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. In 1659, John Pell and Johann Rahn wrote a text which explained how to find all integer solutions to the quadratic equation $u^2 - d\,v^2 = 1$. In 1909, Axel Thue showed that the cubic equation $u^3 - d\,v^3 = 1$ has finitely many integer solutions, so it remains to examine their rational solutions. We explain how to find "large" rational solutions i.e., a sequence of rational points (u_n, v_n) which increase without bound as n increases without bound. Such cubic equations are birationally equivalent to elliptic curves of the form $y^2 = x^3 - D$. The rational points on an elliptic curve form an abelian group, so a "large" rational point (u, v) maps to a rational point (x, y) of "approximate" order 3. Following an idea of Zagier, we explain how to compute such rational points using continued fractions of elliptic logarithms.

Introduction

The equation $u^N - d\,v^N = 1$ seems innocent enough: once we fix an exponent N and a coefficient d, we can try and search for solutions u and v. For example, $u^2 - 2\,v^2 = 1$ has a solution $u = 3$ and $v = 2$; and $u^3 - 7\,v^3 = 1$ has a solution $u = 2$ and $v = 1$. In the exposition that follows, we consider how to find some solutions – whether integral or rational – and examine their properties.

We divide our discussion into two parts. The first concerns the quadratic equation $u^2 - d\,v^2 = 1$. We give an informal discussion of the history of the equation, illuminate the relation with the theory of groups, and review known results on properties of integer solutions through the use of continued fractions. The second concerns the more general equation $u^N - d\,v^N = 1$. We explain why $N = 3$ is the most interesting exponent, present the relation with elliptic curves, and investigate properties of rational solutions through the use of elliptic integrals.

Part 1. John Pell and The Quadratic Equation $u^2 - d\,v^2 = 1$

> *Pell was a striking figure, remarkably handsome, with strong, excellent posture, dark hair and eyes, and a good voice. His temperament was sanguine and melancholic.*
> – Dictionary of National Biography

In 1657, French lawyer and amateur mathematician Pierre de Fermat became interested in positive integer solutions u and v to the equation $u^2 - 61\,v^2 = 1$.

Date: September 29, 2006.

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.

He posed a sadistic challenge to established mathematicians of the day, such as the Englishmen William Brouncker and John Wallis, asking if they could find the solutions he found – without telling them the answer, of course. You see, Fermat had found the solution

$$u = 1766319049 \qquad \text{and} \qquad v = 226153980 \tag{1}$$

by using pen and paper alone! Brouncker and Wallis were intrigued. Over the next year or so, they exchanged letters with Fermat to work out a systematic theory. They eventually found that

> *Given a positive integer d that is not a square, one can always find infinitely many positive integer solutions u and v to the equation $u^2 - d\,v^2 = 1$.*

Soon these methods intrigued other mathematicians as well. In 1659, fellow Englishman John Pell wrote an algebra text with Swiss mathematician Johann Rahn which outlined these methods. A more famous Swiss mathematician eventually learned about this book: Leonhard Euler became interested in these results in 1766, but unfortunately, Euler confused Pell with Brouncker – and to this day the equation $u^2 - d\,v^2 = 1$ is called "Pell's equation" instead of "Brouncker's equation"! But the most rigorous treatment of the equation was given in 1771 by a colleague of Euler's, the Frenchman Joseph-Louis Lagrange. Eventually, Lagrange was bestowed many accolades – including being named to the French Legion of Honor by none less than Napoleon Bonapart himself. It is perhaps fitting then to quote Napoleon on the misnamed equation which is the focus of this paper:

Glory is fleeting, but obscurity is forever.

Poor Brouncker!

Rings and Norms and Groups, Oh My!

We will outline Lagrange's methods, but to do so, we'll use some modern language. Formally, we have the identity

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

Since we want to study integer solutions u and v to the equation $u^2 - d\,v^2 = 1$, we'll consider the following collection of irrational numbers:

$$\mathbb{Z}\big[\sqrt{d}\big] = \left\{u + v\sqrt{d} \;\middle|\; u,\, v \in \mathbb{Z}\right\}. \tag{3}$$

Elements in this set are called *algebraic integers*, as opposed to the rational integers, $\mathbb{Z}$. This definition makes sense for all integers d – not just those that are positive. For example, when $d = -1$ this set forms what are called the *Gaussian integers*. A rational integer u can be thought of as an algebraic integer: indeed, $u = u + 0\sqrt{d}$. For this reason, the rational integers -1, 0, and 1 are elements in $\mathbb{Z}\big[\sqrt{d}\big]$. In general, an algebraic integer a is a number that is a root of a polynomial equation, where the coefficients are rational integers and the leading coefficient is 1:

$$a^N + \alpha_{N-1}\,a^{N-1} + \cdots + \alpha_1\,a + \alpha_0 = 0, \qquad \alpha_i \in \mathbb{Z}. \tag{4}$$

For instance, the algebraic integer $a = u + v\sqrt{d}$ is a root of the quadratic equation $a^2 + \alpha_1\,a + \alpha_0 = 0$, in terms of the rational integers $\alpha_1 = -2\,u$ and $\alpha_0 = u^2 - d\,v^2$.

It is well-known that the collection of all algebraic integers forms a *ring*, just like the rational integers $\mathbb{Z}$. For example, given any two algebraic integers $a = u_1 + v_1\sqrt{d}$ and $b = u_2 + v_2\sqrt{d}$, we can add them and multiply them to get another algebraic integer:

$$\begin{array}{rcccc} a+b & = & (u_1+u_2) & + & (v_1+v_2)\sqrt{d}, \\ a\cdot b & = & (u_1\,u_2 + d\,v_1\,v_2) & + & (u_1\,v_2 + u_2\,v_1)\sqrt{d}. \end{array} \tag{5}$$

When $d = -1$, you'll note the similarity with properties of the complex numbers. We will not formally define a ring, since it does not add to the exposition at hand.

Since we are generalizing properties of the complex numbers to our set $\mathbb{Z}\big[\sqrt{d}\big]$, we make two more familiar definitions. For an algebraic integer $a = u + v\sqrt{d}$, define its *conjugate* as the algebraic integer $\overline{a} = u - v\sqrt{d}$; and its *norm* as the rational integer

$$\mathbb{N}(a) = a \cdot \overline{a} = \left(u + v\sqrt{d}\right)\left(u - v\sqrt{d}\right) = u^2 - d\,v^2. \tag{6}$$

It is easy to show (and we invite the reader to do so) that both the conjugate and norm are multiplicative i.e. $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$ and $\mathbb{N}(a \cdot b) = \mathbb{N}(a) \cdot \mathbb{N}(b)$. We should be a bit careful here: the conjugate and norm are well-defined only when d is not a square. We invite the reader to prove this fact by first considering some examples. (For instance, consider $a = 1 + \sqrt{1} = 2 + 0\sqrt{1}$. What is its conjugate? Norm?)

Now we are ready to consider Pell's (Brouncker's?) equation. Given an integer d that is not a square, we want to consider integer solutions u and v to the equation $u^2 - d\,v^2 = 1$. This is equivalent to considering algebraic integers $a = u + v\sqrt{d}$ with norm $\mathbb{N}(a) = 1$. For this reason, we consider the set

$$G = \left\{ a \in \mathbb{Z}\big[\sqrt{d}\big] \;\middle|\; \mathbb{N}(a) = 1 \right\}. \tag{7}$$

This set has the following properties:

- *Closure*: If both a, $b \in G$ then $a \cdot b \in G$.
- *Identity*: The element $1 \in G$.
- *Inverses*: If $a \in G$ then $1/a \in G$.
- *Associativity:* For all a, b, $c \in G$ we have $a \cdot (b \cdot c) = (a \cdot b)\, c$.
- *Commutativity:* For all a, $b \in G$ we have $a \cdot b = b \cdot a$.

A set with these properties forms an abelian group. We explain why these are true. Closure follows because $\mathbb{N}(a \cdot b) = \mathbb{N}(a) \cdot \mathbb{N}(b) = 1 \cdot 1 = 1$, and the identity exists because $\mathbb{N}(1) = 1$. Associativity and commutativity hold because they hold for all complex numbers. Showing the existence of inverses is a bit tricky. Since $a \in G$, we know that $a \cdot \overline{a} = \mathbb{N}(a) = 1$, so upon dividing both sides by a we have $1/a = \overline{a}$. It suffices to check that $\overline{a}$ is an algebraic integer of norm 1 – which we leave as an exercise.

