

Elliptic Curves in Nature

From Cannonballs to Fermat's Last Theorem

Tyler Genao

Tennessee Tech University
Graduate Student Seminar

September 24, 2026



The Cannonball Problem

Consider a square pyramid made out of cannonballs, with x layers. For which x can the same cannonballs be rearranged into a square?

- $x = 0$ works vacuously. ✓
- $x = 1$ gives the one-cannonball square. ✓
- Is there a **nontrivial** solution? ?

The square pile is formed, as in the annexed figure.



The number of balls in the top layer is 1^2 , in the next layer 2^2 , in the next, 3^2 , and so on. To find the number of balls in a pile of n layers, we have the series,

	1	4	9	16	25	36,	&c.
1st order of diff,	3	5	7	9	11		&c.
2d " "		2	2	2	2		&c.
3d " "			0	0	0		&c.

Hence,

$$a=1, d_1=3, d_2=2, d_3=0, d_4=0, \&c.$$

Depiction from C. Davies and W. G. Peck,
*Mathematical Dictionary and Cyclopaedia of
Mathematical Science*, 1872, p. 427.

- The x th layer is an x -by- x square, so the number of cannonballs in the pyramid is

$$N(x) = 1^2 + 2^2 + \cdots + x^2 = \frac{x(x+1)(2x+1)}{6}.$$

- We want this number to equal an integer square, which we denote by y^2 :

$$y^2 = N(x).$$

- This becomes:

The Cannonball Equation

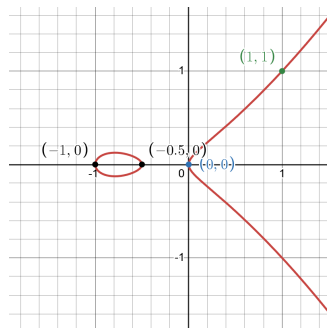
$$6y^2 = x(x+1)(2x+1) = 2x^3 + 3x^2 + x. \quad (*)$$

The Cannonball Problem asks for the nonnegative integer solutions (x, y) of $(*)$.

Over $\mathbb{R}$, the Cannonball Equation (*) draws the curve

$$E : 6y^2 = 2x^3 + 3x^2 + x.$$

- Each cannonball solution is an **integer point** on E .
- The trivial solutions $x = 0, 1$ give points $(0, 0)$ and $(1, 1)$ on the curve.
- How can we find more integer points?



The Cannonball Curve in $\mathbb{R}^2$, with some points drawn.

The Chord Method

- Here is one way to find new points:
- Take

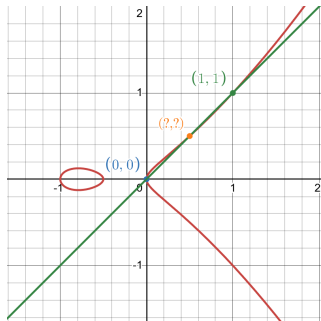
$$P = (0, 0), \quad Q = (1, 1).$$

The line through them is $L : y = x$.

- **Intersect the line with the curve:**
substituting $y = x$ into E gives

$$\begin{aligned} 6x^2 &= 2x^3 + 3x^2 + x, \\ 0 &= x(2x - 1)(x - 1). \end{aligned}$$

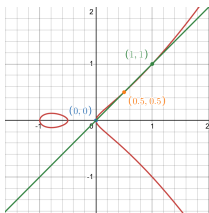
- Two roots recover P and Q . The third root $x = \frac{1}{2}$ gives a *new point* $R = (\frac{1}{2}, \frac{1}{2})$.



L intersects E at three points: $(0, 0)$, $(?, ?)$ and $(1, 1)$.

- Indeed, $6 \cdot \left(\frac{1}{2}\right)^2 = 2 \cdot \left(\frac{1}{2}\right)^3 + 3 \cdot \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)$.
- The three intersections of $L : y = x$ with E are

$$P = (0, 0), \quad Q = (1, 1), \quad R = \left(\frac{1}{2}, \frac{1}{2}\right).$$



Progress, but...

The Chord Method produced a new rational point, but $x = \frac{1}{2}$ makes no sense as a number of layers!

Take Another Chord

- Reflect R across the x -axis:

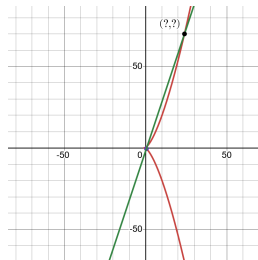
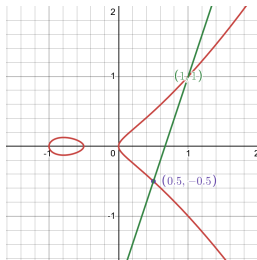
$$S = \left(\frac{1}{2}, -\frac{1}{2}\right).$$

- The line through S and $Q = (1, 1)$ is

$$L' : y = 3x - 2.$$

- Substitution into E produces

$$2x^3 - 51x^2 + 73x - 24 = 0.$$



Line through S and Q , then zoomed out.

