Elliptic Curves and Diophantine Equations

Albert Tam

28 November 2018

1 Introduction

Elliptic curves, which are curves of the form $y^2 = x^3+ax+b$ and related theorems can be used to solve a wide variety of Diophantine equations, equations that only allow integer solutions. With only a little knowledge of elliptic curves and a computer, solutions, especially very complicated ones, to countless Diophantine equations can be found. Even if solutions are unable to be found due to their sparseness, elliptic curves can still give us a general method to find solutions. There are many fascinating Diophantine equations that can be solved using elliptic curves. Here, we consider elliptic curves for the equations $xyz = N = x + y + z$ for rationals x, y, z, and N, and $\frac{R}{r} = N$ for an integer N in a triangle with integer sides, where R is the circumradius of the triangle and r is the inradius. Many of the ideas used are from MacLeod [1].

2 $xyz = N = x + y + z$ in the integers

Proposition 1. *The only positive integer solution to $xyz = N = x + y + z$ is the triple $(x, y, z) = (1, 2, 3)$ and its permutations.*

Proof. Without loss of generality, let $x \leq y \leq z$. Then, $x + y + z \leq 3z$, so $xyz \leq 3z$. We have two cases: $z = 0$ and $z \neq= 0$.

If $z = 0$, then $x = y = z = N = 0$. This is not a valid solution.

If $z \neq= 0$, then we can divide by z, giving us $xy \leq z$. Since our domain is restricted to positive integers, we only need to consider a few pairs for (x, y): $(1, 1)$, $(1, 2)$, and $(1, 3)$, as well as their permutations. $(x, y) = (1, 1)$ gives no solution. $(x, y) = (1, 2)$ and $(x, y) = (1, 3)$ provide the triple $(1, 2, 3)$ in different orders. Therefore, the only positive integer solution to the equation $xyz = N = x + y + z$ is $(x, y, z) = (1, 2, 3)$, in any order. □

3 Isogeny

Isogenies have a broad definition that applies for all groups, but we only need the specific definition for elliptic curves.

Definition 3.1. On elliptic curves, an isogeny from E_1 to E_2 is a rational function ϕ taking points from E_1 to E_2 such that if P and Q are points on E_1, then $\phi(P+Q) = \phi(P) + \phi(Q)$.

Therefore, isogenies between elliptic curves preserve its structure; but most importantly for us, they preserve the group structure and group law of the rational points of the elliptic curve. This allows us to find rational points on an isogenous curve and relate them back to rational points on the original curve.

Discussing isogeny is helpful, since it can help us find rational points on the original elliptic curve when they may have very large height, i.e. the numerator and denominator in the reduced form are large. An isogenous curve, especially that of rank 1, **might** have a more computable rational point of smaller height, and the rational points on an isogenous curve are related to rational points on the original elliptic curve by a change of variables that preserves rationality. While isogenous curves are not useful in all cases, they are especially helpful in the equations we are concerned with here, and they work for many values of N.

We build isogenous curves off of the torsion points of the original curve. While there is a general method for finding isogenous curves, additional substitutions are often needed for the best curve to work with.

Consider the elliptic curve $y^3 = x^3 + ax^2 + bx + c$ for simplicity. Formulas for isogenous curves still work for the more general form $y^3 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, but they are more complicated. There are many ways of computing isogenous curves, and it is a difficult task to prove that there are isogenous, so we will be using isogenous curve formulas adapted from those provided by Vélu [2].

