# Elliptic Curves and Other Things

Brian Ton

July 13, 2024

## 1 Some Preliminaries

Much of mathematics has been dedicated to the study of equations. Perhaps the most famous equation is the Pythagorean Formula, discovered in the Ancient Greek times:

**Theorem 1.1** (Pythagorean Theorem)**.** *If $a$, $b$, and $c$ are side lengths of a right triangle, such that $c > a, b$ (i.e. $c$ is the length of the longest side/hypotenuse of the triangle), then*

$$a^2 + b^2 = c^2 \tag{1}$$

Triplets $(a, b, c) \in (\mathbb{Z}_{>0})^3$ are called **Pythagorean Triples**. One natural question is to see if we can figure out some way to obtain all of them. From high school algebra, we know that right triangles are closely related to the unit circle: If $a^2 + b^2 = c^2$, then $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$, hence if $(a, b, c)$ is a Pythagorean triple, then we have obtained a rational point on the unit circle. Drawing a line through the point $(-1, 0)$ and $\left(\frac{a}{b}, \frac{b}{c}\right)$, we see that its slope $m := \frac{b/c}{1+a/c}$ is rational, and the line is given by $y = m(x + 1)$.

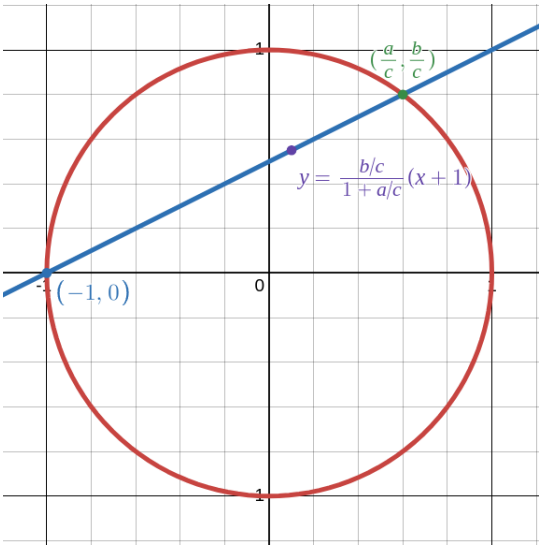


Figure 1: The Unit Circle with Rational Line

Conversely, given a rational number $m = \frac{p}{q}$ where $p$ and $q$ are coprime, then the intersection of the line passing through $(-1, 0)$ and the unit circle is a rational point. With some work, one can show that all the "primitive" Pythagorean triples in the first quadrant (where $a, b, c$ are coprime) can be parameterized by these lines with (positive) rational slope. If $m = \frac{p}{q} > 0$, then since $m$ connects the point $(-1, 0)$ and a point in the first quadrant, $m < 1$, so $p > q$, and the triple $(p^2 - q^2, 2pq, p^2 + q^2)$ is a Pythagorean triple.

Equations like 1 are called Diophantine equations (when we care about integer solutions) and have been a large area of study in number theory. In particular, this is one situation in which elliptic curves naturally arise.

## 2 What is an Elliptic Curve?

We begin here by giving a few equivalent definitions of an elliptic curve given by different authors that give different insights into what an elliptic curve is. In [Loz11], the author gives the following definition of an elliptic curve.

**Definition 2.1** (Elliptic Curve)**.** An **elliptic curve** over $\mathbb{Q}$ is a smooth cubic projective plane curve $E$ defined over $\mathbb{Q}$ with at least one rational point $\mathcal{O} \in E(\mathbb{Q})$ that we call the origin (where $E(\mathbb{Q})$ is the set of points on the projective plane that satisfy $F$).