The One to Rule Them All

Why did we make these definitions? Note that if we are given just one solution to Pell's equation, we can find other solutions by "raising it to an arbitrary integral power." That is, say u_1 and v_1 is a solution to $u^2 - d\,v^2 = 1$, and let $a = u_1 + v_1\sqrt{d}$. Since $\mathbb{N}(a) = 1$ then $\mathbb{N}(a^n) = 1$ as well for any integer n, so denote $u_n + v_n\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^n$. Then u_n and v_n is also a solution to $u^2 - d\,v^2 = 1$! Let's consider an example, say with $d = 2$. By inspection, it is easy to see that $u_1 = 3$ and

$v_1 = 2$ is a solution to $u^2 - 2\,v^2 = 1$. In particular, the norm of an algebraic integer $a = u + v\sqrt{2}$ is $\mathbb{N}(a) = u^2 - 2\,v^2$, and so the element $a = 3 + 2\sqrt{2}$ has norm 1. We can then raise this a to any power in order to obtain other elements with norm 1. For instance, $\left(3 + 2\sqrt{2}\right)^2 = 17 + 12\sqrt{2}$, and it is easy to check that $u_2 = 17$ and $v_2 = 12$ satisfies $u^2 - 2\,v^2 = 1$. We can find other solutions by considering a^3, a^4, and so on. Perhaps we can use this to show there are infinitely many solutions?

Before we get ahead of ourselves, let's focus on three questions:

#1: The integers $u = \pm 1$ and $v = 0$ are trivial integer solutions to $u^2 - d\,v^2 = 1$. Does there even exist *one* nontrivial solution i.e., nontrivial algebraic integer $\delta = u_1 + v_1\sqrt{d}$ of norm 1?

#2: Can we find a nontrivial solution δ so that *all* solutions $a = u_n + v_n\sqrt{d}$ are in the form $a = \pm\delta^n$?

#3: Are there infinitely many positive integer solutions u and v to $u^2 - d\,v^2 = 1$?

We'll focus on Question #1 a bit later, but assuming it is affirmative for the moment, we answer Question #2 with the following statement:

> *Fix a positive integer d that is not a square, and assume that the equation $u^2 - d\,v^2 = 1$ has a nontrivial solution. Then there exists a unique $\delta \in G$ such that*
>
> i. *$\delta > 1$, and*
>
> ii. *for each element $a \in G$ there exists an integer n such that $a = \pm\delta^n$.*

We give the proof stated in LeVeque [3]. Let $a = u + v\sqrt{d} \in G$ be an algebraic integer. Consider the following identities:

$$\begin{aligned} a &= u + v\sqrt{d}, \\ 1/a &= u - v\sqrt{d}, \end{aligned} \qquad \text{and} \qquad \begin{aligned} -a &= -u - v\sqrt{d}, \\ -1/a &= -u + v\sqrt{d}. \end{aligned} \tag{8}$$

Since each of these is an algebraic integer of norm 1, each is an element of G. It follows that we may assume u and v are nonnegative integers, so that $a \geq 1$. If $a = 1$ then $a = \delta^0$, so assume $a > 1$. There exists at least one such algebraic integer $a = u + v\sqrt{d}$ because we're assuming that there is a nontrivial solution to $u^2 - d\,v^2 = 1$. Let $\delta \in G$ be the smallest element such that $\delta = u_1 + v_1\sqrt{d} > 1$; such an element exists because the set $\left\{v \in \mathbb{Z} \;\middle|\; v > 0 \text{ and } u = \sqrt{d\,v^2 + 1} \in \mathbb{Z}\right\}$ has a least element v_1 by the Well Ordering Principle. Then $1 < \delta \leq a$, so choose the positive integer $n = \lfloor \log a / \log \delta \rfloor$ in terms of the floor function. Then $\delta^n \leq a < \delta^{n+1}$, and so $1 \leq (a/\delta^n) < \delta$. By the minimality of δ, we must have $a/\delta^n = 1$.

The element δ above is called the *Fundamental Solution*. Now that Question #2 is answered, we can answer Question #3. We'll use the Fundamental Solution to list infinitely many positive integer solutions! Write $\delta = u_1 + v_1\sqrt{d} > 1$ as the Fundamental Solution, and consider the sequence of algebraic integers $u_n + v_n\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^n$ for $n = 0,\, 1,\, 2, \ldots$. By taking the conjugate of both sides, we have

$$\begin{aligned} u_n + v_n\sqrt{d} &= \delta^n, \\ u_n - v_n\sqrt{d} &= \delta^{-n}; \end{aligned} \qquad \text{so adding and subtracting gives} \qquad \begin{aligned} u_n &= \frac{\delta^n + \delta^{-n}}{2}, \\ v_n &= \frac{\delta^n - \delta^{-n}}{2\sqrt{d}}. \end{aligned} \tag{9}$$

This may look strange, but u_n and v_n are still positive integers. Since $\delta > 1$ yet $\delta^{-1} < 1$ we see that both u_n and v_n increase without bound as n increases without

bound. Hence there are infinitely many positive integer solutions u and v to the equation $u^2 - d\,v^2 = 1$. In fact, the ratios u_n/v_n give great approximations to $\sqrt{d}$ because

$$\frac{u_n}{v_n} = \sqrt{d}\,\frac{\delta^{2n}+1}{\delta^{2n}-1} \to \sqrt{d} \qquad \text{as} \qquad n \to \infty. \tag{10}$$

We mention in passing that the statements above may be expressed using the theory of groups: $\{\pm 1\} \simeq Z_2$ is a cyclic group of order 2, and $\langle \delta^n \mid n \in \mathbb{Z}\rangle \simeq \mathbb{Z}$ is a cyclic group of infinite order, so the statement $a = \pm\delta^n$ means

$$G = \left\{ a \in \mathbb{Z}\big[\sqrt{d}\big] \;\middle|\; \mathbb{N}(a) = 1 \right\} \simeq Z_2 \times \mathbb{Z} \qquad \text{when } d > 0 \text{ is not a square.} \tag{11}$$

We'll explain a bit later why this holds for positive integers d, and not for negative.

Making Sense of Irrational Behavior

Fix a positive integer d that is not a square. We've seen that if a nontrivial integer solution u_1 and v_1 exists for the equation $u^2 - d\,v^2 = 1$, then we can generate infinitely many integer solutions u and v to $u^2 - d\,v^2 = 1$ from the relation

$$u + v\sqrt{d} = \pm\left(u_1 + v_1\sqrt{d}\right)^n \qquad \text{for any integer } n. \tag{12}$$

Conversely, if u_1 and v_1 are small enough (i.e, $\delta = u_1 + v_1\sqrt{d}$ is the Fundamental Solution) then every integer solution arises this way. So when does a nontrivial integer solution exist? We come back to Lagrange. Here is his remarkable result:

> *Given a positive integer d that is not a square, one can always find at least one positive integer solution u and v to the equation $u^2 - d\,v^2 = 1$.*

The proof of this statement relies on properties of continued fractions. Before we outline the proof, we remark that this statement is *false* when d is a negative integer. Indeed, when $d = -1$, we invite the reader to compute all integer solutions to $u^2 + v^2 = 1$. Is it possible to find *positive* integers u and v?

