Elliptic Curves

PROMYS Minicourse

Joshua Im, Joshua Kou

July 31, 2025

1 Motivation

Consider the following innocent equation. We want to find $a, b, c \in \mathbb{Z}^+$ satisfying

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} = 4.$$

A Naive Approach

A computer search yields the solution $(-11, -4, 1)$, which we can check:

$$\frac{-11}{-4+1} + \frac{-4}{-11+1} + \frac{1}{-11-4} = \frac{11}{3} + \frac{2}{5} - \frac{1}{15} = 4,$$

as desired. However, a and b are negative, and we wanted a solution in the positive integers. Unfortunately, this is the furthest a computer search can assist—while running a program longer may find another negative solution, it will not find a positive solution.

In this talk we will present an overview of how to solve this problem.

2 Cubics and Weierstrass Normal Form

A cubic is an equation of the form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

with coefficients in $\mathbb{Q}$.

It is known that such a cubic with a rational point can be rewritten in the form

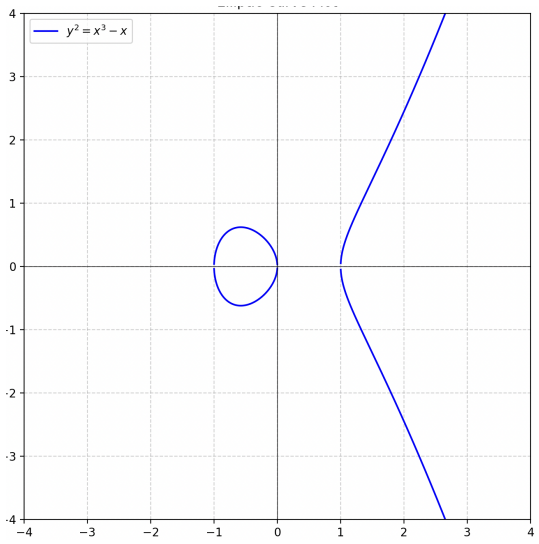
$$y^2 = x^3 + ax + b$$

called the Weierstrass Normal Form, by several change of variables. This is what we call an elliptic curve, or the Weierstrass normal form of an elliptic curve.

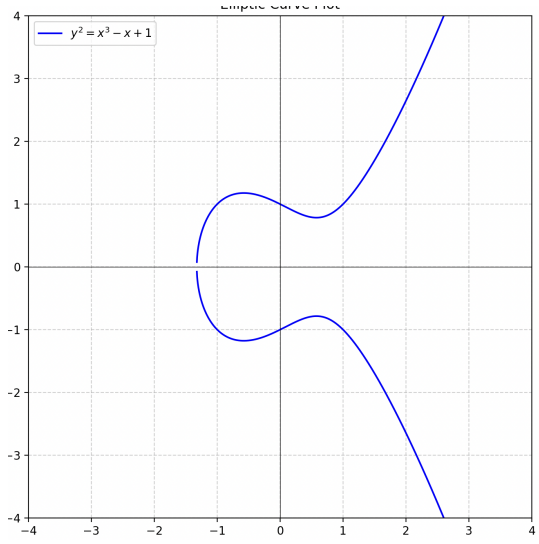
Crucially, this transformation preserves the structure of rational points on the curve. In conclusion, to understand the rational points on cubic equations, we only need to understand the rational points on elliptic curves.

By the fundamental theorem of algebra, the complex roots of $x^3 + ax + b$ come in pairs, so an elliptic curve can have 1 or 3 real roots.

Example 1. In figure 1.1, the curve $y^2 = x^3 - x$ meets three times with the x-axis, so it has three real solutions, while the curve $y^2 = x^3 - x + 1$ meets only once with the x-axis, so it has only one real solution.



(a) Graph of $y^2 = x^3 - x$



(b) Graph of $y^2 = x^3 - x + 1$

Figure 1: Two Elliptic Curves

3 The Group Law

Rational Points on Elliptic Curves

First we define the set of rational points, and the point at infinity.

Definition 1 (Point at Infinity)**.** The **point at infinity** $\mathcal{O}$ is the imagined point infinitely far along the cubic where the two ends of the cubic meet (we assume that the two sides of the cubic meet at this point).

Definition 2 (Rational Points)**.** Given a curve $f(x, y) = 0$, the **rational points** on the curve are the pairs $x_0, y_0 \in \mathbb{Q}$ such that $f(x_0, y_0) = 0$, together with a point at infinity $\mathcal{O}$.

