Elliptic Curves

ANISHA JOSEPH

Cubic Curves

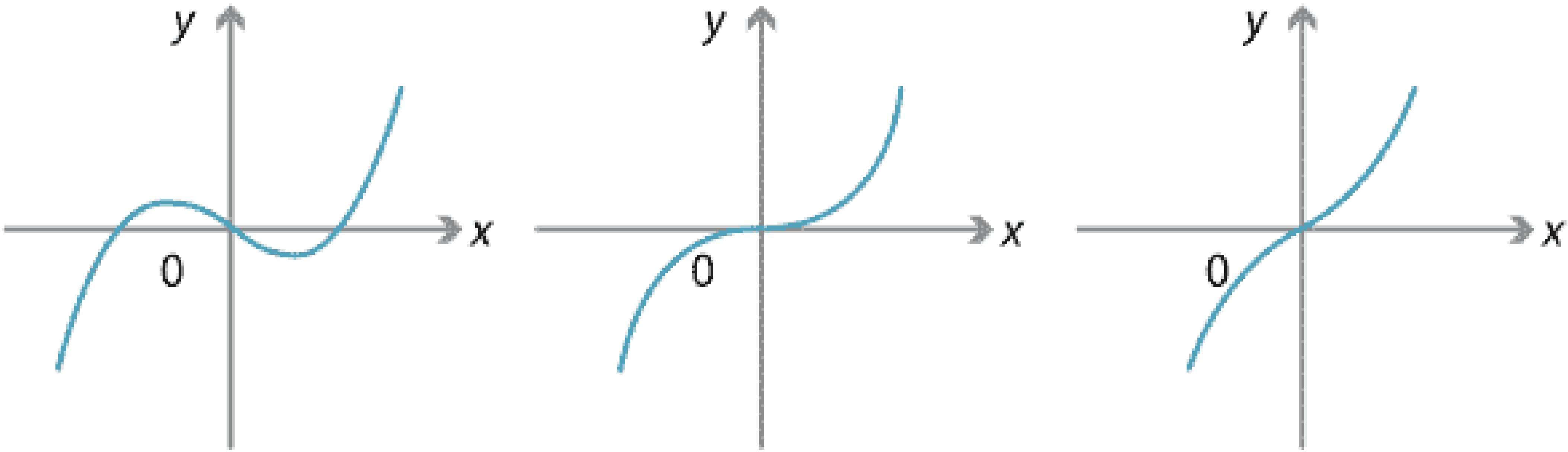
Cubic Curve: Generally refers to any curve defined by a cubic polynomial equation in two variables.

It can take various forms and does not necessarily have any special properties.

A typical example is:

$$y=ax^3+bx^2+cx+d$$

Cubic Curves



Graph of $f(x) = x^3 - x$. Graph of $f(x) = x^3$. Graph of $f(x) = x^3 + x$.

Singular point

A singular point of a curve is a point where the curve exhibits some form of "bad behavior." Specifically, it's a point where the curve fails to be smooth.

Mathematical Condition: For a curve defined by a function F(x, y)=0, a point (x_0, y_0) is a singular point if both partial derivatives vanish at that point:

$$\frac{\partial F}{\partial x}(x_0, y_0) = 0 \quad \text{and} \quad \frac{\partial F}{\partial y}(x_0, y_0) = 0$$

Discriminant

- The **discriminant** D is a scalar value derived from the coefficients a, b, c, and d.
- It provides information about the nature of the roots and singular points of the polynomial.
- The discriminant of a cubic polynomial can be calculated using the following formula:

$$D = 18abcd - 4b^3d + b^2c^2 - 4ac^2 - 27a^2d^2$$

Discriminant

Roots and Singularity:

If D>0: The cubic polynomial has **three distinct real roots.** This means the curve is smooth and does not have singular points.

If D=0: The cubic polynomial has **a multiple root**, indicating that the curve may have singular points .

If D<0: The cubic polynomial has **one real root and two complex conjugate roots.** The curve still might be smooth, but it does not intersect the x-axis three times.

Introduction to Elliptic Curves

- An elliptic curve is the set of solutions to an equation of the form.

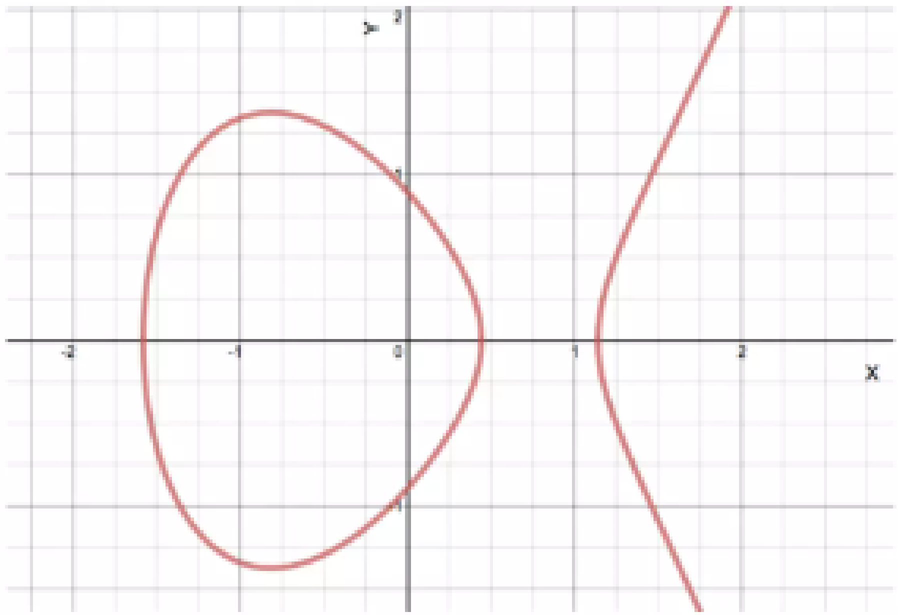
$$Y^2 = X^3 + AX + B$$

- Equations of this type are called **Weierstrass equations.**
- Two examples of elliptic curves,

$$E_1 : Y^2 = X^3 - 3X + 3 \qquad \text{and} \qquad E_2 : Y^2 = X^3 - 6X + 5,$$

Geometry of elliptic curves over reals

- Let a and b be real numbers. An elliptic curve E over the field of real numbers R is the set of points (x,y) with x and y in R that satisfy the equation $y^2 = x^3 + ax + b$
- If the cubic polynomial x^3+ax+b has no repeated roots, we say the elliptic curve is non-singular.
- A necessary and sufficient condition for the cubic polynomial x^3+ax+b to have distinct roots is $4a^3 + 27\ b^2 \neq 0$.



