Elliptic Curves and the Special Values of L-functions

ICTS, 2021

Introduction to Elliptic Curves: Lecture 1

Anupam Saikia

Department of Mathematics,
Indian Institute of Technology Guwahati

Sections

Sections

Motivation

Elliptic curves are ubiquitous in mathematics. Study of elliptic curves brings together number theory, algebra, analysis and algebraic geometry.

- Elliptic curves have been used to prove Fermat's Last Theorem.
- Elliptic curves have provided breakthrough toward resolving the Congruent Number Problem.
- Elliptic curves have been very useful in cryptography, i.e., in coding messages for secure transmission.
- Elliptic curves are also used in factorization algorithm for integers.
- The Birch and Swinnerton-Dyer Conjecture, one of the seven Millennium Problems, is a prediction about relation between the algebraic and the analytic properties of an elliptic curve.

Motivation

Elliptic curves are ubiquitous in mathematics. Study of elliptic curves brings together number theory, algebra, analysis and algebraic geometry.

- Elliptic curves have been used to prove Fermat's Last Theorem.
- Elliptic curves have provided breakthrough toward resolving the Congruent Number Problem.
- Elliptic curves have been very useful in cryptography, i.e., in coding messages for secure transmission.
- Elliptic curves are also used in factorization algorithm for integers.
- The Birch and Swinnerton-Dyer Conjecture, one of the seven Millennium Problems, is a prediction about relation between the algebraic and the analytic properties of an elliptic curve.

Motivation

Introduction
The Point at Infinity
Group Structure

Elliptic curves are ubiquitous in mathematics. Study of elliptic curves brings together number theory, algebra, analysis and algebraic geometry.

- Elliptic curves have been used to prove Fermat's Last Theorem.
- Elliptic curves have provided breakthrough toward resolving the Congruent Number Problem.
- Elliptic curves have been very useful in cryptography, i.e., in coding messages for secure transmission.
- Elliptic curves are also used in factorization algorithm for integers.
- The Birch and Swinnerton-Dyer Conjecture, one of the seven Millennium Problems, is a prediction about relation between the algebraic and the analytic properties of an elliptic curve.

Motivation

Elliptic curves are ubiquitous in mathematics. Study of elliptic curves brings together number theory, algebra, analysis and algebraic geometry.

- Elliptic curves have been used to prove Fermat's Last Theorem.
- Elliptic curves have provided breakthrough toward resolving the Congruent Number Problem.
- Elliptic curves have been very useful in cryptography, i.e., in coding messages for secure transmission.
- Elliptic curves are also used in factorization algorithm for integers.
- The Birch and Swinnerton-Dyer Conjecture, one of the seven Millennium Problems, is a prediction about relation between the algebraic and the analytic properties of an elliptic curve.

Motivation

Introduction

The Point at Infinity

Group Structure

Elliptic curves are ubiquitous in mathematics. Study of elliptic curves brings together number theory, algebra, analysis and algebraic geometry.

- Elliptic curves have been used to prove Fermat's Last Theorem.
- Elliptic curves have provided breakthrough toward resolving the Congruent Number Problem.
- Elliptic curves have been very useful in cryptography, i.e., in coding messages for secure transmission.
- Elliptic curves are also used in factorization algorithm for integers.
- The Birch and Swinnerton-Dyer Conjecture, one of the seven Millennium Problems, is a prediction about relation between the algebraic and the analytic properties of an elliptic curve.

Motivation

Introduction

The Point at Infinity

Group Structure

Elliptic curves are ubiquitous in mathematics. Study of elliptic curves brings together number theory, algebra, analysis and algebraic geometry.

- Elliptic curves have been used to prove Fermat's Last Theorem.
- Elliptic curves have provided breakthrough toward resolving the Congruent Number Problem.
- Elliptic curves have been very useful in cryptography, i.e., in coding messages for secure transmission.
- Elliptic curves are also used in factorization algorithm for integers.
- The Birch and Swinnerton-Dyer Conjecture, one of the seven Millennium Problems, is a prediction about relation between the algebraic and the analytic properties of an elliptic curve.

Weierstrass Equation for an Elliptic Curve

- An elliptic curve over a field K can be defined as *a non-singular projective curve of genus 1 with a specified point $\mathcal{O} \in E(K)$.*

- Using the Riemann-Roch Theorem, one has an equivalent description of elliptic curve as a plane cubic curve:

  An elliptic curve over a field K is a 'non-singular curve' defined by an equation of the form

  $$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K,$$

  together with 'a point at infinity' $\mathcal{O}$.

- When the *characteristic* of the underlying field K is not 2 or 3, the Weierstrass equation above can be simplified to

  $$y^2 = x^3 + ax + b, \qquad a, \; b \in K.$$

Weierstrass Equation for an Elliptic Curve

- An elliptic curve over a field K can be defined as *a non-singular projective curve of genus 1 with a specified point $\mathcal{O} \in E(K)$.*
- Using the Riemann-Roch Theorem, one has an equivalent description of elliptic curve as a plane cubic curve:

  An elliptic curve over a field K is a 'non-singular curve' defined by an equation of the form

  $$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K,$$

  together with 'a point at infinity' $\mathcal{O}$.

- When the *characteristic* of the underlying field K is not 2 or 3, the Weierstrass equation above can be simplified to

$$y^2 = x^3 + ax + b, \qquad a, \ b \in K.$$

Weierstrass Equation for an Elliptic Curve

- An elliptic curve over a field K can be defined as *a non-singular projective curve of genus 1 with a specified point $\mathcal{O} \in E(K)$.*

- Using the Riemann-Roch Theorem, one has an equivalent description of elliptic curve as a plane cubic curve:

  An elliptic curve over a field K is a 'non-singular curve' defined by an equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K,$$

  together with 'a point at infinity' $\mathcal{O}$.

- When the *characteristic* of the underlying field K is not 2 or 3, the Weierstrass equation above can be simplified to

$$y^2 = x^3 + ax + b, \qquad a, \ b \in K.$$

Weierstrass Equation for an Elliptic Curve

- An elliptic curve over a field K can be defined as *a non-singular projective curve of genus 1 with a specified point $\mathcal{O} \in E(K)$.*

- Using the Riemann-Roch Theorem, one has an equivalent description of elliptic curve as a plane cubic curve:

  An elliptic curve over a field K is a 'non-singular curve' defined by an equation of the form

  $$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K,$$

  together with 'a point at infinity' $\mathcal{O}$.

- When the *characteristic* of the underlying field K is not 2 or 3, the Weierstrass equation above can be simplified to

  $$y^2 = x^3 + ax + b, \qquad a,\ b \in K.$$

Weierstrass Equation for an Elliptic Curve

- An elliptic curve over a field K can be defined as *a non-singular projective curve of genus 1 with a specified point $\mathcal{O} \in E(K)$.*
- Using the Riemann-Roch Theorem, one has an equivalent description of elliptic curve as a plane cubic curve:

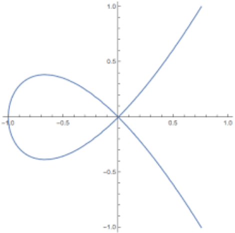
  An elliptic curve over a field K is a 'non-singular curve' defined by an equation of the form

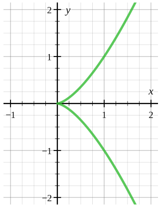
  $$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K,$$

  together with 'a point at infinity' $\mathcal{O}$.
- When the *characteristic* of the underlying field K is not 2 or 3, the Weierstrass equation above can be simplified to

  $$y^2 = x^3 + ax + b, \qquad a,\ b \in K.$$

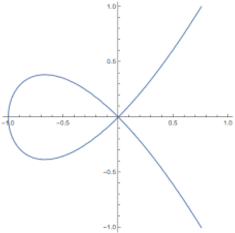
Non-singularity

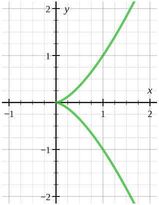




- A curve in $\mathbb{R}^2$ is called non-singular if it has a well-defined tangent at each of its points.
- For example, $y^2 = x^2(x+1)$ and $y^2 = x^3$ are singular at $(0,0)$ in the diagram above.

Non-singularity

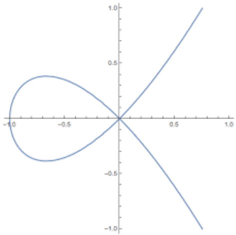


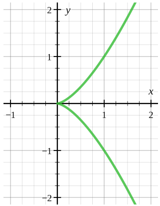


- A curve in $\mathbb{R}^2$ is called non-singular if it has a well-defined tangent at each of its points.

- For example, $y^2 = x^2(x+1)$ and $y^2 = x^3$ are singular at $(0,0)$ in the diagram above.

Non-singularity





- A curve in $\mathbb{R}^2$ is called non-singular if it has a well-defined tangent at each of its points.

- For example, $y^2 = x^2(x+1)$ and $y^2 = x^3$ are singular at $(0,0)$ in the diagram above.

Singular Points

- For a curve $f(x, y) = 0$ in $\mathbb{R}^2$, the slope of the tangent at a point $P = (x_0, y_0)$ is given by

$$\frac{dy}{dx}(P) = -\frac{\partial f/\partial x(P)}{\partial f/\partial y(P)}.$$

- The tangent is not well-defined at (x_0, y_0) on $f(x, y) = 0$ if

$$\frac{\partial f}{\partial x}(x_0, y_0) = 0 = \frac{\partial f}{\partial y}(x_0, y_0).$$

- Thus, (x_0, y_0) is a singular point of the cubic curve given by $f(x, y) = y^2 - (x^3 + ax + b)$ if and only if $y_0 = 0$, $3x_0^2 + a = 0$, and $x_0^3 + ax_0 + b = 0$, i.e., x_0 is a double root of $x^3 + ax + b$.

- In general, a curve over any field K (not necessarily $\mathbb{R}$) defined by a polynomial $f(x, y) \in K[x, y]$ is called non-singular at $P = (x_0, y_0)$ if the Jacobian matrix $\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right)$ has rank 1.

Singular Points

- For a curve $f(x,y)=0$ in $\mathbb{R}^2$, the slope of the tangent at a point $P=(x_0,y_0)$ is given by

$$\frac{dy}{dx}(P) = -\frac{\partial f/\partial x(P)}{\partial f/\partial y(P)}.$$

- The tangent is not well-defined at (x_0,y_0) on $f(x,y)=0$ if

$$\frac{\partial f}{\partial x}(x_0,y_0) = 0 = \frac{\partial f}{\partial y}(x_0,y_0).$$

- Thus, (x_0,y_0) is a singular point of the cubic curve given by $f(x,y)=y^2-(x^3+ax+b)$ if and only if $y_0=0$, $3x_0^2+a=0$, and $x_0^3+ax_0+b=0$, i.e., x_0 is a double root of x^3+ax+b.

- In general, a curve over any field K (not necessarily $\mathbb{R}$) defined by a polynomial $f(x,y)\in K[x,y]$ is called non-singular at $P=(x_0,y_0)$ if the Jacobian matrix $\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right)$ has rank 1.

Singular Points

- For a curve $f(x,y)=0$ in $\mathbb{R}^2$, the slope of the tangent at a point $P=(x_0,y_0)$ is given by

$$\frac{dy}{dx}(P) = -\frac{\partial f/\partial x(P)}{\partial f/\partial y(P)}.$$

- The tangent is not well-defined at (x_0,y_0) on $f(x,y)=0$ if

$$\frac{\partial f}{\partial x}(x_0,y_0) = 0 = \frac{\partial f}{\partial y}(x_0,y_0).$$

- Thus, (x_0,y_0) is a singular point of the cubic curve given by $f(x,y)=y^2-(x^3+ax+b)$ if and only if $y_0=0$, $3x_0^2+a=0$, and $x_0^3+ax_0+b=0$, i.e., x_0 is a double root of x^3+ax+b.

- In general, a curve over any field K (not necessarily $\mathbb{R}$) defined by a polynomial $f(x,y)\in K[x,y]$ is called non-singular at $P=(x_0,y_0)$ if the Jacobian matrix $\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right)$ has rank 1.

Singular Points

- For a curve $f(x,y)=0$ in $\mathbb{R}^2$, the slope of the tangent at a point $P=(x_0,y_0)$ is given by

$$\frac{dy}{dx}(P) = -\frac{\partial f/\partial x(P)}{\partial f/\partial y(P)}.$$

- The tangent is not well-defined at (x_0,y_0) on $f(x,y)=0$ if

$$\frac{\partial f}{\partial x}(x_0,y_0) = 0 = \frac{\partial f}{\partial y}(x_0,y_0).$$

- Thus, (x_0,y_0) is a singular point of the cubic curve given by $f(x,y)=y^2-(x^3+ax+b)$ if and only if $y_0=0$, $3x_0^2+a=0$, and $x_0^3+ax_0+b=0$, i.e., x_0 is a double root of x^3+ax+b.

- In general, a curve over any field K (not necessarily $\mathbb{R}$) defined by a polynomial $f(x,y)\in K[x,y]$ is called non-singular at $P=(x_0,y_0)$ if the Jacobian matrix $\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right)$ has rank 1.

The Discriminant

- The discriminant of a cubic polynomial $g(x) \in K[x]$ is given by

$$\Delta(g) = \prod_{i>j} (\alpha_i - \alpha_j)^2 = (\alpha_1 - \alpha_2)^2 (\alpha_2 - \alpha_3)^2 (\alpha_1 - \alpha_3)^2,$$

  where α_i's are the roots of $g(x)$.

- So $g(x)$ has repeated roots if and only if $\Delta(g) = 0$.

- It can be easily computed that the discriminant of $g(x) = x^3 + ax + b$ is $\Delta(g) = -(4a^3 + 27b^2) \in K$.

- Hence the curve $y^2 = x^3 + ax + b$ is non-singular if

$$4a^3 + 27b^2 \neq 0.$$

The Discriminant

- The discriminant of a cubic polynomial $g(x) \in K[x]$ is given by

$$\Delta(g) = \prod_{i>j} (\alpha_i - \alpha_j)^2 = (\alpha_1 - \alpha_2)^2 (\alpha_2 - \alpha_3)^2 (\alpha_1 - \alpha_3)^2,$$

  where α_i's are the roots of $g(x)$.

- So $g(x)$ has repeated roots if and only if $\Delta(g) = 0$.

- It can be easily computed that the discriminant of $g(x) = x^3 + ax + b$ is $\Delta(g) = -(4a^3 + 27b^2) \in K$.

- Hence the curve $y^2 = x^3 + ax + b$ is non-singular if

$$4a^3 + 27b^2 \neq 0.$$

The Discriminant

Introduction

The Point at Infinity

Group Structure

- The discriminant of a cubic polynomial $g(x) \in K[x]$ is given by

$$\Delta(g) = \prod_{i>j} (\alpha_i - \alpha_j)^2 = (\alpha_1 - \alpha_2)^2 (\alpha_2 - \alpha_3)^2 (\alpha_1 - \alpha_3)^2,$$

where α_i's are the roots of $g(x)$.

- So $g(x)$ has repeated roots if and only if $\Delta(g) = 0$.

- It can be easily computed that the discriminant of $g(x) = x^3 + ax + b$ is $\Delta(g) = -(4a^3 + 27b^2) \in K$.

- Hence the curve $y^2 = x^3 + ax + b$ is non-singular if

$$4a^3 + 27b^2 \neq 0.$$

The Discriminant

- The discriminant of a cubic polynomial $g(x) \in K[x]$ is given by

$$\Delta(g) = \prod_{i>j} (\alpha_i - \alpha_j)^2 = (\alpha_1 - \alpha_2)^2 (\alpha_2 - \alpha_3)^2 (\alpha_1 - \alpha_3)^2,$$

where α_i's are the roots of $g(x)$.