Alternatively, the set of rational points on an elliptic curve is the set of rational projective points on the curve.

It turns out that $\mathcal{O}$ is a point of inflection, and a line $\overline{\mathcal{O}R}$ through $\mathcal{O}$ and any normal point R is a vertical line.

Unfortunately, some cubic curves may not be in good enough condition that allows us to apply the properties we want. There are two types of problematic curves: curves that don't have any rational points or curves which aren't smooth. For example, the curve $x^2 - 2y^2 = 0$ doesn't have any rational points. Non-smooth curves are called singular curves, which we don't consider for this topic. Such example is $y^2 = x^3$, which has a cusp at $(0, 0)$.

If we get rid of the bad curves listed above, so if there is at least one rational point and the curve is non-singular, the set of rational points on a cubic form an abelian group. Recall the definition of an abelian group.

Definition 3 (Abelian Group)**.** An **abelian group** is a set G equipped with a binary operation $*$ with four properties:

1. The existence of an identity: there is an element $e \in G$ such that for all $g \in G$, $e * g = g * e = g$.
2. The existence of an inverse for each element: for all $g \in G$, there is $h \in G$ such that $g * h = h * g = e$.
3. Associativity: for all g, h, and $j \in G$, $(g * h) * j = g * (h * j)$.
4. Commutativity: for all g and $h \in G$, $g * h = h * g$.

We will only consider elliptic curves in Weierstrass normal form, though the group law may be defined for any general non-singular cubic.

The Addition Law

Let C be a non-singular elliptic curve in Weierstrass normal form, and let Γ be the set of rational points on C. Then define the group operation $+$ of Γ as follows: to compute $P + Q$,

1. Take the line $\overline{PQ}$ going through P and Q.
2. Since a non-degenerate cubic and a line intersect in 3 projective points (accounting for multiplicity), we may take the third point of intersection between $\overline{PQ}$ and the curve C, which we denote as $P * Q$.
3. Take the vertical line $\overline{\mathcal{O}(P * Q)}$.
4. $P + Q$ is the third point of intersection between $\overline{O(P * Q)}$ and C, i.e. $(P * Q) * \mathcal{O}$.

All elliptic curves in Weierstrass normal form is symmetric with respect to the x-axis, so $(P * Q) * \mathcal{O}$ is simply the reflection of $P * Q$ across the x-axis.

We first need to show closure, i.e. that the sum of two rational points $P + Q$ is still a rational point. We will use the following lemma.

Lemma 1. *For any points P, $Q \in \Gamma$, $P * Q$ is also in Γ, i.e. $P * Q$ is also a rational point on the elliptic curve.*

Proof. First observe that since P and Q are rational, the line PQ

$$y = mx + k$$

has rational coefficients. Thus the points of intersection of $\overline{PQ}$ and C satisfy the equations

$$y = mx + k$$

$$y^2 = x^3 + ax + b.$$

Substituting, we see that the x coordinates of the three points of intersection satisfy a cubic in x with rational coefficients:

$$0 = x^3 + ax + b - (mx + k)^2.$$

If we let r_1, r_2, and r_3 be the three roots to the equation, then by Vieta, $r_1 r_2 r_3 = b - k^2$, which is rational. Since the line $y = mx + k$ and the curve $y^2 = x^3 + ax + b$ already meet at P and Q, r_1 and r_2, which are x-coordinates of P and Q, are both rational. This forces r_3 to be rational, and since r_3 is the x-coordinate of $P * Q$, this gives that $P * Q$ must be a rational point. □

With this argument, since we know $P * Q$ and $\mathcal{O}$ are rational, $(P * Q) * \mathcal{O} = P + Q$ should also be rational, which implies that $+$ is closed under Γ.

Example 2. Consider the elliptic curve $y^2 = x^3 - x + 1$, and two rational points $P(1, 1)$ and $Q(3, 5)$ on the curve. We first find $P * Q$.

The line $\overline{PQ}$ has equation $y = 2x - 1$. Substituting gives $(2x - 1)^2 = x^3 - x + 1$, which reduces to $x^3 - 4x^2 + 3x = x(x - 1)(x - 3) = 0$. Since 1 and 3 are roots to the equation, the other root is 0. Thus the x-coordinate of $P * Q$ is 0.