Weierstrass normal form

Definition

An elliptic curve in Weierstrass normal form looks like the following:

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

Note that some of the things discussed today will apply to non-singular cubics in the more general form:

$$y^2 = x^3 + ax^2 + bx + c$$

Either type of equation is said to be in Weierstrass form.

Weierstrass normal form

Definition. An *elliptic curve* E is the set of solutions to a Weierstrass equation

$$E : Y^2 = X^3 + AX + B,$$

together with an extra point $\mathcal{O}$, where the constants A and B must satisfy

$$4A^3 + 27B^2 \neq 0.$$

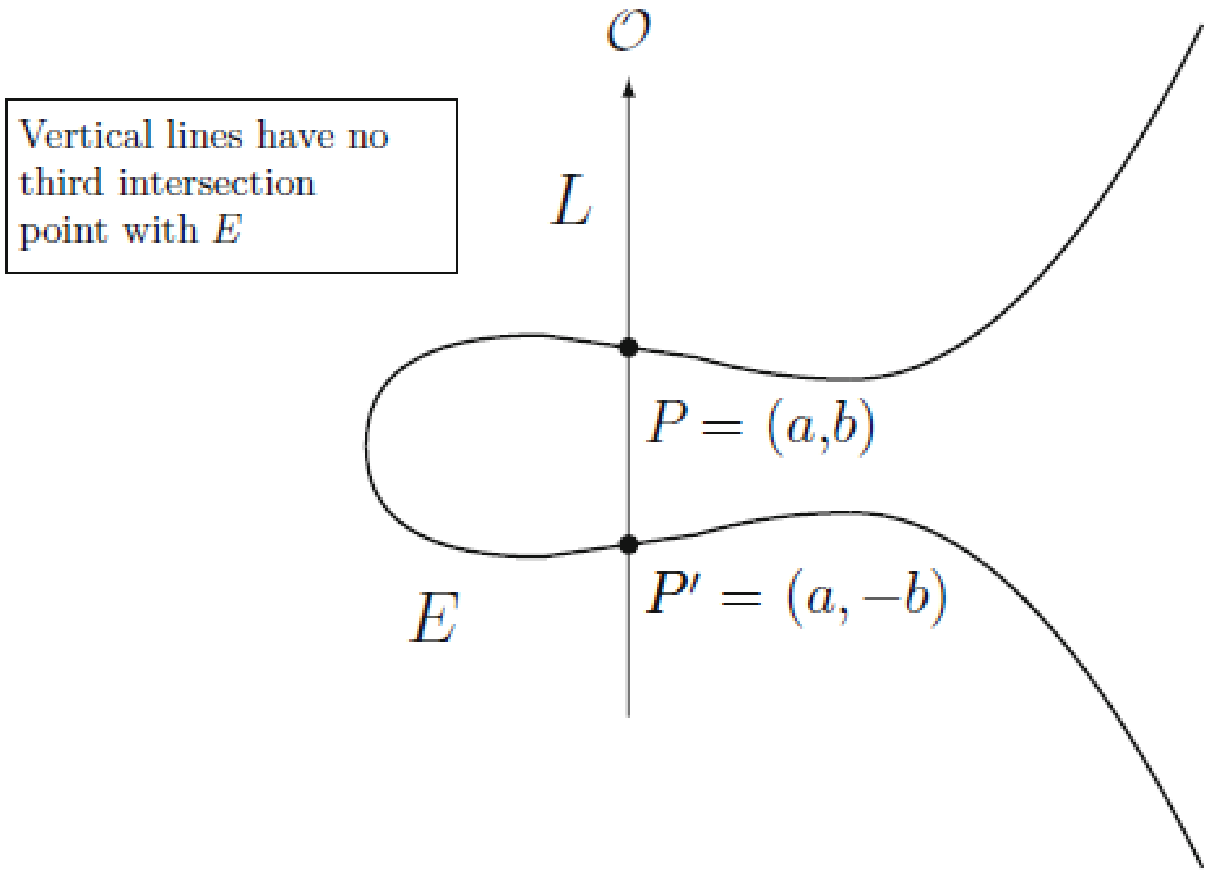


Figure 6.4: The vertical line L through $P = (a, b)$ and $P' = (a, -b)$

$$X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3),$$

where e_1, e_2, e_3 are allowed to be complex numbers, then

$$4A^3 + 27B^2 \neq 0 \qquad \text{if and only if} \qquad e_1, e_2, e_3 \text{ are distinct.}$$

Point at infinity(*O*)

Definition

There is a point $\mathcal{O}$, "at infinity," in any group of points on an elliptic curve. While it can be helpful to think of $\mathcal{O}$ being at an intersection of the two ends of the curve, the ends never really intersect. $\mathcal{O}$ is projective, contained in every vertical line through the curve.

