Fermat's Last Theorem GONE WRONG (The Curious Case of $n = 2$)

Isaac Cheng Henry Greenwold

August 4, 2025

1 Pythagorean Triples

1.1 Introduction

A **Pythagorean triple** is a triple of positive integers (x, y, z) such that $x^2 + y^2 = z^2$. Such triples are not difficult to find; some examples include $(3, 4, 5)$, $(5, 12, 13)$, and $(7, 24, 25)$. In fact, given a Pythagorean triple (x, y, z), then given any integer a we know that (ax, ay, az) is also a Pythagorean triple, as

$$(ax)^2 + (ay)^2 = a^2x^2 + a^2y^2 = a^2(x^2 + y^2) = a^2z^2 = (az)^2.$$

Thus, there are infinitely many Pythagorean triples - for instance, we could start with $(3, 4, 5)$ and multiply by any integer $a > 1$ to get a new Pythagorean triple. This may suggest that equations of the form $x^n + y^n = z^n$ are well-understood and have many solutions, but this is certainly not the case.

Theorem 1.1 (Wiles & Taylor)**.** *If $n > 2$, there do not exist $x, y, z \in \mathbb{N}$ such that $x^n + y^n = z^n$.*[1]

This is Fermat's Last Theorem, proposed in 1637 by Pierre de Fermat, which baffled mathematicians for over 350 years until it was finally solved by Andrew Wiles and Richard Taylor in 1995. The proof would have been incomprehensible to Fermat (or indeed any mathematician living before the twentieth century), using the modern machinery of elliptic curves. This talk will provide a taste of these ideas and how they relate to Fermat's Last Theorem.

To motivate more powerful machinery, let's start by thinking about Pythagorean triples — the $n = 2$ special case of Fermat's Last Theorem. Namely, let's try to find all the possible Pythagorean triples. As previously mentioned, we can create infinitely many triples by multiplying any triple (x, y, z) by integers $a > 1$, so we will focus on **primitive** Pythagorean triples, where $\gcd(x, y, z) = 1$.

[1] Andrew Wiles, "Modular Elliptic Curves and Fermat's Last Theorem," *The Annals of Mathematics* 141, no. 3 (May 1995): 443, https://doi.org/10.2307/2118559.

1.2 An Algebraic Approach

Our first approach to finding Pythagorean triples will be algebraic, and is extremely classical — in fact, it was known to Euclid.[2] This will probably be very similar to the approach you took on the PSets.

Take positive integers x, y, and z such that $x^2 + y^2 = z^2$. If x, y, and z share some common factor m, then letting $x = x'm$, $y = y'm$, and $z = z'm$ we have $x^2 + y^2 = z^2 \implies (x'm)^2 + (y'm)^2 = (z'm)^2 \implies (x')^2 + (y')^2 = (z')^2$. It follows that for any Pythagorean triple (x, y, z) we may obtain a primitive Pythagorean triple by dividing out by $\gcd(x, y, z)$. We'll turn our attention to parameterizing these primitive triples.

Suppose (x, y, z) are pairwise coprime and satisfy $x^2 + y^2 = z^2$. Note that x^2, y^2, and z^2 can only be 0 or 1 mod 4. Because x, y, and z cannot all be even, we may take our equation mod 4 to determine that (without loss of generality) $y^2 \equiv z^2 \equiv 1 \pmod 4$, $x^2 \equiv 0 \pmod 4$. So x is even and y and z are odd.

We may rearrange our equation to obtain $y^2 = z^2 - x^2 = (z - z)(z + x)$. We claim that $(z-x)$ and $(z+x)$ are coprime. To see this, suppose $(z-x)$ and $(z+x)$ share some common factor $d > 1$. We then have $d \mid ((z-x)+(z+x)) \implies d \mid 2z$ and $d \mid ((z+x)-(z-x)) \implies d \mid 2x$. As x and z are coprime, it must be that $d = 2$. But this is impossible because y is odd, and thus $2 \nmid y^2 \implies 2 \nmid (x-z)(x+z)$.

We've split y^2 into a product of two coprime factors, and so we must have that $z - x = r^2$, $z + x = s^2$ for positive integers r and s. (Note that by the way we've determined r and s, these two integers must be odd and coprime, and we must have $r > s$.) Solving for x, y, and z then gives $x = \frac{s^2-r^2}{2}$, $y = rs$, and $z = \frac{r^2+s^2}{2}$.