To find the y-coordinate of $P * Q$, you simply substitute $x = 0$ on $y = 2x - 1$ since $P * Q$ is on this line. This gives $P * Q = (0, -1)$. Therefore, $P + Q = (P * Q) * \mathcal{O}$ is the reflection of $(0, -1)$ with respect to x-axis, which is $(0, 1)$. The diagram of the process is shown below.

It is clear that this operation is commutative, as the line $\overline{PQ}$ is the same as the line $\overline{QP}$. Using the property that $\mathcal{O}$ is a point of inflection and the definition of the group law, we get

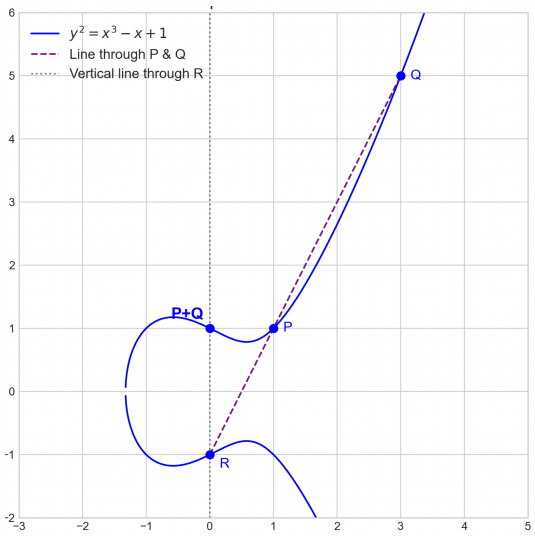


Figure 2: Elliptic Curve Addition

- $\mathcal{O} + \mathcal{O} = \mathcal{O}$
- $\mathcal{O} + P = P + \mathcal{O} = P$.

Thus $\mathcal{O}$ is the identity.

The last property to show is associativity. For any points $P, Q, R \in \Gamma$, it is not evident that

$$P + (Q + R) = P + (Q + R).$$

This will be proved in the next few sections.

4 Cayley-Bacharach Theorem

The following theorem is used as a lemma to prove associativity.

Theorem 1 (Cayley-Bacharach Theorem)**.** *Suppose two cubics C_1 and C_2 intersect at 9 points. Any cubic C that passes through eight of the nine intersections of C_1 and C_2 must also pass through the ninth intersection.*

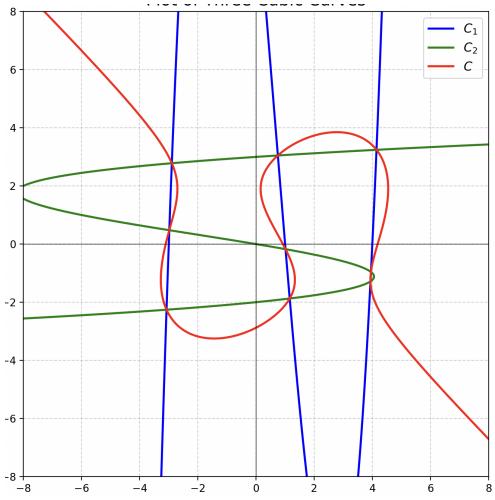


Figure 3: Three Cubics at Nine Points

To make the theorem intuitive, see the diagram above. Suppose the blue and green graphs are cubic curves (they are cubic curves even though it is not drawn outside of ± 8) meet at nine points. Then if any cubic, drawn in red, passes eight of the nine intersection, then it also pass the remaining one intersection.

For a proof see Terence Tao's blog on "Pappus's Theorem and Elliptic Curves" [4].

Applications

The Cayley-Bacharach Theorem can be used to give a pretty proof of two theorems in Euclidean geometry.