- We already know two roots: $x = \frac{1}{2}$ and $x = 1$. Using long division, the cubic factors as

$$2x^3 - 51x^2 + 73x - 24 = (2x - 1)(x - 1)(x - 24).$$

- Therefore the third root is $x = 24$, and $L' : y = 3x - 2$ gives $y = 70$.

A nontrivial solution to the Cannonball Problem:

$$1^2 + 2^2 + \cdots + 24^2 = 4900 = 70^2.$$

Thus, a 24-layer square pyramid can be reconfigured as a 70×70 square.

The Complete Solution

The Cannonball Theorem

The only nonnegative integers x for which

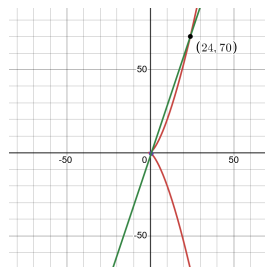
$$1^2 + 2^2 + \cdots + x^2$$

is a square are

$$x = 0, 1, 24.$$

- The full set of integer points is

$$E(\mathbb{Z}) = \{(-1, 0), (0, 0), (1, \pm 1), (24, \pm 70)\}.$$



É. Lucas posed the problem in 1875. G.N. Watson gave the first complete proof in 1918 using *elliptic functions*.

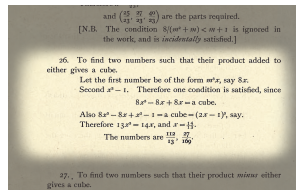
An Idea From Antiquity

Diophantus and Arithmetica

- Diophantus worked in Alexandria, probably in the third century.
- His *Arithmetica* (written almost nineteen centuries ago) presented algebraic problems with worked solutions.
- Ten of its original thirteen books survive: six in Greek and four in Arabic.



Diophantus of Alexandria



T.L. Heath, *Diophantus of Alexandria*,
1910.

Problem IV.26

Find two numbers such that their product, added to either number, gives a cube:

$$ab + a \stackrel{?}{=} \text{cube}, \quad ab + b \stackrel{?}{=} \text{cube}.$$

- Diophantus' idea: choose $a = m^3x$ and $b = x^2 - 1$. Then $ab + a = (mx)^3$ is automatically a cube.
- Requiring the second expression to be a cube gives (taking $y = mx - 1$)

$$(x^2 - 1)(m^3x + 1) = (mx - 1)^3,$$

and simplification gives

$$x = 0 \quad \text{or} \quad x = \frac{m(m^2 + 3)}{3m^2 + 1}.$$

Geometrically, the line $y = mx - 1$ intersects the cubic

$$y^3 = (x^2 - 1)(m^3x + 1).$$

The remaining intersection point appears by the same algebra as in our Cannonball Problem calculation.

- Diophantus also explicitly takes $m = 2$. Then

$$x = \frac{2(2^2 + 3)}{3 \cdot 2^2 + 1} = \frac{14}{13},$$

and therefore

$$a = m^3 x = \frac{112}{13}, \quad b = x^2 - 1 = \frac{27}{13^2}.$$

These numbers satisfy

$$ab + a = \left(\frac{28}{13}\right)^3, \quad ab + b = \left(\frac{15}{13}\right)^3.$$

The recurring idea

A line through a known point on a cubic equation can create another rational point.

Fermat's Last Theorem

Three Centuries Towards a Proof

- c. **1637** Fermat states the problem and proves the exponent 4 case by infinite descent.
- 1770** Euler publishes a proof for exponent 3.
- 1825** Dirichlet and Legendre prove exponent 5.
- 1839** Lamé proves exponent 7.
- 1847** Kummer proves the theorem for regular prime exponents and develops ideal theory.
- ⋮
- 1986** Ribet proves the key link between Fermat's equation and modularity.
- 1994–95** Wiles and Taylor–Wiles complete the proof.

A Hypothetical Solution Creates a Curve

- After the standard exponent reduction, suppose

$$a^p + b^p = c^p, \quad p \geq 5 \text{ prime}, \quad \gcd(a, b, c) = 1.$$

- Frey associated to such a solution the curve

$$\begin{aligned} E_{a,b} : y^2 &= x^3 + (b^p - a^p)x^2 - a^p b^p x \\ &= x(x - a^p)(x + b^p). \end{aligned}$$

The Frey Curve

The roots of the cubic are 0, a^p , and $-b^p$. The equation $a^p + b^p = c^p$ forces unusually restrictive arithmetic behavior.