We may also verify that any selection of odd, coprime integers r and s with $s > r$ results in a primitive Pythagorean triple by the equations above. For example, taking $r = 1, s = 3$ gives $x = \frac{3^2-1^2}{2} = 4, y = 3 \cdot 1 = 3, z = \frac{3^2+1^2}{2} = 5$. And taking $r = 3, s = 5$ gives $(x, y, z) = (8, 15, 17)$. Our above work lends itself to a neat bijective correspondence: every ordered pair of odd, coprime positive integers (r, s) with $s > r$ corresponds to a primitive Pythagorean triple (x, y, z) with x even and y, z odd.

1.3 Connecting Algebra and Geometry

With the classical approach in hand, we can move towards a more geometric understanding.

Definition 1.2. *A **rational point** in $\mathbb{R}^2$ is a point where both coordinates are rational.*

[2] A proof can be found in Euclid's Elements, Book X, Proposition XXIX.

Lemma 1.3. *Primitive Pythagorean triples are in bijection with rational points on the curve $x^2 + y^2 = 1$.*

Proof. Recall that primitive Pythagorean triples are triples of positive integers (a, b, c) such that $\gcd(a, b, c) = 1$ and $a^2 + b^2 = c^2$. By dividing on both sides, we get $\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$, which simplifies to $\frac{a}{c}^2 + \frac{b}{c}^2 = 1$. $(\frac{a}{c}, \frac{b}{c})$ is then a rational point on the curve $x^2 + y^2 = 1$.

Conversely, let $(\frac{p}{q}, \frac{r}{s})$ be a rational point on the curve $x^2 + y^2 = 1$. Without loss of generality, we may let $\frac{p}{q}$ and $\frac{r}{s}$ both be in simplest form. Now

$$\begin{aligned} \left(\frac{p}{q}\right)^2 + \left(\frac{r}{s}\right)^2 &= 1 \\ \frac{p^2}{q^2} + \frac{r^2}{s^2} &= 1 \\ p^2s^2 + r^2q^2 &= s^2q^2 \\ (ps)^2 + (rq)^2 &= (sq)^2, \end{aligned}$$

giving us a Pythagorean triple (ps, rq, sq). This is primitive as any common divisor of ps, rq, sq divides either $\gcd(p, q)$ or $\gcd(r, s)$, both of which are 1.[3]

We have thus shown a way to transform primitive Pythagorean triples into rational points on the curve $x^2 + y^2 = 1$ and vice versa. It can be verified that these methods are inverses, and hence this is a bijection. □

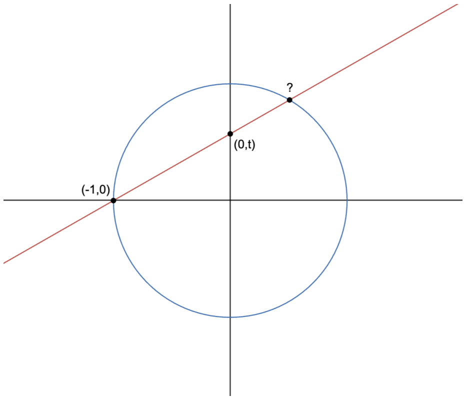
This lemma transforms our problem — instead of a question about integer squares, it becomes a question about curves. However, has it made the problem any easier? The answer, surprisingly, is yes.

1.4 A Geometric Approach

We want to find rational points on the curve $x^2 + y^2 = 1$. Luckily for us, this curve is very familiar — it's a circle! We will use a method called **stereographic projection** to relate points on the circle to points on the y-axis.

For any rational number t, consider the line $y = t(x+1)$. This intersects the y-axis at the point $(0, t)$, and intersects the circle at two points, one of which is $(-1, 0)$.

[3] The result follows by casework and repeated application of FTA.



What is this other intersection point? Given $y = t(x+1)$, we may substitute into $x^2 + y^2 = 1$:

$$\begin{aligned} x^2 + y^2 &= 1 \\ x^2 + (t(x+1))^2 &= 1 \\ x^2 + t^2(x^2 + 2x + 1) &= 1 \\ x^2 + t^2x^2 + 2xt^2 + t^2 - 1 &= 0 \\ (t^2+1)x^2 + (2t^2)x + (t^2 - 1) &= 0 \end{aligned}$$

Since t is rational, this is a quadratic with rational coefficients. Because one intersection point is $(-1, 0)$, one solution is $x = -1$, which is rational, so the other solution must be rational. In fact, we may compute it explicitly using the quadratic formula:

$$\begin{aligned} \frac{-2t^2 \pm \sqrt{4t^4 - 4(t^2+1)(t^2-1)}}{2(t^2+1)} &= \frac{-2t^2 \pm \sqrt{4t^4 - 4(t^4-1)}}{2(t^2+1)} \\ &= \frac{-2t^2 \pm \sqrt{4}}{2(t^2+1)} \\ &= \frac{-2t^2 \pm 2}{2(t^2+1)} \\ &= \frac{-t^2 \pm 1}{t^2+1} \end{aligned}$$