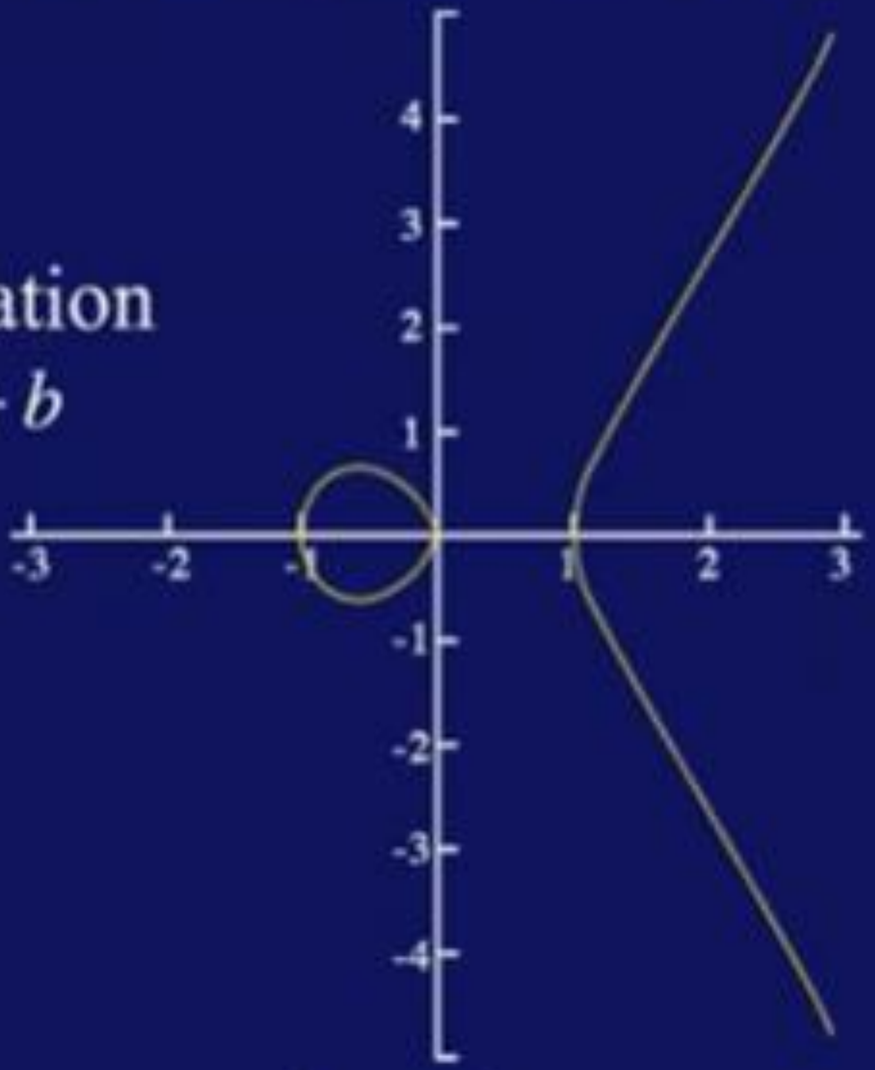
By the definition of point addition, $\mathcal{O}$ is the additive identity in any group of points on elliptic curves.

What is an **elliptic curve**?

But this

General equation

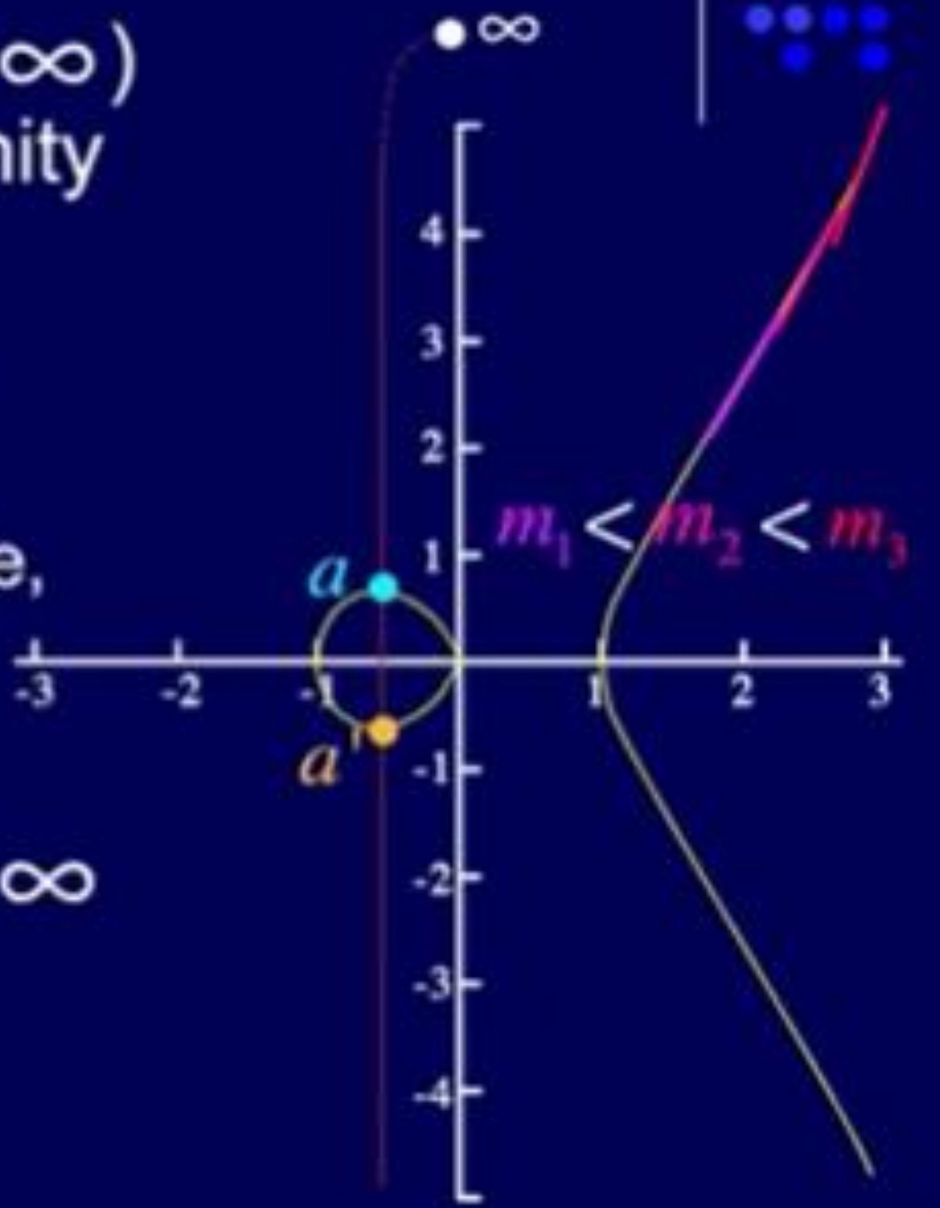
$$y^2 = x^3 + ax + b$$



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

...the vertical line?