Unpacking this definition, we note a few things. Often, we take our $\mathcal{O}$ to be the point at infinity $[0:1:0]$. In particular, we see that elliptic curves are defined on the projective plane $\mathbb{P}^2(\mathbb{Q})$, and they are defined by a cubic curve with rational coefficients. That is, they are given by the projective variety $F(X,Y,Z) = 0$, where $F$ has the general form

$$F(X,Y,Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + jYZ^2 + kZ^3 = 0$$

where $a, b, \ldots, k \in \mathbb{Q}$ (noting that $F$ gives a well-defined projective variety, as it is given by a homogenous polynomial). Replacing $\mathbb{Q}$ with other fields, like $\mathbb{C}$, $\mathbb{R}$, $\mathbb{F}_p$, or $K$, we obtain the definition of an elliptic curve over a more general field. The formula for $F$ that we currently have is very unwieldy (there are 11 terms)! We can turn to the definition found in [ST15] for something much easier to work with.

**Definition 2.2** (Elliptic Curve & Weierstrass Form)**.** An **elliptic curve** $E$ over a field $K$ is the graph of an equation of the form $y^2 = x^3 + Ax + B$ where $A, B \in K$ such that $4A^3 + 27B^2 \neq 0$. This is called the **Weierstrass equation** for an elliptic curve.

In what sense are Definition 2.1 and Definition 2.2 equivalent? Well, we firstly note that the condition $4A^3 + 27B^2 \neq 0$ in Definition 2.2 and the "smooth" condition in Definition 2.1 are to ensure that our elliptic curves are non-singular (that is, there are no self-intersections or cusps). If $E$ is an elliptic curve, given by Definition 2.1, we can find a suitable change of coordinates between $E$ and a curve $\hat{E}$ given by an equation given by a Weierstrass equation.

**Proposition 2.1.** *Let $E$ be an elliptic curve, given by Definition 2.1, defined over a field $K$ of characteristic not 2 or 3. Then, there exists a curve $\hat{E}$ given by*

$$zy^2 = x^3 + Axz^2 + Bz^3$$

*where $A, B \in K$ with $4A^3 + 27B^2 \neq 0$ and an invertible change of variables $\psi : E \to \hat{E}$ of the form*

$$\psi([X:Y:Z]) = \left[\frac{f_1(X,Y,Z)}{g_1(X,Y,Z)}, \frac{f_2(X,Y,Z)}{g_2(X,Y,Z)}, \frac{f_3(X,Y,Z)}{g_3(X,Y,Z)}\right]$$

*where $f_i, g_i \in K[X,Y,Z]$ and $\psi(\mathcal{O}) = [0:1:0]$.*

Here, we say that $E$ and $\hat{E}$ are "birationally equivalent", as the transformation between them is given by rational functions. And, in affine coordinates, our equation becomes $y^2 = x^3 + Ax + b$. One proof of this is by seeing that this is a corollary of the Riemann-Roch theorem. Alternatively, there is a more elementary (albeit, longer) proof of this fact in [ST15] that gives an explicit construction of the map $\psi$. The idea behind the proof is that we would like to choose axes (lines) in the projective plane so that our equation for the curve has a simple form. Given our rational point $\mathcal{O}$ on $E$, we take the line $Z = 0$ to be the tangent line to $C$ at $\mathcal{O}$. This tangent line intersects $E$ at one other point (because we are on the projective plane!), and we can take the $X = 0$ axis to be tangent to $E$ at this new point, and $Y = 0$ to be any line going through $\mathcal{O}$ other than the $Z = 0$ axis. Then, letting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, one can obtain an equation in Weierstrass form (noting that $x$ and $y$ are rational functions of our original variables). Of course, this is implemented in Sage using the `WeierstrassForm(cubic)` function! From now on, we will put our elliptic curves in the form of Definition 2.2 or something slightly more general, i.e. an equation of the form $y^2 = x^3 + ax^2 + bx + c$.