The $-$ case yields $x = -1$, and the $+$ case yields $x = \frac{-t^2+1}{t^2+1} = \frac{1-t^2}{1+t^2}$, which is rational as predicted above. We can also compute that

$$\begin{aligned} y &= t(x+1) \\ &= t(\frac{1-t^2}{1+t^2}+1) \\ &= t(\frac{1-t^2+1+t^2}{1+t^2}) \\ &= \frac{2t}{1+t^2}. \end{aligned}$$

Thus we have transformed a rational point on the y-axis into a rational point on the circle. Similarly, given a rational point (x, y) on the circle, the line passing through $(-1, 0)$ and (x, y) will have rational slope, so it will intersect the y-axis at a rational point. This completes a bijection between the rational points of the circle $x^2 + y^2 = 1$ (besides $(-1, 0)$) and the rational points of the y-axis $x = 0$, called a **birational equivalence**. Thus all primitive Pythagorean triples are exactly those derived from the rational points $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ for t rational. This is a full solution to the Pythagorean Theorem!

Exercise 1.4. *Demonstrate that this parameterization is the same as the algebraic version from the previous section.*

2 A Fun Cubic Curve

In the previous section we built up some tools to consider algebraic equations geometrically. We can now apply these same tools to solve some interesting problems in much the same spirit. For example, consider the following question from Dudeney's *The Canterbury Puzzles*: find positive rational numbers x and y such that $x^3 + y^3 = 9$, other than the obvious solutions $(x, y) = (2, 1), (1, 2)$.[4] The solution given in the back of the book is $x = \frac{415280564497}{348671682660}$, $y = \frac{676702467503}{348671682660}$. How on earth did they find these numbers?

Our solution begins, of course, with interpreting the problem geometrically. We want to find a rational point on this curve, specifically one in the first quadrant.

[4] The original puzzle, called the *Puzzle of the Doctor of Physic*, starts with a sphere with circumference one foot and a sphere with circumference two feet, and asks the reader to find two other spheres with the same combined volume. Some manipulation gives this question about positive rational numbers.

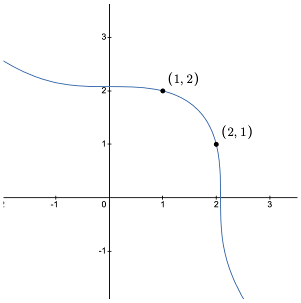


Figure 1: $x^3 + y^3 = 9$

Let's think for a second about our *key trick* in the case of the circle. We took a line with rational slope which we knew to intersect the circle at a rational point, namely $(-1, 0)$. The equation describing the intersection of this line and the circle was a quadratic with rational coefficients, and the rationality of the first intersection point, $(-1, 0)$, essentially forced the second intersection point be rational.

We'll attempt something similar with this cubic. Consider the tangent line to the cubic at the point $(1, 2)$:

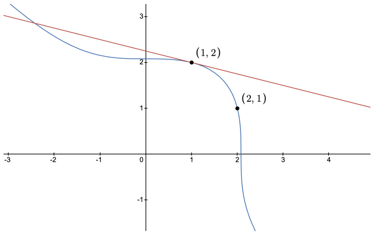


Figure 2: Tangent line at $(1, 2)$

We may determine that this line has rational slope via implicit differentation:

$$\begin{aligned} x^3 + y^3 = 9 &\implies y^3 = 9 - x^3 \\ &\implies \frac{d}{dx}(y^3) = \frac{d}{dx}(9 - x^3) \\ &\implies 3y^2 \cdot \frac{dy}{dx} = -3x^2 \\ &\implies \frac{dy}{dx} = -\frac{x^2}{y^2} \\ &\implies \left.\frac{dy}{dx}\right|_{(1,2)} = -\frac{1}{4} \end{aligned}$$

So the equation for this tangent line is given by $y = -\frac{1}{4}(x-1)+2$. Following our example from Section 1, we'll want to consider the other intersection point of this line with the cubic. We may algebraically determine such intersection points by substituting $y = -\frac{1}{4}(x-1)+2$ into our cubic:

$$\begin{aligned} x^3 + y^3 &= 9 \\ x^3 + (-\frac{1}{4}(x-1)+2)^3 &= 9 \\ \frac{63}{64}x^3 + \frac{27}{64}x^2 - \frac{243}{64}x + \frac{153}{64} &= 0 \end{aligned}$$

We have that $x = 1$ is a root of the above polynomial, because we took the tangent line to pass through $(1, 2)$. In fact, we may observe that $x = 1$ is a double root, since by definition the tangent line touches the original curve at $x = 1$ without crossing it.