- All vertical lines (slope = ∞) intersect the point at infinity
- The curve has an ever-increasing slope after a point of inflection
  - The slope becomes infinite, so it also intersects ∞
- Thus, a line from a to a' would intersect the curve at ∞



Elliptic curve – Addition Law

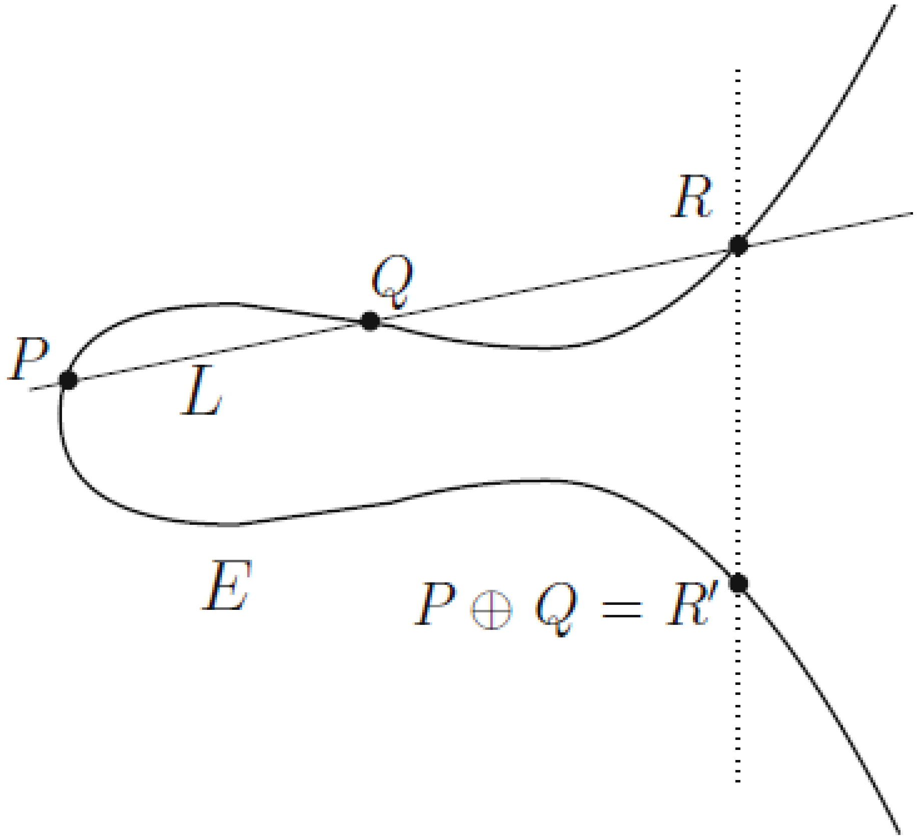


Figure 6.2: The addition law on an elliptic curve

Elliptic curve – Addition Law

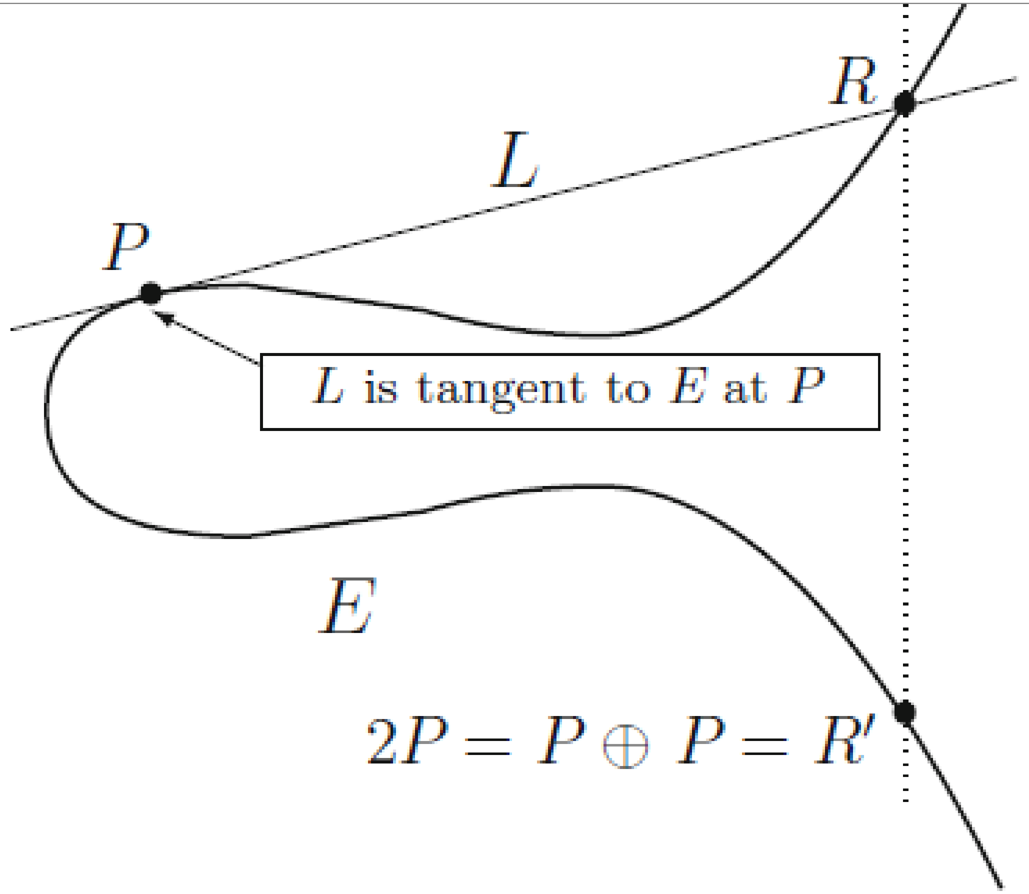
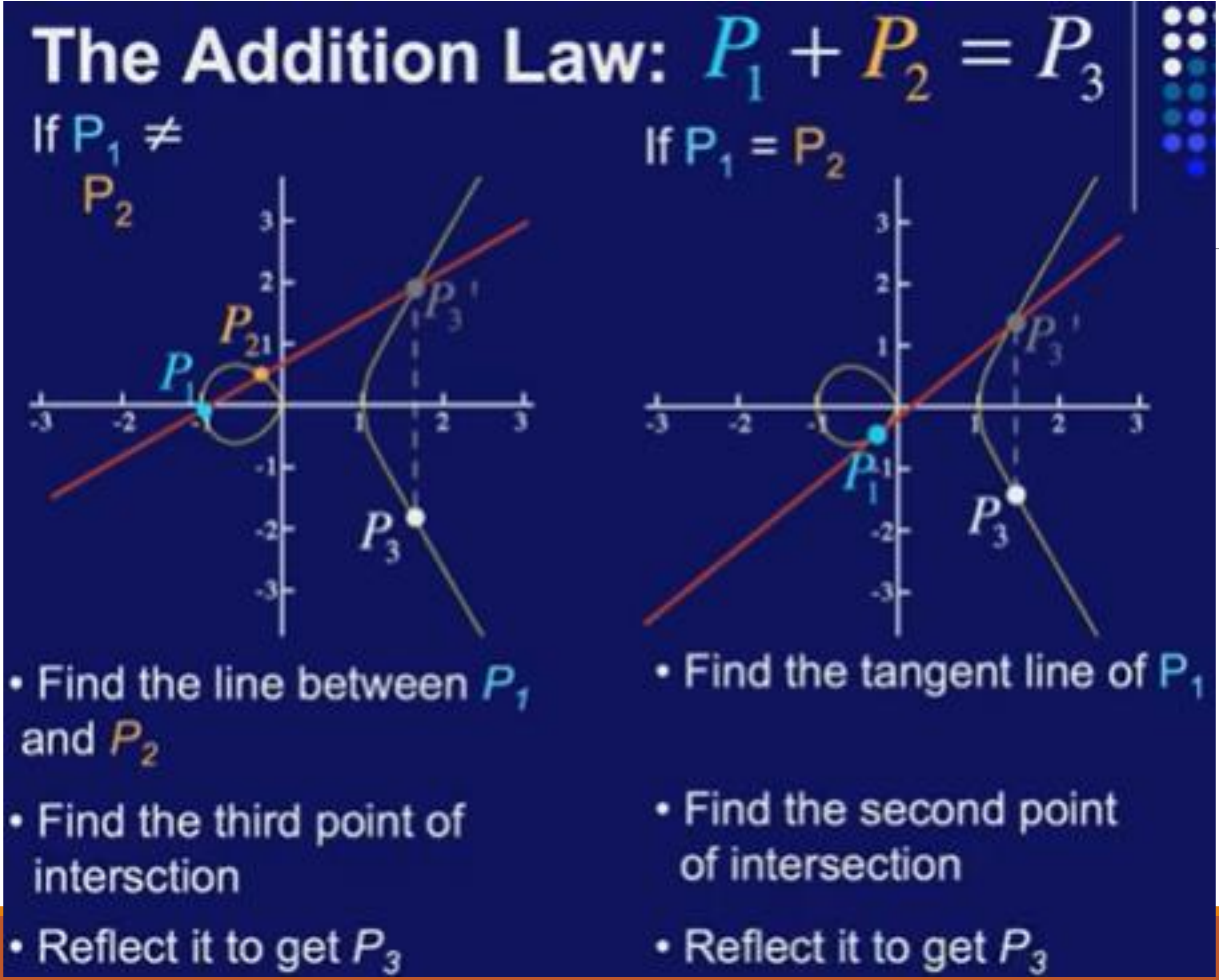


Figure 6.3: Adding a point P to itself


The Addition Law: $P_1 + P_2 = P_3$
If $P_1 \neq P_2$
P_2
P_1
P_3'
P_3
-3 -2 -1 1 2 3
3 2 1 -1 -2 -3
• Find the line between P_1 and P_2
• Find the third point of intersction
• Reflect it to get P_3
If $P_1 = P_2$
P_1
P_3'
P_3
• Find the tangent line of P_1
• Find the second point of intersection
• Reflect it to get P_3

The Line

$$P_1 = (x_1, y_1) \quad P_2 = (x_2, y_2)$$

- The point-slope form of the line

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

Slope of line joining P1 and P2

$$y - y_1 = \lambda(x - x_1)$$