- So $g(x)$ has repeated roots if and only if $\Delta(g) = 0$.
- It can be easily computed that the discriminant of $g(x) = x^3 + ax + b$ is $\Delta(g) = -(4a^3 + 27b^2) \in K$.
- Hence the curve $y^2 = x^3 + ax + b$ is non-singular if

$$4a^3 + 27b^2 \neq 0.$$

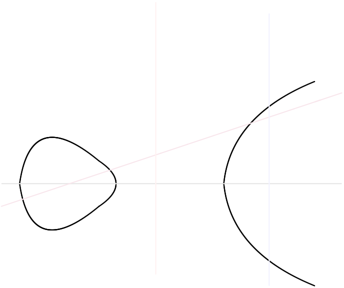
Sections

Sections

Intersection with a Straight Line: a diagram

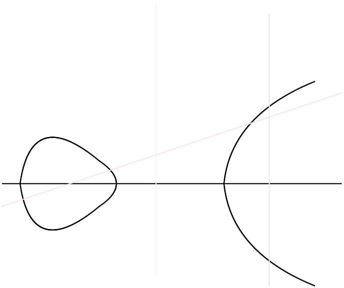
The points with real coordinates on $E : y^2 = x^3 - 25x$ and intersection with a straight line $y = mx + c$:

$(mx + c)^2 = x^3 - 25x$



The points with real coordinates on $E : y^2 = x^3 - 25x$ and intersection with a straight line $y = mx + c$:

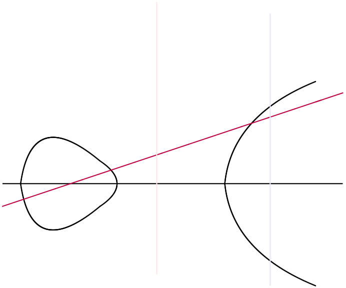
$(mx + c)^2 = x^3 - 25x$



Intersection with a Straight Line: a diagram

The points with real coordinates on $E : y^2 = x^3 - 25x$ and intersection with a straight line $y = mx + c$:

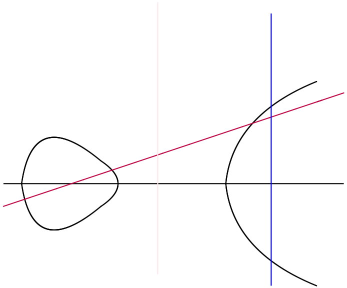
$(mx + c)^2 = x^3 - 25x$



Intersection with a Straight Line: a diagram

The points with real coordinates on $E : y^2 = x^3 - 25x$ and intersection with a straight line $y = mx + c$:

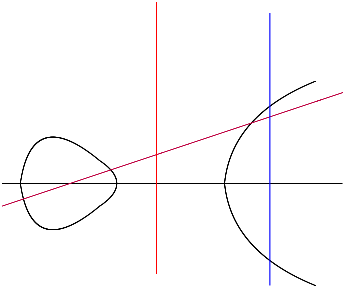
$(mx + c)^2 = x^3 - 25x$



Intersection with a Straight Line: a diagram

The points with real coordinates on $E : y^2 = x^3 - 25x$ and intersection with a straight line $y = mx + c$:

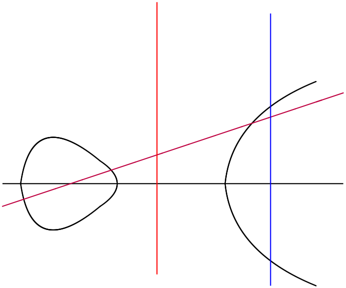
$(mx + c)^2 = x^3 - 25x$



Intersection with a Straight Line: a diagram

The points with real coordinates on $E : y^2 = x^3 - 25x$ and intersection with a straight line $y = mx + c$:

$(mx + c)^2 = x^3 - 25x$



The Point at Infinity on an Elliptic Curve

- Any non-vertical straight line intersects the curve at three points.
- A non-vertical line $y = mx + c$ ($m, c \in \mathbb{R}$) will have three real points of intersection or one real and two complex points of intersection, as seen by substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.
- However, the vertical lines $x = x_0$ will have either two real or two complex points of intersection. For a consistent theory, we need a third point of intersection. We adjoin an additional 'point at infinity' to the curve.
- This point can be visualized as lying on the top (and the bottom) of the xy-plane at infinity.
- Any two vertical lines intersect at the point at infinity, say $\mathcal{O}$.
- The point at infinity is best understood in terms of projective coordinates.

The Point at Infinity on an Elliptic Curve

- Any non-vertical straight line intersects the curve at three points.
- A non-vertical line $y = mx + c$ ($m, c \in \mathbb{R}$) will have three real points of intersection or one real and two complex points of intersection, as seen by substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.
- However, the vertical lines $x = x_0$ will have either two real or two complex points of intersection. For a consistent theory, we need a third point of intersection. We adjoin an additional 'point at infinity' to the curve.
- This point can be visualized as lying on the top (and the bottom) of the xy-plane at infinity.
- Any two vertical lines intersect at the point at infinity, say $\mathcal{O}$.
- The point at infinity is best understood in terms of projective coordinates.

The Point at Infinity on an Elliptic Curve

- Any non-vertical straight line intersects the curve at three points.
- A non-vertical line $y = mx + c$ ($m, c \in \mathbb{R}$) will have three real points of intersection or one real and two complex points of intersection, as seen by substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.
- However, the vertical lines $x = x_0$ will have either two real or two complex points of intersection. For a consistent theory, we need a third point of intersection. We adjoin an additional 'point at infinity' to the curve.
- This point can be visualized as lying on the top (and the bottom) of the xy-plane at infinity.
- Any two vertical lines intersect at the point at infinity, say $\mathcal{O}$.
- The point at infinity is best understood in terms of projective coordinates.

The Point at Infinity on an Elliptic Curve

- Any non-vertical straight line intersects the curve at three points.
- A non-vertical line $y = mx + c$ ($m, c \in \mathbb{R}$) will have three real points of intersection or one real and two complex points of intersection, as seen by substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.
- However, the vertical lines $x = x_0$ will have either two real or two complex points of intersection. For a consistent theory, we need a third point of intersection. We adjoin an additional 'point at infinity' to the curve.
- This point can be visualized as lying on the top (and the bottom) of the xy-plane at infinity.
- Any two vertical lines intersect at the point at infinity, say $\mathcal{O}$.
- The point at infinity is best understood in terms of projective coordinates.

The Point at Infinity on an Elliptic Curve

- Any non-vertical straight line intersects the curve at three points.
- A non-vertical line $y = mx + c$ ($m, c \in \mathbb{R}$) will have three real points of intersection or one real and two complex points of intersection, as seen by substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.
- However, the vertical lines $x = x_0$ will have either two real or two complex points of intersection. For a consistent theory, we need a third point of intersection. We adjoin an additional 'point at infinity' to the curve.
- This point can be visualized as lying on the top (and the bottom) of the xy-plane at infinity.
- Any two vertical lines intersect at the point at infinity, say $\mathcal{O}$.
- The point at infinity is best understood in terms of projective coordinates.

The Point at Infinity on an Elliptic Curve

- Any non-vertical straight line intersects the curve at three points.
- A non-vertical line $y = mx + c$ ($m, c \in \mathbb{R}$) will have three real points of intersection or one real and two complex points of intersection, as seen by substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.
- However, the vertical lines $x = x_0$ will have either two real or two complex points of intersection. For a consistent theory, we need a third point of intersection. We adjoin an additional 'point at infinity' to the curve.
- This point can be visualized as lying on the top (and the bottom) of the xy-plane at infinity.
- Any two vertical lines intersect at the point at infinity, say $\mathcal{O}$.
- The point at infinity is best understood in terms of projective coordinates.

The Point at Infinity on an Elliptic Curve

- Any non-vertical straight line intersects the curve at three points.
- A non-vertical line $y = mx + c$ ($m, c \in \mathbb{R}$) will have three real points of intersection or one real and two complex points of intersection, as seen by substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.
- However, the vertical lines $x = x_0$ will have either two real or two complex points of intersection. For a consistent theory, we need a third point of intersection. We adjoin an additional 'point at infinity' to the curve.
- This point can be visualized as lying on the top (and the bottom) of the xy-plane at infinity.
- Any two vertical lines intersect at the point at infinity, say $\mathcal{O}$.
- The point at infinity is best understood in terms of projective coordinates.

The Projective Space over a Field K

- Let $\overline{K}$ denote the algebraic closure of a field K. Define a relation $\sim$ on the set of non-zero $(n+1)$-tuples

$$(a_0, a_2, \ldots, a_n) \in \overline{K}^{n+1} \setminus \{(0, 0, \ldots, 0)\} \qquad \text{by}$$

$$(a_0, a_1, a_2, \ldots, a_n) \sim (a_0', a_1', a_2', \ldots, a_n') \text{ if and only if}$$

$$a_0' = ta_0, \;\; a_1' = ta_1, \;\; \ldots, \;\; a_n' = ta_n \;\text{ for some } t \in \overline{K}^{\times}.$$

Clearly, $\sim$ is an equivalence relation.

- The projective n-space over K is defined as the set of equivalence classes

$$\mathbb{P}^n = \frac{\{(a_0, a_1, a_2, \ldots, a_n) \in \overline{K}^{n+1} \setminus (0, 0, \ldots, 0)\}}{\sim}.$$

- We denote the *affine n-space* over K by

$$\mathbb{A}^n = \{(x_1, x_2, \ldots, x_n) \; : \; x_i \in \overline{K}\}.$$

The Projective Space over a Field K

- Let $\overline{K}$ denote the algebraic closure of a field K. Define a relation $\sim$ on the set of non-zero $(n+1)$-tuples

$$(a_0, a_2, \ldots, a_n) \in \overline{K}^{n+1} \setminus \{(0, 0, \ldots, 0)\} \qquad \text{by}$$

$$(a_0, a_1, a_2, \ldots, a_n) \sim (a_0', a_1', a_2', \ldots, a_n') \text{ if and only if}$$

$$a_0' = ta_0, \;\; a_1' = ta_1, \; \ldots, \;\; a_n' = ta_n \;\text{ for some } t \in \overline{K}^{\times}.$$

Clearly, $\sim$ is an equivalence relation.

- The projective n-space over K is defined as the set of equivalence classes

$$\mathbb{P}^n = \frac{\{(a_0, a_1, a_2, \ldots, a_n) \in \overline{K}^{n+1} \setminus (0, 0, \ldots, 0)\}}{\sim}.$$

- We denote the *affine n-space* over K by

$$\mathbb{A}^n = \{(x_1, x_2, \ldots, x_n) \; : \; x_i \in \overline{K}\}.$$

The Projective Space over a Field K

- Let $\overline{K}$ denote the algebraic closure of a field K. Define a relation $\sim$ on the set of non-zero $(n+1)$-tuples

$$(a_0, a_2, \ldots, a_n) \in \overline{K}^{n+1} \setminus \{(0,0,\ldots,0)\} \qquad \text{by}$$

$$(a_0, a_1, a_2, \ldots, a_n) \sim (a_0', a_1', a_2', \ldots, a_n') \text{ if and only if}$$
$$a_0' = ta_0,\ \ a_1' = ta_1,\ \ldots,\ \ a_n' = ta_n \ \text{ for some } t \in \overline{K}^{\times}.$$

  Clearly, $\sim$ is an equivalence relation.

- The projective n-space over K is defined as the set of equivalence classes

$$\mathbb{P}^n = \frac{\{(a_0, a_1, a_2, \ldots, a_n) \in \overline{K}^{n+1} \setminus (0,0,\ldots,0)\}}{\sim}.$$

- We denote the *affine* n-*space* over K by

$$\mathbb{A}^n = \{(x_1, x_2, \ldots, x_n) \ : \ x_i \in \overline{K}\}.$$

The Projective Space over a Field K

- Let $\overline{K}$ denote the algebraic closure of a field K. Define a relation $\sim$ on the set of non-zero $(n+1)$-tuples

$$(a_0, a_2, \ldots, a_n) \in \overline{K}^{n+1} \setminus \{(0,0,\ldots,0)\} \qquad \text{by}$$

$$(a_0, a_1, a_2, \ldots, a_n) \sim (a_0', a_1', a_2', \ldots, a_n') \text{ if and only if}$$

$$a_0' = ta_0, \quad a_1' = ta_1, \quad \ldots, \quad a_n' = ta_n \text{ for some } t \in \overline{K}^{\times}.$$

Clearly, $\sim$ is an equivalence relation.

- The projective n-space over K is defined as the set of equivalence classes

$$\mathbb{P}^n = \frac{\{(a_0, a_1, a_2, \ldots, a_n) \in \overline{K}^{n+1} \setminus (0,0,\ldots,0)\}}{\sim}.$$

- We denote the *affine n-space* over K by

$$\mathbb{A}^n = \{(x_1, x_2, \ldots, x_n) \ : \ x_i \in \overline{K}\}.$$

The Points in the Projective Plane

- Let $[a : b : c]$ denote a point in $\mathbb{P}^2$, i.e.,

$$[a : b : c] = \{t(a, b, c) \in \overline{K}^3 \setminus (0, 0, 0) \mid t \neq 0\}.$$

- Any point (x, y) in the affine plane $\mathbb{A}^2$ corresponds to a unique point $[x : y : 1]$ in $\mathbb{P}^2$.

- For a point $[a : b : c]$ in $\mathbb{P}^2$ with $c \neq 0$, we get a unique point $(\frac{a}{c}, \frac{b}{c})$ in the affine plane A^2.

- However, $\mathbb{P}^2$ has additional points with $c = 0$ which cannot be identified with the points in the affine plane in this way. The points $[a : b : 0]$ in $\mathbb{P}^2$ can be thought of as representation of *directions of straight lines parallel to the line $ay = bx$ in the affine plane A^2*. These additional points are known as the points at infinity in $\mathbb{P}^2$.

The Points in the Projective Plane

- Let $[a : b : c]$ denote a point in $\mathbb{P}^2$, i.e.,

$$[a : b : c] = \{t(a, b, c) \in \overline{K}^3 \setminus (0, 0, 0) \mid t \neq 0\}.$$

- Any point (x, y) in the affine plane $\mathbb{A}^2$ corresponds to a unique point $[x : y : 1]$ in $\mathbb{P}^2$.

- For a point $[a : b : c]$ in $\mathbb{P}^2$ with $c \neq 0$, we get a unique point $(\frac{a}{c}, \frac{b}{c})$ in the affine plane A^2.

- However, $\mathbb{P}^2$ has additional points with $c = 0$ which cannot be identified with the points in the affine plane in this way. The points $[a : b : 0]$ in $\mathbb{P}^2$ can be thought of as representation of *directions of straight lines parallel to the line $ay = bx$ in the affine plane A^2*. These additional points are known as the points at infinity in $\mathbb{P}^2$.

The Points in the Projective Plane

- Let $[a:b:c]$ denote a point in $\mathbb{P}^2$, i.e.,

$$[a:b:c] = \{t(a,b,c) \in \overline{K}^3 \setminus (0,0,0) \mid t \neq 0\}.$$

- Any point (x,y) in the affine plane $\mathbb{A}^2$ corresponds to a unique point $[x:y:1]$ in $\mathbb{P}^2$.
- For a point $[a:b:c]$ in $\mathbb{P}^2$ with $c \neq 0$, we get a unique point $(\frac{a}{c}, \frac{b}{c})$ in the affine plane A^2.
- However, $\mathbb{P}^2$ has additional points with $c = 0$ which cannot be identified with the points in the affine plane in this way. The points $[a:b:0]$ in $\mathbb{P}^2$ can be thought of as representation of *directions of straight lines parallel to the line $ay = bx$ in the affine plane A^2*. These additional points are known as the points at infinity in $\mathbb{P}^2$.

The Points in the Projective Plane

- Let $[a:b:c]$ denote a point in $\mathbb{P}^2$, i.e.,

$$[a:b:c] = \{t(a,b,c) \in \overline{K}^3 \setminus (0,0,0) \mid t \neq 0\}.$$

- Any point (x,y) in the affine plane $\mathbb{A}^2$ corresponds to a unique point $[x:y:1]$ in $\mathbb{P}^2$.
- For a point $[a:b:c]$ in $\mathbb{P}^2$ with $c \neq 0$, we get a unique point $(\frac{a}{c}, \frac{b}{c})$ in the affine plane A^2.
- However, $\mathbb{P}^2$ has additional points with $c = 0$ which cannot be identified with the points in the affine plane in this way. The points $[a:b:0]$ in $\mathbb{P}^2$ can be thought of as representation of *directions of straight lines parallel to the line $ay = bx$ in the affine plane A^2*. These additional points are known as the points at infinity in $\mathbb{P}^2$.

The Points in the Projective Plane

- Let $[a:b:c]$ denote a point in $\mathbb{P}^2$, i.e.,

$$[a:b:c] = \{t(a,b,c) \in \overline{K}^3 \setminus (0,0,0) \mid t \neq 0\}.$$

- Any point (x,y) in the affine plane $\mathbb{A}^2$ corresponds to a unique point $[x:y:1]$ in $\mathbb{P}^2$.
- For a point $[a:b:c]$ in $\mathbb{P}^2$ with $c \neq 0$, we get a unique point $(\frac{a}{c}, \frac{b}{c})$ in the affine plane A^2.
- However, $\mathbb{P}^2$ has additional points with $c = 0$ which cannot be identified with the points in the affine plane in this way. The points $[a:b:0]$ in $\mathbb{P}^2$ can be thought of as representation of *directions of straight lines parallel to the line $ay = bx$ in the affine plane A^2*. These additional points are known as the points at infinity in $\mathbb{P}^2$.

The Points in the Projective Plane

- Let $[a : b : c]$ denote a point in $\mathbb{P}^2$, i.e.,

$$[a : b : c] = \{t(a, b, c) \in \overline{K}^3 \setminus (0, 0, 0) \mid t \neq 0\}.$$

- Any point (x, y) in the affine plane $\mathbb{A}^2$ corresponds to a unique point $[x : y : 1]$ in $\mathbb{P}^2$.
- For a point $[a : b : c]$ in $\mathbb{P}^2$ with $c \neq 0$, we get a unique point $(\frac{a}{c}, \frac{b}{c})$ in the affine plane A^2.
- However, $\mathbb{P}^2$ has additional points with $c = 0$ which cannot be identified with the points in the affine plane in this way. The points $[a : b : 0]$ in $\mathbb{P}^2$ can be thought of as representation of *directions of straight lines parallel to the line $ay = bx$ in the affine plane A^2*. These additional points are known as the points at infinity in $\mathbb{P}^2$.

Lines in the Projective Plane

- A line in $\mathbb{P}^2$ consists of a line in $\mathbb{A}^2$ together with the point at infinity specified by its direction.

- Any two parallel lines in $\mathbb{P}^2$ intersect at the point at infinity corresponding to their common direction.

- The set of all points at infinity is itself considered to be a line L_∞, and the intersection of any other line L with L_∞ is the point at infinity corresponding to the direction of L.

- A vertical line in $\mathbb{A}^2$ contains the additional point $[0:1:0]$ in $\mathbb{P}^2$ (as its direction), therefore we can say that any two vertical lines intersect at the point $[0:1:0]$ at infinity.