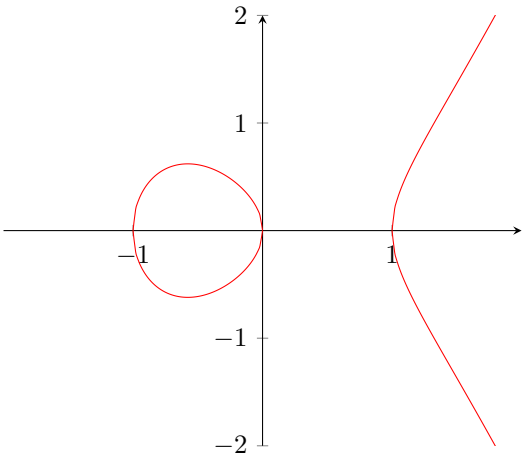


Figure 2: $y^2 = x^3 - x$

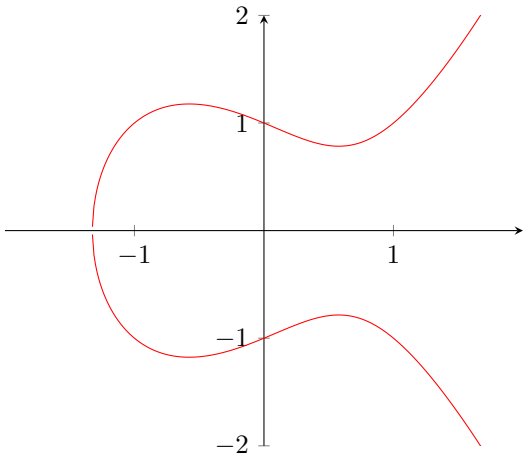


Figure 3: $y^2 = x^3 - x + 1$

## 2.1 The Group Law

We would like to attempt to find an analog of finding rational solutions on our circle. We do this by creating the group of points on our curve, given by a group law. The group law can be described as follows (from [ST15]):

> Let $P$ and $Q$ be points on the elliptic curve $E(K)$, where $K$ is some field. To add two points on $E$, draw the line through $P$ and $Q$, which must intersect $E$ in exactly one other place, $P \cap Q$. If $P = Q$, then take the tangent line to $P$. Draw the line through $\mathcal{O}$ and $P \cap Q$, and take the third intersection point on $E$, and take this to be $P + Q$.

In the particular case of $\mathcal{O}$ being a point at infinity, we have that the last step of finding the intersection of the line through $\mathcal{O}$ and $P \cap Q$ is equivalent to reflecting $P \cap Q$ over the $x$-axis:

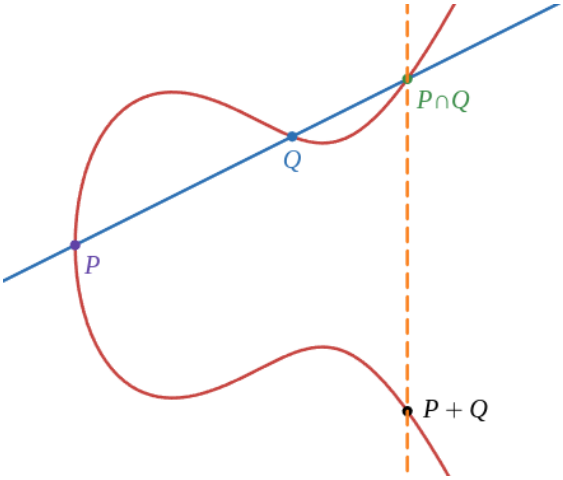


Figure 4: Diagram of the group law

One can find explicit formulas for the group law, splitting into the cases of $P = Q$ and $P \neq Q$. Checking that the points on the curve do form a group under the group law using explicit formulas is very easy for two of the axioms (identity and inverses), but is quite tedious for associativity! However, can invoke the Riemann-Roch theorem again to show this fact. And, we notice here that similar to the case of the unit circle, if $P$ and $Q$ are rational points on the curve, $P + Q$ is also a rational point on the curve. Once we

know that this group law does give us a group, however, it is easy to see that the group is abelian, since the line through $P$ and $Q$ is the same as the line through $Q$ and $P$.

*Remark.* There is a lot of theory on the group of rational points $E(\mathbb{Q})$ of the elliptic curve $E$ that is outside the scope of this essay. In particular, Barry Mazur can showed that over the rationals, this group is finitely generated as an abelian group, hence $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{e_1} \oplus \cdots \oplus \mathbb{Z}/p_r^{e_r}$ for some primes $p_1, \ldots, p_r \in \mathbb{Z}$ by the classification of finitely generated abelian groups. This $r$ is known as the "rank" of $E$, and is the subject of a few open problems (including the Birch Swinerton-Dyer conjecture, one of the Millenium problems).