Theorem 2 (Pappus's Theorem)**.** *Let A_1, A_2, and A_3 be points on a line ℓ and B_1, B_2, B_3 be points on another line m. If X_1 is the intersection of $\overline{A_2B_3}$ and $\overline{A_3B_2}$, X_2 the intersection of $\overline{A_1B_3}$ and $\overline{A_3B_1}$, and X_3 the intersection of $\overline{A_1B_2}$ and $\overline{A_2B_1}$, then X_1, X_2, X_3 are colinear.*

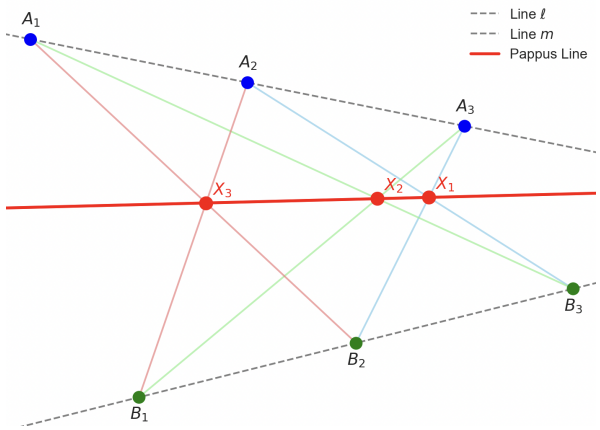


Figure 4: Pappus's Theorem

Proof. We will use the fact that the union of three lines is a degenerate cubic. To see this, note that a line is an equation of the form

$$ax + by + c = 0.$$

Then the union of three lines is

$$(a_1x + b_1y + c_1)(a_2x + b_2y + c_2)(a_3x + b_3y + c_3) = 0,$$

an equation of degree 3.

Then consider the following 3 cubics

1. $C_1 = \overline{A_1B_2} \cup \overline{A_2B_3} \cup \overline{A_3B_1}$,
2. $C_2 = \overline{A_2B_1} \cup \overline{A_3B_2} \cup \overline{A_1B_3}$,
3. $C_3 = \ell \cup m \cup \overline{X_1X_3}$.

The three cubics simultaneously intersect at eight points: A_1, A_2, A_3, B_1, B_2, B_3, X_1, X_3, and C_1 and C_2 intersect at X_3 as well. Therefore, by Cayley-Bacharach, C_3 passes through X_3 as well. □

A similar proof is possible for another classical result.

Theorem 3 (Pascal's Theorem)**.** *Let c be a conic, with points A, B, C, D, E, F on c. Let X_1 be the intersection of $\overline{AB}$ and $\overline{DE}$, X_2 be the intersection of $\overline{BC}$ and $\overline{EF}$, and X_3 be the intersection of $\overline{CD}$ and $\overline{FA}$. Then X_1, X_2, X_3 are colinear.*

Proof. Consider the following cubics: Then consider the following 3 cubics

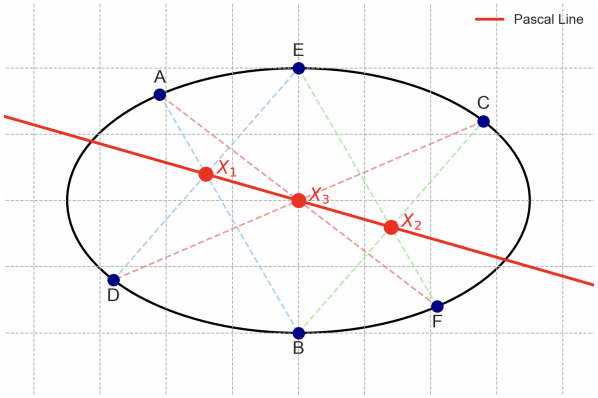


Figure 5: Pascal's Theorem

1. $C_1 = \overline{A_1B_2} \cup \overline{A_2B_3} \cup \overline{A_3B_1}$,
2. $C_2 = \overline{A_2B_1} \cup \overline{A_3B_2} \cup \overline{A_1B_3}$,
3. $C_3 = c \cup \overline{X_1X_3}$.

The proof proceeds in the same way with the proof to the Pappus's theorem. □

5 Associativity of the Group Law

Having seen some applications of the Cayley-Bacharach Theorem, we will now apply it to prove the associativity of the group law on elliptic curves.

Theorem 4 (Associativity of the Group Law)**.** *Suppose C is a nonsingular elliptic curve in Weierstrass normal form, Γ the set of rational points on C, and P, Q, R any points in Γ. Then*

$$(P + Q) + R = P + (Q + R).$$

Proof. Define six lines:

- ℓ_1 the line passing P, Q, and $P * Q$,
- ℓ_2 the line passing $Q * R$, $\mathcal{O}$, and $Q + R$,
- ℓ_3 the line passing $P + Q$, R, and $(P + Q) * R$,
- m_1 the line passing Q, R, and $Q * R$,
- m_2 the line passing $P * Q$, $\mathcal{O}$, $P + Q$,
- m_3 the line passing $Q + R$, P, $P * (Q + R)$.