Continued fractions are a way to approximate an irrational number by a sequence of rational numbers. Given a positive integer d that is not a square, the irrational number of interest is $\sqrt{d}$. Given any irrational number x, define the sequence of irrational numbers recursively by

$$x_0 = x, \qquad x_{k+1} = \frac{1}{x_k - \lfloor x_k \rfloor} \quad \text{for } k = 0,\, 1,\, 2, \ldots \tag{13}$$

in terms of the floor function. The *continued fraction* of x is the infinite nested fraction

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \qquad \text{where } a_k = \lfloor x_k \rfloor \text{ is an integer.} \tag{14}$$

We really only want to deal with finitely many terms, so for each positive integer n denote the *nth convergent* as that quantity obtained by including just the first n

terms of the continued fraction:

$$\{a_0;\, a_1,\, a_2, \ldots,\, a_{n-1}\} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_{n-1}}}}}. \tag{15}$$

(*Warning*: this is *not* the standard convention for the nth convergent!) This is some rational number which we denote in lowest terms by

$$\{a_0;\, a_1,\, a_2, \ldots,\, a_{n-1}\} = \frac{u_n}{v_n}. \tag{16}$$

We give an example. Consider $d = 2$ i.e., we compute the continued fraction of $\sqrt{2} = 1.4142135\ldots$. The table below on the left lists the irrational numbers x_k and their integer parts a_k, whereas the table below on the right lists the convergents:

k	x_k	a_k
0	1.4142135	1
1	2.4142135	2
2	2.4142135	2
3	2.4142135	2
4	2.4142135	2

n	$\{a_0; a_1, \ldots, a_{n-1}\}$	u_n	v_n
1	$\{1\}$	1	1
2	$\{1; 2\}$	3	2
3	$\{1; 2, 2\}$	7	5
4	$\{1; 2; 2; 2\}$	17	12
5	$\{1; 2; 2; 2; 2\}$	41	29

As for the table on the left, note that eventually the a_k's repeat, and do so forever. It's easy to see why: Upon rationalizing the denominator

$$\frac{1}{1+\sqrt{2}} = \sqrt{2} - 1 \qquad \text{we find that} \qquad \sqrt{2} = 1 + \frac{1}{1+\sqrt{2}}. \tag{17}$$

Now we can substitute $\sqrt{2}$ iteratively in the denominator:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{1+\sqrt{2}}} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2+\cdots}}} = \{1; 2, 2, 2, \ldots\}. \tag{18}$$

As for the table on the right, did you notice the pattern $u_n^2 - 2\,v_n^2 = (-1)^n$?

Lagrange proved two remarkable facts about the continued fraction of $\sqrt{d}$ and the relationship with solutions to Pell's equation:

Fix a positive integer d which is not a square.

i. *The continued fraction of $\sqrt{d}$ is in the form*

$$\sqrt{d} = \{a_0;\, \overline{a_1,\, a_2, \ldots,\, a_{h-1},\, 2\,a_0}\} \tag{19}$$

where the bar means the sequence of h terms repeats indefinitely.

ii. *Write the hth convergent of the continued fraction above as the rational number*

$$\{a_0;\, a_1,\, a_2, \ldots,\, a_{h-1}\} = \frac{u_h}{v_h}. \tag{20}$$

Then u_h and v_h are positive integers which satisfy the relation $u_h^2 - d\,v_h^2 = (-1)^h$.

Instead of giving a proof, we explain how to use this to find the Fundamental Solution δ. The process when h is even is slightly different than when h is odd. In the former case we have $u_h^2 - d\,v_h^2 = 1$, whereas in the latter case h is odd we have $u_h^2 - d\,v_h^2 = -1$. Hence, whenever h is the smallest period, the Fundamental Solution is

$$\delta = \begin{cases} u_h + v_h\sqrt{d} & \text{if } h \text{ is even,} \\ u_{2h} + v_{2h}\sqrt{d} = \left(u_h + v_h\sqrt{d}\right)^2 & \text{if } h \text{ is odd.} \end{cases} \tag{21}$$

Let's use this to work through a couple of examples. First consider $d = 2$; we want to recover our solution $u = 3$ and $v = 2$ to the equation $u^2 - 2\,v^2 = 1$. The continued fraction of interest is $\sqrt{2} = \{1; \overline{2}\}$, so $h = 1$. The first convergent gives $u_1 = 1$ and $v_1 = 1$, which satisfies $u_1^2 - 2\,v_1^2 = -1$. The second convergent gives $u_2 = 3$ and $v_2 = 2$, which satisfies $u_2^2 - 2\,v_2^2 = 1$. Hence $\delta = 3 + 2\sqrt{2} = \left(1 + \sqrt{2}\right)^2$ is the Fundamental Solution in this case. Now consider $d = 61$; we want to recover Fermat's nontrivial solution to the equation $u^2 - 61\,v^2 = 1$. The continued fraction of interest is

$$\sqrt{61} = \left\{7; \overline{1,\ 4,\ 3,\ 1,\ 2,\ 2,\ 1,\ 3,\ 4,\ 1,\ 14}\right\}. \tag{22}$$

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

$$\frac{u_{11}}{v_{11}} = \{7;\ 1, 4, 3, 1, 2, 2, 1, 3, 4, 1\} = \frac{29718}{3805}. \tag{23}$$

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

$$\frac{u_{22}}{v_{22}} = \{7; 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1\} = \frac{1766319049}{226153980}. \tag{24}$$

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

$$\delta = 1766319049 + 226153980\sqrt{61} = \left(29718 + 3805\sqrt{61}\right)^2. \tag{25}$$

In other words, a positive integer solution u and v to the equation $u^2 - 61\,v^2 = 1$ is

$$u = 1766319049 \qquad \text{and} \qquad v = 226153980. \tag{26}$$

Remarkably, this is Fermat's original solution!

Part 2. Axel Thue and the Cubic Equation $u^3 - d\,v^3 = 1$

> *The further removed from usefulness or practical application, the more important.*
> – Axel Thue.

With the publication of Joseph-Louis Lagrange's results in 1771, we know that the equation $u^2 - d\,v^2 = 1$ has infinitely many integer solutions u and v for each positive integer d that is not a square. Can we generalize this? For instance, why consider just integer solutions? Why not consider rational solutions? And what's special about the exponent 2? Why not consider the equation $u^N - d\,v^N = 1$?

Let's Think Rationally About This!

Let's try and tackle the most general case – but looking for integer solutions. Consider a homogeneous polynomial of degree N with integer coefficients:

$$f(u,v) = \alpha_N\, u^N + \alpha_{N-1}\, u^{N-1}\, v + \cdots + \alpha_0\, v^N, \qquad \alpha_i \in \mathbb{Z}. \tag{27}$$

We consider only irreducible polynomials i.e., we cannot factor $f(u,v) = g(u,v) \cdot h(u,v)$ into homogeneous polynomials g and h of smaller degree with integer coefficients. In particular, we assume that not all of the integers α_i have a common divisor. For example, Pell's equation is related to the polynomial $f(u,v) = u^2 - d\,v^2$ for integers d. This polynomial is irreducible precisely when d is not a square.

For each nonzero integer m, what can we say about the number of integer solutions u and v to an equation $f(u,v) = m$? In 1909, Norwegian mathematician Axel Thue proved a remarkable result:

> *Fix an irreducible homogeneous polynomial of degree N with integer coefficients. For each nonzero integer m, consider the equation*
>
> $$\alpha_N\, u^N + \alpha_{N-1}\, u^{N-1}\, v + \cdots + \alpha_0\, v^N = m.$$
>
> *If $N = 1$ there are infinitely many integer solutions u and v. If $N \geq 3$ there are only finitely many integer solutions u and v.*

The interested reader should consult Silverman and Tate [7] for a proof.

As an example of Thue's result, consider $N = 3$. As a special case of the above theorem, it follows that, given an integer d that is not a cube, the equation $u^3 - d\,v^3 = 1$ has only finitely many integer solutions u and v. This is by no means obvious.

The case $N = 1$ is actually a well-known result. Here we have the linear equation $a\,u + b\,v = m$, where a, b, and m are relatively prime integers. One proves in an introductory course in Abstract Algebra (or even Number Theory) that this equation has infinitely many integer solutions u and v. Indeed, if u_0 and v_0 is one integer solution, then other solutions are given by

$$\begin{aligned} u &= u_0 + b\,n \\ v &= v_0 - a\,n \end{aligned} \qquad \text{for any integer } n.$$

One can find the initial solution u_0 and v_0 through the Euclidean algorithm. It turns out that *every* integer solution u and v is in the form above for some integer n. (We leave this an exercise for the reader; here is one approach. Start by showing the relation $a\,(u - u_0) = b\,(v_0 - v)$, and observe that a and b are relatively prime. Conclude that $u - u_0$ is a multiple of b, and that $v_0 - v$ is a multiple of a.)

Why is $N = 2$ missing from the theorem? Let's revisit the equation $u^2 - d\,v^2 = 1$ once more. When $d > 0$ is not a square, there are infinitely many integer solutions, but when $d < 0$ there are only finitely many integer solutions. Unfortunately, equations with exponent $N = 2$ don't have a simple classification of their integer solutions; you can't determine the number of solutions based on the degree alone.