Equation of line passing through P1

- The slope-intercept form of the line

$$y = \lambda x - \lambda x_1 + y_1$$

Rearrange above equation

$$\beta = y_1 - \lambda x_1$$

Let assign β

$$y = \lambda x + \beta$$

y in terms of β

Finding x_3 and y_3

$$y = \lambda x + \beta$$

$$y^2 = (\lambda x + \beta)^2 \text{ — } 1$$

Squaring on both sides

(the curve) $y^2 = x^3 + ax + b$ — 2

General equation for elliptic curve

$$(\lambda x + \beta)^2 = x^3 + ax + b$$

Equating 1 and 2

$$0 = x^3 - \lambda^2 x^2 - 2\lambda x\beta - \beta^2 + ax + b$$

x_1, x_2, x_3 are the roots

$$(x_1 + x_2 + x_3) = \lambda^2$$

The coefficient of x^2 is the opposite sum of the roots

coefficient of x^2 is -(sum of roots)

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

Equation of line passing through P1 and P3

Elliptic Curve Addition of points

If P1=P2 , slope can be calculated by taking derivative on both sides with respect to x.

$$Y^2 = X^3 + AX + B$$

Slope is dy/dx = λ

$$\boxed{\lambda = \frac{3x_1^2 + A}{2y_1}}$$

Why reflect?