Now, define two cubics C_1 and C_2 by $C_1 = \ell_1 \cup \ell_2 \cup \ell_3$ and $C_2 = m_1 \cup m_2 \cup m_3$. Then C and C_1 have nine intersections, which are

$$\mathcal{O},\ P,\ Q,\ R,\ P * Q,\ Q * R,\ P + Q,\ Q + R, \text{ and } (P + Q) * R.$$

Since C_2 passes eight of the nine intersections, which are

$$\mathcal{O},\ P,\ Q,\ R,\ P * Q,\ Q * R,\ P + Q, \text{ and } Q + R,$$

applying Cayley-Bacharach gives that C_2 should pass through the ninth intersection, which is $(P + Q) * R$. But it is given that C_2 and C already have a ninth intersection, namely $P * (Q + R)$, we should have

$$(P + Q) * R = P * (Q + R).$$

Therefore $\big((P + Q) * R\big) * \mathcal{O} = \big(P * (Q + R)\big) * \mathcal{O}$, i.e. $(P + Q) + R = P + (Q + R)$, as desired. □

6 The Original Problem

We now come back to the original problem that we introduced earlier, and will try to find a positive integer solution to the equation

$$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}=4.$$

First, notice that all the expressions on the numerator and the denominator are linear, so they are homogeneous. This means if (a_0, b_0, c_0) is a solution, then $(2a_0, 2b_0, 2c_0)$ is also a solution, so as $(3a_0, 3b_0, 3c_0)$, and (na_0, nb_0, nc_0) for any positive integer n. So what really matters is the ratio between solutions. Thus, we could fix one variable as 1!

For each fraction, divide c from both the numerator and the denominator. This gives

$$\frac{\frac{a}{c}}{\frac{b}{c}+1}+\frac{\frac{b}{c}}{\frac{a}{c}+1}+\frac{1}{\frac{a}{c}+\frac{b}{c}}=4.$$

This is now an equation with two variables! This is still better even though the variables are now positive rational numbers. Rewriting the equation gives

$$\frac{x}{y+1}+\frac{y}{x+1}+\frac{1}{x+y}=4.$$

Getting rid of the denominator, we get the following equation:

$$x(x+1)(x+y)+y(y+1)(x+y)+(x+1)(y+1)=4(x+1)(y+1)(x+y),$$

Rearranging gives

$$x^3-3x^2y-3xy^2+y^3-3x^2-5xy-3y^2-3x-3y+1=0.$$

Recall the integral solution we found earlier: $(a, b, c) = (-11, -4, 1)$. This gives $(x, y) = (-11, -4)$, which is a pair of solutions of this equation.

If you make substitutions and change to Weierstrass normal form, then it will be in the form

$$y^2=x^3+109x^2+224x.$$

We have mentioned that the transformation to Weierstrass normal form preserves the rational points on the curve. The rational point $(-11, 4)$ is mapped to the point $P(-100, 260)$, which is a rational point on the elliptic curve $y^2 = x^3 + 109x^2 + 224x$.

We now to try to find a point on the elliptic curve $y^2 = x^3 + 109x^2 + 224x$ that corresponds to a rational point on

$$x^3-3x^2y-3xy^2+y^3-3x^2-5xy-3y^2-3x-3y+1=0$$

whose x-coordinate and y-coordinate are both positive. We try with a new point. Calculating $P+P = 2P$ gives

$$P+P=2P=\left(\frac{8836}{25},-\frac{950716}{125}\right),$$

which corresponds to the solution $(x, y) = \left(\frac{9499}{5165}, -\frac{8784}{5165}\right)$. Still not positive. We try more.

Since the operation $+$ is commutative and associative, we have $2P + 2P = P + 3P$. So the points don't depend on the order of how you apply $+$, and only depends on how many times you applied the operation $+$. Looking for the corresponding rational points for $3P$, $4P$, ... gives that the desired positive rational point occurs at $9P$, which is

$$9P=\left(\frac{662023684042295852648424098838788747074536766450382 25}{135144002927162885120709079450029433526925780004069 21},\right.$$

$$\left.\frac{588008351573080833073767517273471813300856728502967303518717487133079887006112 10}{157106866859797843455636470729189626883808694543003132219675439042028040734646 9}\right).$$

