{R}/\mathbb{Z}, \quad (x, y) \mapsto \frac{1}{2\Omega_E}\int_x^\infty \frac{d\xi}{\sqrt{\xi^3 - D}} \pmod{\mathbb{Z}}$$

where

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

is the real period of the elliptic curve. Let $P = (x_1, y_1)$ be a point of infinite order on E, and define the elliptic logarithm

$$\gamma = \frac{1}{\Omega_E}\int_{x_1}^\infty \frac{d\xi}{\sqrt{\xi^3 - D}}.$$

Using continued fractions, define the sequence of points on E by

$$(x_n, y_n) = [q_n](x_1, y_1) \qquad \text{where} \qquad \frac{p_n}{q_n} \approx \frac{3}{2}\,\gamma \quad \text{for} \quad n = 1, 2, 3, \ldots$$

These rational points have "approximate" order 3:

$$\varphi([3](x_n, y_n)) \equiv \pm 3\,q_n \cdot \frac{\gamma}{2} \approx \pm p_n \equiv 0 \pmod{\mathbb{Z}}.$$

Since φ is an isomorphism, the corresponding point (u_n, v_n) on C has large rational coefficients.

Example: $u^3 - 7\,v^3 = 1$

Consider the Thue equation $C: u^3 - 7\,v^3 = 1$; the corresponding elliptic curve is $E: y^2 = x^3 - 21168$. 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:

1. Using a program such as `mwrank`, we determine that this elliptic curve has rank 1 with the generator $(84, 756)$.
2. We compute
$$\frac{3}{2}\,\gamma = 0.7106994116\ldots,$$
find the convergents p/q of the corresponding continued fraction, and multiply the generator by q – assuming that p is not divisible by three.
3. Finally we use the transformation given above to find large rational points (u, v) satisfying $u^3 - 7\,v^3 = 1$.

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 approaches a point of order 3:

$$\left(-4m\left(\frac{\text{Disc}}{m}\right)^{\frac{1}{3}},\ 4m\sqrt{-3\text{Disc}}\right) = (43.91166852\ldots, -252).$$

As q gets larger, we obtain a better approximation for this point. We also see that $|u|$, $|v|$ are getting larger as q gets larger, and that

$$\left(\frac{u}{v}\right)^3 - 7 = \frac{1}{v^3} \qquad \Longrightarrow \qquad \frac{u}{v} \mapsto \sqrt[3]{7} = 1.912931183\ldots.$$

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

We look for cubic Thue equations having a rational inflection point, such that the corresponding elliptic curve has positive rank. We consider a list of relatively prime integers a, b, c, and d such that

$$|a|,\ |b|,\ |c|,\ |d| \leq 50 \qquad \text{and} \qquad \text{Disc} \neq 0.$$

When $\sqrt{-3\,\text{Disc}}$ is an integer, we choose m so that there is a rational point of inflection; only 0.16% have this property. Finally we use `Maple` and `apecs` to compute the rank and the generators. The symbol $(a, b, c, d; m)$ denotes the Thue equation.