We have a satisfactory answer for the number of integer solutions to $f(u,v) = m$, but what about *rational* solutions? If an integer solution exists, then it is by definition a rational solution. Unfortunately, the converse is not true: just because a rational solution exists, that's not enough to say an integer solution does as well. For instance, consider solutions to $2\,u = 3$. For each nonzero integer m, what can we say about the number of *rational* solutions u and v to an equation $f(u,v) = m$?

Surprisingly, not much was known until 1983. That year, a 29 year-old German mathematician named Gerd Faltings proved a series of results in a branch known

as Algebraic Geometry, verifying a long-standing conjecture of L. J. Mordell. One consequence of his work is the following result:

> *Fix an irreducible homogeneous polynomial of degree N with integer coefficients. For each nonzero integer m, consider the equation*
>
> $$\alpha_N\, u^N + \alpha_{N-1}\, u^{N-1}\, v + \cdots + \alpha_0\, v^N = m.$$
>
> *If $N = 1$ there are infinitely many rational solutions u and v. If $N \geq 4$ there are only finitely many rational solutions u and v.*

For this result (which was not even the main result of his work), Faltings won the Fields Medal in 1986, the most prestigious award to be given to a mathematician. In fact, he was – and still is! – the only German to ever win the prize.

The above result suggests that equations with exponent $N = 2$ or 3 don't have a simple classification of their rational solutions. Indeed, we'll show that this is the case. Let's focus on $N = 2$ for the moment. We'll show the following:

> *Given an integer d which is not a square, the equation $u^2 - d\, v^2 = 1$ has infinitely many rational solutions u and v.*

Surprisingly, this result holds for d positive or negative – regardless of the number of integer solutions! For example, when $d = -1$, there are only finitely many integers u and v such that $u^2 + v^2 = 1$, but there are infinitely many rational points (u, v) on the unit circle. To explain why this result is true in general, we first parametrize all rational solutions u and v. We know that $u = \pm 1$ and $v = 0$ are solutions, so consider now only the nontrivial rational solutions. Denote $x = d\, v/(u-1)$. Solving for v and then substituting this into the equation $u^2 - d\, v^2 = 1$ gives

$$u = \frac{x^2 + d}{x^2 - d} \qquad \text{and} \qquad v = \frac{2\, x}{x^2 - d}. \tag{28}$$

Conversely, making these choices for u and v for *any* rational number x gives rational solutions to $u^2 - d\, v^2 = 1$. Since there are infinitely many choices for x, there are infinitely many solutions.

What about $N = 3$? What can we say about the number of rational solutions u and v to the equation $a\, u^3 + b\, u^2\, v + c\, u\, v^2 + d\, v^3 = m$?

Three is A Magic Number

The following table recaps what we know about the solutions u and v to the equation $f(u, v) = m$:

N	Number of Integer Solutions	Number of Rational Solutions
1	Infinitely Many	Infinitely Many
2	?	?
3	Finitely Many	?
≥ 4	Finitely Many	Finitely Many

We've spent the first half of this exposition discussing the integer solutions of quadratic equations, so we spend this half discussing the rational solutions of cubic equations.

Fortunately for us, rational points on cubic equations such as

$$a\, u^3 + b\, u^2\, v + c\, u\, v^2 + d\, v^3 = m \tag{29}$$

have a long and rich history. In order to simplify our exposition, we'll make the following two assumptions:

- *Nonsingularity:* The cubic equation above involves the cubic polynomial $f(u,1) = a\,u^3 + b\,u^2 + c\,u + d$, so we assume that its discriminant

$$\text{Disc}(f) = b^2\,c^2 - 4\,a\,c^3 - 4\,b^3\,d + 18\,a\,b\,c\,d - 27\,a^2\,d^2 \tag{30}$$

  is nonzero. We do not assume $f(u,v) = a\,u^3 + b\,u^2\,v + c\,u\,v^2 + d\,v^3$ is irreducible.
- *Normal Form:* We assume there is a rational *point of inflection* on the curve. That means there are rational numbers u_0 and v_0 such that the Hessian matrix of the cubic polynomial $a\,u^3+b\,u^2\,v+c\,u\,v^2+d\,v^3$ is singular. Rather explicitly, there is a rational solution u_0 and v_0 to the system of equations

$$\begin{aligned} a\,u_0^3 + b\,u_0^2\,v_0 + c\,u_0\,v_0^2 + d\,v_0^3 &= m \\ \left(b^2 - 3\,a\,c\right)u_0^2 + (b\,c - 9\,a\,d)\,u_0\,v_0 + \left(c^2 - 3\,b\,d\right)v_0^2 &= 0 \end{aligned} \tag{31}$$

  Given such a solution, let w_0 be a nonzero rational number such that $v_0\,w_0 = \left(b^2 - 3\,a\,c\right)$. Since the quadratic equation has a rational root, the quantity $\sqrt{-3\,\text{Disc}(f)}$ will be an integer. (We leave this as an exercise.)

These criteria are not as harsh as one might imagine. As a generalization of the quadratic equation $u^2 - d\,v^2 = 1$, consider the cubic equation $u^3 - d\,v^3 = 1$. The discriminant is $-27\,d^2$, and so it is nonzero whenever d is nonzero – a criterion that is certainly satisfied if d is not a cube. The rational point $(u_0, v_0) = (1, 0)$ is a rational point of inflection because $u_0 = 1$ and $v_0 = 0$ is a rational solution for the set of equations $u_0^3 - d\,v_0^3 = 1$ and $9\,d\,u_0\,v_0 = 0$.

Why make these assumptions in the first place? There is a method to the madness! We make these assumptions for the following result:

Fix integers a, b, c and d such that $Disc(f) \neq 0$. For each nonzero integer m, consider the cubic curve

$$C: \qquad a\,u^3 + b\,u^2\,v + c\,u\,v^2 + d\,v^3 = m. \tag{32}$$

Assume the existence of rational numbers u_0, v_0, and w_0 as above. If (u,v) is a rational point on C, then via the substitution

$$\begin{aligned} x &= 4\,m\,\frac{v_0\,(u-u_0) - u_0\,(v-v_0)}{(3\,a\,u_0 + b\,v_0)\,(u-u_0) + (b\,u_0 + c\,v_0)\,(v-v_0)}\,w_0 \\ y &= 4\,m\,\frac{(3\,a\,u_0 + b\,v_0)\,(u+u_0) + (b\,u_0 + c\,v_0)\,(v+v_0)}{(3\,a\,u_0 + b\,v_0)\,(u-u_0) + (b\,u_0 + c\,v_0)\,(v-v_0)}\,\sqrt{-3\,Disc(f)} \end{aligned} \tag{33}$$

the point (x,y) is a rational point on the cubic curve

$$E: \qquad y^2 = x^3 - D \qquad \text{where} \qquad D = -16\,m^2\,Disc(f). \tag{34}$$

Conversely, we can recover (u,v) via the substitution

$$\begin{aligned} u &= u_0\,\frac{y + 4\,m\sqrt{-3\,Disc(f)}}{y - 4\,m\sqrt{-3\,Disc(f)}} + \frac{b\,u_0 + c\,v_0}{w_0}\,\frac{2\sqrt{-3\,Disc(f)}\;x}{y - 4\,m\sqrt{-3\,Disc(f)}} \\ v &= v_0\,\frac{y + 4\,m\sqrt{-3\,Disc(f)}}{y - 4\,m\sqrt{-3\,Disc(f)}} - \frac{3\,a\,u_0 + b\,v_0}{w_0}\,\frac{2\sqrt{-3\,Disc(f)}\;x}{y - 4\,m\sqrt{-3\,Disc(f)}} \end{aligned} \tag{35}$$

Moreover, this transformation sends the point of inflection $(u_0,\, v_0)$ *on* C *to a point "at infinity" on* E*.*

Plain and simple, this result states that the study of rational points on the cubic $a\,u^3 + b\,u^2\,v + c\,u\,v^2 + d\,v^3 = m$ may be reduced to the study of rational points on $y^2 = x^3 - D$. We remark that similar formulas can be found in Mordell [4].

Here is a specific example. Consider a curve $u^3 - d\,v^3 = 1$ such that $\mathrm{Disc}(f) = -27\,d^2$ is nonzero. The substitutions

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

give a one-to-one correspondence with rational points (u, v) on $C:\ u^3 - d\,v^3 = 1$ and rational points (x, y) on $E:\ y^2 = x^3 - 432\,d^2$.