Why Is It a Contradiction?

1. A nonzero solution to Fermat's equation produces a *semistable* Frey Curve.
2. Ribet's Theorem shows that this curve could not be *modular*.
3. Wiles and Taylor–Wiles proved that every semistable elliptic curve over $\mathbb{Q}$ is modular.

Contradiction

The same Frey Curve would have to be *both* modular and non-modular. Therefore the proposed Fermat solution **cannot** exist.

- The curves we have seen in this talk have been **elliptic curves**, which serve as a bridge between algebra and geometry.

Elliptic Curves

What Is an Elliptic Curve?

- Formally, an **elliptic curve over $\mathbb{R}$** , written $E/\mathbb{R}$, is a *nonsingular, projective genus one curve* with a fixed real point.
- An equivalent definition is a curve in $\mathbb{R}^2$ of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{R}$, satisfy a particular nonzero condition related to *nonsingularity*.

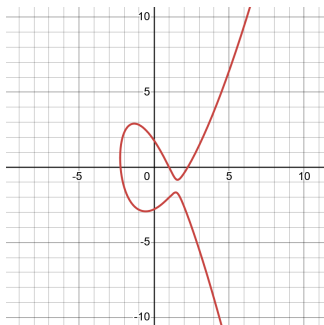
- Elliptic curves also have the shorter form

$$E : y^2 = x^3 + Ax + B$$

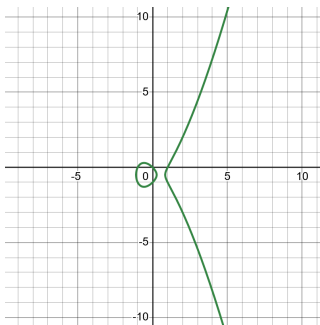
where $A, B \in \mathbb{R}$ and $4A^3 + 27B^2 \neq 0$.

- We will define these terms in the next talk!

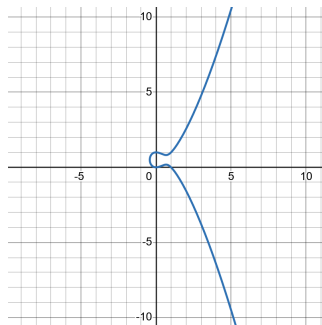
Examples of Elliptic Curves



$$E_1 : y^2 + xy + y = x^3 - x^2 - 5x + 5$$



$$E_2 : y^2 + y = x^3 - x$$

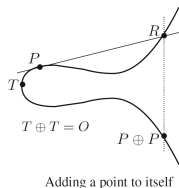
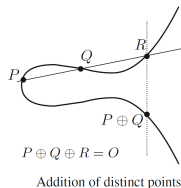


$$E_3 : y^2 - y = x^3 - x^2$$

- The Cannonball Curve and the “Diophantus Curve” also become elliptic curves after suitable changes of variables.

The Chord and Tangent Method

- **Important:** elliptic curves $E/\mathbb{R}$ have a binary operation called the *Chord and Tangent Method* which turns the set of points $E(\mathbb{R})$ into a group.
- To add two points P and Q on an elliptic curve:
 1. Draw the line through P and Q . If $P = Q$, use the tangent line at P .
 - Let $P * Q$ be the third intersection with the curve.
 2. Reflect $P * Q$ across the x -axis.* The reflected point is $P + Q$.



*For elliptic curves in short form, reflection across the x -axis sends (x, y) to $(x, -y)$. Picture from Silverman.

An Illustrative Example

- We will try an example: consider

$$E : y^2 = x^3 - 7x + 10$$

with $P = (1, 2)$ and $Q = (3, 4)$.

- The line through them is

$$L : y = x + 1.$$

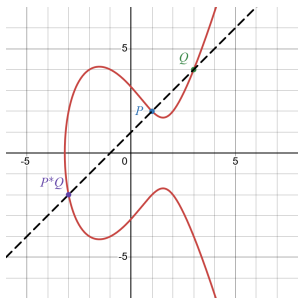
- Substituting $y = x + 1$ into E gives

$$x^3 - x^2 - 9x + 9 = (x - 1)(x - 3)(x + 3) = 0.$$

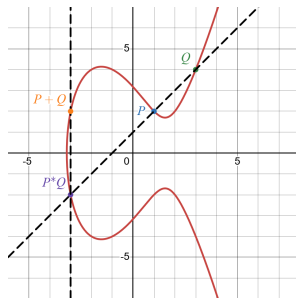
- The third intersection is $P * Q = (-3, -2)$, so reflection gives

$$(1, 2) + (3, 4) = (-3, 2).$$

Adding Two Points



The line through P and Q meets E at P^*Q .