Rank	Curve	Inflect'n Pt	Generators
1	$(-3,-3,-1,-3;-3)$	$(1:0:1)$	$(0:1:1)$
	$(-3,-3,-1,-2;-3)$	$(1:0:1)$	$(-2:7:6)$
	$(-3,-3,-1,3;-3)$	$(1:0:1)$	$(0:1:-1)$
	$(-3,-1,3,-3;-84)$	$(3:1:1)$	$(-855201:7891703:2691683)$
	$(-3,0,0,-1;-3)$	$(1:0:1)$	$(-1:3:2)$
	$(-3,0,0,1;-3)$	$(1:0:1)$	$(1:3:-2)$
	$(-3,1,3,3;84)$	$(-3:1:1)$	$(-8075049:-5485087:-285067)$
	$(-3,3,-1,-3;-3)$	$(1:0:1)$	$(0:1:1)$
	$(-3,3,-1,2;-3)$	$(1:0:1)$	$(2:7:-6)$
	$(-3,3,-1,3;-3)$	$(1:0:1)$	$(0:1:-1)$
	$(-2,-3,3,-1;-3)$	$(1:1:1)$	$(-1:2:2)$
	$(-2,-1,-3,-3;-51)$	$(3:-1:1)$	$(-270:617:199)$
	$(-2,0,0,-3;-2)$	$(1:0:1)$	$(-19:78:89)$
	$(-2,0,0,3;-2)$	$(1:0:1)$	$(19:78:-89)$
	$(-2,1,-3,3;-51)$	$(3:1:1)$	$(270:617:-199)$
	$(-2,3,3,1;3)$	$(-1:1:1)$	$(-2:-1:-1)$
	$(2,-3,-3,-1;-3)$	$(-1:1:1)$	$(1:2:2)$
	$(2,-1,3,-3;51)$	$(3:1:1)$	$(-199:-242:30)$
	$(2,0,0,-3;2)$	$(1:0:1)$	$(-89:-78:19)$
	$(2,0,0,3;2)$	$(1:0:1)$	$(89:-78:-19)$
	$(2,1,3,3;51)$	$(3:-1:1)$	$(199:-242:-30)$
	$(2,3,-3,1;3)$	$(1:1:1)$	$(2:-1:-1)$
	$(3,-3,1,-3;3)$	$(1:0:1)$	$(-4:-3:-1)$
	$(3,-3,1,-2;3)$	$(1:0:1)$	$(-25:-21:-1)$
	$(3,-3,1,3;3)$	$(1:0:1)$	$(2:-3:-1)$
	$(3,-1,-3,-3;-84)$	$(-3:1:1)$	$(855201:7891703:2691683)$
	$(3,0,0,-1;3)$	$(1:0:1)$	$(-2:-3:1)$
	$(3,0,0,1;3)$	$(1:0:1)$	$(2:-3:-1)$
	$(3,1,-3,3;84)$	$(3:1:1)$	$(8075049:-5485087:-285067)$
	$(3,3,1,-3;3)$	$(1:0:1)$	$(-2:-3:1)$
	$(3,3,1,2;3)$	$(1:0:1)$	$(25:-21:1)$
	$(3,3,1,3;3)$	$(1:0:1)$	$(4:-3:1)$
2	$(-3,-3,-1,2;-3)$	$(1:0:1)$	$(-2:9:-8),\ (-10:13:-12)$
	$(-3,3,-1,-2;-3)$	$(1:0:1)$	$(2:9:8),\ (10:13:12)$
	$(3,-3,1,2;3)$	$(1:0:1)$	$(5:-9:-1),\ (23:-39:17)$
	$(3,3,1,-2;3)$	$(1:0:1)$	$(-5:-9:1),\ (-23:-39:-17)$

Homogeneous Spaces and Isogenous Curves

Given a cubic Thue equation

$$C: \qquad a\,u^3 + b\,u^2\,v + c\,u\,v^2 + d\,v^3 = m$$

with arbitrary integers a, b, c, d such that $\text{Disc} \neq 0$, 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.) In general, one does not expect C to be birationally equivalent to an elliptic curve, but we may use homogeneous spaces.

There exists a rational map from C to the elliptic curve

$$E': \qquad Y^2 = X^3 - D' \qquad \text{with} \qquad D' = -27\,D.$$

This map sends a point (u, v) on C to

$$X = 4\left[(b^2 - 3\,a\,c)\,u^2 + (b\,c - 9\,a\,d)\,u\,v + (c^2 - 3\,b\,d)v^2\right]$$
$$Y = 4\left[(2\,b^3 - 9\,a\,b\,c + 27\,a^2\,d)\,u^3 + 3\,(b^2\,c - 6\,a\,c^2 + 9\,a\,b\,d)\,u^2\,v\right.$$
$$\left. -3\,(b\,c^2 - 6\,b^2\,d + 9\,a\,c\,d)\,u\,v^2 - (2\,c^3 - 9\,b\,c\,d + 27\,a\,d^2)\,v^3\right]$$

We say that C and E' are isogeneous curves. The elliptic curve E' is 3-isogeneous to the elliptic curve

$$E: \qquad y^2 = x^3 - D \qquad \text{with} \qquad D = -16\,m^2\,\text{Disc}.$$

That is, there is a map is defined by

$$X = \frac{x^3 - 4\,D}{x^2} \qquad Y = \frac{x^3 + 8\,D}{x^3}\,y \qquad \text{with dual map} \qquad x = \frac{1}{9}\,\frac{X^3 - 4\,D'}{X^3} \qquad y = \frac{1}{27}\,\frac{X^3 + 8\,D'}{X^3}\,Y$$

The composition of the map $\psi: E \to E'$ and its dual $\widehat{\psi}: E' \to E$ yields $\widehat{\psi} \circ \psi = [3]$ as the "multiplication-by-3" map on E.

With the composition

$$C \longrightarrow E' \xrightarrow{\widehat{\psi}} E$$

we say that E is a homogeneous space for C – even if C does not have a rational point of inflection. Hence, if we find a rational point on E, we may hope to "pull back" this point to a rational point on C.