So we may write $\frac{63}{64}x^3 + \frac{27}{64}x^2 - \frac{243}{64}x + \frac{153}{64} = a(x-1)^2(x-r)$, where r gives the x-coordinate of the second intersection point and a is some constant. Comparing coefficients yields: $-ra = \frac{153}{64}, a = \frac{63}{64} \implies r = -\frac{17}{7}$. We can easily recover that the corresponding y-coordinate of the intersection point is $-\frac{1}{4}(-\frac{17}{7}-1)+2 = \frac{20}{7}$. The reader should verify that $(-\frac{17}{7})^3 + (\frac{20}{7})^3$ is indeed equal to 9.

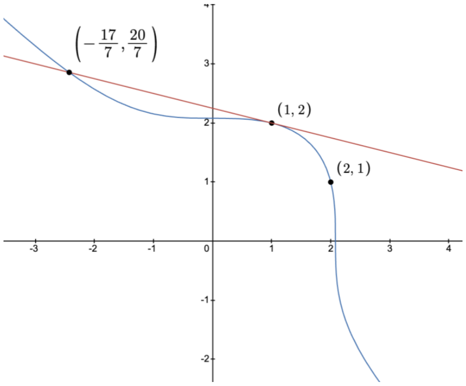


Figure 3: That's a new rational point!

This is wonderful! We were able to use a rational point on our curve to generate another rational point. Generalizing our above approach, we obtain that if (a, b) is a rational point on $x^3 + y^3 = 9$ then the intersection of the tangent line at (a, b) with the cubic is the rational point $(\frac{a(a^3+2b^3)}{a^3-b^3}, \frac{-b(2a^3+b^3)}{a^3-b^3})$. We can check that for $a = 1, b = 2$, this equation gives $(-\frac{17}{7}, \frac{20}{7})$ as expected. Note that this procedure gives us a way to generate infinitely many rational points on $x^3 + y^3 = 9$ by taking successive tangents.

But we still haven't answered our question, which was to find rational points in the *first quadrant!* The method described above relied purely on tangents to rational points. But we could also generate a rational point on the curve by taking a line between two rational points and considering its third intersection with the cubic. For example, consider the line interpolating $(-\frac{17}{7}, \frac{20}{7})$ and $(2, 1)$. We know that this line will have rational slope (namely, $-\frac{13}{31}$) and thus the equation for the intersection of this line with the curve will be a cubic with rational coefficients. If we take this equation in terms of x, we know it has two rational roots $\frac{17}{7}$ and $\frac{20}{7}$, and thus its third root must be rational. Geometrically, this means the third intersection of the line with the cubic must be a rational point—in this case, the point $(-\frac{271}{438}, \frac{919}{438})$:

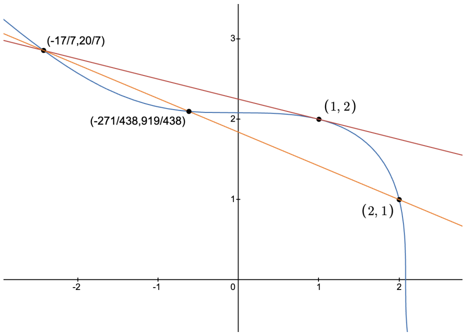


Figure 4: More ways to get rational points!

Argh! This is a rational point, but it still isn't in the first quadrant. It doesn't seem like we can interpolate any pair of rational points to get a first quadrant intersection point. What if we tried tangents again? The tangent to $(-\frac{271}{438}, \frac{919}{438})$ seems promising...

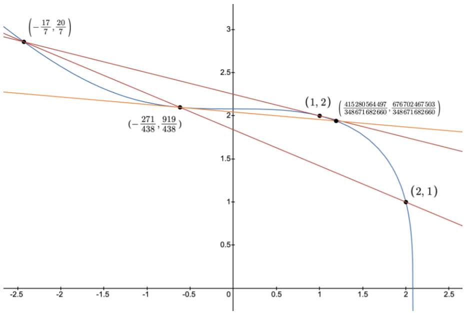


Figure 5: Finally a Q1 intersection point!