Try adding infinity to a point

- Adding infinity results in a vertical line
- Then find the third point of intersection
- Reflect it and the result is the original point

$P + \infty = P$ Infinity is the identity for point addition

Inverses

$$P + P' = \infty$$

The reflection of a point is its inverse

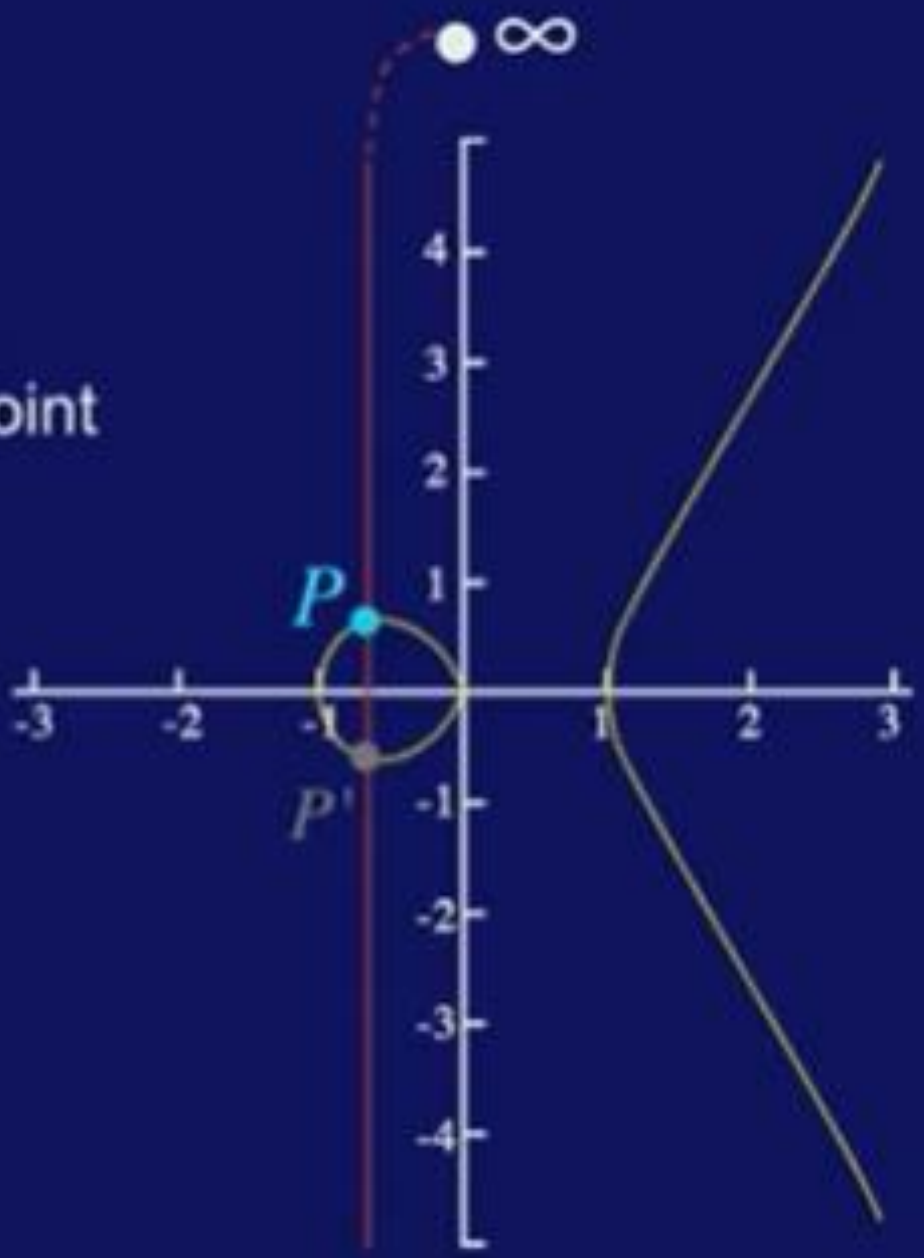
So, if we define

$$P = (x, y)$$

and

$$-P = (x, -y)$$

$$P - P = \infty$$



Elliptic Curve Addition Algorithm

Let $E : Y^2 = X^3 + AX + B$

be an elliptic curve and let P1 and P2 be points on E.

(a) If $P1 = \mathcal{O}$, then $P1 + P2 = P2$.

(b) Otherwise, if $P2 = \mathcal{O}$, then $P1 + P2 = P1$.

(c) Otherwise, write $P1 = (x1, y1)$ and $P2 = (x2, y2)$.

(d) If $x1 = x2$ and $y1 = -y2$, then $P1 + P2 = \mathcal{O}$.

Elliptic Curve Addition Algorithm

(e) Otherwise, define λ by

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \textit{if } P_1 \neq P_2, \\[2ex] \dfrac{3x_1^2 + A}{2y_1} & \textit{if } P_1 = P_2, \end{cases}$$