3.1 Vélu's isogenous curve formulas

Here, we present the formulas for generating isogenous curves by Vélu. On any curve E, a point P has order 2 if and only if it is of the form $(p, 0)$. The other torsion points are of the form $(p, \pm q)$; another way to say this is that all other torsion points occur in pairs of additive inverses. Let $T' \subset T$ be a subset of the torsion subgroup T, where T' contains all 2-torsion points and one point from each pair $(p, \pm q)$ for other torsion points. Now, define the following functions:

$$g(x) = 3x^2 + 2ax + b$$

$$h(x) = -2y$$

For each point $P = (s_P, t_P) \in T'$, define the following:

$$v_P = \begin{cases} g(s_P) & 2P = \infty \\ 2g(s_P) & 2P \neq \infty \end{cases}$$

$$u_P = h^2(t_P)$$

Then let

$$v = \sum_{P \in T'} v_P$$

$$u = \sum_{P \in T'} u_P$$

$$w = \sum_{P \in T'} (u_P + s_P v_P)$$

The isogenous elliptic curve E' is defined by:

$$Y^2 = X^3 + aX^2 + (b - 5v)X + (c - 4av - 7w)$$

and the variables are related by the following equations:

$$X = x + \textstyle\sum_{P \in T'} (\frac{v_P}{x - s_P} + \frac{u_P}{(x - s_P)^2})$$

$$Y = y - \textstyle\sum_{P \in T'} (\frac{2u_P y}{(x - s_P)^3} + \frac{v_P (y - t_P)}{(x - s_P)^2} - \frac{g(s_P)h(t_P)}{(x - s_P)^2})$$

These formulas can be used to generate multiple isogenous curves, depending on the choice of torsion points for T'. A proof that Vélu's formulas produce a valid isogeny can be found in Washington's *Elliptic Curves* [3].

4 $xyz = N = x + y + z$ in the rationals

This problem is much more interesting than its equivalent in the integers, since it has many solutions that are difficult to find. Let $z = \frac{N}{xy}$, which gives the quadratic $xy^2 + x(x - N)y + N = 0$. A naive search method not involving elliptic curves would fix N, generate rational x, and see if the quadratic factors linearly in y. However, this only makes sense for small values of N, and if a certain N does not yield any rational points after a certain amount of time, we don't know whether N does not have rational points or we just haven't searched for long enough.

To begin transforming our equation into an elliptic curve, we first realize that for there to be rational points, the discriminant of the quadratic must be a rational square. This makes sense because the quadratic formula has a term for the square root of the discriminant. If this square root is irrational, the roots of the quadratic cannot be rational. Therefore, there exists a rational D such that $D^2 = x^2(x-N)^2 - 4Nx = x^4 - 2Nx^3 + N^2x^2 - 4Nx$. We can make the necessary substitutions to yield the elliptic curve $G^2 = H^3 + N^2H^2 + 8N^2H + 16N^2$, with $G = \frac{4ND}{x^2}$ and $H = \frac{-4N}{x}$. Because x, D, and N are rational, H and G are rational. Therefore, rational (H, G) translate to rational (x, y, z).