I Sing the Curve Elliptic

Let's spend some time discussing the equation $y^2 = x^3 - D$ where D is a nonzero integer. In general, cubic equations in the form

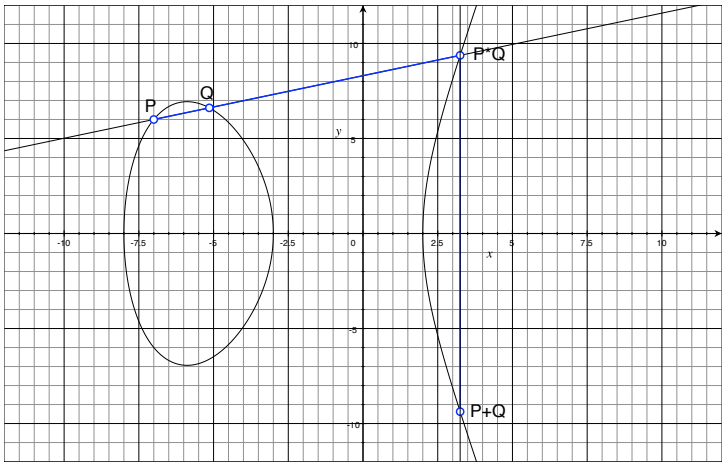
$$E: \quad y^2 = x^3 + A\,x + B \tag{37}$$

for integers A and B with $4\,A^3 + 27\,B^2 \neq 0$, are called *elliptic curves*. Maybe you've heard of them. So what makes these curves so interesting? Well, the set of rational points forms an abelian group.

The *group law* describes a way of combining two rational points P and Q to yield a third rational point $P \oplus Q$ also on the curve. Here's how: Given two rational points, we draw the line through them, then mark where it intersects the cubic curve. Call this third rational point $P * Q$. Reflecting this point through the x-axis will yield another rational point, which we denote as $P \oplus Q$. The order in which we draw the line is unimportant, so $P \oplus Q = Q \oplus P$. The *identity element* is the "point at infinity" mentioned above; we denote it by $\mathcal{O}$. The inverse $[-1]P$ of a rational point P is its reflection through the x-axis i.e., $[-1]P = P * \mathcal{O}$. Adding a point to its inverse will yield the identity $\mathcal{O}$ because the line through the two points will be vertical.

For explicit formulas, express the line through two rational points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ as $y = \lambda\,x + \nu$. If $P \neq Q$ we may choose $\lambda = (y_2 - y_1)/(x_2 - x_1)$; otherwise we take the slope of the line tangent at P. (The criteria $4\,A^3 + 27\,B^2 \neq 0$ guarantees that the slope always exists.) We have

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\lambda^2 - x_1 - x_2,\ \frac{3\,\lambda\,(x_1 + x_2) - y_1 - y_2}{2} - \lambda^3\right). \tag{38}$$



Group Law on an Elliptic Curve

The group law isn't really specific to the rational numbers $\mathbb{Q}$. In fact, we can consider points $P = (x, y)$ with coordinates x and y which are real numbers or even complex numbers. Hence, if we set $K = \mathbb{Q}$, $\mathbb{R}$, or even $\mathbb{C}$, the set of K-rational points as enlarged by the "point at infinity"

$$E(K) = \left\{ (x, y) \in K \times K \;\middle|\; y^2 = x^3 + A\,x + B \right\} \cup \{\mathcal{O}\} \tag{39}$$

has the following properties:

- *Closure:* If both P, $Q \in E(K)$ then $P \oplus Q \in E(K)$.
- *Identity:* The element $\mathcal{O} \in E(K)$.
- *Inverses:* If $P \in E(K)$ then $[-1]P \in E(K)$.
- *Associativity:* For all P, Q, $R \in E(K)$ we have $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$.
- *Commutativity:* For all P, $Q \in E(K)$ we have $P \oplus Q = Q \oplus P$.

The only property we haven't explained is associativity. Did you wonder why we chose $P \oplus Q = (P * Q) * \mathcal{O}$ instead of $P * Q$? This is because of the five properties above, only associativity doesn't hold for $*$. This means $E(K)$ is an abelian group.

We'll study $E(\mathbb{R})$ and $E(\mathbb{C})$ later, but for now, let's consider the structure of this abelian group $E(\mathbb{Q})$ in more detail. Given a positive integer m, denote $[m]\,P = P \oplus P \oplus \cdots \oplus P$ as the point P added to itself m times. Rather explicitly,

$$\begin{aligned} [-1](x, y) &= (x, -y) \\ [2](x, y) &= \left(\frac{x^4 - 2\,A\,x^2 - 8\,B\,x + A^2}{{\psi_2}^2},\ \frac{x^6 + 5\,A\,x^4 + \cdots}{{\psi_2}^3} \right) \\ [3](x, y) &= \left(\frac{x^9 - 12\,A\,x^7 + \cdots}{{\psi_3}^2},\ y\,\frac{x^{12} + 22\,A\,x^{10} + \cdots}{{\psi_3}^3} \right) \end{aligned} \tag{40}$$

where we have denoted the 2- and 3-*division polynomials* as $\psi_2 = 2\,y$ and $\psi_3 = 3\,x^4 + 6\,A\,x^2 + 12\,B\,x - A^2$, respectively. We say P is an m-*torsion point* if $[m]\,P = \mathcal{O}$ i.e., if $\psi_m = 0$. Denote the collection of these points of finite order by $E(\mathbb{Q})_{\text{tors}}$; this is a subgroup of $E(\mathbb{Q})$. In the cases of interest for us, this torsion subgroup is easy to compute:

With assumptions as above, let $E : y^2 = x^3 - D$ be the elliptic curve corresponding to the equation $a\,u^3 + b\,u^2\,v + c\,u\,v^2 + d\,v^3 = m$ i.e. $D = -16\,m^2\,Disc(f)$. Then $\#E(\mathbb{Q})_{tors} = 1$, 2 or 3.

We sketch why this statement is true. It is well-known that $\#E(\mathbb{Q})_{\text{tors}}$ divides 6. (The proof uses some results on elliptic curves over finite fields; see for instance Silverman and Tate [7, Exercise 4.11, pg. 142].) If we had equality, then we would have both a point of order 2 and a point of order 3; assume this is the case in order to find a contradiction. The 2-division polynomial is $\phi_2 = 2\,y$, so $P = (x, y)$ is a 2-torsion point when $y = 0$ and $x^3 = D$. Hence D must be a perfect cube. The 3-division polynomial is $\psi_3 = 3\,x\left(x^3 - 4\,D\right)$, so $P = (x, y)$ is a 3-torsion point when either $x = 0$ and $y^2 = -D$ or $x = \sqrt[3]{4\,D}$ and $y = \sqrt{3\,D}$. The latter cannot happen since D is a perfect cube, so $-D$ must be a perfect square. We know $\sqrt{-3\,\text{Disc}(f)}$ is an integer, so write $\text{Disc}(f) = -3\,n^2$ for some integer n. Then $D = -16\,m^2\,\text{Disc}(f) = 48\,m^2\,n^2$ is positive which means $-D$ cannot be a perfect square! Hence $\#E(\mathbb{Q})_{\text{tors}} \neq 6$.

This discussion explains how to find examples of interesting torsion subgroups. Recall that rational points on the cubic $C : u^3 - d\,v^3 = 1$ are in one-to-one correspondence with rational points on $E : y^2 = x^3 - 432\,d^2$. When $d = 3$, the torsion subgroup $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$ is trivial. When $d = 2$, we find that $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (12, 0)\}$ has two elements, where $[2](12, 0) = \mathcal{O}$. When $d = 1$, we find that $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (12, 36), (12, -36)\}$ has three elements, where $[2](12, 36) = (12, -36)$ and $[3](12, 36) = \mathcal{O}$. You may wish to work directly with C instead of E to find these torsion points. We may define a group law on C as being that induced by the group law on E:

$$(u_1, v_1) \oplus (u_2, v_2) = \left(\frac{u_1\,v_1 - u_2\,v_2}{u_2^2\,v_1 - u_1^2\,v_2},\ \frac{u_2\,v_1^2 - u_1\,v_2^2}{u_2^2\,v_1 - u_1^2\,v_2}\right). \tag{41}$$

The identity element is just the point of inflection, $(1, 0)$. One also checks that

$$\begin{aligned}
[-1](u, v) &= \left(\frac{1}{u},\ -\frac{v}{u}\right) \\
[2](u, v) &= \left(-\frac{2\,u^3 - 1}{u^4 - 2\,u},\ -\frac{v\,(u^3 + 1)}{u^4 - 2\,u}\right) \qquad (42) \\
[3](u, v) &= \left(\frac{u^9 - 6\,u^6 + 3\,u^3 + 1}{u^9 + 3\,u^6 - 6\,u^3 + 1},\ -\frac{3\,u\,v\,(u^6 - u^3 + 1)}{u^9 + 3\,u^6 - 6\,u^3 + 1}\right)
\end{aligned}$$

We invite the reader to find the 2-torsion points on $u^3 - 2\,v^3 = 1$, or even the 3-torsion points on $u^3 - v^3 = 1$.