Lines in the Projective Plane

- A line in $\mathbb{P}^2$ consists of a line in $\mathbb{A}^2$ together with the point at infinity specified by its direction.
- Any two parallel lines in $\mathbb{P}^2$ intersect at the point at infinity corresponding to their common direction.
- The set of all points at infinity is itself considered to be a line L_∞, and the intersection of any other line L with L_∞ is the point at infinity corresponding to the direction of L.
- A vertical line in $\mathbb{A}^2$ contains the additional point $[0:1:0]$ in $\mathbb{P}^2$ (as its direction), therefore we can say that any two vertical lines intersect at the point $[0:1:0]$ at infinity.

Lines in the Projective Plane

- A line in $\mathbb{P}^2$ consists of a line in $\mathbb{A}^2$ together with the point at infinity specified by its direction.
- Any two parallel lines in $\mathbb{P}^2$ intersect at the point at infinity corresponding to their common direction.
- The set of all points at infinity is itself considered to be a line L_∞, and the intersection of any other line L with L_∞ is the point at infinity corresponding to the direction of L.
- A vertical line in $\mathbb{A}^2$ contains the additional point $[0:1:0]$ in $\mathbb{P}^2$ (as its direction), therefore we can say that any two vertical lines intersect at the point $[0:1:0]$ at infinity.

Lines in the Projective Plane

- A line in $\mathbb{P}^2$ consists of a line in $\mathbb{A}^2$ together with the point at infinity specified by its direction.

- Any two parallel lines in $\mathbb{P}^2$ intersect at the point at infinity corresponding to their common direction.

- The set of all points at infinity is itself considered to be a line L_∞, and the intersection of any other line L with L_∞ is the point at infinity corresponding to the direction of L.

- A vertical line in $\mathbb{A}^2$ contains the additional point $[0 : 1 : 0]$ in $\mathbb{P}^2$ (as its direction), therefore we can say that any two vertical lines intersect at the point $[0 : 1 : 0]$ at infinity.

Lines in the Projective Plane

- A line in $\mathbb{P}^2$ consists of a line in $\mathbb{A}^2$ together with the point at infinity specified by its direction.
- Any two parallel lines in $\mathbb{P}^2$ intersect at the point at infinity corresponding to their common direction.
- The set of all points at infinity is itself considered to be a line L_∞, and the intersection of any other line L with L_∞ is the point at infinity corresponding to the direction of L.
- A vertical line in $\mathbb{A}^2$ contains the additional point $[0 : 1 : 0]$ in $\mathbb{P}^2$ (as its direction), therefore we can say that any two vertical lines intersect at the point $[0 : 1 : 0]$ at infinity.

Affine Variety

- Given an ideal I the polynomial ring $\overline{K}[Y_1, \ldots, Y_n]$, we define an affine algebraic set as

$$V_I = \{P \in \mathbb{A}^n \mid f(P) = 0 \qquad \forall f \in I\}.$$

- Given an affine algebraic set V, we associate an ideal $I(V)$ in $\overline{K}[Y_1, \ldots, Y_n]$ generated by

$$\{f \in \overline{K}[Y_1, \ldots, Y_n] \mid \quad f(P) = 0 \quad \forall P \in V\}.$$

- An affine algebraic set is called an affine variety if $I(V)$ is a prime ideal in $\overline{K}[Y_1, \ldots, Y_n]$.

- An affine variety V is said to be defined over K if its ideal $I(V)$ can be generated by polynomials in $K[Y_1, \ldots, Y_n]$.

Affine Variety

- Given an ideal I the polynomial ring $\overline{K}[Y_1, \ldots, Y_n]$, we define an affine algebraic set as

$$V_I = \{P \in \mathbb{A}^n \mid f(P) = 0 \qquad \forall f \in I\}.$$

- Given an affine algebraic set V, we associate an ideal $I(V)$ in $\overline{K}[Y_1, \ldots, Y_n]$ generated by

$$\{f \in \overline{K}[Y_1, \ldots, Y_n] \mid \quad f(P) = 0 \quad \forall P \in V\}.$$

- An affine algebraic set is called an affine variety if $I(V)$ is a prime ideal in $\overline{K}[Y_1, \ldots, Y_n]$.

- An affine variety V is said to be defined over K if its ideal $I(V)$ can be generated by polynomials in $K[Y_1, \ldots, Y_n]$.

Affine Variety

- Given an ideal I the polynomial ring $\overline{K}[Y_1, \ldots, Y_n]$, we define an affine algebraic set as

$$V_I = \{P \in \mathbb{A}^n \mid f(P) = 0 \qquad \forall f \in I\}.$$

- Given an affine algebraic set V, we associate an ideal $I(V)$ in $\overline{K}[Y_1, \ldots, Y_n]$ generated by

$$\{f \in \overline{K}[Y_1, \ldots, Y_n] \mid \quad f(P) = 0 \quad \forall P \in V\}.$$

- An affine algebraic set is called an affine variety if $I(V)$ is a prime ideal in $\overline{K}[Y_1, \ldots, Y_n]$.

- An affine variety V is said to be defined over K if its ideal $I(V)$ can be generated by polynomials in $K[Y_1, \ldots, Y_n]$.

Affine Variety

- Given an ideal I the polynomial ring $\overline{K}[Y_1, \ldots, Y_n]$, we define an affine algebraic set as

$$V_I = \{P \in \mathbb{A}^n \mid f(P) = 0 \qquad \forall f \in I\}.$$

- Given an affine algebraic set V, we associate an ideal $I(V)$ in $\overline{K}[Y_1, \ldots, Y_n]$ generated by

$$\{f \in \overline{K}[Y_1, \ldots, Y_n] \mid \; f(P) = 0 \quad \forall P \in V\}.$$

- An affine algebraic set is called an affine variety if $I(V)$ is a prime ideal in $\overline{K}[Y_1, \ldots, Y_n]$.
- An affine variety V is said to be defined over K if its ideal $I(V)$ can be generated by polynomials in $K[Y_1, \ldots, Y_n]$.

Projective Variety

- A polynomial $f \in \overline{K}[X_0, \ldots, X_n]$ is called homogenous of degree d if

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n) \qquad \forall \lambda \in \overline{K}^{\times}.$$

  An ideal I in $\in \overline{K}[X_0, \ldots, X_n]$ is called a homogenous ideal if it generated by homogenous polynomials.

- Given a homogenous ideal I, we define a projective algebraic set as

$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all homoegenous } f \in I\}.$$

- Given a projective algebraic set V, we associate a homogenous ideal $I(V)$ in $\overline{K}[X_0, \ldots, X_n]$ generated by

$$\{f \in \overline{K}[X_0, \ldots, X_n] \mid f \text{ is homoenegous, } f(P) = 0 \quad \forall P \in V\}.$$

- A projective algebraic set is called a projective variety if $I(V)$ is a prime ideal in $\overline{K}[X_0, \ldots, X_n]$.

Projective Variety

- A polynomial $f \in \overline{K}[X_0, \ldots, X_n]$ is called homogenous of degree d if

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n) \qquad \forall \lambda \in \overline{K}^{\times}.$$

An ideal I in $\in \overline{K}[X_0, \ldots, X_n]$ is called a homogenous ideal if it generated by homogenous polynomials.

- Given a homogenous ideal I, we define a projective algebraic set as

$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all homoegenous } f \in I\}.$$

- Given a projective algebraic set V, we associate a homogenous ideal $I(V)$ in $\overline{K}[X_0, \ldots, X_n]$ generated by

$$\{f \in \overline{K}[X_0, \ldots, X_n] \mid f \text{ is homoenegous, } f(P) = 0 \quad \forall P \in V\}.$$

- A projective algebraic set is called a projective variety if $I(V)$ is a prime ideal in $\overline{K}[X_0, \ldots, X_n]$.

Projective Variety

- A polynomial $f \in \overline{K}[X_0, \ldots, X_n]$ is called homogenous of degree d if
$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n) \qquad \forall \lambda \in \overline{K}^\times.$$
An ideal I in $\in \overline{K}[X_0, \ldots, X_n]$ is called a homogenous ideal if it generated by homogenous polynomials.

- Given a homogenous ideal I, we define a projective algebraic set as
$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all homoegenous } f \in I\}.$$

- Given a projective algebraic set V, we associate a homogenous ideal $I(V)$ in $\overline{K}[X_0, \ldots, X_n]$ generated by
$$\{f \in \overline{K}[X_0, \ldots, X_n] \mid f \text{ is homoenegous, } f(P) = 0 \quad \forall P \in V\}.$$

- A projective algebraic set is called a projective variety if $I(V)$ is a prime ideal in $\overline{K}[X_0, \ldots, X_n]$.

Projective Variety

- A polynomial $f \in \overline{K}[X_0, \ldots, X_n]$ is called homogenous of degree d if
$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n) \qquad \forall \lambda \in \overline{K}^\times.$$
An ideal I in $\in \overline{K}[X_0, \ldots, X_n]$ is called a homogenous ideal if it generated by homogenous polynomials.

- Given a homogenous ideal I, we define a projective algebraic set as
$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all homoegenous } f \in I\}.$$

- Given a projective algebraic set V, we associate a homogenous ideal $I(V)$ in $\overline{K}[X_0, \ldots, X_n]$ generated by
$$\{f \in \overline{K}[X_0, \ldots, X_n] \mid f \text{ is homoenegous, } f(P) = 0 \quad \forall P \in V\}.$$

- A projective algebraic set is called a projective variety if $I(V)$ is a prime ideal in $\overline{K}[X_0, \ldots, X_n]$.

Projective Variety

- A polynomial $f \in \overline{K}[X_0, \ldots, X_n]$ is called homogenous of degree d if
$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n) \qquad \forall \lambda \in \overline{K}^{\times}.$$
An ideal I in $\in \overline{K}[X_0, \ldots, X_n]$ is called a homogenous ideal if it generated by homogenous polynomials.

- Given a homogenous ideal I, we define a projective algebraic set as
$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all homoegenous } f \in I\}.$$

- Given a projective algebraic set V, we associate a homogenous ideal $I(V)$ in $\overline{K}[X_0, \ldots, X_n]$ generated by
$$\{f \in \overline{K}[X_0, \ldots, X_n] \mid f \text{ is homoenegous, } f(P) = 0 \quad \forall P \in V\}.$$

- A projective algebraic set is called a projective variety if $I(V)$ is a prime ideal in $\overline{K}[X_0, \ldots, X_n]$.

The Projective Closure of an Affine Variety

- Given any $f \in \overline{K}[Y_1, \ldots, Y_n]$ of degree d, we can define a homogenous polynomial
$$f^*(X_0, \ldots, X_n) = X_n^d f\left(\frac{X_0}{X_n}, \ldots, \frac{X_0}{X_n}\right) \in \overline{K}[X_0, \ldots, X_n].$$

- Given an affine algebraic set V in $\mathbb{A}^n$, we can think of it as a subset of $\mathbb{P}^n$ via the embedding
$$\phi_n : \mathbb{A}^n \longrightarrow \mathbb{P}^n, \qquad (y_1, \ldots, y_n) \mapsto [y_1 : \ldots : y_n : 1].$$

- The projective closure of V is the projective algebraic set $\overline{V}$ whose homogenous ideal $I(V)$ is generated by $\{f^*(X_0, \ldots, X_n) \mid f \in I(V)\}$.

- If V is an affine variety, the $\overline{V}$ is a projective variety with $\overline{V} \cap \mathbb{A}^n = V$.

- We consider an elliptic curve as the projective closure of the affine curve corresponding to the ideal generated by the polynomial $f(x, y) = y^2 - (x^3 + ax + b) \in K[x, y]$.

The Projective Closure of an Affine Variety

- Given any $f \in \overline{K}[Y_1, \ldots, Y_n]$ of degree d, we can define a homogenous polynomial
$$f^*(X_0, \ldots, X_n) = X_n^d f\left(\frac{X_0}{X_n}, \ldots, \frac{X_0}{X_n}\right) \in \overline{K}[X_0, \ldots, X_n].$$
- Given an affine algebraic set V in $\mathbb{A}^n$, we can think of it as a subset of $\mathbb{P}^n$ via the embedding
$$\phi_n : \mathbb{A}^n \longrightarrow \mathbb{P}^n, \qquad (y_1, \ldots, y_n) \mapsto [y_1 : \ldots : y_n : 1].$$
- The projective closure of V is the projective algebraic set $\overline{V}$ whose homogenous ideal $I(V)$ is generated by $\{f^*(X_0, \ldots, X_n) \mid f \in I(V)\}$.
- If V is an affine variety, the $\overline{V}$ is a projective variety with $\overline{V} \cap \mathbb{A}^n = V$.
- We consider an elliptic curve as the projective closure of the affine curve corresponding to the ideal generated by the polynomial $f(x, y) = y^2 - (x^3 + ax + b) \in K[x, y]$.

The Projective Closure of an Affine Variety

- Given any $f \in \overline{K}[Y_1, \ldots, Y_n]$ of degree d, we can define a homogenous polynomial
$$f^*(X_0, \ldots, X_n) = X_n^d f\left(\frac{X_0}{X_n}, \ldots, \frac{X_0}{X_n}\right) \in \overline{K}[X_0, \ldots, X_n].$$
- Given an affine algebraic set V in $\mathbb{A}^n$, we can think of it as a subset of $\mathbb{P}^n$ via the embedding
$$\phi_n : \mathbb{A}^n \longrightarrow \mathbb{P}^n, \qquad (y_1, \ldots, y_n) \mapsto [y_1 : \ldots : y_n : 1].$$
- The projective closure of V is the projective algebraic set $\overline{V}$ whose homogenous ideal $I(V)$ is generated by $\{f^*(X_0, \ldots, X_n) \mid f \in I(V)\}$.
- If V is an affine variety, the $\overline{V}$ is a projective variety with $\overline{V} \cap \mathbb{A}^n = V$.
- We consider an elliptic curve as the projective closure of the affine curve corresponding to the ideal generated by the polynomial $f(x, y) = y^2 - (x^3 + ax + b) \in K[x, y]$.

- Given any $f \in \overline{K}[Y_1, \dots, Y_n]$ of degree d, we can define a homogenous polynomial
$$f^*(X_0, \dots, X_n) = X_n^d f\left(\frac{X_0}{X_n}, \dots, \frac{X_0}{X_n}\right) \in \overline{K}[X_0, \dots, X_n].$$
- Given an affine algebraic set V in $\mathbb{A}^n$, we can think of it as a subset of $\mathbb{P}^n$ via the embedding
$$\phi_n : \mathbb{A}^n \longrightarrow \mathbb{P}^n, \qquad (y_1, \dots, y_n) \mapsto [y_1 : \dots : y_n : 1].$$
- The projective closure of V is the projective algebraic set $\overline{V}$ whose homogenous ideal $I(V)$ is generated by $\{f^*(X_0, \dots, X_n) \mid f \in I(V)\}$.
- If V is an affine variety, the $\overline{V}$ is a projective variety with $\overline{V} \cap \mathbb{A}^n = V$.
- We consider an elliptic curve as the projective closure of the affine curve corresponding to the ideal generated by the polynomial $f(x, y) = y^2 - (x^3 + ax + b) \in K[x, y]$.

The Projective Closure of an Affine Variety

- Given any $f \in \overline{K}[Y_1, \ldots, Y_n]$ of degree d, we can define a homogenous polynomial
$$f^*(X_0, \ldots, X_n) = X_n^d f\left(\frac{X_0}{X_n}, \ldots, \frac{X_0}{X_n}\right) \in \overline{K}[X_0, \ldots, X_n].$$
- Given an affine algebraic set V in $\mathbb{A}^n$, we can think of it as a subset of $\mathbb{P}^n$ via the embedding
$$\phi_n : \mathbb{A}^n \longrightarrow \mathbb{P}^n, \qquad (y_1, \ldots, y_n) \mapsto [y_1 : \ldots : y_n : 1].$$
- The projective closure of V is the projective algebraic set $\overline{V}$ whose homogenous ideal $I(V)$ is generated by $\{f^*(X_0, \ldots, X_n) \mid f \in I(V)\}$.
- If V is an affine variety, the $\overline{V}$ is a projective variety with $\overline{V} \cap \mathbb{A}^n = V$.
- We consider an elliptic curve as the projective closure of the affine curve corresponding to the ideal generated by the polynomial $f(x, y) = y^2 - (x^3 + ax + b) \in K[x, y]$.

Elliptic Curve as a Projective Variety

- In the projective plane, the equation of an elliptic curve is the homogenized equation $E_H : Y^2Z = X^3 + aXZ^2 + bZ^3$ using the substitution $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ in the affine equation $E : y^2 = x^3 + ax + b$.
- The affine points on E correspond to the points $[X : Y : 1]$ lying on E_H. But the elliptic curve has additional points $[X : Y : Z]$ in the projective plane given by $Z = 0$.
- Substituting $Z = 0$ in the homogenized equation, we obtain $X^3 = 0$, i.e., $X = 0$, and hence $Y \neq 0$. Therefore, an elliptic curve contains only one additional point in the projective plane, which can be taken as $[0 : 1 : 0]$.
- The point $[0 : 1 : 0]$ is known as the point at infinity on the elliptic curve and denoted by $\mathcal{O}$. It is a point of inflection for the curve, as it is a point of multiplicity 3.

Elliptic Curve as a Projective Variety

- In the projective plane, the equation of an elliptic curve is the homogenized equation $E_H : Y^2Z = X^3 + aXZ^2 + bZ^3$ using the substitution $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ in the affine equation $E : y^2 = x^3 + ax + b$.
- The affine points on E correspond to the points $[X : Y : 1]$ lying on E_H. But the elliptic curve has additional points $[X : Y : Z]$ in the projective plane given by $Z = 0$.
- Substituting $Z = 0$ in the homogenized equation, we obtain $X^3 = 0$, i.e., $X = 0$, and hence $Y \neq 0$. Therefore, an elliptic curve contains only one additional point in the projective plane, which can be taken as $[0 : 1 : 0]$.
- The point $[0 : 1 : 0]$ is known as the point at infinity on the elliptic curve and denoted by $\mathcal{O}$. It is a point of inflection for the curve, as it is a point of multiplicity 3.