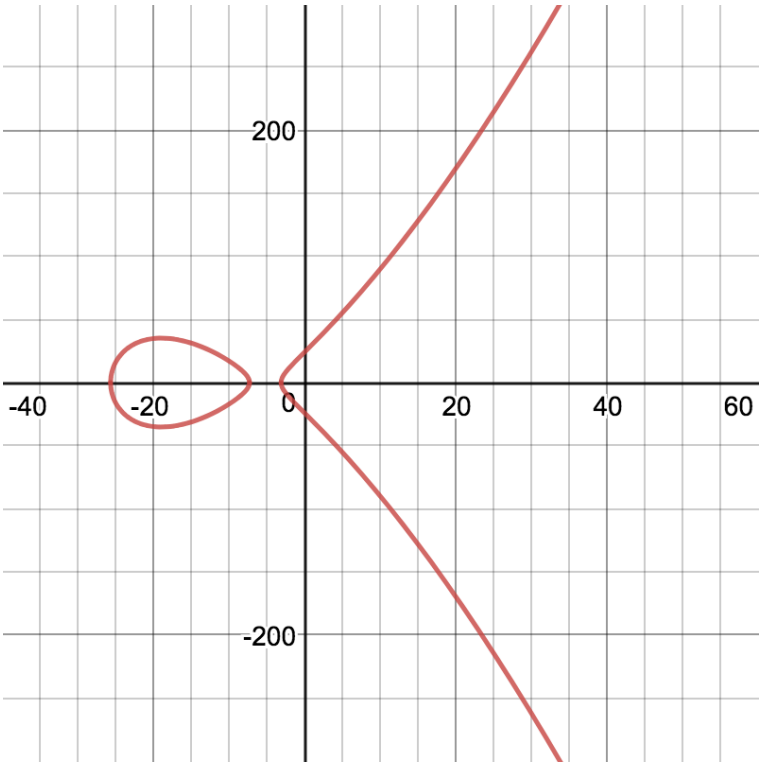

Figure 1: The elliptic curve for $xyz = x + y + z = 6$

This actually allows us to solve elliptic curves for each value of N. Let's take a small sample of integer values of N, say $N \in [1, 999]$. Calculating the ranks of each of these curves with a computer gives us that there are 374 curves with rank zero, 514 curves with rank one, and 111 curves of rank greater than one. We can ignore the curves with rank zero, because numerical tests confirm that the only rational points there are related to $(0, \pm 4N)$. This does not give a solution to the original problem, because $H = \frac{-4N}{x}$ cannot be zero for rational x if N is not. Now, we only consider the 625 curves with rank greater than one.

We turn to isogenous curves to give us easier-to-find solutions that we can translate back to rational points on the original elliptic curve. Following the isogenous curve formulas provided in Section 3 gives the 3-isogenous curve $V^2 = U^3 - 27N^2U^2 + 54N^2(4N^2 + 108)U - (4N^2 + 108)^2$. Finding solutions on this curve with a naive search method is easier for some values of N, which reduces the number of values of N for which it is hard to compute rational points.

5 $\frac{R}{r} = N$ for a triangle with integer lengths

The equilateral triangle has a circumradius R that is twice as large as the inradius r, giving the ratio $\frac{R}{r} = 2$. (This is the minimum value of the ratio $\frac{R}{r}$.) Naturally, we ask: do any other triangles with integer sides also give an integer ratio between R and r?

We first notice that the integer side length constraint in this question is redundant, because we can simply scale the triangle and scale the circumradius and inradius accordingly. We use the relations $R = \frac{abc}{4[ABC]}$ and $r = \frac{[ABC]}{s}$, where $[ABC]$ is the area of triangle ABC and $s = \frac{a+b+c}{2}$ is the semiperimeter. Plugging these in and using Heron's formula gives the following equation:

$$N = \frac{2abc}{(a+b-c)(b+c-a)(c+a-b)}$$

This will be a cubic, but letting $c = P-a-b$ where P is the perimeter gives us a quadratic in a:

$$2(2NP-(4N+1)b)a^2 - 2(b^2(4N+1) - bP(6N+1) + 2NP^2)a + NP(4b^2 - 4bP + P^2) = 0$$

Like for the previous Diophantine equation $xyz = N = x+y+z$, this quadratic has rational solutions if and only if the discriminant is the square of a rational number. Let this rational number be D. Therefore, there is some D such that:

$$D^2 = -2NbP^3 + (4N^2+8N+1)b^2P^2 - 2(2N+1)(4N+1)b^3P + (4N+1)^2b^4$$

Let $D = b^2v$ and $P = bu$. We can assume that $b \neq 0$ because that would be a degenerate triangle, so we can divide by b^4:

$$v^2 = -2Nu^3 + (4N^2+8N+1)u^2 - 2(2N+1)(4N+1)u + (4N+1)^2$$

Now, let $v = \frac{y}{2N}$, $u = -\frac{z}{2N}$, and $z = x - 4N - 1$. Then multiply by $4N^2$:

$$y^2 = z^3 + (4N^2+8N+1)z^2 + 4N(2N+1)(4N+1)z + 4N^2(4N+1)^2$$

Substitute $z = x - 4N - 1$ for our final elliptic curve:

$$y^2 = x^3 + 2(2N^2-2N-1)x^2 + (4N+1)x$$

where $y = \frac{2DN}{b^2}$ and $x = -\frac{2NP}{b} + 4N + 1$.