Reflection across the x-axis gives $P+Q$.

- Next, we add a point to itself.
- Let $P = (1, 2)$ on $E : y^2 = x^3 - 7x + 10$.
- Need the tangent slope to E at P . Implicit differentiation gives

$$\frac{dy}{dx} = \frac{3x^2 - 7}{2y}, \quad \left. \frac{dy}{dx} \right|_P = -1.$$

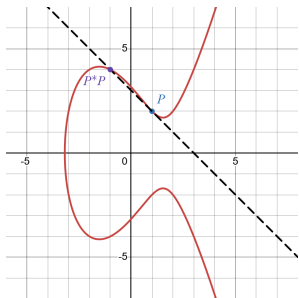
- Thus the tangent line at P is $T : y = -x + 3$. Substitution gives

$$x^3 - x^2 - x + 1 = (x - 1)^2(x + 1) = 0.$$

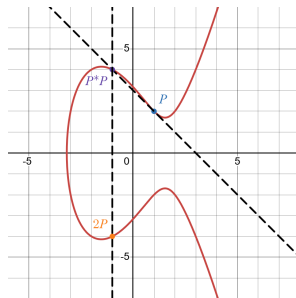
- The repeated root records the tangency at P . The third intersection is $P * P = (-1, 4)$, and therefore

$$2P = P + P = (-1, -4).$$

Doubling a Point



The tangent to E at P has another intersection $P * P$.



Reflection gives the doubled point $2P$.

Group Law Axioms for an Elliptic Curve

The Chord and Tangent Method turns the set $E(\mathbb{R})$ of real points into an **abelian group**. This means the binary operation

$$+: E(\mathbb{R}) \times E(\mathbb{R}) \rightarrow E(\mathbb{R}), \quad (P, Q) \mapsto P + Q$$

satisfies the *group axioms* +1:

1. **Associativity:**

$$\forall P, Q, R \in E(\mathbb{R}), \quad (P + Q) + R = P + (Q + R).$$

2. **Identity:**

$$\exists O \in E(\mathbb{R}), \quad \forall P \in E(\mathbb{R}) \quad O + P = P + O = P.$$

3. **Inverses:**

$$\forall P \in E(\mathbb{R}), \quad \exists Q \in E(\mathbb{R}) \quad P + Q = Q + P = O. \quad (\text{We write } -P := Q.)$$

4. **Abelian:**

$$\forall P, Q \in E(\mathbb{R}), \quad P + Q = Q + P.$$

Revisiting the Cannonball Curve

- On the Cannonball Curve

$$E : 6y^2 = 2x^3 + 3x^2 + x,$$

the first chord through $P = (0, 0)$ and $Q = (1, 1)$ found

$$R = \left(\frac{1}{2}, \frac{1}{2}\right).$$

- Reflection then gave $S = -R = \left(\frac{1}{2}, -\frac{1}{2}\right)$. Thus, we did the calculation

$$P + Q = S.$$

- Finally, the chord through S and Q intersected the curve at $(24, 70)$, so that

$$(24, 70) = S * Q.$$

- We were secretly working with elliptic curve arithmetic the whole time!

A Summary

- Using the geometric Chord Method, we found a nontrivial solution to the Cannonball Problem, with 24 layers and 70^2 cannonballs.
- Diophantus used an algebraic construction that we can reinterpret geometrically as the same chord-intersection idea.
- The proof of Fermat's Last Theorem attaches *elliptic curves* to hypothetical solutions.
- Under the Chord and Tangent Method, the set of points on an elliptic curve is an abelian group.

Next time

A more detailed introduction to elliptic curves, and their appearances over various fields; their use in cryptography; and some outstanding results and conjectures about the arithmetic of elliptic curves.

Thank you!



Select References (In Order of Appearance)

1. C. Davies and W. G. Peck, *Mathematical Dictionary and Cyclopedia of Mathematical Science*, A. S. Barnes, 1872.
2. G. N. Watson, "The Problem of the Square Pyramid," *The Messenger of Mathematics* **48** (1918), 1–22.
3. T. L. Heath, *Diophantus of Alexandria: A Study in the History of Greek Algebra*, Cambridge University Press, 1910.
4. K. A. Ribet, "On Modular Representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ Arising from Modular Forms," *Inventiones Mathematicae* **100** (1990), 431–476.
5. A. Wiles, "Modular Elliptic Curves and Fermat's Last Theorem," *Annals of Mathematics* **141** (1995), 443–551; R. Taylor and A. Wiles, "Ring-Theoretic Properties of Certain Hecke Algebras," *Annals of Mathematics* **141** (1995), 553–572.
6. J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, 2009.