All Ranks: Fall In!

In 1922, the English mathematician L. J. Mordell proved a long-standing conjecture of Henri Poincaré:

Let $E : y^2 = x^3 + A\,x + B$ be an elliptic curve. Then $E(\mathbb{Q})$ is a finitely generated abelian group. That is, there is a finite set $\{P_1, P_2, \ldots, P_r\} \subseteq E(\mathbb{Q})$ such that for each $P \in E(\mathbb{Q})$, there exist integers m_1, m_2, $\ldots$, m_r as well as a torsion element $T \in E(\mathbb{Q})_{tors}$ for which we may express

$$P = T \oplus [m_1]P_1 + \oplus[m_2]P_2 \oplus \cdots \oplus [m_r]P_r. \tag{43}$$

Using the language of group theory, this result says there is a nonnegative integer r, called the *rank*, such that $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$. This result was vastly generalized by the Frenchman André Weil in 1930. In honor of both Mordell and Weil, the set $E(\mathbb{Q})$ is called the *Mordell-Weil group*. For more information, see Silverman and Tate [7]. (For more advanced reading, see Silverman [5] and [6].)

We've seen that the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ of the elliptic curve $E: y^2 = x^3 - D$ is well-understood. But what about the rank r? To give an idea, the table below lists information about the Mordell-Weil group $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$ when $D = 432\,d^2$ for positive integers d up to 100. Recall that this is equivalent to the curve $u^3 - d\,v^3 = 1$.

Mordell-Weil Group of $u^3 - d\,v^3 = 1$

Rank	Torsion	Corresponding d's
0	1	3, 4, 5, 10, 11, 14, 18, 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
0	Z_2	2, 16, 54
0	Z_3	1, 8, 27, 64
1	1	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
2	1	19, 30, 37, 65, 86, 91

In general, it's not too hard to show that the Mordell-Weil group of the curve $E: y^2 = x^3 - 432\,d^2$ is one of three types:

$$E(\mathbb{Q}) \simeq \begin{cases} Z_3 & \text{if } d \text{ is a cube,} \\ Z_2 & \text{if } d \text{ is twice a cube,} \\ \mathbb{Z}^r & \text{otherwise.} \end{cases} \tag{44}$$

(The reader should prove this as an exercise. Here is an approach: The equation $u^3 - d\,v^3 = 1$ only depends on the cube-free part of d. You should be able to determine $E(\mathbb{Q})_{\text{tors}}$ by considering roots of the division polynomials ψ_2 and ψ_3.) You'll note that of the 100 integers listed above, 48 correspond to curves with rank 0 and 46 correspond to curves with rank 1. In general, one expects that a random elliptic curve will have either rank 0 or 1, with each possibility occurring roughly 50% of the time. The first curve with rank 3 doesn't appear until $d = 657$!

There are computer packages, such as `mwrank` and `MAGMA` [1], which will compute the rank r for a given elliptic curve E. Unfortunately these programs use an algorithm which may take anywhere from five seconds to five months to compute this integer. In fact, the algorithm is not guaranteed to terminate at all! You'll note that in the table above, there are $*$'s next to 41 and 59; this is because the aforementioned programs failed to determine the rank exactly. Indeed, computing ranks of elliptic curves is a difficult task.

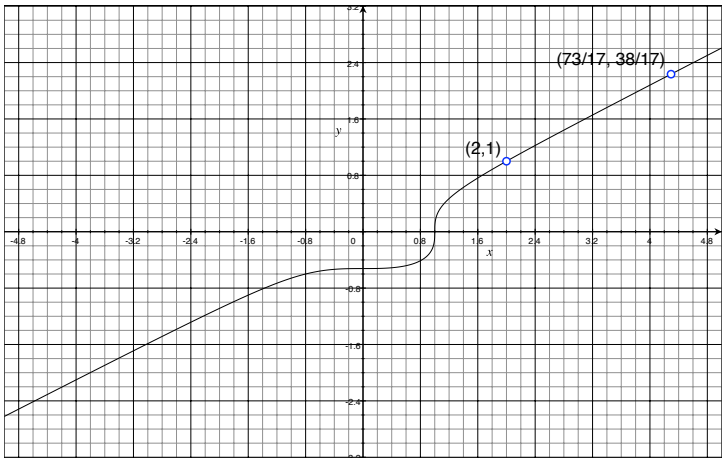
Let's return our attention to the general cubic equation

$$C: \quad a\,u^3 + b\,u^2\,v + c\,u\,v^2 + d\,v^3 = m. \tag{45}$$

As always, we assume that

- the discriminant $\mathrm{Disc}(f)$ is nonzero, and
- there is a rational point of inflection (u_0, v_0) on the curve.

The cubic equation is equivalent to the elliptic curve $y^3 = x^3 - D$ with $D = -16\,m^2\,\mathrm{Disc}(f)$, so we can discuss its rank. If it is zero, then there are only finitely many rational points; in fact, we've seen that there are at most three rational points. We may as well focus on the cases where the curve has positive rank, so that there are infinitely many rational points.



Graph of $u^3 - 7\,v^3 = 1$

We expect these points to be "evenly distributed" on the curve: if we pick any region of the graph, we should be able to find as many rational points as we'd like. But *how* do we find these points? We focus on a couple of questions:

#1: Are the rational points (u, v) on C clustered in any finite region of the graph? Or can we find a sequence of rational points (u_n, v_n) such that $|u_n|$, $|v_n| \to \infty$ as n increases without bound?

#2: How do we explicitly compute such a sequence?

Maybe focusing on the cubic equation C is too difficult, and we should look closely at the elliptic curve E:

> *With notation as above, say* (x_n, y_n) *is the sequence of rational points on* E *corresponding to the sequence of rational points* (u_n, v_n) *on* C*. If* $|u_n|$, $|v_n| \to \infty$ *as* n *increases without bound, let*
>
> $$P = \lim_{n\to\infty} (x_n, y_n) = \left(-4\,m\,\sqrt[3]{\frac{Disc(f)}{m}},\ 4\,m\,\sqrt{-3\,Disc(f)} \right) \tag{46}$$
>
> *be the corresponding limit as a point on* E*. Then* $[3]P = \mathcal{O}$ *i.e.,* P *is 3-torsion point.*

The proof of this isn't very hard. First, one computes the limit using the formulas in (33). Second, one uses the 3-division polynomial $\psi_3 = 3\,x\left(x^3 - 4\,D\right)$ to show P is a 3-torsion point. We remark in general P is not a rational point on E; it may be irrational. But since $\sqrt{-3\,\mathrm{Disc}(f)}$ is an integer, P is actually a *real* point.

As an example of this result, consider the curve $C:\ u^3 - d\,v^3 = 1$. We wish to find a sequence of rational points (u_n, v_n) that increase without bound, so consider

the sequence of rational points on $E: y^2 = x^3 - 432\,d^2$ defined by

$$(x_n, y_n) = \left(12\,d\,\frac{v_n}{u_n - 1},\ 36\,d\,\frac{u_n + 1}{u_n - 1}\right). \tag{47}$$

As n increases without bound,

$$\frac{u_n}{v_n} \to \sqrt[3]{d} \qquad \text{and} \qquad (x_n,\, y_n) \to \left(12\,d^{2/3},\ 36\,d\right). \tag{48}$$

We modify slightly our motivating questions above:

#1: How much control do we have on the rational points (x, y) on E? Can we find a sequence of rational points (x_n, y_n) such that $(x_n, y_n) \to P$ a 3-torsion point as n increases without bound?