Running rank calculations for $N \in [1, 999]$ gives 415 curves of rank 0, 502 curves of rank 1, and 80 curves of rank greater than 1. Some calculation gives us that that there are torsion points at $(0,0)$, $(1, \pm 2N)$, and $(4N+1, \pm 2N(4N+1))$.

Once again, we can use isogenous curves. Depending on our choices of torsion points, we have a few options for isogenous curves to solve for various values of N. We could use:

The 2-isogenous curve $v^2 = u^3 - 4(2N^2 - 2N - 1)u^2 + 16N^3(N - 2)u$

The 3-isogenous curve $g^2 = f^3 + 18(2N^2 + 10N - 1)f^2 + 81(4N + 1)^3 f$

The 2-isogenous curve from the above 3-isogenous curve
$i^2 = j^3 - 36(2N^2 + 10N - 1)j^2 + 1296N(N - 2)^3 j$

With these isogenous curves, we can use naive search on various values of N up to a certain number of digits. There is still the possibility that these solutions do not yield positive values for the side lengths. For example, if we let $N = 7$, the only solutions give a positive value for z, which means that $\frac{P}{b}$ is negative. Therefore, one of P and b must be negative, implying negative side lengths. This means that there is still work to be done there to ensure positive side length solutions.

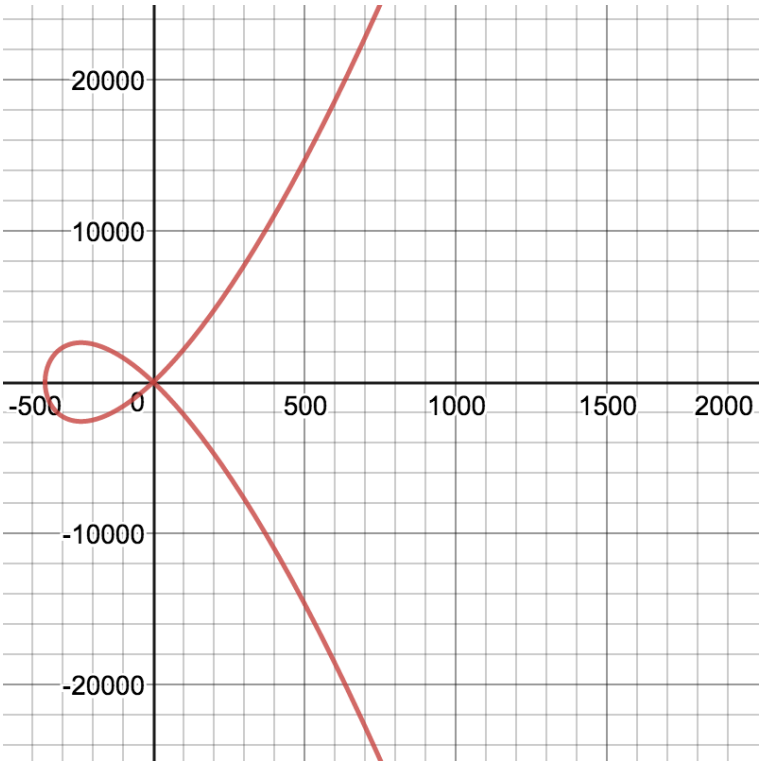

Figure 2: The elliptic curve for $\frac{R}{r} = 10$. The egg component and the infinite component are not touching. They're just very close.

References

[1] A. MacLeod. *Elliptic Curves in Recreational Number Theory.* 2016.

[2] J. Vélu. Isogénies entre courbes elliptiques. *C.R. Acad. Sci. Paris (A)*, 273:238–241, 1971.

[3] L. Washington. *Elliptic Curves: Number Theory and Cryptography.* Taylor & Francis, Boca Raton, Florida, 2008.