Elliptic Curve as a Projective Variety

- In the projective plane, the equation of an elliptic curve is the homogenized equation $E_H : Y^2Z = X^3 + aXZ^2 + bZ^3$ using the substitution $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ in the affine equation $E : y^2 = x^3 + ax + b$.
- The affine points on E correspond to the points $[X : Y : 1]$ lying on E_H. But the elliptic curve has additional points $[X : Y : Z]$ in the projective plane given by $Z = 0$.
- Substituting $Z = 0$ in the homogenized equation, we obtain $X^3 = 0$, i.e., $X = 0$, and hence $Y \neq 0$. Therefore, an elliptic curve contains only one additional point in the projective plane, which can be taken as $[0 : 1 : 0]$.
- The point $[0 : 1 : 0]$ is known as the point at infinity on the elliptic curve and denoted by $\mathcal{O}$. It is a point of inflection for the curve, as it is a point of multiplicity 3.

Elliptic Curve as a Projective Variety

- In the projective plane, the equation of an elliptic curve is the homogenized equation $E_H : Y^2Z = X^3 + aXZ^2 + bZ^3$ using the substitution $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ in the affine equation $E : y^2 = x^3 + ax + b$.
- The affine points on E correspond to the points $[X : Y : 1]$ lying on E_H. But the elliptic curve has additional points $[X : Y : Z]$ in the projective plane given by $Z = 0$.
- Substituting $Z = 0$ in the homogenized equation, we obtain $X^3 = 0$, i.e., $X = 0$, and hence $Y \neq 0$. Therefore, an elliptic curve contains only one additional point in the projective plane, which can be taken as $[0 : 1 : 0]$.
- The point $[0 : 1 : 0]$ is known as the point at infinity on the elliptic curve and denoted by $\mathcal{O}$. It is a point of inflection for the curve, as it is a point of multiplicity 3.

Elliptic Curve as a Projective Variety

- In the projective plane, the equation of an elliptic curve is the homogenized equation $E_H : Y^2Z = X^3 + aXZ^2 + bZ^3$ using the substitution $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ in the affine equation $E : y^2 = x^3 + ax + b$.
- The affine points on E correspond to the points $[X : Y : 1]$ lying on E_H. But the elliptic curve has additional points $[X : Y : Z]$ in the projective plane given by $Z = 0$.
- Substituting $Z = 0$ in the homogenized equation, we obtain $X^3 = 0$, i.e., $X = 0$, and hence $Y \neq 0$. Therefore, an elliptic curve contains only one additional point in the projective plane, which can be taken as $[0 : 1 : 0]$.
- The point $[0 : 1 : 0]$ is known as the point at infinity on the elliptic curve and denoted by $\mathcal{O}$. It is a point of inflection for the curve, as it is a point of multiplicity 3.

Elliptic Curve as a Projective Variety

- In the projective plane, the equation of an elliptic curve is the homogenized equation $E_H : Y^2Z = X^3 + aXZ^2 + bZ^3$ using the substitution $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ in the affine equation $E : y^2 = x^3 + ax + b$.

- The affine points on E correspond to the points $[X : Y : 1]$ lying on E_H. But the elliptic curve has additional points $[X : Y : Z]$ in the projective plane given by $Z = 0$.

- Substituting $Z = 0$ in the homogenized equation, we obtain $X^3 = 0$, i.e., $X = 0$, and hence $Y \neq 0$. Therefore, an elliptic curve contains only one additional point in the projective plane, which can be taken as $[0 : 1 : 0]$.

- The point $[0 : 1 : 0]$ is known as the point at infinity on the elliptic curve and denoted by $\mathcal{O}$. It is a point of inflection for the curve, as it is a point of multiplicity 3.

Sections

Sections

Group Structure

- The points on an elliptic curve have the structure of a group.
- Given two points P and Q on E, we can add them in a geometric way to get a third point R on E.
- For this addition of points, we have
  - identity element,
  - inverse for each point,
  - associativity and
  - commutativity.

Group Structure

- The points on an elliptic curve have the structure of a group.
- Given two points P and Q on E, we can add them in a geometric way to get a third point R on E.
- For this addition of points, we have
  - identity element,
  - inverse for each point,
  - associativity and
  - commutativity.

Group Structure

- The points on an elliptic curve have the structure of a group.
- Given two points P and Q on E, we can add them in a geometric way to get a third point R on E.
- For this addition of points, we have
  - identity element,
  - inverse for each point,
  - associativity and
  - commutativity.

Group Structure

- The points on an elliptic curve have the structure of a group.
- Given two points P and Q on E, we can add them in a geometric way to get a third point R on E.
- For this addition of points, we have
  - identity element,
  - inverse for each point,
  - associativity and
  - commutativity.

Group Structure

- The points on an elliptic curve have the structure of a group.
- Given two points P and Q on E, we can add them in a geometric way to get a third point R on E.
- For this addition of points, we have
  - identity element,
  - inverse for each point,
  - associativity and
  - commutativity.

Group Structure

- The points on an elliptic curve have the structure of a group.
- Given two points P and Q on E, we can add them in a geometric way to get a third point R on E.
- For this addition of points, we have
  - identity element,
  - inverse for each point,
  - associativity and
  - commutativity.

The Chord and Tangent Method

- Let us fix a point O on E. It is convenient to take the point at infinity $\mathcal{O}$ as O.
- We join P and Q by a chord, which hits E at a third point $S = P * Q$ (as $(mx+c)^2 = x^3 + ax + b$ has 3 roots).
- Then we draw a chord joining $P * Q$ and O, and this chord hits E at a third point R, which we declare to be the sum of P and Q, denoted $P \oplus Q = R$.
- One can verify that this operation is commutative, associative (the proof is non-trivial), has O as the identity (ie, $P \oplus O = P$ for all P), and each point P has an inverse (ie, given a point P on E, we can find a point T on E with $P \oplus T = O$).

The Chord and Tangent Method

- Let us fix a point O on E. It is convenient to take the point at infinity $\mathcal{O}$ as O.

- We join P and Q by a chord, which hits E at a third point $S = P * Q$ (as $(mx+c)^2 = x^3 + ax + b$ has 3 roots).

- Then we draw a chord joining $P * Q$ and O, and this chord hits E at a third point R, which we declare to be the sum of P and Q, denoted $P \oplus Q = R$.

- One can verify that this operation is commutative, associative (the proof is non-trivial), has O as the identity (ie, $P \oplus O = P$ for all P), and each point P has an inverse (ie, given a point P on E, we can find a point T on E with $P \oplus T = O$).

The Chord and Tangent Method

- Let us fix a point O on E. It is convenient to take the point at infinity $\mathcal{O}$ as O.
- We join P and Q by a chord, which hits E at a third point $S = P * Q$ (as $(mx+c)^2 = x^3 + ax + b$ has 3 roots).
- Then we draw a chord joining $P * Q$ and O, and this chord hits E at a third point R, which we declare to be the sum of P and Q, denoted $P \oplus Q = R$.
- One can verify that this operation is commutative, associative (the proof is non-trivial), has O as the identity (ie, $P \oplus O = P$ for all P), and each point P has an inverse (ie, given a point P on E, we can find a point T on E with $P \oplus T = O$).

The Chord and Tangent Method

- Let us fix a point O on E. It is convenient to take the point at infinity $\mathcal{O}$ as O.
- We join P and Q by a chord, which hits E at a third point $S = P * Q$ (as $(mx+c)^2 = x^3 + ax + b$ has 3 roots).
- Then we draw a chord joining $P * Q$ and O, and this chord hits E at a third point R, which we declare to be the sum of P and Q, denoted $P \oplus Q = R$.
- One can verify that this operation is commutative, associative (the proof is non-trivial), has O as the identity (ie, $P \oplus O = P$ for all P), and each point P has an inverse (ie, given a point P on E, we can find a point T on E with $P \oplus T = O$).

The Chord and Tangent Method

- Let us fix a point O on E. It is convenient to take the point at infinity $\mathcal{O}$ as O.
- We join P and Q by a chord, which hits E at a third point $S = P * Q$ (as $(mx + c)^2 = x^3 + ax + b$ has 3 roots).
- Then we draw a chord joining $P * Q$ and O, and this chord hits E at a third point R, which we declare to be the sum of P and Q, denoted $P \oplus Q = R$.
- One can verify that this operation is commutative, associative (the proof is non-trivial), has O as the identity (ie, $P \oplus O = P$ for all P), and each point P has an inverse (ie, given a point P on E, we can find a point T on E with $P \oplus T = O$).

The Chord and Tangent Method

- Let us fix a point O on E. It is convenient to take the point at infinity $\mathcal{O}$ as O.
- We join P and Q by a chord, which hits E at a third point $S = P * Q$ (as $(mx+c)^2 = x^3 + ax + b$ has 3 roots).
- Then we draw a chord joining $P * Q$ and O, and this chord hits E at a third point R, which we declare to be the sum of P and Q, denoted $P \oplus Q = R$.
- One can verify that this operation is commutative, associative (the proof is non-trivial), has O as the identity (ie, $P \oplus O = P$ for all P), and each point P has an inverse (ie, given a point P on E, we can find a point T on E with $P \oplus T = O$).

The Chord and Tangent Method

- Let us fix a point O on E. It is convenient to take the point at infinity $\mathcal{O}$ as O.
- We join P and Q by a chord, which hits E at a third point $S = P * Q$ (as $(mx+c)^2 = x^3 + ax + b$ has 3 roots).
- Then we draw a chord joining $P * Q$ and O, and this chord hits E at a third point R, which we declare to be the sum of P and Q, denoted $P \oplus Q = R$.
- One can verify that this operation is commutative, associative (the proof is non-trivial), has O as the identity (ie, $P \oplus O = P$ for all P), and each point P has an inverse (ie, given a point P on E, we can find a point T on E with $P \oplus T = O$).

The Chord and Tangent Method

- Let us fix a point O on E. It is convenient to take the point at infinity $\mathcal{O}$ as O.
- We join P and Q by a chord, which hits E at a third point $S = P * Q$ (as $(mx + c)^2 = x^3 + ax + b$ has 3 roots).
- Then we draw a chord joining $P * Q$ and O, and this chord hits E at a third point R, which we declare to be the sum of P and Q, denoted $P \oplus Q = R$.
- One can verify that this operation is commutative, associative (the proof is non-trivial), has O as the identity (ie, $P \oplus O = P$ for all P), and each point P has an inverse (ie, given a point P on E, we can find a point T on E with $P \oplus T = O$).

The Chord and Tangent Method

- Let us fix a point O on E. It is convenient to take the point at infinity $\mathcal{O}$ as O.
- We join P and Q by a chord, which hits E at a third point $S = P * Q$ (as $(mx+c)^2 = x^3 + ax + b$ has 3 roots).
- Then we draw a chord joining $P * Q$ and O, and this chord hits E at a third point R, which we declare to be the sum of P and Q, denoted $P \oplus Q = R$.
- One can verify that this operation is commutative, associative (the proof is non-trivial), has O as the identity (ie, $P \oplus O = P$ for all P), and each point P has an inverse (ie, given a point P on E, we can find a point T on E with $P \oplus T = O$).

The Chord and Tangent Method

- Let us fix a point O on E. It is convenient to take the point at infinity $\mathcal{O}$ as O.
- We join P and Q by a chord, which hits E at a third point $S = P * Q$ (as $(mx+c)^2 = x^3 + ax + b$ has 3 roots).
- Then we draw a chord joining $P * Q$ and O, and this chord hits E at a third point R, which we declare to be the sum of P and Q, denoted $P \oplus Q = R$.
- One can verify that this operation is commutative, associative (the proof is non-trivial), has O as the identity (ie, $P \oplus O = P$ for all P), and each point P has an inverse (ie, given a point P on E, we can find a point T on E with $P \oplus T = O$).

The Chord and Tangent Method

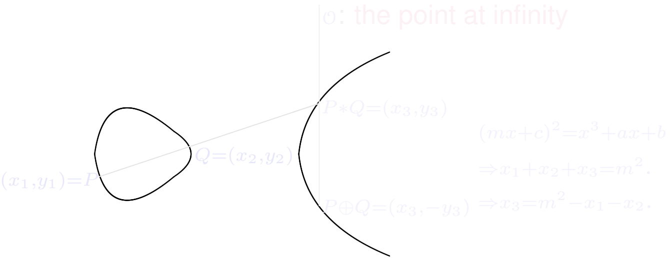
- Let us fix a point O on E. It is convenient to take the point at infinity $\mathcal{O}$ as O.

- We join P and Q by a chord, which hits E at a third point $S = P * Q$ (as $(mx+c)^2 = x^3 + ax + b$ has 3 roots).

- Then we draw a chord joining $P * Q$ and O, and this chord hits E at a third point R, which we declare to be the sum of P and Q, denoted $P \oplus Q = R$.

- One can verify that this operation is commutative, associative (the proof is non-trivial), has O as the identity (ie, $P \oplus O = P$ for all P), and each point P has an inverse (ie, given a point P on E, we can find a point T on E with $P \oplus T = O$).

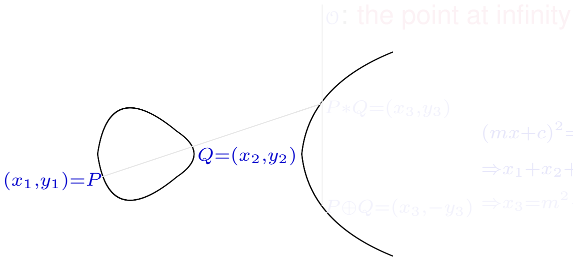
Addition on Elliptic Curve: A Diagram



- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E. The x-coordinate of the sum is given by

$$x(P \oplus Q) = \left(\frac{y(P)-y(Q)}{x(P)-x(Q)}\right)^2 - x(P) - x(Q).$$

Addition on Elliptic Curve: A Diagram



$(mx+c)^2=x^3+ax+b$

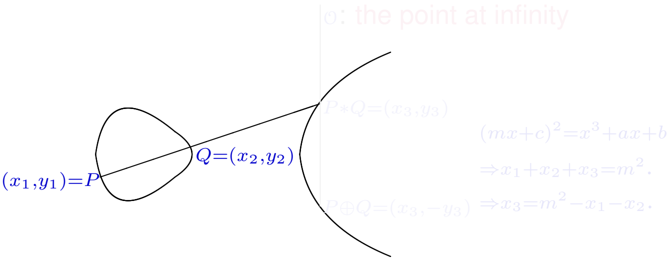
$\Rightarrow x_1+x_2+x_3=m^2.$

$\Rightarrow x_3=m^2-x_1-x_2.$

- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E. The x-coordinate of the sum is given by

$$x(P \oplus Q) = \left(\frac{y(P) - y(Q)}{x(P) - x(Q)}\right)^2 - x(P) - x(Q).$$

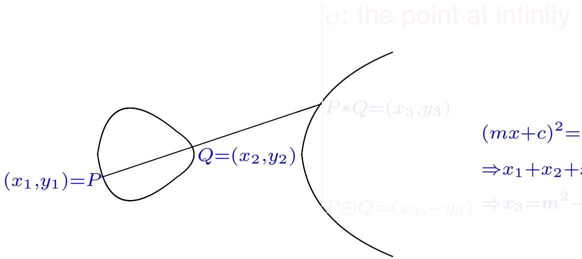
Addition on Elliptic Curve: A Diagram



- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E. The x-coordinate of the sum is given by

$$x(P \oplus Q) = \left(\frac{y(P)-y(Q)}{x(P)-x(Q)}\right)^2 - x(P) - x(Q).$$

Addition on Elliptic Curve: A Diagram



$(mx+c)^2=x^3+ax+b$

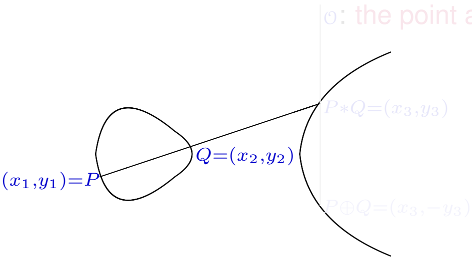
$\Rightarrow x_1+x_2+x_3=m^2.$

$\Rightarrow x_3=m^2-x_1-x_2.$

- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E. The x-coordinate of the sum is given by

$$x(P \oplus Q) = \left(\frac{y(P)-y(Q)}{x(P)-x(Q)}\right)^2 - x(P) - x(Q).$$

Addition on Elliptic Curve: A Diagram

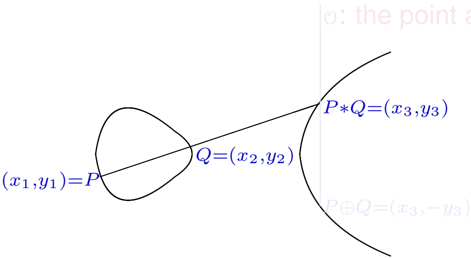


$$(mx+c)^2=x^3+ax+b$$
$$\Rightarrow x_1+x_2+x_3=m^2.$$
$$\Rightarrow x_3=m^2-x_1-x_2.$$

- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E. The x-coordinate of the sum is given by

$$x(P \oplus Q) = \left(\frac{y(P)-y(Q)}{x(P)-x(Q)}\right)^2 - x(P) - x(Q).$$

Addition on Elliptic Curve: A Diagram

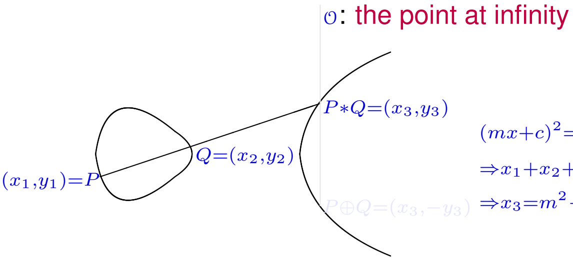


$$(mx + c)^2 = x^3 + ax + b$$
$$\Rightarrow x_1 + x_2 + x_3 = m^2.$$
$$\Rightarrow x_3 = m^2 - x_1 - x_2.$$

- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E. The x-coordinate of the sum is given by

$$x(P \oplus Q) = \left(\frac{y(P) - y(Q)}{x(P) - x(Q)}\right)^2 - x(P) - x(Q).$$

Addition on Elliptic Curve: A Diagram



$(mx+c)^2=x^3+ax+b$

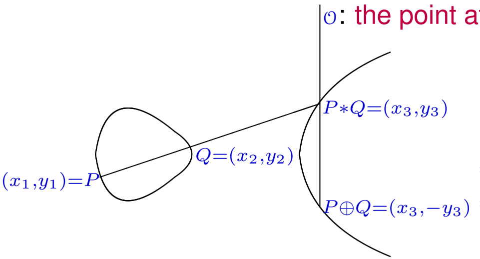
$\Rightarrow x_1+x_2+x_3=m^2.$

$\Rightarrow x_3=m^2-x_1-x_2.$

- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E. The x-coordinate of the sum is given by

$$x(P \oplus Q) = \left(\frac{y(P) - y(Q)}{x(P) - x(Q)}\right)^2 - x(P) - x(Q).$$

Addition on Elliptic Curve: A Diagram

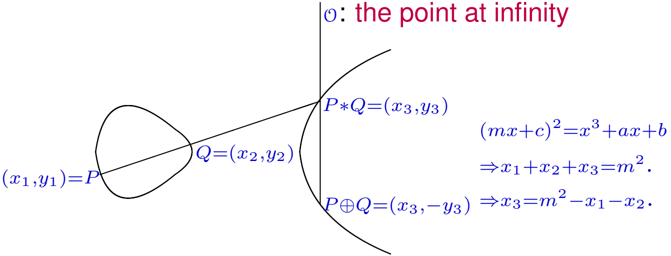


$$(mx+c)^2=x^3+ax+b$$
$$\Rightarrow x_1+x_2+x_3=m^2.$$
$$\Rightarrow x_3=m^2-x_1-x_2.$$

- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E. The x-coordinate of the sum is given by

$$x(P \oplus Q) = \left(\frac{y(P)-y(Q)}{x(P)-x(Q)}\right)^2 - x(P) - x(Q).$$

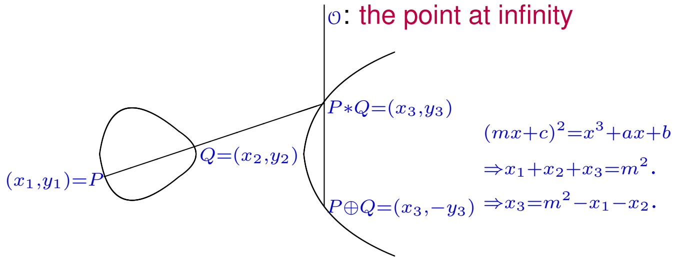
Addition on Elliptic Curve: A Diagram



- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E. The x-coordinate of the sum is given by

$$x(P \oplus Q) = \left(\frac{y(P) - y(Q)}{x(P) - x(Q)}\right)^2 - x(P) - x(Q).$$

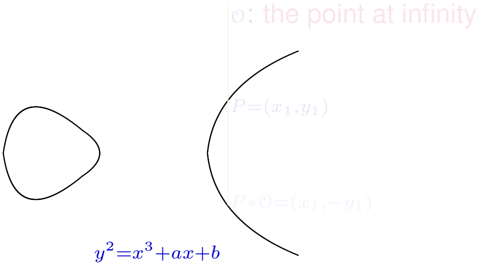
Addition on Elliptic Curve: A Diagram



- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E. The x-coordinate of the sum is given by

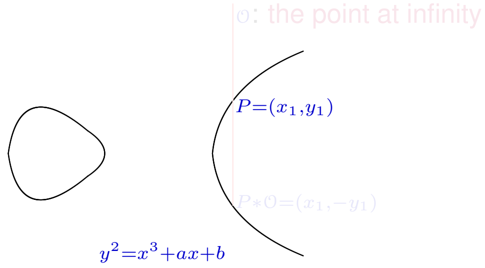
$$x(P \oplus Q) = \left(\frac{y(P) - y(Q)}{x(P) - x(Q)}\right)^2 - x(P) - x(Q).$$

$\mathcal{O}$ is the Identity



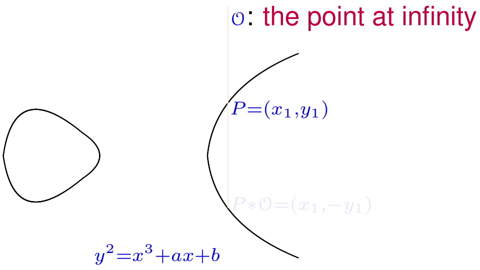
- The point $\mathcal{O}$ serves as the identity for addition on elliptic curve.

$\mathcal{O}$ is the Identity



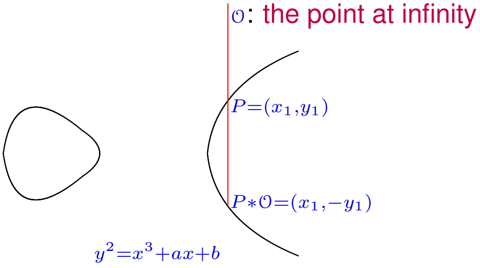
- The point $\mathcal{O}$ serves as the identity for addition on elliptic curve.

$\mathcal{O}$ is the Identity



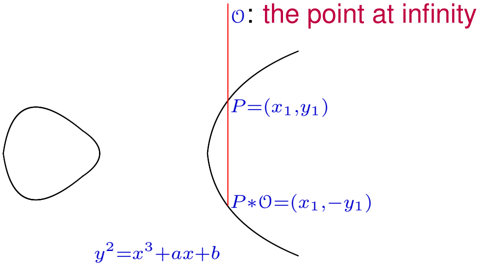
- The point $\mathcal{O}$ serves as the identity for addition on elliptic curve.

$\mathcal{O}$ is the Identity



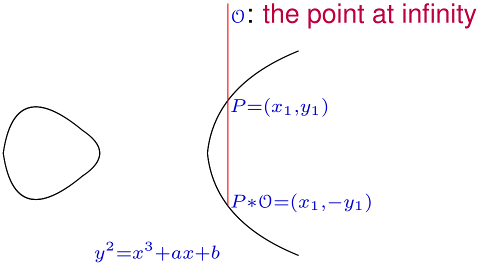
- The point $\mathcal{O}$ serves as the identity for addition on elliptic curve.

$\mathcal{O}$ is the Identity



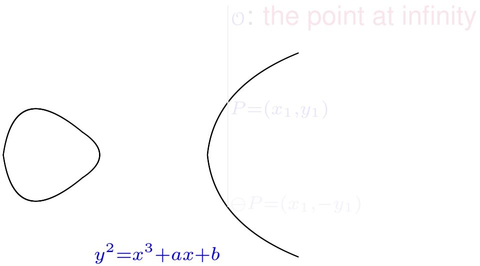
- The point $\mathcal{O}$ serves as the identity for addition on elliptic curve.

$\mathcal{O}$ is the Identity



- The point $\mathcal{O}$ serves as the identity for addition on elliptic curve.

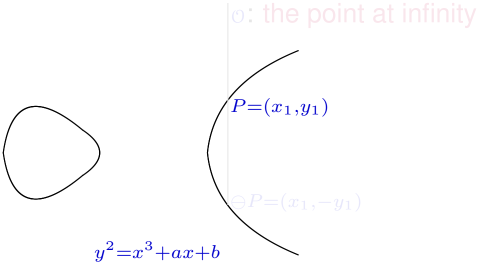
The Inverse of a Point



- The tangent at $\mathcal{O}$ hits the curve again at $\mathcal{O}$. This can be seen by substituting $u = \frac{X}{Y}, \;\; v = \frac{Z}{Y}$ in $Y^2Z = X^3 + aXZ^2 + bZ^3$, which yields $v = u^3 + auv^2 + bv^3$. The tangent $v = 0$ at $\mathcal{O}(u = 0, v = 0)$ gives $u^3 = 0$.

- The additive inverse of the point $P = (x_1, y_1)$ is given by $\ominus P = (x_1, -y_1)$.

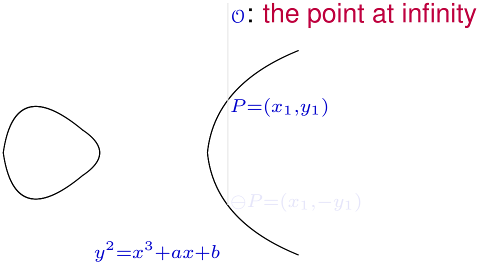
The Inverse of a Point



- The tangent at $\mathcal{O}$ hits the curve again at $\mathcal{O}$. This can be seen by substituting $u = \frac{X}{Y},\ \ v = \frac{Z}{Y}$ in $Y^2Z = X^3 + aXZ^2 + bZ^3$, which yields $v = u^3 + auv^2 + bv^3$. The tangent $v = 0$ at $\mathcal{O}(u = 0, v = 0)$ gives $u^3 = 0$.

- The additive inverse of the point $P = (x_1, y_1)$ is given by $\ominus P = (x_1, -y_1)$.

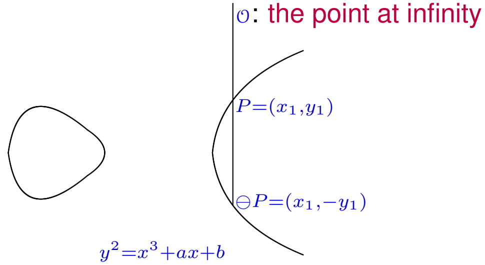
The Inverse of a Point



- The tangent at $\mathcal{O}$ hits the curve again at $\mathcal{O}$. This can be seen by substituting $u = \frac{X}{Y}, \quad v = \frac{Z}{Y}$ in $Y^2Z = X^3 + aXZ^2 + bZ^3$, which yields $v = u^3 + auv^2 + bv^3$. The tangent $v = 0$ at $\mathcal{O}(u = 0, v = 0)$ gives $u^3 = 0$.

- The additive inverse of the point $P = (x_1, y_1)$ is given by $\ominus P = (x_1, -y_1)$.

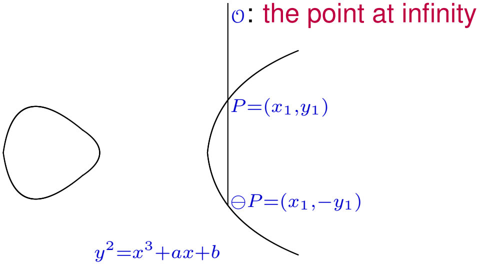
The Inverse of a Point



- The tangent at $\mathcal{O}$ hits the curve again at $\mathcal{O}$. This can be seen by substituting $u = \frac{X}{Y}, \;\; v = \frac{Z}{Y}$ in $Y^2Z = X^3 + aXZ^2 + bZ^3$, which yields $v = u^3 + auv^2 + bv^3$. The tangent $v = 0$ at $\mathcal{O}(u = 0, v = 0)$ gives $u^3 = 0$.

- The additive inverse of the point $P = (x_1, y_1)$ is given by $\ominus P = (x_1, -y_1)$.

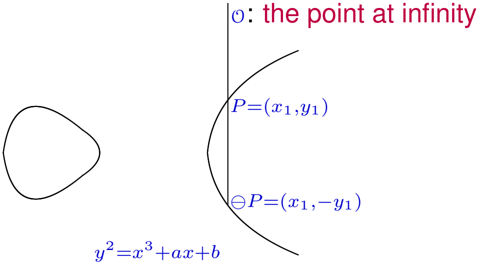
The Inverse of a Point



- The tangent at $\mathcal{O}$ hits the curve again at $\mathcal{O}$. This can be seen by substituting $u = \frac{X}{Y}, \ \ v = \frac{Z}{Y}$ in $Y^2Z = X^3 + aXZ^2 + bZ^3$, which yields $v = u^3 + auv^2 + bv^3$. The tangent $v = 0$ at $\mathcal{O}(u = 0, v = 0)$ gives $u^3 = 0$.

- The additive inverse of the point $P = (x_1, y_1)$ is given by $\ominus P = (x_1, -y_1)$.

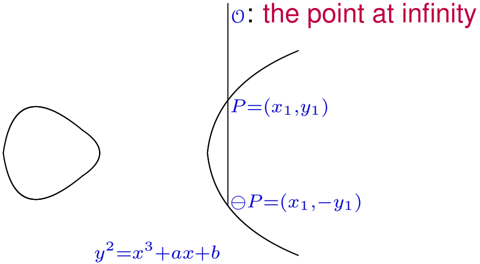
The Inverse of a Point



- The tangent at $\mathcal{O}$ hits the curve again at $\mathcal{O}$. This can be seen by substituting $u = \frac{X}{Y}, \;\; v = \frac{Z}{Y}$ in $Y^2Z = X^3 + aXZ^2 + bZ^3$, which yields $v = u^3 + auv^2 + bv^3$. The tangent $v = 0$ at $\mathcal{O}(u = 0, v = 0)$ gives $u^3 = 0$.

- The additive inverse of the point $P = (x_1, y_1)$ is given by $\ominus P = (x_1, -y_1)$.

The Inverse of a Point



- The tangent at $\mathcal{O}$ hits the curve again at $\mathcal{O}$. This can be seen by substituting $u = \frac{X}{Y}, \;\; v = \frac{Z}{Y}$ in $Y^2Z = X^3 + aXZ^2 + bZ^3$, which yields $v = u^3 + auv^2 + bv^3$. The tangent $v = 0$ at $\mathcal{O}(u = 0, v = 0)$ gives $u^3 = 0$.

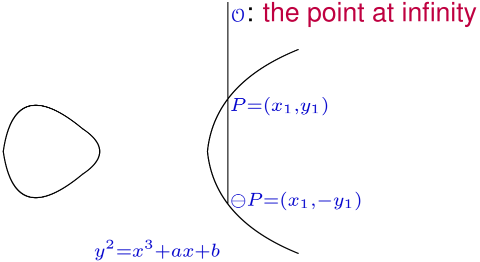
- The additive inverse of the point $P = (x_1, y_1)$ is given by $\ominus P = (x_1, -y_1)$.

The Inverse of a Point

Introduction

The Point at Infinity

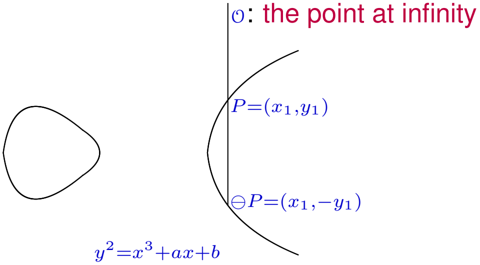
Group Structure



- The tangent at $\mathcal{O}$ hits the curve again at $\mathcal{O}$. This can be seen by substituting $u = \frac{X}{Y}, \quad v = \frac{Z}{Y}$ in $Y^2Z = X^3 + aXZ^2 + bZ^3$, which yields $v = u^3 + auv^2 + bv^3$. The tangent $v = 0$ at $\mathcal{O}(u = 0, v = 0)$ gives $u^3 = 0$.

- The additive inverse of the point $P = (x_1, y_1)$ is given by $\ominus P = (x_1, -y_1)$.

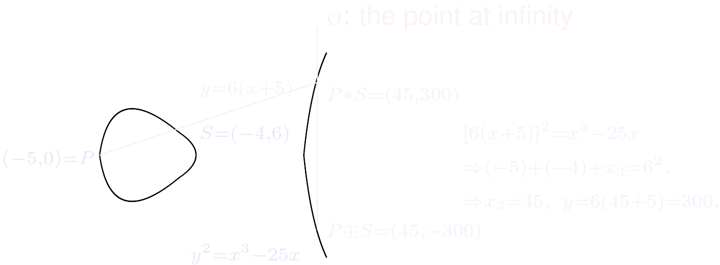
The Inverse of a Point



- The tangent at $\mathcal{O}$ hits the curve again at $\mathcal{O}$. This can be seen by substituting $u = \frac{X}{Y}, \;\; v = \frac{Z}{Y}$ in $Y^2Z = X^3 + aXZ^2 + bZ^3$, which yields $v = u^3 + auv^2 + bv^3$. The tangent $v = 0$ at $\mathcal{O}(u = 0, v = 0)$ gives $u^3 = 0$.

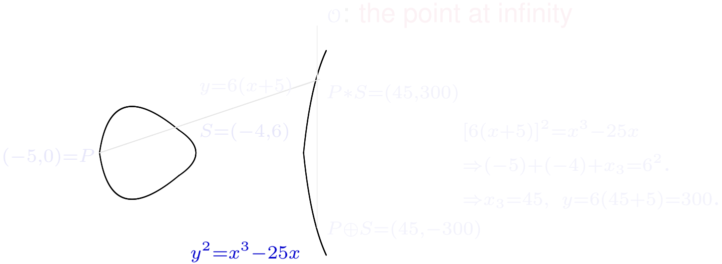
- The additive inverse of the point $P = (x_1, y_1)$ is given by $\ominus P = (x_1, -y_1)$.