#2: How do we explicitly compute such a sequence?

If we have a sequence of rational points (x_n, y_n) on E, then we can recover the desired sequence of rational points (u_n, v_n) on C by using the formulas in (35). We will use continued fractions again to construct such a sequence (x_n, y_n).

Before we continue, we should point out a contrast to the previous half of this exposition. In Part I, we gave an algorithm using continued fractions to construct an initial point (u_1, v_1) on a quadratic curve $u^2 - d\,v^2 = 1$, then used group theory to construct a sequence of points (u_n, v_n) such that $|u_n|, |v_n| \to \infty$ as n increases without bound. Cubic equations in general and elliptic curves in particular are mysterious objects, so we'll present an algorithm which constructs points (u_n, v_n) on a cubic curve $u^3 - d\,v^3 = 1$ – assuming that an initial point (u_1, v_1) can be found by some unspecified method.

Not Your Grandfather's Logarithms

Eventually, we want to construct a sequence of rational points (x_n, y_n) on an elliptic curve which tend to a *real* point P. In fact, we'll prove the following result to help keep track of the real points:

Given the elliptic curve $E: y^2 = x^3 - D$, denote the set of real points P on E by $E(\mathbb{R})$, and the real period of E by the integral

$$\Omega = \int_{\sqrt[3]{D}}^{\infty} \frac{dt}{\sqrt{t^3 - D}}. \tag{49}$$

The map $E(\mathbb{R}) \to \mathbb{R}/\mathbb{Z}$ defined by

$$\log_E : \qquad P = (x, y) \quad \mapsto \quad \frac{1}{2\,\Omega} \int_x^{\infty} \frac{dt}{\sqrt{t^3 - D}} \pmod{\mathbb{Z}} \tag{50}$$

is an isomorphism of abelian groups. (The sign of the square root is the same as the sign of y.)

The isomorphism $\log_E$ is called an *elliptic logarithm*. This result says the real points on E are in one-to-one correspondence with the elements of $\mathbb{R}/\mathbb{Z}$. In particular, if P is a real m-torsion point i.e., $[m]\,P = \mathcal{O}$, then $\log_E(P) = \frac{k}{m}$ for some integer k. Here's an example. The elliptic curve $E: y^2 = x^3 - 432$ has real period $\Omega = 0.883319$. We saw before that $P = (12, 36)$ is a 3-torsion point, so we compute its elliptic logarithm as

$$\log_E(P) = \frac{1}{2\,\Omega} \int_{12}^{\infty} \frac{dt}{\sqrt{t^3 - 432}} = \frac{0.58888}{1.76664} = 0.333333 = \frac{1}{3}. \tag{51}$$

In order to understand where this result comes from, let's try to understand more about the points (x, y) on a general elliptic curve $E : y^2 = x^3 + A\,x + B$. We've considered rational points so far, but as we saw above we need to consider irrational points as well. The Mordell-Weil group $E(\mathbb{Q})$ is a subset of $E(\mathbb{R})$, and the set of real points is a subset of $E(\mathbb{C})$. We know that $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$, but what can we say about $E(\mathbb{R})$ and $E(\mathbb{C})$?

Consider for the moment a function $\wp(z)$ that is the solution to the differential equation

$$\left(\frac{d\wp}{dz}\right)^2 = \wp^3 + A\,\wp + B. \tag{52}$$

Once this function is known, then $(x, y) = (\wp(z),\, \wp'(z))$ is a *complex* point on the elliptic curve $E : y^2 = x^3 + A\,x + B$. We construct the solution in a clever way. Define a function $\wp : \mathbb{C} \to \mathbb{C}$ implicitly as follows. Given $z \in \mathbb{C}$, integrate the function $1/\sqrt{t^3 + A\,t + B}$ along a path integral in the complex plane from ∞ (interpreted as the limit of $i\,y$ as y increases without bound) to a complex number x so that we find a value of z:

$$z = \int_x^\infty \frac{dt}{\sqrt{t^3 + A\,t + B}}. \tag{53}$$

Define $\wp(z) = x$. There is a pole at $z = 0$ because $\wp(0) = \infty$. By the Fundamental Theorem of Calculus, we can differentiate this relation with respect to z:

$$1 = \frac{1}{\sqrt{\wp^3 + A\,\wp + B}}\,\frac{d\wp}{dz} \qquad \text{so that} \qquad \frac{d\wp}{dz} = \sqrt{\wp^3 + A\,\wp + B}. \tag{54}$$

Upon squaring both sides, we find the differential equation above! Not only have we found a solution to the differential equation, but we have defined a map $\mathbb{C} \to E(\mathbb{C})$ that sends $z \mapsto (\wp(z),\, \wp'(z))$.

Actually, we cheated a little bit: we never showed that $\wp$ is a *well-defined* function. Indeed, the integral is not path independent. For motivation, consider the following similar integral:

$$z = \int_x^1 \frac{dt}{\sqrt{1 - t^2}} = \arccos x \qquad \text{so that} \qquad x = \cos z. \tag{55}$$

The function $\arccos x$ is only defined modulo multiples of $2\,\pi$. The integrand has poles at the zeroes ± 1 of the quadratic $t^2 - 1$, so consider an integral which loops m times around this pair of complex numbers:

$$\oint \frac{dt}{\sqrt{1 - t^2}} = 2\,m \int_{-1}^1 \frac{dx}{\sqrt{1 - t^2}} = 2\,\pi\,m \in 2\,\pi\,\mathbb{Z}. \tag{56}$$

That means $x = \cos z$ is a well-defined function $\mathbb{C}/\,(2\,\pi\,\mathbb{Z}) \to \mathbb{C}$. Via the map $z \mapsto (x(z),\, x'(z)) = (\cos z,\, -\sin z)$ we may identify each complex point (x, y) on the unit circle with a complex number $z \in \mathbb{C}/\,(2\,\pi\,\mathbb{Z})$. Indeed, given a point (x, y) on the unit circle, we can recover z as the integral $\int_x^1 \frac{dt}{\sqrt{1-t^2}} \pmod{2\,\pi\,\mathbb{Z}}$.

Let's return to the original integral in (53). The integrand has poles at the zeroes $e_1,\, e_2,\, e_3$ of the cubic $t^3 + A\,t + B$, so consider the integral around closed loops which wind around pairs of these zeroes:

$$\omega_1 = 2\int_{e_1}^\infty \frac{dt}{\sqrt{t^3 + A\,t + B}} \qquad \text{and} \qquad \omega_2 = 2\int_{e_2}^{e_3} \frac{dt}{\sqrt{t^3 + A\,t + B}}. \tag{57}$$

This means $\wp$ is a well-defined function $\mathbb{C}/\Lambda \to \mathbb{C}$ in terms of the *period lattice*

$$\Lambda = \left\{ m\,\omega_1 + n\,\omega_2 \,\middle|\, m,\, n \in \mathbb{Z} \right\} = \omega_1\,\mathbb{Z} + \omega_2\,\mathbb{Z}. \tag{58}$$

Via the map $z \mapsto (\wp(z),\, \wp'(z))$, we may identify each complex point (x, y) on the elliptic curve E with a complex number $z \in \mathbb{C}/\Lambda$. Indeed, given a complex point $P = (x, y)$, we can recover z as the integral

$$\int_P^{\mathcal{O}} \frac{dx}{y} = \int_x^{\infty} \frac{dt}{\sqrt{t^3 + A\,t + B}} \pmod{\Lambda}. \tag{59}$$

Here the sign of the square root is chosen to match the sign of y.

