On Large Rational Solutions of Cubic Thue Equations: What Thue Did to Pell

Referee Report

0.1 Summary:

The paper is largely expository. The first part is devoted to studying integer solutions to Pell's Equation: $u^2 - dv^2 = 1$. The authors present the classic construction of a fundamental solution via continued fractions, from which all solutions can be derived. The primary focus of the second part is on rational solutions to the Thue's equation, $u^3 - dv^3 = 1$. The authors explain why these rational solutions correspond to rational points on the elliptic curve, $y^2 = x^3 - 432d^2$ (as a special case of a more general result). They then cite the famous result of Mordell, which says that the set of rational points of an elliptic curve over $\mathbb{Q}$ is a finitely generated abelian group, listing the rank for the above family of curves when $1 \leq d \leq 100$.

At this point the paper comes a little closer to the frontier (perhaps partially original?), asking a specific question about the topological distribution of solutions to the above Thue's equation. Specifically, if one has a point (x, y) of infinite order on the associated elliptic curve, can it be used to produce a sequence (u_n, v_n) of solutions for which $|u_n|, |v_n| \to \infty$? The authors answer this question in the affirmative, by giving an algorithm based on the elliptic logarithm and (again) continued fractions. The paper concludes by explicitly calculating such a sequence of solutions to the specific Thue equation, $u^3 - 7v^3 = 1$.

0.2 General Comments

For many (but not all) mathematical journals, the lack of original material would detract from the value of this paper. However, it is certainly suitable in content for the Rose-Hulman Undergraduate Math Journal, for which it is being reviewed. I found the exposition to be very clear and interesting, and feel very comfortable recommending its acceptance. One general comment is that it might be helpful for the reader to know up front how the material will be laid out and what will be the scope of the paper. A good 4-5 sentence abstract would go a long way toward this end. Another general comment is that the authors often write in a very informal style, in particular referring to the reader in the second person. This is generally frowned upon, but not wholly inappropriate for an undergraduate math journal. In a few cases (which I point out below), I would definitely suggest being more formal.

0.3 Specific Recommendations (by page)

pg. 1

(1) Are Brouncker and Wallis both Englishmen? Or only Brouncker?
(2) The sentence beginning with "See, Fermat..." is very informal. I might at least begin with, "You see, etc."

pg. 2

(1) It might be worth clarifying what algebraic integers are. Specifically, they satisfy monic polynomials with (rational) integer coefficients. In this case, $u + v\sqrt{d}$ satisfies

$$x^2 - 2ux + (u^2 - dv^2) = 0.$$

One could state as well-known fact that algebraic integers form a ring, and then discuss in detail the arithmetic of the subring, $\mathbb{Z}[\sqrt{d}]$, as it is most relevant to the paper.
(2) I would change "and you should do this" to something like, "and we invite the reader to do so" or "and we leave this as an exercise for the reader."

pg. 3

(1) "You can play around..." is again very familiar. I might suggest, "By inspection it is easy to see that..."
(2) The proof from Leveque could be cleaned up quite a bit. In the statement itself, I would include for clarification the assumption that a nontrivial solution exists. We are showing here that if one exists, then a fundamental one exists. Perhaps one could then let

$$G_+ := \{\ a = u + v\sqrt{d} \mid u, v \geq 0,\ \mathbb{N}(a) = 1\ \}.$$

By the argument given, a nontrivial Pell solution immediately implies a nontrivial element of G_+. The proof then hinges upon being able to choose a least $\delta > 1$ in G_+. Why is there such a δ? This is probably worth a brief explanation. The remainder of the argument then seems clear to me.

pg. 5-6

(1) The continued fraction construction of a Pell solution does not mention how to check when one has reached the full period. The given example

of $\sqrt{2}$ ends with, "Note that eventually the a_k's repeat." I would go one step farther and show that

$$\{1; \bar{2}\} = \sqrt{2}$$

(and perhaps do the same for the $\sqrt{61}$ example).

pg. 7

(1) "The theorem above says that..." should be changed to, "As a special case of the above theorem, it follows that..." If I see, "the theorem says," I read this to mean that the theorem will now be paraphrased somehow. That is of course not what is being said here.
(2) I think $\gcd(a, b) = 1$ in this context ($N = 1$ case). If we say that $f(u, v)$ is irreducible over $\mathbb{Z}$, this means in particular that we can not factor out an integer (other than ± 1, of course). Otherwise, one has no solutions to $au + bv = m$ if $\gcd(a, b)$ does not divide m. So either way, something has to be changed here.
(3) "You should prove this!" is again very familiar.

pg. 8

(1) Instead of "As you can probably guess," I'd probably say "the above result suggests..." One could even then say something like, "Indeed, we'll show that this is the case, etc."

pg. 10

(1) The explicit formula for addition on the elliptic curve shows that the sum of two points is always at least as rational as the points themselves. This is a salient point. If one adds two $\mathbb{Q}$-rational points, λ is in $\mathbb{Q}$ and subsequently $(x_1, y_1) \oplus (x_2, y_2)$ is defined over $\mathbb{Q}$. The same can be said of *any* field, though. The paper does deal with elliptic curves over $\mathbb{R}$ and $\mathbb{C}$ later. So this is a good place to make an important point about a more general idea of rationality. If K is any field with $A, B \in K$, the K-rational points of E (denoted $E(K)$) form an abelian group. The authors could make this point and say something like, "for example, we address elliptic curves over $\mathbb{R}$ and $\mathbb{C}$ a little later."

pg. 11-12

(1) A reference should be given for "$\#E(\mathbb{Q})_{tor}$ divides 6." I am familiar with Mazur's theorem (see Silverman-Tate pg. 58). Of course, the authors are considering a more special elliptic curve. The exposition would benefit, though, from giving the reference and perhaps making the point that more general elliptic curves over $\mathbb{Q}$ can have larger (although still very few options) rational torsion subgroups.
(2) Missing an "a" in the first sentence of **All Ranks: Fall In!**

pg. 14-15

(1) The options in Question #1 (pg. 14) could be clarified a little. As I see it, the rational solutions (u, v) of a given Thue equation (with positive rank) are being viewed as a countably infinite subset of $\mathbb{R}^2$ as a topological space (or the Riemann sphere if we throw in the infinite point). As such, we are investigating whether the subset has any cluster/limit points, and in particular if infinity is one. Furthermore, can a sequence converging to infinity be explicitly computed?

Along these same lines, it would be helpful to draw a contrast with the previous sections. Here, the authors are *not* presenting an algorithm for constructing rational points on the elliptic curve or rational solutions to a Thue equation. Rather, they are presenting an algorithm which takes as input a rational point of infinite order, and then produces a sequence of rational points as above. Very interesting question (in my opinion), but fundamentally different in nature from the other type of question.
(2) The statement involving Equation (43) could be clarified a little. Does the limit necessarily always exist? Is the y coordinate of P always positive? Is the converse true? (that a sequence converging to a point of order 3 pulls back to a sequence (u_n, v_n) with desired properties).
pg. 15-17

(1) I would shorten this material on elliptic curves over $\mathbb{R}$ and $\mathbb{C}$. We need an understanding of how the elliptic logarithm works, but not necessarily why it works. My suggestion is to summarize the construction and refer to Silverman, perhaps cutting out say 2/3 of a page to 1 page. Don't cut out the $(12, 36)$ example, though! That is actually very useful for the exposition, I think. I would even add another example which illustrates that the log respects the two group operations. That seems to be the key point for the specific application in the paper.