Addition on E: an Example



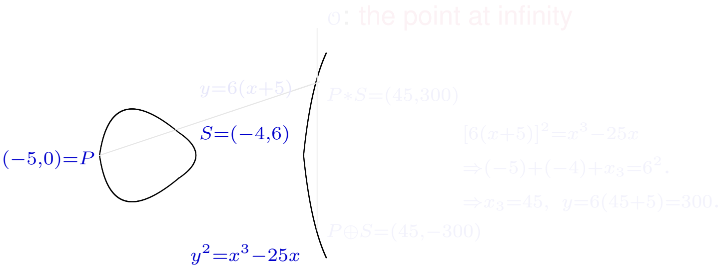
- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36 = (-5) + (-4) + x$, or $x(P * S) = 45$, and $y(P * S) = 6(45 + 5) = 300$.
- Note that the vertical line through $P * S = (45, 300)$ (and $\mathcal{O}$) hits the curve at the point $(45, -300)$.
- By our definition, $P \oplus S = (45, -300)$.

Addition on E: an Example



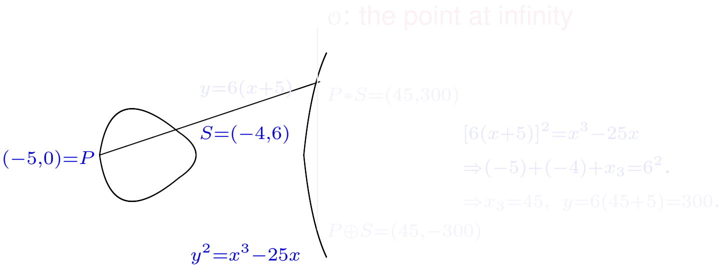
- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36 = (-5) + (-4) + x$, or $x(P * S) = 45$, and $y(P * S) = 6(45 + 5) = 300$.
- Note that the vertical line through $P * S = (45, 300)$ (and $\mathcal{O}$) hits the curve at the point $(45, -300)$.
- By our definition, $P \oplus S = (45, -300)$.

Addition on E: an Example



- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36 = (-5) + (-4) + x$, or $x(P * S) = 45$, and $y(P * S) = 6(45 + 5) = 300$.
- Note that the vertical line through $P * S = (45, 300)$ (and $\mathcal{O}$) hits the curve at the point $(45, -300)$.
- By our definition, $P \oplus S = (45, -300)$.

Addition on E: an Example

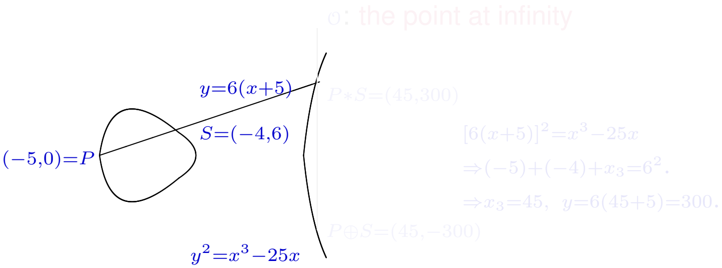


- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36 = (-5) + (-4) + x$, or $x(P * S) = 45$, and $y(P * S) = 6(45 + 5) = 300$.

- Note that the vertical line through $P * S = (45, 300)$ (and $\mathcal{O}$) hits the curve at the point $(45, -300)$.

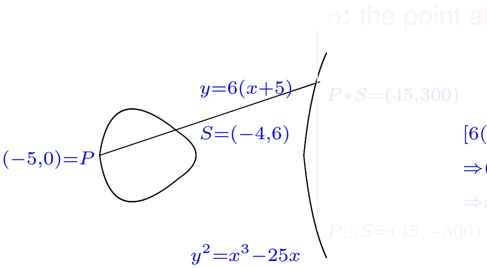
- By our definition, $P \oplus S = (45, -300)$.

Addition on E: an Example



- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36=(-5)+(-4)+x$, or $x(P*S)=45$, and $y(P*S)=6(45+5)=300$.
- Note that the vertical line through $P*S=(45,300)$ (and $\mathcal{O}$) hits the curve at the point $(45,-300)$.
- By our definition, $P\oplus S=(45,-300)$.

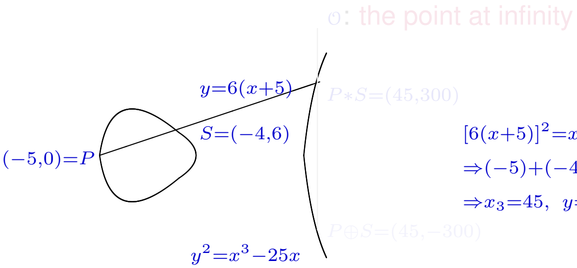
Addition on E: an Example



$[6(x+5)]^2 = x^3 - 25x$
$\Rightarrow (-5) + (-4) + x_3 = 6^2.$
$\Rightarrow x_3 = 45, \;\; y = 6(45+5) = 300.$

- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36 = (-5) + (-4) + x$, or $x(P * S) = 45$, and $y(P * S) = 6(45 + 5) = 300$.
- Note that the vertical line through $P * S = (45, 300)$ (and $\mathcal{O}$) hits the curve at the point $(45, -300)$.
- By our definition, $P \oplus S = (45, -300)$.

Addition on E: an Example



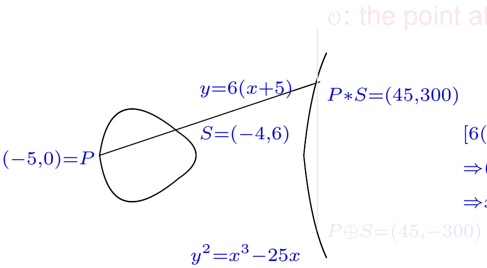
$[6(x+5)]^2=x^3-25x$

$\Rightarrow(-5)+(-4)+x_3=6^2.$

$\Rightarrow x_3=45,\ \ y=6(45+5)=300.$

- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36=(-5)+(-4)+x$, or $x(P*S)=45$, and $y(P*S)=6(45+5)=300$.
- Note that the vertical line through $P*S=(45,300)$ (and $\mathcal{O}$) hits the curve at the point $(45,-300)$.
- By our definition, $P\oplus S=(45,-300)$.

Addition on E: an Example



$$[6(x+5)]^2=x^3-25x$$
$$\Rightarrow(-5)+(-4)+x_3=6^2.$$
$$\Rightarrow x_3=45,\ \ y=6(45+5)=300.$$

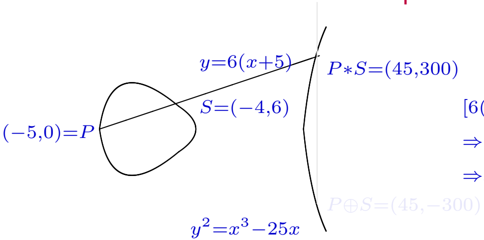
- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36=(-5)+(-4)+x$, or $x(P*S)=45$, and $y(P*S)=6(45+5)=300$.

- Note that the vertical line through $P*S=(45,300)$ (and $\mathcal{O}$) hits the curve at the point $(45,-300)$.

- By our definition, $P\oplus S=(45,-300)$.

Addition on E: an Example

$\mathcal{O}$: the point at infinity



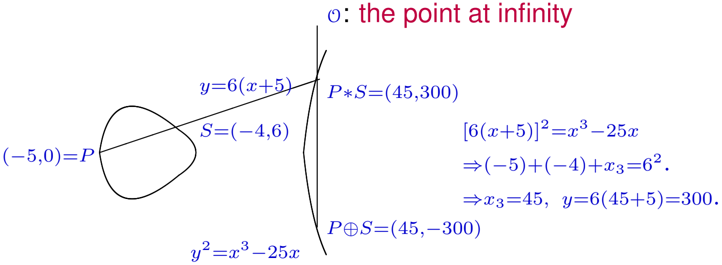
$[6(x+5)]^2=x^3-25x$

$\Rightarrow (-5)+(-4)+x_3=6^2.$

$\Rightarrow x_3=45,\;\; y=6(45+5)=300.$

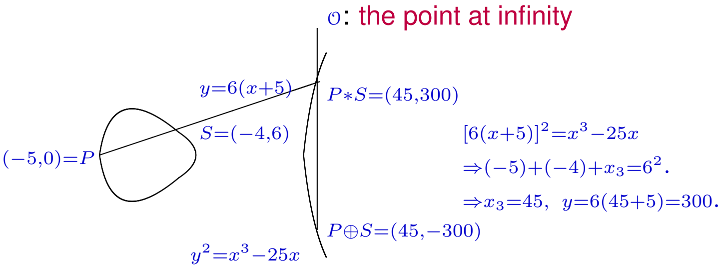
- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36 = (-5) + (-4) + x$, or $x(P * S) = 45$, and $y(P * S) = 6(45 + 5) = 300$.
- Note that the vertical line through $P * S = (45, 300)$ (and $\mathcal{O}$) hits the curve at the point $(45, -300)$.
- By our definition, $P \oplus S = (45, -300)$.

Addition on E: an Example



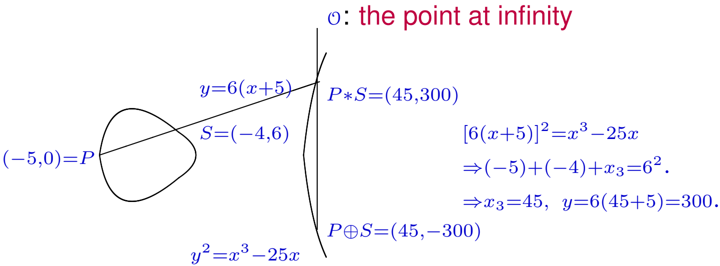
- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36 = (-5) + (-4) + x$, or $x(P * S) = 45$, and $y(P * S) = 6(45 + 5) = 300$.
- Note that the vertical line through $P * S = (45, 300)$ (and $\mathcal{O}$) hits the curve at the point $(45, -300)$.
- By our definition, $P \oplus S = (45, -300)$.

Addition on E: an Example



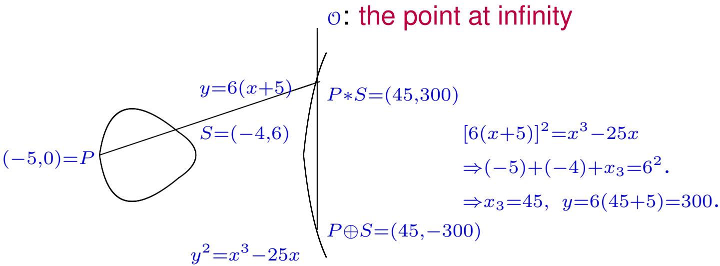
- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36 = (-5) + (-4) + x$, or $x(P * S) = 45$, and $y(P * S) = 6(45 + 5) = 300$.
- Note that the vertical line through $P * S = (45, 300)$ (and $\mathcal{O}$) hits the curve at the point $(45, -300)$.
- By our definition, $P \oplus S = (45, -300)$.

Addition on E: an Example



- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36 = (-5) + (-4) + x$, or $x(P * S) = 45$, and $y(P * S) = 6(45 + 5) = 300$.
- Note that the vertical line through $P * S = (45, 300)$ (and $\mathcal{O}$) hits the curve at the point $(45, -300)$.
- By our definition, $P \oplus S = (45, -300)$.

Addition on E: an Example

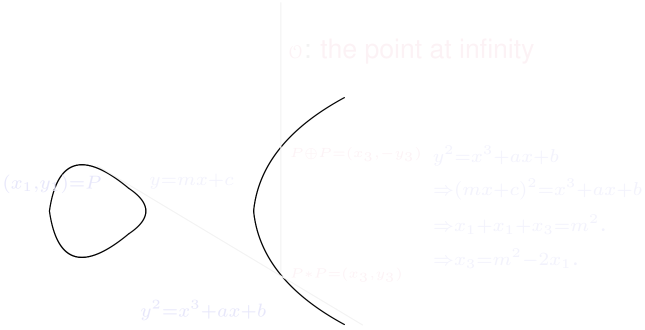


- The coefficient of x^2 will be the negative of the sum of the three roots. Thus $36 = (-5) + (-4) + x$, or $x(P * S) = 45$, and $y(P * S) = 6(45 + 5) = 300$.

- Note that the vertical line through $P * S = (45, 300)$ (and $\mathcal{O}$) hits the curve at the point $(45, -300)$.

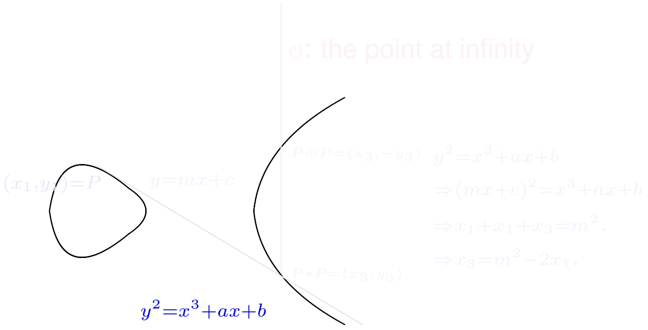
- By our definition, $P \oplus S = (45, -300)$.

Doubling of a Point



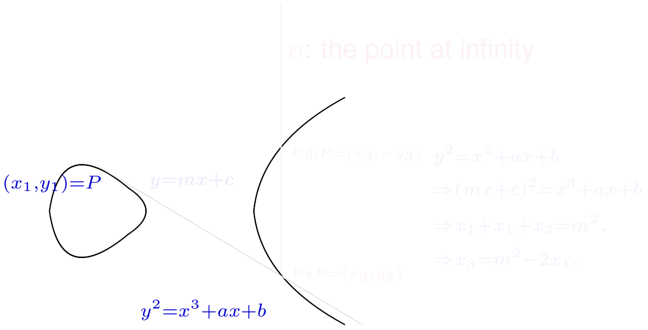
- The double of the point $P = (x, y)$ is given by $2P = P \oplus P = (x_3, -y_3)$.

Doubling of a Point



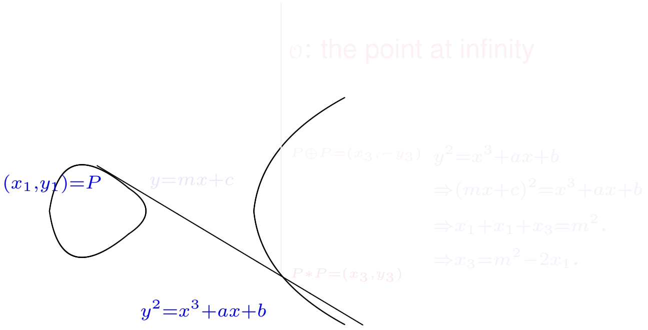
- The double of the point $P=(x,y)$ is given by $2P=P\oplus P=(x_3,-y_3)$.

Doubling of a Point



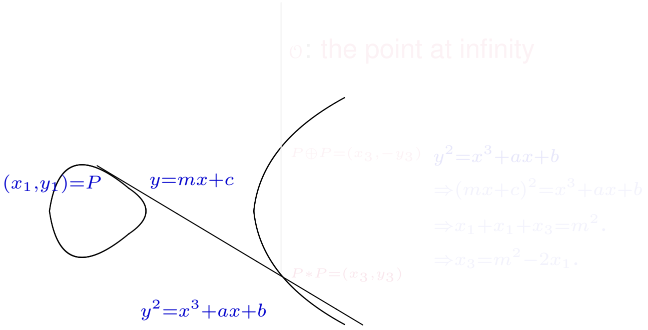
- The double of the point $P = (x, y)$ is given by $2P = P \oplus P = (x_3, -y_3)$.

Doubling of a Point



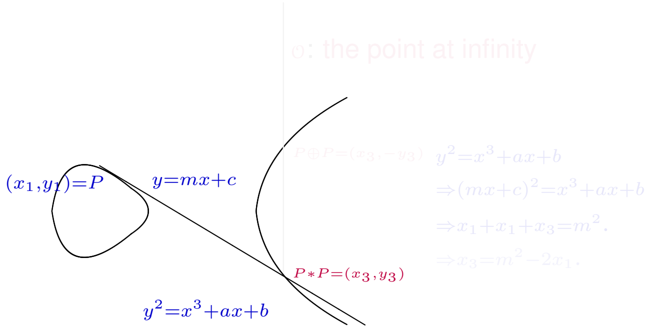
- The double of the point $P = (x, y)$ is given by $2P = P \oplus P = (x_3, -y_3)$.

Doubling of a Point



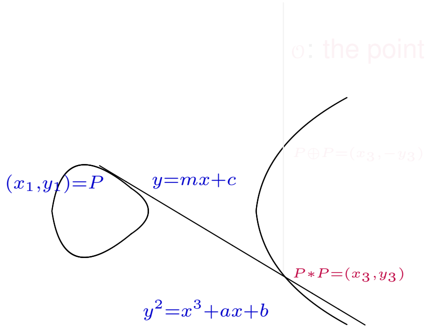
- The double of the point $P=(x,y)$ is given by $2P=P\oplus P=(x_3,-y_3)$.

Doubling of a Point



- The double of the point $P = (x, y)$ is given by $2P = P \oplus P = (x_3, -y_3)$.