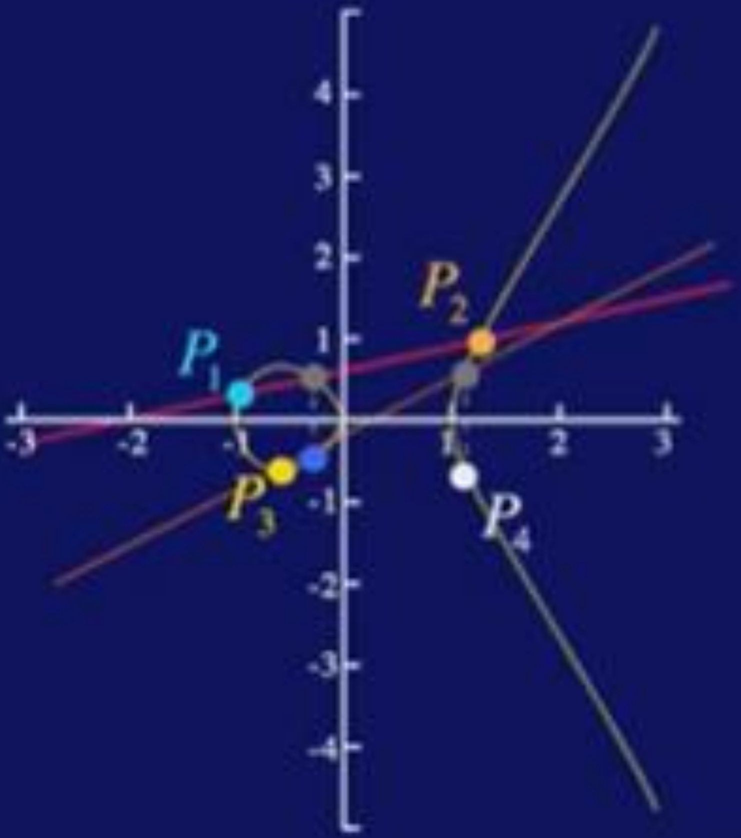
and let

$$x_3 = \lambda^2 - x_1 - x_2 \qquad \textit{and} \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

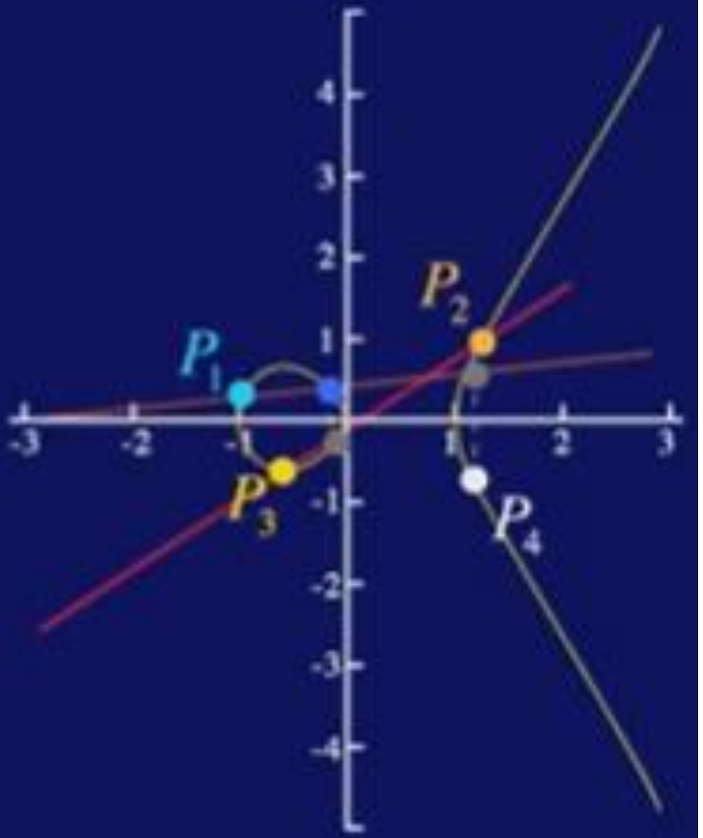
Then $P_1 + P_2 = (x_3, y_3)$.

Associativity

- $(P_1 + P_2) + P_3 = P_4$



- $P_1 + (P_2 + P_3) = P_4$



$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$$

Group Structure

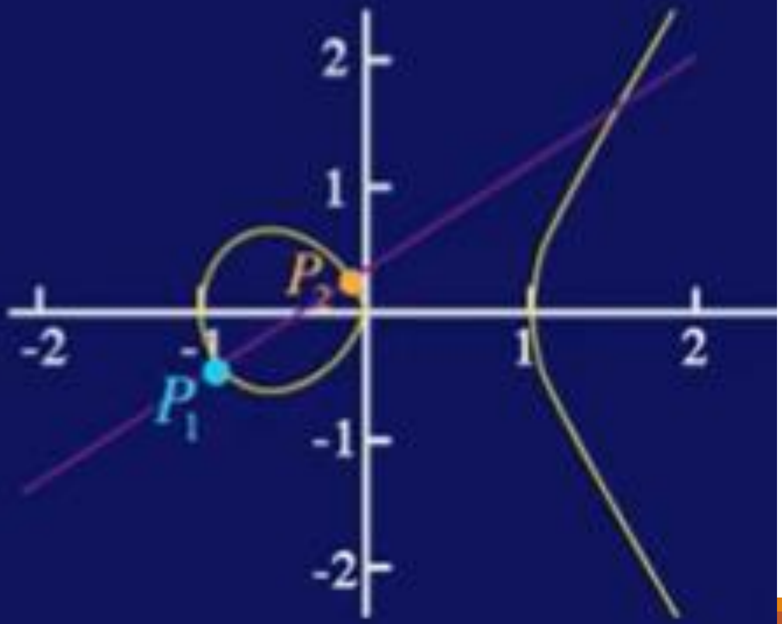
The curve *E* under point addition is a group

- Identity - at infinity
- Inverses - the reflection of a point
- Associative
- Closed

The curve *E* under point addition is an Abelian group

- Identity - at infinity
- Inverses - the reflection of a point
- Associative
- Closed
- Commutative

$$P_1 + P_2 = P_2 + P_1$$



Bezout's theorem

Theorem 4.1 (Bezout's Theorem). *Let C_1 and C_2 be projective curves with no common components, and $I(P, C_1 \cap C_2)$ the intersection mulitiplicity of point $P \in C_1 \cap C_2$. Then*

$$\sum_{P \in C_1 \cap C_2} I(P, C_1 \cap C_2) = (\deg C_1)(\deg C_2).$$

Bezout's theorem for projective plane curves claims that the number of common points (counting multiplicities) between two projective plane curves without common components is equal to the product of their degrees.