This corresponds to the solution

$$(x,y) = \left(\frac{1544768021087461664419513150199198374856643256695654317000266348982532020352779 99}{4373612677928697257861252602371390152816537558161613618621437993378423467772036}, \right.$$

$$\left. \frac{3687513179412999982719781156522547482549297996897197099628313747163722463405557 9}{4373612677928697257861252602371390152816537558161613618621437993378423467772036} \right).$$

Therefore we get that the triplet (a, b, c), where

$$a = 1544768021087461664419513150199198374856643256695654317000266348982532020352779 99$$

$$b = 3687513179412999982719781156522547482549297996897197099628313747163722463405557 9$$

$$c = 4373612677928697257861252602371390152816537558161613618621437993378423467772036,$$

is a positive integral solution to the equation

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} = 4.$$

One surprising fact is that this is the smallest solution! It can be proved that this is the smallest solution, but it's omitted here. We will touch on this again later.

7 The Structure of the Group of Rational Points

Now that we have a group Γ, one important question to consider is how we can describe every element of the group, i.e. every rational point on a given elliptic curve. We have seen that if we had two (or even one) rational points, we can generate another one by the group law. Does this process cover all the rational points?

Definition 4 (Finitely Generated Abelian Group)**.** An abelian group $(G, +)$ is **finitely generated** if there exist a finite set of elements $\{a_1, a_2, \ldots, a_n\}$ such that any $g \in G$ can be expressed as a finite sum

$$g = \sum_{i=0}^{n} n_i a_i,$$

where n_i is the number of a_is that appear for each $i = 1, 2, \ldots, n$ that may differ.

Example 3. We have the following finitely generated abelian groups.

1. $(\mathbb{Z}, +)$ is finitely generated by 1.
2. $(\mathbb{Z}[i], +)$ is finitely generated by 1, i.
3. $(\mathbb{Z}[x], +)$ is not finitely generated. The basis $\{1, x, x^2, \ldots\}$ is a basis for $(\mathbb{Z}[x], +)$, but this set is infinite.

The following theorem states that for any elliptic curve C, the set of rational points Γ on C is finitely generated.

Theorem 5 (Mordell's Theorem)**.** *The group of rational points on an elliptic curve is finitely generated.*

This is a powerful theorem, which says that we only need a finite set of points to find all rational points of the elliptic curve.

Definition 5 (Rank)**.** The **rank** of an elliptic curve is the number of rational points you need to generate $(\Gamma, +)$, i.e. all of the rational points.

If we revisit the elliptic curve in our problem, it is known that the elliptic curve $y^2 = x^3 + 109x^2 + 224x$ has rank one and is isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}$[2] so it is sufficient to find two elements generating the group. It turns out that the generator of the infinite part of the group is precisely our point P, though this is not easy to show.

8 Some Open Questions

The rank of an elliptic curve is a very mysterious object, and there are a number of open problems surrounding it.

Conjecture 1. *As $X \to \infty$, the average rank of elliptic curves with height less than X is 0.5. In particular, 50% have rank 0, 50% have rank 1, and 0% have rank > 1.*

The height is defined as $\max(4|a|^3, 27b^2)$, and it allows us to make a statement about density. The current best known bound on the average rank is 7/6 [5].

Conjecture 2. *The maximum rank of an elliptic curve is bounded.*

The current record is an elliptic curve of rank at least 29, found in 2024 by Elkies and Klagsbrun[1].

Conjecture 3 (Birch-Swinnerton-Dyer Conjecture [3])**.** *The rank of an elliptic curve E is the order of the zero of $L(E, s)$ at $s = 1$.*

References

[1] Andrej Dujella. History of elliptic curves rank records. https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html. Accessed 31 July 2025.

[2] The LMFDB Collaboration. The L-functions and modular forms database, home page of the elliptic curve with lmfdb label 910.a4. https://www.lmfdb.org/EllipticCurve/Q/910/a/4, 2025. Accessed 31 July 2025.

[3] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Springer, 2015.

[4] Terence Tao. Pappus's theorem and elliptic curves. https://terrytao.wordpress.com/2011/07/15/pappuss-theorem-and-elliptic-curves/, July 2011. Accessed 31 July 2025.

[5] Wikipedia contributors. Rank of an elliptic curve. https://en.wikipedia.org/wiki/Rank_of_an_elliptic_curve, 2025. Accessed 31 July 2025.