Doubling of a Point



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

$\Rightarrow (mx + c)^2 = x^3 + ax + b$

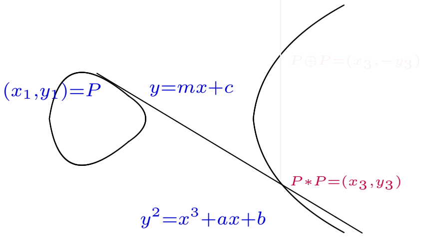
$\Rightarrow x_1 + x_1 + x_3 = m^2.$

$\Rightarrow x_3 = m^2 - 2x_1.$

- The double of the point $P = (x, y)$ is given by $2P = P \oplus P = (x_3, -y_3)$.

Doubling of a Point

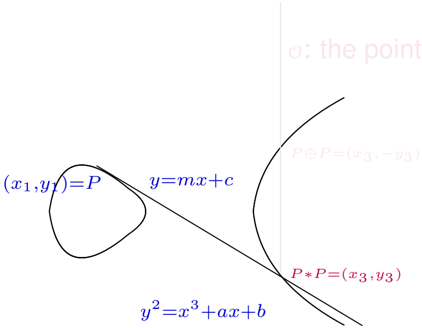
$\mathcal{O}$: the point at infinity



$y^2=x^3+ax+b$
$\Rightarrow(mx+c)^2=x^3+ax+b$
$\Rightarrow x_1+x_1+x_3=m^2.$
$\Rightarrow x_3=m^2-2x_1.$

- The double of the point $P=(x,y)$ is given by $2P=P\oplus P=(x_3,-y_3)$.

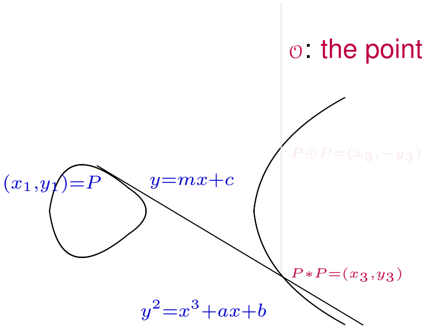
Doubling of a Point



$$y^2 = x^3 + ax + b$$
$$\Rightarrow (mx+c)^2 = x^3 + ax + b$$
$$\Rightarrow x_1 + x_1 + x_3 = m^2.$$
$$\Rightarrow x_3 = m^2 - 2x_1.$$

- The double of the point $P = (x, y)$ is given by $2P = P \oplus P = (x_3, -y_3)$.

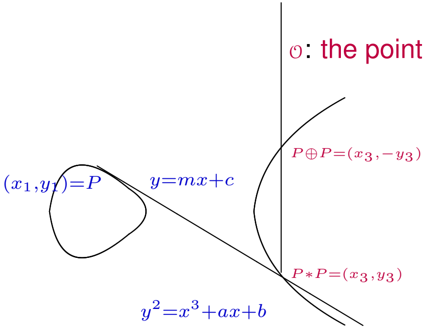
Doubling of a Point



$$y^2 = x^3 + ax + b$$
$$\Rightarrow (mx+c)^2 = x^3 + ax + b$$
$$\Rightarrow x_1 + x_1 + x_3 = m^2.$$
$$\Rightarrow x_3 = m^2 - 2x_1.$$

- The double of the point $P = (x, y)$ is given by $2P = P \oplus P = (x_3, -y_3)$.

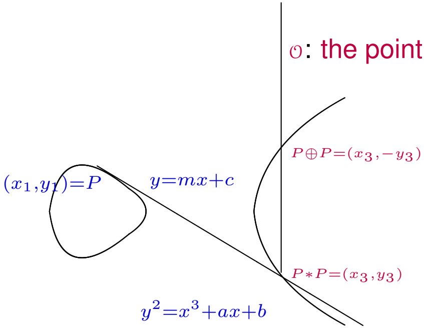
Doubling of a Point



$$y^2 = x^3 + ax + b$$
$$\Rightarrow (mx + c)^2 = x^3 + ax + b$$
$$\Rightarrow x_1 + x_1 + x_3 = m^2.$$
$$\Rightarrow x_3 = m^2 - 2x_1.$$

- The double of the point $P = (x, y)$ is given by $2P = P \oplus P = (x_3, -y_3)$.

Doubling of a Point



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

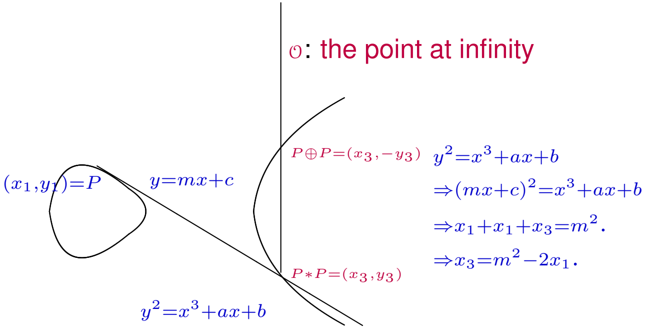
$\Rightarrow (mx+c)^2 = x^3 + ax + b$

$\Rightarrow x_1 + x_1 + x_3 = m^2.$

$\Rightarrow x_3 = m^2 - 2x_1.$

- The double of the point $P = (x, y)$ is given by $2P = P \oplus P = (x_3, -y_3)$.

Doubling of a Point



- The double of the point $P = (x, y)$ is given by $2P = P \oplus P = (x_3, -y_3)$.

Doubling a Point: an example

- Consider the elliptic curve $E: \quad y^2 = x^3 + x + 1$ over the finite field $\mathbb{F}_{23} = \{0,\ 1,\ \ldots, 22\}$. Note that $4.1^3 + 27.1^3 \neq 0$ in $\mathbb{F}_{23}$.
- $P = (3, 10)$ is a point on E as $3^3 + 3 + 1 = 31 = 10^2$ in $\mathbb{F}_{23}$.
- To compute $P * P = (x_3, y_3)$, the slope of the tangent at P is

$$m = \frac{3x^2+1}{2y} = \frac{3.3^2+1}{2.10} = \frac{7}{5} = \frac{7\times 9}{5\times 9} = \frac{63}{-1} = 6 \in \mathbb{F}_{23}.$$

- The tangent at $P = (3, 10)$ is
$$y - 10 = 6(x-3), \text{ i.e., } y = 6x - 8.$$

$$(6x_3 - 8)^2 = x_3^3 + x_3 + 1$$
$$\implies x_3 = 36 - (3+3) = 30 = 7 \in \mathbb{F}_{23},$$
$$y_3 = 6 \times 7 - 8 = 11 \in \mathbb{F}_{23},$$
$$\implies 2P = (7, -11) = (7, 12).$$

Doubling a Point: an example

- Consider the elliptic curve $E: \quad y^2 = x^3 + x + 1$ over the finite field $\mathbb{F}_{23} = \{0,\ 1,\ \dots, 22\}$. Note that $4.1^3 + 27.1^3 \neq 0$ in $\mathbb{F}_{23}$.

- $P = (3, 10)$ is a point on E as $3^3 + 3 + 1 = 31 = 10^2$ in $\mathbb{F}_{23}$.

- To compute $P * P = (x_3, y_3)$, the slope of the tangent at P is

$$m = \frac{3x^2+1}{2y} = \frac{3.3^2+1}{2.10} = \frac{7}{5} = \frac{7 \times 9}{5 \times 9} = \frac{63}{-1} = 6 \in \mathbb{F}_{23}.$$

- The tangent at $P = (3, 10)$ is

$$y - 10 = 6(x - 3), \text{ i.e., } y = 6x - 8.$$

$$(6x_3 - 8)^2 = x_3^3 + x_3 + 1$$

$$\implies x_3 = 36 - (3 + 3) = 30 = 7 \in \mathbb{F}_{23},$$

$$y_3 = 6 \times 7 - 8 = 11 \in \mathbb{F}_{23},$$

$$\implies 2P = (7, -11) = (7, 12).$$

Doubling a Point: an example

- Consider the elliptic curve $E: \quad y^2 = x^3 + x + 1$ over the finite field $\mathbb{F}_{23} = \{0,\ 1,\ \ldots, 22\}$. Note that $4.1^3 + 27.1^3 \neq 0$ in $\mathbb{F}_{23}$.
- $P = (3, 10)$ is a point on E as $3^3 + 3 + 1 = 31 = 10^2$ in $\mathbb{F}_{23}$.
- To compute $P * P = (x_3, y_3)$, the slope of the tangent at P is

$$m = \frac{3x^2 + 1}{2y} = \frac{3.3^2 + 1}{2.10} = \frac{7}{5} = \frac{7 \times 9}{5 \times 9} = \frac{63}{-1} = 6 \in \mathbb{F}_{23}.$$

- The tangent at $P = (3, 10)$ is

$$y - 10 = 6(x - 3), \text{ i.e., } y = 6x - 8.$$

$$(6x_3 - 8)^2 = x_3^3 + x_3 + 1$$

$$\implies x_3 = 36 - (3 + 3) = 30 = 7 \in \mathbb{F}_{23},$$

$$y_3 = 6 \times 7 - 8 = 11 \in \mathbb{F}_{23},$$

$$\implies 2P = (7, -11) = (7, 12).$$

Doubling a Point: an example

- Consider the elliptic curve $E: \; y^2 = x^3 + x + 1$ over the finite field $\mathbb{F}_{23} = \{0, \; 1, \; \ldots, 22\}$. Note that $4.1^3 + 27.1^3 \neq 0$ in $\mathbb{F}_{23}$.

- $P = (3, 10)$ is a point on E as $3^3 + 3 + 1 = 31 = 10^2$ in $\mathbb{F}_{23}$.

- To compute $P * P = (x_3, y_3)$, the slope of the tangent at P is

$$m = \frac{3x^2 + 1}{2y} = \frac{3.3^2 + 1}{2.10} = \frac{7}{5} = \frac{7 \times 9}{5 \times 9} = \frac{63}{-1} = 6 \in \mathbb{F}_{23}.$$

- The tangent at $P = (3, 10)$ is

$$y - 10 = 6(x - 3), \text{ i.e., } y = 6x - 8.$$

$$(6x_3 - 8)^2 = x_3^3 + x_3 + 1$$

$$\implies x_3 = 36 - (3 + 3) = 30 = 7 \in \mathbb{F}_{23},$$

$$y_3 = 6 \times 7 - 8 = 11 \in \mathbb{F}_{23},$$

$$\implies 2P = (7, -11) = (7, 12).$$

Doubling a Point: an example

- Consider the elliptic curve $E: \; y^2 = x^3 + x + 1$ over the finite field $\mathbb{F}_{23} = \{0, \ 1, \ \ldots, 22\}$. Note that $4.1^3 + 27.1^3 \neq 0$ in $\mathbb{F}_{23}$.

- $P = (3, 10)$ is a point on E as $3^3 + 3 + 1 = 31 = 10^2$ in $\mathbb{F}_{23}$.

- To compute $P * P = (x_3, y_3)$, the slope of the tangent at P is

$$m = \frac{3x^2 + 1}{2y} = \frac{3.3^2 + 1}{2.10} = \frac{7}{5} = \frac{7 \times 9}{5 \times 9} = \frac{63}{-1} = 6 \in \mathbb{F}_{23}.$$

- The tangent at $P = (3, 10)$ is

$$y - 10 = 6(x - 3), \text{ i.e., } y = 6x - 8.$$

$$(6x_3 - 8)^2 = x_3^3 + x_3 + 1$$

$$\implies x_3 = 36 - (3 + 3) = 30 = 7 \in \mathbb{F}_{23},$$

$$y_3 = 6 \times 7 - 8 = 11 \in \mathbb{F}_{23},$$

$$\implies 2P = (7, -11) = (7, 12).$$

Doubling a Point: an example

- Consider the elliptic curve $E: \quad y^2 = x^3 + x + 1$ over the finite field $\mathbb{F}_{23} = \{0,\ 1,\ \ldots, 22\}$. Note that $4.1^3 + 27.1^3 \neq 0$ in $\mathbb{F}_{23}$.
- $P = (3, 10)$ is a point on E as $3^3 + 3 + 1 = 31 = 10^2$ in $\mathbb{F}_{23}$.
- To compute $P * P = (x_3, y_3)$, the slope of the tangent at P is

$$m = \frac{3x^2 + 1}{2y} = \frac{3.3^2 + 1}{2.10} = \frac{7}{5} = \frac{7 \times 9}{5 \times 9} = \frac{63}{-1} = 6 \in \mathbb{F}_{23}.$$

- The tangent at $P = (3, 10)$ is
$$y - 10 = 6(x - 3), \text{ i.e., } y = 6x - 8.$$

$$(6x_3 - 8)^2 = x_3^3 + x_3 + 1$$
$$\implies x_3 = 36 - (3 + 3) = 30 = 7 \in \mathbb{F}_{23},$$
$$y_3 = 6 \times 7 - 8 = 11 \in \mathbb{F}_{23},$$
$$\implies 2P = (7, -11) = (7, 12).$$

Doubling a Point: an example

- Consider the elliptic curve $E: \quad y^2 = x^3 + x + 1$ over the finite field $\mathbb{F}_{23} = \{0,\ 1,\ \ldots, 22\}$. Note that $4.1^3 + 27.1^3 \neq 0$ in $\mathbb{F}_{23}$.
- $P = (3, 10)$ is a point on E as $3^3 + 3 + 1 = 31 = 10^2$ in $\mathbb{F}_{23}$.
- To compute $P * P = (x_3, y_3)$, the slope of the tangent at P is

$$m = \frac{3x^2 + 1}{2y} = \frac{3.3^2 + 1}{2.10} = \frac{7}{5} = \frac{7 \times 9}{5 \times 9} = \frac{63}{-1} = 6 \in \mathbb{F}_{23}.$$

- The tangent at $P = (3, 10)$ is
$$y - 10 = 6(x - 3), \text{ i.e., } y = 6x - 8.$$

$$\begin{aligned}(6x_3 - 8)^2 &= x_3^3 + x_3 + 1 \\ \implies x_3 &= 36 - (3 + 3) = 30 = 7 \in \mathbb{F}_{23}, \\ y_3 &= 6 \times 7 - 8 = 11 \in \mathbb{F}_{23}, \\ \implies 2P &= (7, -11) = (7, 12).\end{aligned}$$

Multiplication by Integers

- We can add P to itself and get another point $2P = P \oplus P$, and in general,

$$[n]P = nP = \underbrace{P \oplus P \oplus \ldots \oplus P}_{n\text{-times}}, \qquad n = 1, 2, 3, \ldots.$$

- For a negative integer n, we can define nP as

$$nP = \ominus[(-n)P],$$

  where $\ominus Q$ denoted the inverse of a point Q on the elliptic curve.

- A point P on E is called a torsion point if $[n]P = \mathcal{O}$ for some non-zero integer n.

Multiplication by Integers

- We can add P to itself and get another point $2P = P \oplus P$, and in general,

$$[n]P = nP = \underbrace{P \oplus P \oplus \ldots \oplus P}_{n\text{-times}}, \qquad n = 1, 2, 3, \ldots.$$

- For a negative integer n, we can define nP as

$$nP = \ominus[(-n)P],$$

where $\ominus Q$ denoted the inverse of a point Q on the elliptic curve.

- A point P on E is called a torsion point if $[n]P = \mathcal{O}$ for some non-zero integer n.

Multiplication by Integers

- We can add P to itself and get another point $2P = P \oplus P$, and in general,

$$[n]P = nP = \underbrace{P \oplus P \oplus \ldots \oplus P}_{n\text{-times}}, \qquad n = 1, 2, 3, \ldots.$$

- For a negative integer n, we can define nP as

$$nP = \ominus[(-n)P],$$

where $\ominus Q$ denoted the inverse of a point Q on the elliptic curve.

- A point P on E is called a torsion point if $[n]P = \mathcal{O}$ for some non-zero integer n.

Multiplication by Integers

- We can add P to itself and get another point $2P = P \oplus P$, and in general,

$$[n]P = nP = \underbrace{P \oplus P \oplus \ldots \oplus P}_{n\text{-times}}, \qquad n = 1, 2, 3, \ldots.$$

- For a negative integer n, we can define nP as

$$nP = \ominus[(-n)P],$$

where $\ominus Q$ denoted the inverse of a point Q on the elliptic curve.

- A point P on E is called a torsion point if $[n]P = \mathcal{O}$ for some non-zero integer n.