Bezout's theorem

(1) This is a generic example where nothing seems to go wrong. We have a circle (curve of degree 2) and a line (curve of degree 1), see Figure 2 below. They intersect at two distinct points which is clearly the product of their degrees.

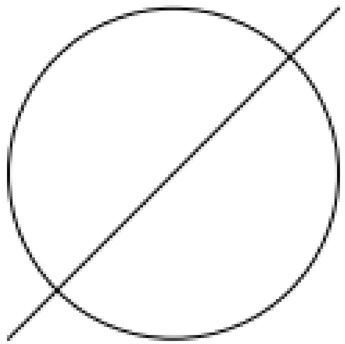


FIGURE 2. $X^2 + Y^2 - 1$ and $X - Y$

Bezout's theorem

(2) Here we also have a line and a circle, however they intersect only in one point, see Figure 3 below. This does not disprove Bézout's Theorem, since it counts common points up to multiplicity: the line and the circle intersect in the point $P = (0, 1)$ with multiplicity two.

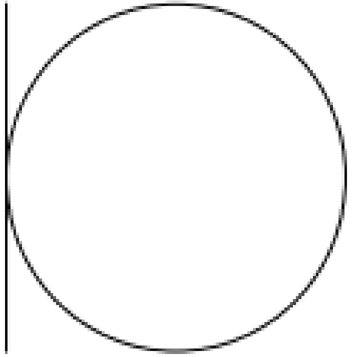


FIGURE 3. $X^2 + Y^2 - 1$ and $X + 1$

Bezout's theorem

(2) Here we also have a line and a circle, however they intersect only in one point, see Figure 3 below. This does not disprove Bézout's Theorem, since it counts common points up to multiplicity: the line and the circle intersect in the point $P = (0, 1)$ with multiplicity two.

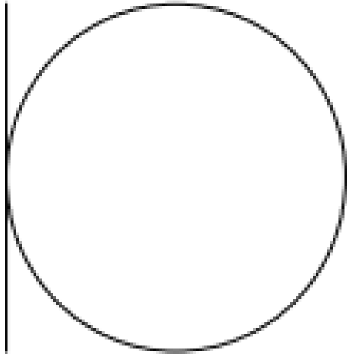
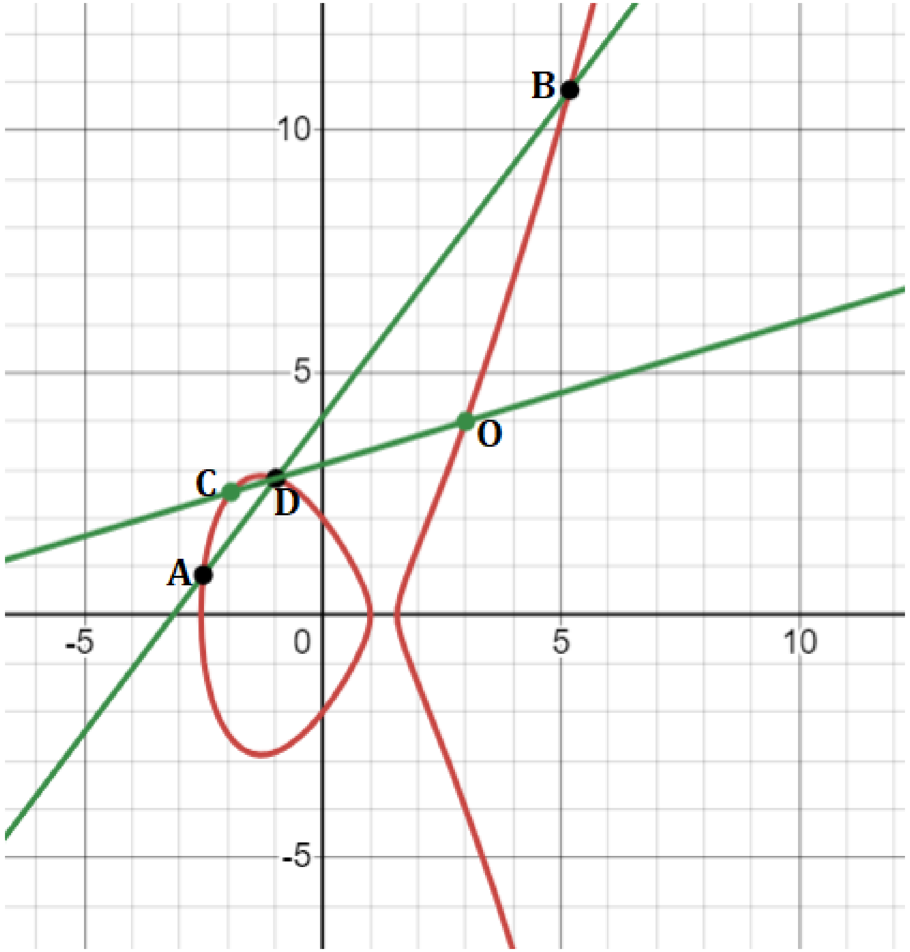


FIGURE 3. $X^2 + Y^2 - 1$ and $X + 1$

Bezout's theorem

What about number intersecting points on elliptic curve and line?

- Elliptic curve – Degree is 3
- Line – Degree is 1
- Total Number of Intersecting points = 3.1=3



Points of Finite Order

Definition. Let **m ≥ 1** be an integer. A point P ∈ E satisfying **mP = *O*** *is* called a point of order **m** in the group **E.** We denote the set of points of order **m** by,

$$E[m] = \{P \in E : mP = \mathcal{O}\}$$

Such points are called points of ***finite order or torsion points.***

Points of Finite Order

Example 1:

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

P=(2,3) is his means 6P=*O* (the point at infinity), indicating that P is of order 6.

P=(0,1) is his means 3P=*O* (the point at infinity), indicating that P is of order 3.