We have shown that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ as sets. There is a slightly stronger result:

> *With notation as above, the map $\mathbb{C}/\Lambda \to E(\mathbb{C})$ defined by $z \mapsto (\wp(z),\, \wp'(z))$ is an isomorphism of abelian groups. That is, for $P, Q \in E(\mathbb{C})$,*
>
> i. *there exist $z_1,\, z_2 \in \mathbb{C}/\Lambda$ such that*
>
> $$P = (\wp(z_1),\, \wp'(z_1)) \qquad \text{and} \qquad Q = (\wp(z_2),\, \wp'(z_2))\,, \tag{60}$$
>
> ii. *under the group law on the elliptic curve we have*
>
> $$P \oplus Q = (\wp(z_1 + z_2),\, \wp'(z_1 + z_2))\,. \tag{61}$$

The complete proof of this result can be found in Silverman [6, Corollary 2.3.1, pg. 420]; the hard part is showing the relation with the group law. In particular, the *real* points on the elliptic curve correspond to the real values of $\wp(z)$. The isomorphism above implies the group isomorphism

$$E(\mathbb{R}) = \left\{ (x, y) \in \mathbb{R} \times \mathbb{R} \,\middle|\, y^2 = x^3 + A\,x + B \right\} \cup \{\mathcal{O}\} \simeq \frac{\mathbb{R}}{\Lambda \cap \mathbb{R}}. \tag{62}$$

Finally, we explain how this is all related to the elliptic logarithm in (50). Let's focus on the elliptic curve $E : y^2 = x^3 - D$. The cubic $t^3 - D$ has just one real root $e_1 = \sqrt[3]{D}$, so $\omega_1 = 2\,\Omega$ – in terms of the real period – is a real number. On the other hand, ω_2 is a purely imaginary number. That means $\Lambda \cap \mathbb{R} = \omega_1\,\mathbb{Z}$, so we have an isomorphism $\mathbb{R}/\,(2\,\Omega\,\mathbb{Z}) \to E(\mathbb{R})$ defined by $z \mapsto (\wp(z),\, \wp'(z))$. The inverse of this map is essentially the elliptic logarithm.

The Point Is to Roam Freely

From now on, we consider a cubic equation

$$C: \quad a\,u^3 + b\,u^2\,v + c\,u\,v^2 + d\,v^3 = m \tag{63}$$

satisfying three criteria:

- $\mathrm{Disc}(f) = b^2\,c^2 - 4\,a\,c^3 - 4\,b^3\,d + 18\,a\,b\,c\,d - 27\,a^2\,d^2$ is nonzero.
- There is a rational point (u_0, v_0) on C satisfying

$$\left(b^2 - 3\,a\,c\right) u_0^2 + (b\,c - 9\,a\,d)\,u_0\,v_0 + \left(c^2 - 3\,b\,d\right) v_0^2 = 0. \tag{64}$$

- $E : y^3 = x^3 - D$ with $D = -16\,m^2\,\mathrm{Disc}(f)$ has positive rank.

Remember that every cubic equation $u^3 - d\,v^3 = 1$ satisfies the first two criteria, because $\mathrm{Disc}(f) = -27\,d^2$ is nonzero and $(u_0, v_0) = (1, 0)$ is a rational point of inflection. We explain how to find a sequence of rational points (u_n, v_n) such that

$|u_n|, |v_n| \to \infty$ as n increases without bound. We use an idea following Guy [2], which in turn is motivated by a paper of Zagier [8].

Perform the following algorithm:

Step 1. Find a rational point $P_1 = (x_1, y_1)$ on E that is not a torsion point. Choose $y_1 > 0$. (Such a point exists because E has positive rank. It suffices to pick a rational point that is not a 2- or 3-torsion point.) Set $n = 1$ and $m_0 = 0$.

Step 2. Compute

$$\gamma = 3 \cdot \frac{1}{2\,\Omega} \int_{x_1}^{\infty} \frac{dt}{\sqrt{t^3 - D}} \qquad \text{in terms of} \qquad \Omega = \int_{\sqrt[3]{D}}^{\infty} \frac{dt}{\sqrt{t^3 - D}}. \tag{65}$$

(These are real numbers which can be computed with any calculator.)

Step 3. Use continued fractions to approximate $\gamma \approx \frac{k_n}{m_n}$ for a numerator k_n not divisible by 3, and a denominator $|m_n| > |m_{n-1}|$.

Step 4. Compute $P_n = [m_n]P_1 = (x_n, y_n)$ as a rational point on E. Choose the sign of m_n so that $y_n > 0$. (Recall that $[-1]\,(x, y) = (x, -y)$.)

Step 5. Return the rational point (u_n, v_n) on C through the formulas in (35). For the curve $u^3 - d\,v^3 = 1$, the formulas simplify to

$$(u_n, v_n) = \left(\frac{y_n + 36\,d}{y_n - 36\,d},\ \frac{6\,x_n}{y_n - 36\,d} \right). \tag{66}$$

Step 6. Increase n, and return to Step 3.

We explain why this algorithm works. Say that (u, v) is a rational point on C corresponding to a rational point $P = (x, y)$ on E. We have seen that $|u|, |v|$ are "large" if and only if $[3]\,P$ is "approximately" $\mathcal{O}$. Say that we've approximated $\gamma \approx \frac{k}{m}$, and write $P = [m]\,P_1$. We compute

$$\log_E\left([3]\,P\right) = 3\,m \cdot \log_E(P_1) = 3\,m \cdot \frac{1}{2\,\Omega} \int_{x_1}^{\infty} \frac{dt}{\sqrt{t^3 - D}} = m\,\gamma \approx k. \tag{67}$$

Hence $\log_E\left([3]\,P\right) \approx 0 \pmod{\mathbb{Z}}$ so that $[3]\,P \approx \mathcal{O}$. Note that if k is divisible by 3, then $\log_E(P) \approx 0 \pmod{\mathbb{Z}}$ so that $P \approx \mathcal{O}$. This is why we stay away from such points.

Let's work through an example. Consider the curve $C:\ u^3 - 7\,v^3 = 1$. It is easy to check that $(u_1, v_1) = (2, 1)$ is one rational point. This cubic equation is equivalent to the elliptic curve $E:\ y^2 = x^3 - 21168$ with $d = 7$; in fact, $(u_1, v_1) = (2, 1)$ corresponds to the rational point $P_1 = (84, 756)$. Rather nicely, the elliptic curve has Mordell-Weil group

$$E(\mathbb{Q}) = \left\{ [m](84, 756) \,\middle|\, m \in \mathbb{Z} \right\} \simeq \mathbb{Z}, \tag{68}$$

so that it has positive rank. We will use the generator $P_1 = (84, 756)$ to construct the desired sequence. The real period is $\Omega = 0.461762$, and we have the continued fraction

$$\gamma = 0.710699\ldots = \{0; 1, 2, 2, 5, 3, 1, 4, 2, 4, \ldots\}. \tag{69}$$

The following table contains the relevant information at the various stages of the algorithm.

Stage n	Convergent of γ	P_n
1	$\{0;1\} = 1/1$	$[1]\,P_1 = (84,\ 756)$
2	$\{0;1,2\} = 2/3$	$[-3]\,P_1 = (57,\ 405)$
3	$\{0;1,2,2\} = 5/7$	$[-7]\,P_1 \approx (42.0481,\ 230.597)$
–	$\{0;1,2,2,5\} = 27/38$	$[38]\,P_1 \approx (9.76 \times 10^5,\ 9.64 \times 10^8)$
4	$\{0;1,2,2,5,3\} = 86/121$	$[-121]\,P_1 \approx (43.4989,\ 247.263)$
5	$\{0;1,2,2,5,3,1\} = 113/159$	$[-159]\,P_1 \approx (44.0055,\ 253.077)$

Note that just after the third stage we find that $[38]\,P \approx \mathcal{O}$ has very large coefficients. This is because the numerator of the convergent, namely 27, is divisible by 3. The $P_n = (x_n, y_n)$ are rational points on E, so we may translate these back to rational points (u_n, v_n) on C:

Stage n	(x_n, y_n)	(u_n, v_n)
1	$P_1 = (84,\ 756)$	$(2,\ 1)$
2	$P_2 = (57,\ 405)$	$(73/17,\ 38/17)$
3	$P_3 \approx (42.0481,\ 230.597)$	$(-22.5476,\ -11.7873)$
4	$P_4 \approx (43.4989,\ 247.263)$	$(-105.386,\ -55.0912)$
5	$P_5 \approx (44.0055,\ 253.077)$	$(469.183,\ 245.269)$

We see that $|u_n|, |v_n| \to \infty$ as desired. What about the rational points P_n on C? They're tending to the limit

$$(x_n,\, y_n) \to \Big(12\,d^{2/3},\ 36\,d\Big) = (43.9117,\, 252)\,. \tag{70}$$

It seems that our mission is accomplished!

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

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

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

[4] L. J. Mordell. *Diophantine equations*. Academic Press, London, 1969.

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

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

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

[8] 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@yale.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