Secrets of Elliptic Curves

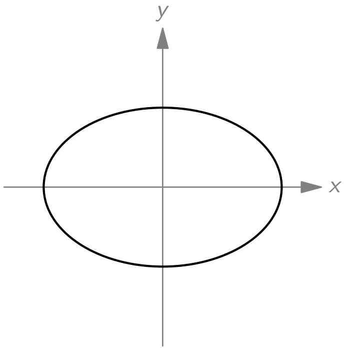
Pitchayut Saengrungkongka

MIT

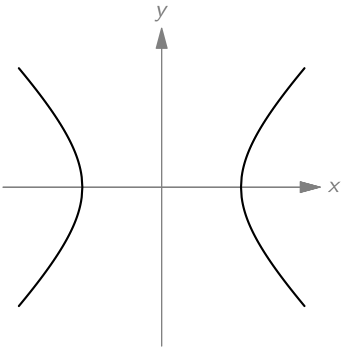
October 24, 2025

Conics

In high school, we learned about conics, which are curves described by degree 2 equations.



$$\frac{x^2}{9} + \frac{y^2}{4} = 1$$

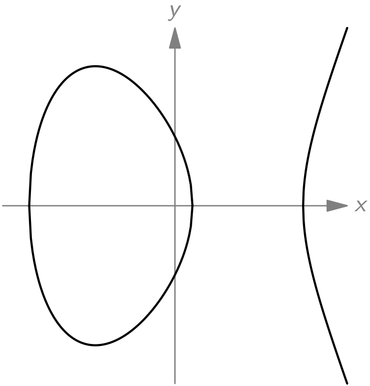


$$x^2 - y^2 = 1$$

Elliptic Curve

Today, we are going to talk about elliptic curves, which are curves of the form

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

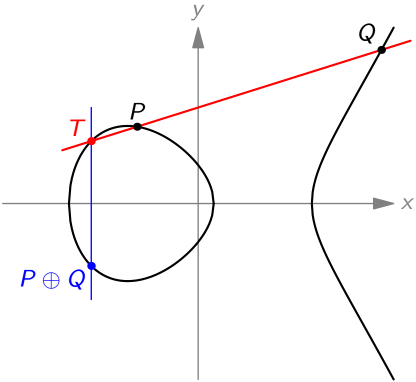


$$y^2 = x^3 - 4x + 1$$

Group Operation

Given points P and Q on the elliptic curves, we **add** those two points by

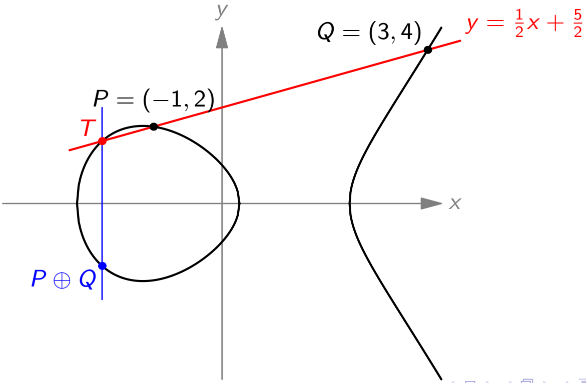
- Draw the line through point P and Q.
- This line intersects the elliptic curve at one other point. Let this point be T.
- Reflect T across the x-axis to get point $P \oplus Q$.



Example

Let E be the curve $y^2 = x^3 - 4x + 1$, $P = (-1, 2)$, and $Q = (3, 4)$.

- The line through P and Q has equation $y = \frac{1}{2}x + \frac{5}{2}$.
- This line intersect the elliptic curve again at $T = \left(-\frac{7}{4}, \frac{13}{8}\right)$.
- Therefore, $P \oplus Q = \boxed{\left(-\frac{7}{4}, -\frac{13}{8}\right)}$.



Do order matter?

If we have three points P, Q, and R, we can add them in two ways:

$$(P \oplus Q) \oplus R \quad \text{and} \quad P \oplus (Q \oplus R).$$

Example

In the curve $y^2 = x^3 - 4x + 1$, if

$$P = (-1, 2), \quad Q = (3, 4), \quad R = (0, 1).$$

Then

$$P \oplus Q = \left(-\frac{7}{4}, -\frac{13}{8}\right), \quad (P \oplus Q) \oplus R = \left(\frac{92}{49}, \frac{113}{343}\right)$$
$$Q \oplus R = \left(-\frac{2}{9}, \frac{37}{27}\right), \quad P \oplus (Q \oplus R) = \left(\frac{92}{49}, \frac{113}{343}\right).$$

The Miracle

Theorem (Associativity of $\oplus$)

For any points P, Q, R on an elliptic curve, we have

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

One can prove this by deriving the formula for $P \oplus Q$. Let's see how it goes.

The Miracle

Theorem (Associativity of $\oplus$)

For any points P, Q, R on an elliptic curve, we have

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

One can prove this by deriving the formula for $P \oplus Q$. Let's see how it goes.