We've finally achieved a first quadrant intersection point! In fact, it's the same one that Dudeney found, $(\frac{415280564497}{348671682660}, \frac{676702467503}{348671682660})$. Fascinating!

3 Rational Points on Elliptic Curves

The equation $x^3 + y^3 = 9$ is one example of an **elliptic curve**. Elliptic curves are equations of the form $y^2 = x^3 + ax + b$, where a, b are elements of some field.[5] While $x^3 + y^3 = 9$ is not of this form (called **Weierstrass normal form**), it is birationally equivalent to the curve $y^2 = x^3 - 34992$, much like how the circle (besides the point $(-1, 0)$) is birationally equivalent to the y-axis. Therefore we also consider this equation to be an elliptic curve. In fact, this particular argument generalizes:

Lemma 3.1. *Any curve of the form $x^3 + y^3 = \alpha$ is an elliptic curve — it is birationally equivalent to the curve $y^2 = x^3 - 432\alpha^2$.*[6]

This insight allows us to reduce some problems to finding rational points on elliptic curves. Any solution to the $n = 3$ version of Fermat's Last Theorem is a triple of integers (A, B, C) such that $A^3 + B^3 = C^3$. Much like we did for Pythagorean triples, dividing both sides by C^3 gives $\left(\frac{A}{C}\right)^3 + \left(\frac{B}{C}\right)^3 = 1$, so solving FLT for $n = 3$ is equivalent to finding rational points on the curve $x^3 + y^3 = 1$.[7] By the lemma this is equivalent to finding rational points on the curve $y^2 = x^3 - 432$.

There are many fascinating results about rational points on elliptic curves. For one, given a rational point x on an elliptic curve E, a certain operation makes the rational points on E into an abelian group $E(G)$ with x as the identity. A powerful result known as the Mordell–Weil theorem guarantees that this abelian group is finitely generated. Using the structure theorem for finitely generated abelian groups, this guarantees that $E(G)$ is the direct sum of finitely many cyclic groups. Therefore, understanding all the rational points on E reduces to understanding the finitely many generators of these cyclic groups. While this simplifies things dramatically, the problem still remains difficult in general; understanding the number of copies of $\mathbb{Z}$ in the decomposition of $E(G)$ is the subject of the **Birch and Swinnerton-Dyer conjecture**, one of the seven Millennium Prize problems.

Elliptic curves also played a large part in Wiles's proof of Fermat's Last Theorem. Fermat himself reduced the theorem to the case of prime n,[8] and over the next several hundred years, mathematicians used various approaches to solve for all primes up to four million. In 1974, Yves Hellegouarch demonstrated that given an integer triple (A, B, C) and prime p such that $A^p + B^p = C^p$,[9] the el-

[5] Technically, this only works if the field's characteristic is not 2 or 3, but here we are only concerned with $\mathbb{Q}$, which is characteristic 0.

[6] Joseph H. Silverman and John Torrence Tate, *Rational Points on Elliptic Curves* (Cham: Springer, 2015).

[7] Besides $(0, 1)$ and $(1, 0)$, of course.

[8] $n = 4$ is on the PROMYS problem sets.

[9] Technically, we must have $p \geq 5$, but the case of $p = 3$ has been proven many times (including by Euler!).

liptic curve $y^2 = x(x-A^p)(x+B^p)$ over $\mathbb{Q}$ could not be "modular."[10] Wiles then showed that a large family of elliptic curves, including $y^2 = x(x-A^p)(x+B^p)$, were modular, proving Fermat's Last Theorem. His work was subsequently generalized to show that all elliptic curves over $\mathbb{Q}$ are modular.

We hope that these notes have offered a glimpse into the incredibly deep topic of finding rational points on curves, as well as elliptic curves more generally. Furthermore, we hope to convey how algebraic concepts like Pythagorean triples can have beautiful geometric parallels, a connection that forms the basis for the field of algebraic geometry. Below are some resources to explore these amazing ideas more deeply:

1. Rational Points on Elliptic Curves; Joseph Silverman and John Tate. An excellent introduction to the theory of elliptic curves at the undergraduate level.
2. Algebraic Geometry I: Varieties; Richard E. Borcherds.[11] A series of introductory algebraic geometry lectures where the authors learned all the material presented above. The first lecture can be found at https://youtu.be/JZKDmTIFR7A.
3. The Rising Sea: Foundations of Algebraic Geometry; Ravi Vakil. A brand-new (as of 2025) introductory textbook on algebraic geometry at the introductory graduate level. Well written, detailed, and conversational.

[10] The term modular is related to a certain connection between elliptic curves and modular forms.

[11] 🐐