# 3 What can we do now?

## 3.1 The Congruent Number Problem

In the first section, we parameterized all the Pythagorean triples (and all the right triangles with rational side lengths). Any of these triangles have a rational area. A natural question might be whether all rational numbers occur as the area of some rational triangle (i.e. a triangle such that all side lengths are rational). Unfortunately, this is not true.

**Proposition 3.1.** 1 *does not occur as the area of any rational triangle.*

*Proof Sketch.* Suppose a rational triangle with side lengths $a/d, b/d, c/d$ has area 1 where $a, b, c, d$ are in $\mathbb{Z}$. Then, $a^2 + b^2 = c^2$ and $ab = 2d^2$. One can reduce to the case that $a$ and $b$ are coprime, by dividing by the greatest common divisor to get another set $a', b', c', d'$ that satisfy the same equations. Then, one can deduce that one of $a$ and $b$ is odd since $ab$ is twice a square number (so one can write $a = 2k^2$ and $b = \ell^2$ for some integer $k$ and $\ell$, where $\ell$ is odd). So, $\frac{c+b}{2} = r^4$ and $\frac{c-b}{2} = s^4$, for some relatively prime integers $r, s$. One can deduce that $r^2 + s^2 = t^2$ and $r^2 - s^2 = u^2$ for some relatively prime integers $u$ and $t$. Letting $a'' = \frac{t+u}{2}$, $b'' = \frac{t-u}{2}$, and $c'' = r$ gives another solution to our earlier equations, with $c'' < c$. This process can be infinitely repeated, so we have obtained an infinitely descending chain of integers, a contradiction. □

The proof of this fact was first given by Fermat, and this method of infinite descent is what he used to prove Fermat's Last Theorem for $n = 3$ and 4 (and one can deduce the latter from a very similar argument). Knowing that not all rational numbers are the areas of right triangles, the next natural question to ask is whether we can find a criterion for exactly which rationals do appear as the area of some rational triangle. This leads to a long-open problem called the **congruent number problem**. Such rational numbers that are the areas of rational triangles are called **congruent numbers**.

For any rational number $\frac{p}{q} \in \mathbb{Q}$, we have that there exists some other rational $\frac{r}{s} \in \mathbb{Q}$ such that $\frac{p}{q} \cdot \frac{r}{s}$ is a squarefree positive integer (by inspecting the prime factorizations of the numerator and denominator). So it suffices to consider the squarefree positive integers. But how does this relate to elliptic curves? Much like the question of parameterizing Pythagorean triples, they arise as rational points on certain elliptic curves. We have the following proposition:

**Proposition 3.2.** *A positive squarefree integer $n > 0$ is congruent if and only if the curve $y^2 = x^3 - n^2x$ has a point $(x, y)$ with $x, y \in \mathbb{Q}$ and $y \neq 0$. Moreover, there is a bijection between the sets*

$$C_n = \{(a, b, c) : a^2 + b^2 = c^2, \frac{ab}{2} = n\}, \quad E_n = \{(x, y) : y^2 = x^3 - n^2x, y \neq 0\}$$

*with mutually inverse functions $f : C_n \to E_n$ and $g : E_n \to C_n$*

$$f((a, b, c)) = \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right), \quad g((x, y)) = \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y^2}\right)$$

*Proof.* One simply has to verify the bijections, which can be done via direct computation. □

As an aside, the best-known result on congruent numbers is the following, which partially resolves the problem (and is a full resolution, hinging on the famous Birch Swinnerton-Dyer conjecture).