K-Rational Points on Elliptic Curve

- Let K be a field, and E be an elliptic curve defined over K.
- The points (x, y) on E where $x, y \in K$ are are called K-rational points on E and denoted by $E(K)$.
- If we start with two points on E with K-rational co-ordinates, their sum also has K-rational co-ordinates:

The straight line $y = mx + c$ joining $(x_1, y_1), (x_2, y_2) \in E(K)$ has slope $c, m = \frac{y_2 - y_1}{x_2 - x_1} \in K$. The third point of intersection (x_3, y_3) of this line with $y^2 = x^3 + ax + b$ is obtained as

$$\begin{aligned} (mx + c)^2 &= x^3 + ax + b \\ \implies x_1 + x_2 + x_3 &= m^2 \\ \implies x_3 &= m^2 - x_1 - x_2 \in K, \\ y_3 &= mx_3 + c \in K. \end{aligned}$$

K-Rational Points on Elliptic Curve

- Let K be a field, and E be an elliptic curve defined over K.
- The points (x, y) on E where $x, y \in K$ are are called K-rational points on E and denoted by $E(K)$.
- If we start with two points on E with K-rational co-ordinates, their sum also has K-rational co-ordinates:

  The straight line $y = mx + c$ joining $(x_1, y_1), (x_2, y_2) \in E(K)$ has slope $c, m = \frac{y_2 - y_1}{x_2 - x_1} \in K$. The third point of intersection (x_3, y_3) of this line with $y^2 = x^3 + ax + b$ is obtained as

$$
\begin{aligned}
(mx + c)^2 &= x^3 + ax + b \\
\implies x_1 + x_2 + x_3 &= m^2 \\
\implies x_3 &= m^2 - x_1 - x_2 \in K, \\
y_3 &= mx_3 + c \in K.
\end{aligned}
$$

K-Rational Points on Elliptic Curve

- Let K be a field, and E be an elliptic curve defined over K.
- The points (x, y) on E where $x, y \in K$ are are called K-rational points on E and denoted by $E(K)$.
- If we start with two points on E with K-rational co-ordinates, their sum also has K-rational co-ordinates:

The straight line $y = mx + c$ joining $(x_1, y_1), (x_2, y_2) \in E(K)$ has slope $c, m = \frac{y_2 - y_1}{x_2 - x_1} \in K$. The third point of intersection (x_3, y_3) of this line with $y^2 = x^3 + ax + b$ is obtained as

$$
\begin{aligned}
(mx + c)^2 &= x^3 + ax + b \\
\implies x_1 + x_2 + x_3 &= m^2 \\
\implies x_3 &= m^2 - x_1 - x_2 \in K, \\
y_3 &= mx_3 + c \in K.
\end{aligned}
$$

K-Rational Points on Elliptic Curve

- Let K be a field, and E be an elliptic curve defined over K.
- The points (x, y) on E where $x, y \in K$ are are called K-rational points on E and denoted by $E(K)$.
- If we start with two points on E with K-rational co-ordinates, their sum also has K-rational co-ordinates:

  The straight line $y = mx + c$ joining (x_1, y_1), $(x_2, y_2) \in E(K)$ has slope $c, m = \frac{y_2 - y_1}{x_2 - x_1} \in K$. The third point of intersection (x_3, y_3) of this line with $y^2 = x^3 + ax + b$ is obtained as

$$
\begin{aligned}
&(mx + c)^2 = x^3 + ax + b \\
\implies &x_1 + x_2 + x_3 = m^2 \\
\implies &x_3 = m^2 - x_1 - x_2 \in K, \\
&y_3 = mx_3 + c \in K.
\end{aligned}
$$

K-Rational Points on Elliptic Curve

- Let K be a field, and E be an elliptic curve defined over K.
- The points (x, y) on E where $x, y \in K$ are are called K-rational points on E and denoted by $E(K)$.
- If we start with two points on E with K-rational co-ordinates, their sum also has K-rational co-ordinates:

  The straight line $y = mx + c$ joining (x_1, y_1), $(x_2, y_2) \in E(K)$ has slope $c, m = \frac{y_2 - y_1}{x_2 - x_1} \in K$. The third point of intersection (x_3, y_3) of this line with $y^2 = x^3 + ax + b$ is obtained as

$$
\begin{aligned}
&(mx + c)^2 = x^3 + ax + b \\
\implies &x_1 + x_2 + x_3 = m^2 \\
\implies &x_3 = m^2 - x_1 - x_2 \in K, \\
&y_3 = mx_3 + c \in K.
\end{aligned}
$$

The Mordell-Weil Group

- Let $E(K) = \{(x, y) \mid x,\ y \in K,\ \ y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$. Then

$$P, Q \in E(K) \implies P \oplus Q \in E(K).$$

- The abelian group $E(K)$ is called the Mordell-Weil group of E/K.
- Mordell-Weil Theorem: For any finite extension K of $\mathbb{Q}$, $E(K)$ is a finitely generated abelian group, i.e.,

$$E(K) \cong \mathbb{Z}^{r_E(K)} \oplus E(K)_{tors}.$$

The integer $r_E(K)$ is called the (algebraic) rank of E over K.

The Mordell-Weil Group

- Let $E(K) = \{(x,y) \mid x,\ y \in K,\ \ y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$. Then

$$P, Q \in E(K) \implies P \oplus Q \in E(K).$$

- The abelian group $E(K)$ is called the Mordell-Weil group of E/K.
- Mordell-Weil Theorem: For any finite extension K of $\mathbb{Q}$, $E(K)$ is a finitely generated abelian group, i.e.,

$$E(K) \cong \mathbb{Z}^{r_E(K)} \oplus E(K)_{tors}.$$

The integer $r_E(K)$ is called the (algebraic) rank of E over K.

The Mordell-Weil Group

- Let $E(K) = \{(x, y) \mid x,\ y \in K,\ \ y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$. Then

$$P, Q \in E(K) \implies P \oplus Q \in E(K).$$

- The abelian group $E(K)$ is called the Mordell-Weil group of E/K.
- Mordell-Weil Theorem: For any finite extension K of $\mathbb{Q}$, $E(K)$ is a finitely generated abelian group, i.e.,

$$E(K) \cong \mathbb{Z}^{r_E(K)} \oplus E(K)_{tors}.$$

The integer $r_E(K)$ is called the (algebraic) rank of E over K.

The Mordell-Weil Group

- Let $E(K) = \{(x, y) \mid x,\ y \in K,\ \ y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$. Then

$$P, Q \in E(K) \implies P \oplus Q \in E(K).$$

- The abelian group $E(K)$ is called the Mordell-Weil group of E/K.
- Mordell-Weil Theorem: For any finite extension K of $\mathbb{Q}$, $E(K)$ is a finitely generated abelian group, i.e.,

$$E(K) \cong \mathbb{Z}^{r_E(K)} \oplus E(K)_{tors}.$$

The integer $r_E(K)$ is called the (algebraic) rank of E over K.

The Mordell-Weil Group

- Let $E(K) = \{(x, y) \mid x, y \in K, \ y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$. Then

$$P, Q \in E(K) \implies P \oplus Q \in E(K).$$

- The abelian group $E(K)$ is called the Mordell-Weil group of E/K.
- Mordell-Weil Theorem: For any finite extension K of $\mathbb{Q}$, $E(K)$ is a finitely generated abelian group, i.e.,

$$E(K) \cong \mathbb{Z}^{r_E(K)} \oplus E(K)_{tors}.$$

The integer $r_E(K)$ is called the (algebraic) rank of E over K.

The Mordell-Weil Group

- Let $E(K) = \{(x,y) \mid x,\ y \in K,\ \ y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$. Then

$$P, Q \in E(K) \implies P \oplus Q \in E(K).$$

- The abelian group $E(K)$ is called the Mordell-Weil group of E/K.
- Mordell-Weil Theorem: For any finite extension K of $\mathbb{Q}$, $E(K)$ is a finitely generated abelian group, i.e.,

$$E(K) \cong \mathbb{Z}^{r_E(K)} \oplus E(K)_{tors}.$$

The integer $r_E(K)$ is called the (algebraic) rank of E over K.

The Torsion Subgroup

- **Lutz-Nagell Theorem**: Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a,\ b \in \mathbb{Z}$. If $(x, y) \in E(\mathbb{Q})$ is a non-zero torsion point, then $x, y \in \mathbb{Z}$, and $y = 0$ or $y^2 \mid (4a^3 + 27b^2)$.

- **Mazur's Theorem**: Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{tors}(\mathbb{Q})$ is isomorphic to one of the following 15 groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, &\qquad \text{with } 1 \le N \le 10 \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, &\qquad \text{with } 1 \le N \le 4. \end{aligned}$$

  Further, each of these subgroup occurs as $E_{tors}(\mathbb{Q})$ for infinitely many elliptic curves $E/\mathbb{Q}$. (*Conjectured by Levi 1906*)

- **Merel**: For every integer $d \geq 1$, there is a constant $N(d)$ such that for all number fields $[K : \mathbb{Q}] \leq d$ and all elliptic curves E/K,

$$\#E_{tors}(K) \leq N(d).$$

The Torsion Subgroup

- **Lutz-Nagell Theorem**: Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a,\ b \in \mathbb{Z}$. If $(x, y) \in E(\mathbb{Q})$ is a non-zero torsion point, then $x, y \in \mathbb{Z}$, and $y = 0$ or $y^2 \mid (4a^3 + 27b^2)$.

- **Mazur's Theorem**: Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{tors}(\mathbb{Q})$ is isomorphic to one of the following 15 groups:

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && \text{with } 1 \leq N \leq 10 \text{ or } N = 12, \\ &\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, && \text{with } 1 \leq N \leq 4. \end{aligned}$$

  Further, each of these subgroup occurs as $E_{tors}(\mathbb{Q})$ for infinitely many elliptic curves $E/\mathbb{Q}$. (*Conjectured by Levi 1906*)

- **Merel**: For every integer $d \geq 1$, there is a constant $N(d)$ such that for all number fields $[K : \mathbb{Q}] \leq d$ and all elliptic curves E/K,

$$\#E_{tors}(K) \leq N(d).$$

The Torsion Subgroup

- Lutz-Nagell Theorem: Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a,\ b \in \mathbb{Z}$. If $(x, y) \in E(\mathbb{Q})$ is a non-zero torsion point, then $x, y \in \mathbb{Z}$, and $y = 0$ or $y^2 \mid (4a^3 + 27b^2)$.
- Mazur's Theorem: Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{tors}(\mathbb{Q})$ is isomorphic to one of the following 15 groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, &\qquad \text{with } 1 \leq N \leq 10 \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, &\qquad \text{with } 1 \leq N \leq 4. \end{aligned}$$

  Further, each of these subgroup occurs as $E_{tors}(\mathbb{Q})$ for infinitely many elliptic curves $E/\mathbb{Q}$. (*Conjectured by Levi 1906*)
- Merel: For every integer $d \geq 1$, there is a constant $N(d)$ such that for all number fields $[K : \mathbb{Q}] \leq d$ and all elliptic curves E/K,

$$\#E_{tors}(K) \leq N(d).$$

The Torsion Subgroup

- Lutz-Nagell Theorem: Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a,\ b \in \mathbb{Z}$. If $(x, y) \in E(\mathbb{Q})$ is a non-zero torsion point, then $x, y \in \mathbb{Z}$, and $y = 0$ or $y^2 \mid (4a^3 + 27b^2)$.

- Mazur's Theorem: Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{tors}(\mathbb{Q})$ is isomorphic to one of the following 15 groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, &\qquad \text{with } 1 \leq N \leq 10 \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, &\qquad \text{with } 1 \leq N \leq 4. \end{aligned}$$

  Further, each of these subgroup occurs as $E_{tors}(\mathbb{Q})$ for infinitely many elliptic curves $E/\mathbb{Q}$. (*Conjectured by Levi 1906*)

- Merel: For every integer $d \geq 1$, there is a constant $N(d)$ such that for all number fields $[K : \mathbb{Q}] \leq d$ and all elliptic curves E/K,

$$\#E_{tors}(K) \leq N(d).$$

The Torsion Subgroup

- Lutz-Nagell Theorem: Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a,\ b \in \mathbb{Z}$. If $(x, y) \in E(\mathbb{Q})$ is a non-zero torsion point, then $x, y \in \mathbb{Z}$, and $y = 0$ or $y^2 \mid (4a^3 + 27b^2)$.

- Mazur's Theorem: Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{tors}(\mathbb{Q})$ is isomorphic to one of the following 15 groups:

$$\mathbb{Z}/N\mathbb{Z}, \qquad \text{with } 1 \leq N \leq 10 \text{ or } N = 12,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \qquad \text{with } 1 \leq N \leq 4.$$

  Further, each of these subgroup occurs as $E_{tors}(\mathbb{Q})$ for infinitely many elliptic curves $E/\mathbb{Q}$. (*Conjectured by Levi 1906*)

- Merel: For every integer $d \geq 1$, there is a constant $N(d)$ such that for all number fields $[K : \mathbb{Q}] \leq d$ and all elliptic curves E/K,

$$\#E_{tors}(K) \leq N(d).$$

Points of Infinite Order

- Bhargava and Shankar showed that at least 83% of elliptic curves have rank either 0 or 1.
- We have example of $E(\mathbb{Q})$ with the highest possible rank 28.
- Conjecture: There exist elliptic curves $E/\mathbb{Q}$ of arbitrarily large rank.
- Mordell's Conjecture (for plane curves): Let C be a non-singular curve over $\mathbb{Q}$ of degree strictly greater than 3. Then the set $C(\mathbb{Q})$ of rational point on C is finite. Faltings proved the conjecture in the 1980's.
- There is no effective algorithm to compute the rank of $E(\mathbb{Q})$.
- The first part of the BSD Conjecture connects the rank of $E(\mathbb{Q})$ to an analytic object, called the Hasse-Weil L-function of the elliptic curve.

Points of Infinite Order

- Bhargava and Shankar showed that at least 83% of elliptic curves have rank either 0 or 1.
- We have example of $E(\mathbb{Q})$ with the highest possible rank 28.
- Conjecture: There exist elliptic curves $E/\mathbb{Q}$ of arbitrarily large rank.
- Mordell's Conjecture (for plane curves): Let C be a non-singular curve over $\mathbb{Q}$ of degree strictly greater than 3. Then the set $C(\mathbb{Q})$ of rational point on C is finite. Faltings proved the conjecture in the 1980's.
- There is no effective algorithm to compute the rank of $E(\mathbb{Q})$.
- The first part of the BSD Conjecture connects the rank of $E(\mathbb{Q})$ to an analytic object, called the Hasse-Weil L-function of the elliptic curve.

Points of Infinite Order

- Bhargava and Shankar showed that at least 83% of elliptic curves have rank either 0 or 1.
- We have example of $E(\mathbb{Q})$ with the highest possible rank 28.
- Conjecture: There exist elliptic curves $E/\mathbb{Q}$ of arbitrarily large rank.
- Mordell's Conjecture (for plane curves): Let C be a non-singular curve over $\mathbb{Q}$ of degree strictly greater than 3. Then the set $C(\mathbb{Q})$ of rational point on C is finite. Faltings proved the conjecture in the 1980's.
- There is no effective algorithm to compute the rank of $E(\mathbb{Q})$.
- The first part of the BSD Conjecture connects the rank of $E(\mathbb{Q})$ to an analytic object, called the Hasse-Weil L-function of the elliptic curve.

Points of Infinite Order

- Bhargava and Shankar showed that at least 83% of elliptic curves have rank either 0 or 1.
- We have example of $E(\mathbb{Q})$ with the highest possible rank 28.
- Conjecture: There exist elliptic curves $E/\mathbb{Q}$ of arbitrarily large rank.
- Mordell's Conjecture (for plane curves): Let C be a non-singular curve over $\mathbb{Q}$ of degree strictly greater than 3. Then the set $C(\mathbb{Q})$ of rational point on C is finite. Faltings proved the conjecture in the 1980's.
- There is no effective algorithm to compute the rank of $E(\mathbb{Q})$.
- The first part of the BSD Conjecture connects the rank of $E(\mathbb{Q})$ to an analytic object, called the Hasse-Weil L-function of the elliptic curve.

Points of Infinite Order

- Bhargava and Shankar showed that at least 83% of elliptic curves have rank either 0 or 1.
- We have example of $E(\mathbb{Q})$ with the highest possible rank 28.
- Conjecture: There exist elliptic curves $E/\mathbb{Q}$ of arbitrarily large rank.
- Mordell's Conjecture (for plane curves): Let C be a non-singular curve over $\mathbb{Q}$ of degree strictly greater than 3. Then the set $C(\mathbb{Q})$ of rational point on C is finite. Faltings proved the conjecture in the 1980's.
- There is no effective algorithm to compute the rank of $E(\mathbb{Q})$.
- The first part of the BSD Conjecture connects the rank of $E(\mathbb{Q})$ to an analytic object, called the Hasse-Weil L-function of the elliptic curve.

Points of Infinite Order

- Bhargava and Shankar showed that at least 83% of elliptic curves have rank either 0 or 1.
- We have example of $E(\mathbb{Q})$ with the highest possible rank 28.
- Conjecture: There exist elliptic curves $E/\mathbb{Q}$ of arbitrarily large rank.
- Mordell's Conjecture (for plane curves): Let C be a non-singular curve over $\mathbb{Q}$ of degree strictly greater than 3. Then the set $C(\mathbb{Q})$ of rational point on C is finite. Faltings proved the conjecture in the 1980's.
- There is no effective algorithm to compute the rank of $E(\mathbb{Q})$.
- The first part of the BSD Conjecture connects the rank of $E(\mathbb{Q})$ to an analytic object, called the Hasse-Weil L-function of the elliptic curve.

Points of Infinite Order

- Bhargava and Shankar showed that at least 83% of elliptic curves have rank either 0 or 1.
- We have example of $E(\mathbb{Q})$ with the highest possible rank 28.
- Conjecture: There exist elliptic curves $E/\mathbb{Q}$ of arbitrarily large rank.
- Mordell's Conjecture (for plane curves): Let C be a non-singular curve over $\mathbb{Q}$ of degree strictly greater than 3. Then the set $C(\mathbb{Q})$ of rational point on C is finite. Faltings proved the conjecture in the 1980's.
- There is no effective algorithm to compute the rank of $E(\mathbb{Q})$.
- The first part of the BSD Conjecture connects the rank of $E(\mathbb{Q})$ to an analytic object, called the Hasse-Weil L-function of the elliptic curve.

References

- *Introduction to Elliptic Curves and Modular forms*, N. Koblitz, Springer 1993.
- *Elliptic Curves*, J. S. Milne.
- *Rational Points on Elliptic Curves*, Joseph H. Silverman and John Tate, Undergraduate Text in Mathematics, Springer, 2005.
- *The Arithmetic of Elliptic Curves*, Joseph H. Silverman, Graduate Text in Mathematics, Springer, 1986.

THANK YOU