Let $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $R = (x_R, y_R)$. Then the line through P and Q has equation

$$y - y_P = \frac{y_P - y_Q}{x_P - x_Q}(x - x_P),$$

which intersects the elliptic curve again at

$$\left(\left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 - x_P - x_Q,\ \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^3 + \frac{y_P + y_Q}{2} - \frac{3}{2} \cdot \frac{y_P - y_Q}{x_P - x_Q}(x_P + x_Q)\right).$$

Negating the y-coordinate gives point $P \oplus Q$.

The Miracle

Theorem (Associativity of $\oplus$)

For any points P, Q, R on an elliptic curve, we have

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

Thus, we have that $P \oplus Q$ is the point

$$\left(\left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 - x_P - x_Q,\ -\left(\frac{y_P - y_Q}{x_P - x_Q}\right)^3 - \frac{y_P + y_Q}{2} + \frac{3}{2} \cdot \frac{y_P - y_Q}{x_P - x_Q}(x_P + x_Q)\right).$$

We now need to perform the same addition operation with R, getting a messy expression for the coordinates of $(P \oplus Q) \oplus R$.

The Miracle

Theorem (Associativity of $\oplus$)

For any points P, Q, R on an elliptic curve, we have

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

Thus, we have that $P \oplus Q$ is the point

$$\left(\left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 - x_P - x_Q,\ -\left(\frac{y_P - y_Q}{x_P - x_Q}\right)^3 - \frac{y_P + y_Q}{2} + \frac{3}{2} \cdot \frac{y_P - y_Q}{x_P - x_Q}(x_P + x_Q)\right).$$

We now need to perform the same addition operation with R, getting a messy expression for the coordinates of $(P \oplus Q) \oplus R$.

Similarly, we can get another messy expression for $P \oplus (Q \oplus R)$.

These expressions have about 500 terms. However, they miraculously turn out to be equal!

Why do we care?

The property that we just proved allows us to add points in any order. For example,

$$
\begin{aligned}
P \oplus P &= 2P \\
2P \oplus 2P &= 4P \\
4P \oplus 4P &= 8P \\
&\vdots
\end{aligned}
$$

(where $nP = \underbrace{P \oplus \cdots \oplus P}_{n\ P\text{'s}}$). This allows us to compute nP for large n quickly.

On the other hand, the relation between P and, e.g., $1000P$ is very complicated. Given nP and P, no one knows how to efficiently determine n.

This hardness is a foundation of **elliptic curve cryptography**.

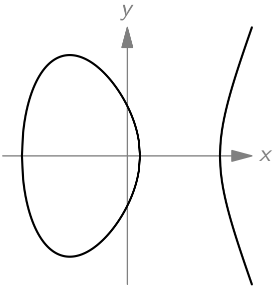
Is this the end?

Our proof of $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ raises some burning questions.

- Is there any way to avoid these massive computations?
- Why should we expect this to be true?

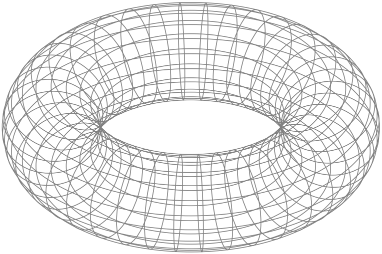
Mathematicians have answer to these questions through two different perspectives.

Perspective 1: Complex Analysis

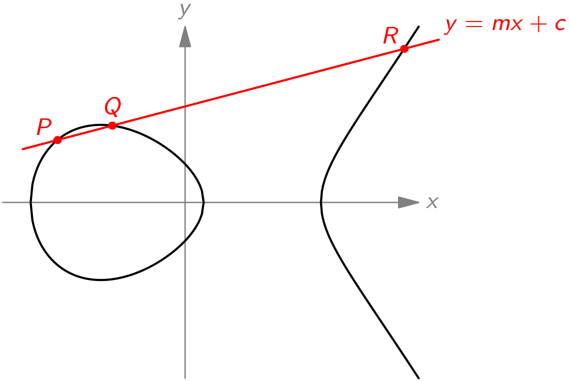


$$y^2 = x^3 - 4x + 1$$

$$\simeq$$



Perspective 2: Divisors

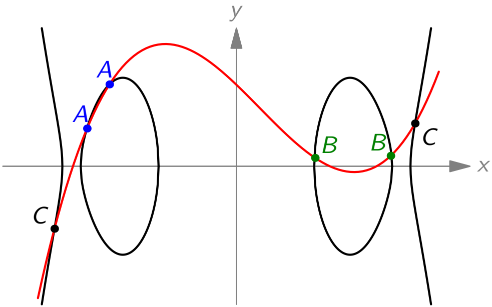


$$\mathrm{div}(y - mx - c) = (P) + (Q) + (R).$$

More Complicated Curves

Either of these two perspectives allow us to **see** how to generalize the addition law to more complicated curves.

For example, the curve $y^2 = x^6 + ax^5 + bx^4 + \cdots + ex + f$ have an addition law on **pairs** of points.



$$A + B + C = 0 \iff \text{there is a cubic passing through } A,\ B,\ C$$

Any curve have an addition law of g-tuples of points, where g is the **genus**, which measures complexity of a curve.

Why do we study advanced mathematics?

Advanced mathematics can **abstract away** complicated equations, allowing us to see things (e.g., elliptic curves addition law) in a simpler ways.

With new understanding, we can reveal hidden structure that we haven't seen before (e.g., higher-genus curves).

Thank You!