**Theorem 3.1** (Tunnell)**.** *Let $n$ be a square-free positive integer. Set*

$$f(n) = \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 8z^2 = n\}, \quad g(n) = \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 32z^2 = n\}$$
$$h(n) = \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 4y^2 + 8z^2 = n/2\}, \quad k(n) = \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 4y^2 + 32z^2 = n/2\}$$

*For odd $n$, if $n$ is congruent then $f(n) = 2g(n)$. For even $n$, if $n$ is congruent then $h(n) = 2k(n)$. Moreover, if the Birch Swinnerton-Dyer conjecture is true for the curve $y^2 = x^3 - n^2x$ then the converse of the implications are true (i.e. they become equivalences).*

## 3.2 A Viral Problem

This section is just a remark on a fun problem, and will not go too in-depth with a solution. A few years ago, this innocent looking problem was floating around the internet [Ami]:

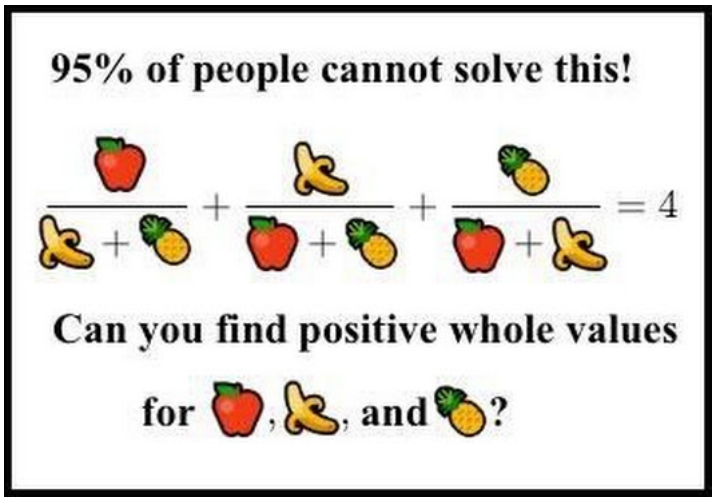


Figure 5: Math with Fruits!

Written in a more compact form, the problem can be expressed as finding $x, y, z \in \mathbb{Z}_{>0}$ such that

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4 \tag{2}$$

which we can recognize as a Diophantine equation (so we know that an elliptic curve might be lurking around the corner). With some trial and error, one can find that $x = 4$, $y = -1$, and $z = 11$ works as a solution, but finding a positive solution is much harder. Bremmer and Macleod showed that solutions to Equation 2 are in bijection to points on the elliptic curve

$$y^2 = x^3 + 109x^2 + 224x \tag{3}$$

using a similar method to Proposition 2.1. Using the group law and starting at the point $P = (9499, -8784, 5165)$ on the curve, one can find other rational points on the curve. With a computer, we can find that $9P$ is a positive integer point on 3! Unfortunately, the solution is a tad big - the smallest coordinate is 81 digits long, and they also showed that this is the solution with the smallest number of digits. So, the meme is correct, at least 95 percent of people likely couldn't have solved it!

# References


[Ami] Alon Amit. *How do you find the positive integer solutions to* $\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4$?. URL: https://w%20ww.quora.com/How-do-you-find-the-positive-integer-solutions-to-frac-x-y+z-+-frac-y-z+x-+-frac-z-x+y-4/answer/Alon-Amit.

[BM14] A. Bremmer and A. Macleod. "An unusual cubic representation problem". In: *Annales Mathematicae et Informaticae* (2014). URL: https://ami.uni-eszterhazy.hu/uploads/papers/finalpdf/AMI_43_from29to41.pdf.

[Cona] Keith Conrad. *Pythagorean Triples*. URL: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pythagtriple.pdf.

[Conb] Keith Conrad. *The Congruent Number Problem*. URL: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/congnumber.pdf.

[Loz11] Á. Lozano-Robledo. *Elliptic Curves, Modular Forms, and Their L-functions*. IAS/Park City mathematics series. American Mathematical Society, 2011. ISBN: 9780821852422. URL: https://books.google.com/books?id=ty-IAwAAQBAJ.

[ST15] J.H. Silverman and J.T. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer International Publishing, 2015. ISBN: 9783319185880. URL: https://books.google.com/books?id=2_PLCQAAQBAJ.

[Was03] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Discrete Mathematics and Its Applications. CRC Press, 2003. ISBN: 9780203484029. URL: https://books.google.com/books?id=vPL19KNdm2wC.