Example: $2\,u^3 + 9\,u^2\,v + 13\,u\,v^2 + 6\,v^3 = 6$

Consider the curve $C: 2\,u^3 + 9\,u^2\,v + 13\,u\,v^2 + 6\,v^3 = 6$. Since $\text{Disc} = 1$, there are no rational inflection points. However, it will be "isogenous" to the elliptic curve $E': Y^2 = X^3 - 15552$. Explicitly, we map (u, v) on C to (X, Y) on E' via the substitution

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

Looking at these transformations, we see that a "large" rational point (X, Y) will be the image of a "large" rational point (u, v), so we modify our algorithm slightly our algorithm to find "large" rational points on E'.

Using `mwrank`, we determine that E' has rank 1 with generator $(X, Y) = (28, 80)$. This corresponds to the three rational points $(-8, 5)$, $(3, -1)$, and $(5, -4)$ on C. To find a "large" rational point, we consider approximations

$$\frac{p}{q} \approx \frac{1}{2}\,\gamma' \quad \text{in terms of} \quad \gamma' = \frac{1}{\Omega_{E'}}\int_{X_1}^\infty \frac{d\xi}{\sqrt{\xi^3 - D'}} = 0.83737\ldots.$$

For the approximation $p/q = 5/12$, consider $(X, Y) = [12]\,(28, 80)$:

$$X = 7215.4351885546\ldots, \qquad Y = 612905.8775557362\ldots.$$

Substituting these values into the transformations, we find the following "large" rational points on C:

$$(u_1, v_1) = (42.48017, -42.47684),$$
$$(u_2, v_2) = (-127.41723, 84.94371),$$
$$(u_3, v_3) = (84.93706, -42.46686).$$

For even "larger" rational points, consider the approximation $p/q = 18/43$, and the point $[43]\,(28, 80)$; this corresponds to the points

$$(u_4, v_4) = (-895.159, 596.773),$$
$$(u_5, v_5) = (298.387, -298.386),$$
$$(u_6, v_6) = (596.773, -298.386).$$

Example: $2\,u^3 + 9\,u^2\,v + 13\,u\,v^2 + 6\,v^3 = 2$

Consider the curve $C: 2\,u^3 + 9\,u^2\,v + 13\,u\,v^2 + 6\,v^3 = 2$; it does not have a rational inflection point. The related elliptic curves are $E: y^2 = x^3 + 64$ and $E': Y^2 = X^3 - 1728$. Both curves have finite Mordell-Weil group:

$$E(\mathbb{Q}) = \left\{[n]\,(8, 24)\,\middle|\,n \in \mathbb{Z}\right\} \simeq \frac{\mathbb{Z}}{6\,\mathbb{Z}},$$
$$E'(\mathbb{Q}) = \left\{(12, 0),\,\mathcal{O}\right\} \simeq \frac{\mathbb{Z}}{2\,\mathbb{Z}}.$$

Using the map $C \longrightarrow E'$ via the substitution

$$X = 4\,(3\,u^2 + 9\,u\,v + 7\,v^2), \qquad Y = -4\,v\,(3\,u + 4\,v)\,(3\,u + 5\,v);$$

the Thue equation also has a finite number of rational solutions:

$$C(\mathbb{Q}) = \left\{\begin{array}{c}(-5:3:1),\,(-4:3:1),\,(-1:0:1),\\ (1:0:1),\,(4:-3:1),\,(5:-3:1),\\ (-3:2:0),\,(-2:1:0),\,(-1:1:0)\end{array}\right\}$$

Therefore, we are unable to construct an infinite sequence of "large" rational points, but we are able to enumerate all rational points.

Conclusions and Future Research

1. Our algorithm for finding large rational solutions to cubic Thue equations having a rational inflection point was tested extensively for the "generalized Pellian" $u^3 - d\,v^3 = 1$ for different values of d. More work needs to be done in order to determine the connection between the value of d and the rank and torsion subgroup of the corresponding elliptic curve. This will allow for a quick determination of whether a cubic equation has finitely or infinitely many solutions.
2. When a Thue eqation does not have a rational point of inflection, our algorithm needs to be tested further to determine its effectiveness in finding large rational solutions of the cubic Thue equation.
3. If the map from C to E' were surjective, then infinitely many rational points on E' would imply that there were infinitely many rational points on C. However this map is not surjective, and therefore further research is necessary to determine how much information rational points on E' give us about rational points on C.

Acknowledgements

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.

REFERENCES

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

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

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

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

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

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

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

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

This poster was prepared with Brian Wolven's Poster LaTeX macros v2.1.