

Elliptic curves

Bjorn Poonen
MIT



Arnold Ross Lecture
May 31, 2019

Plane curves

Degree 1 (lines)

$$\begin{aligned} 3x + 7y \\ + 6 = 0 \end{aligned}$$



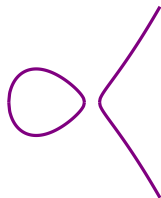
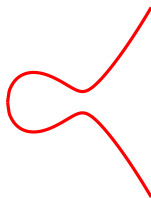
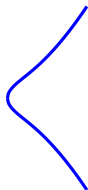
Degree 2 (conics)

$$\begin{aligned} 2x^2 + 9xy + 3y^2 \\ 3x + 7y \\ + 6 = 0 \end{aligned}$$



Degree 3 (cubic curves)

$$\begin{aligned} 4x^3 + 5x^2y + xy^2 + 8y^3 \\ 2x^2 + 9xy + 3y^2 \\ 3x + 7y \\ + 6 = 0 \end{aligned}$$



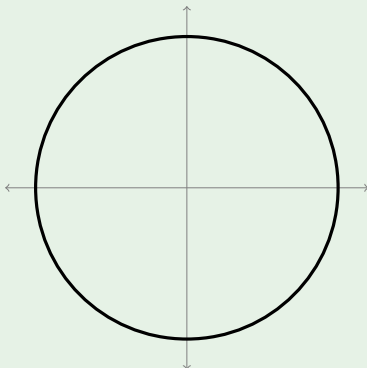
Elliptic curves are special cubic curves.

Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

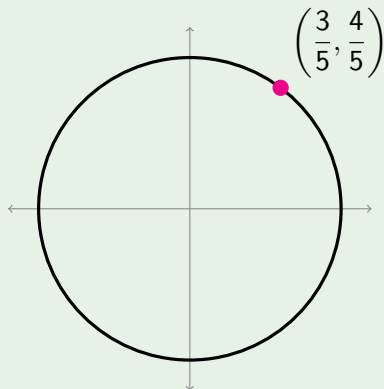


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

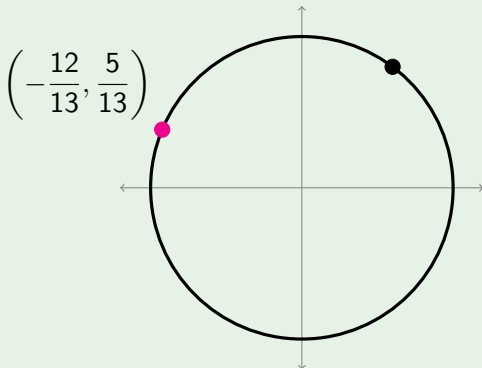


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

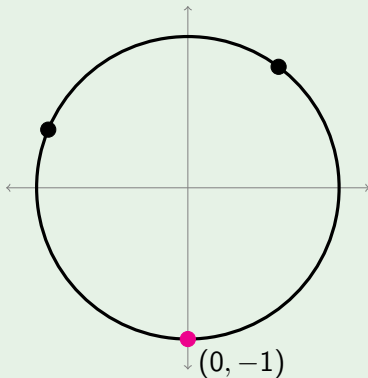


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

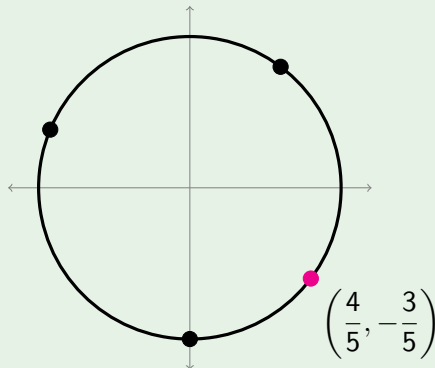


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

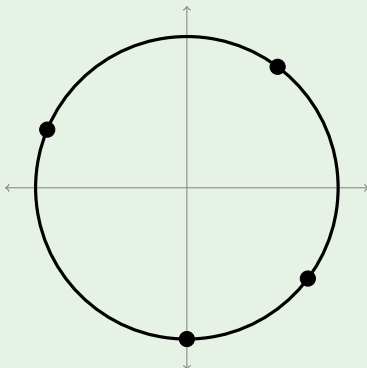


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

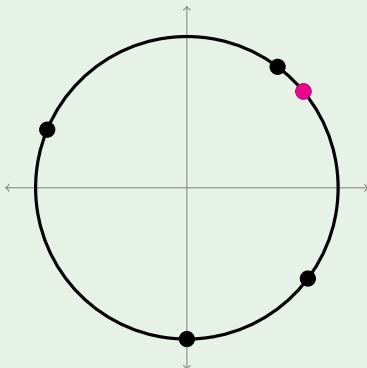


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

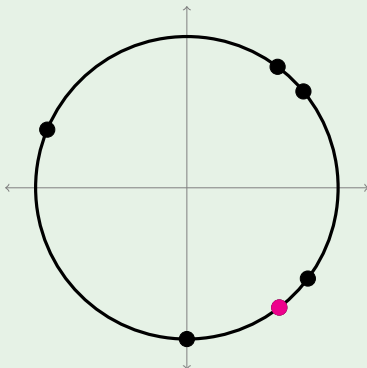


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

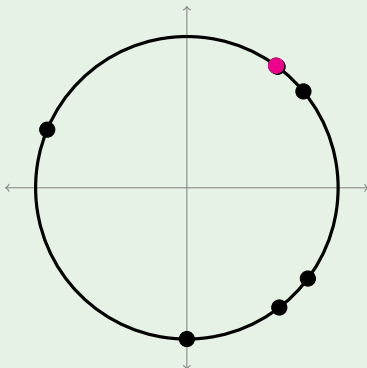


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

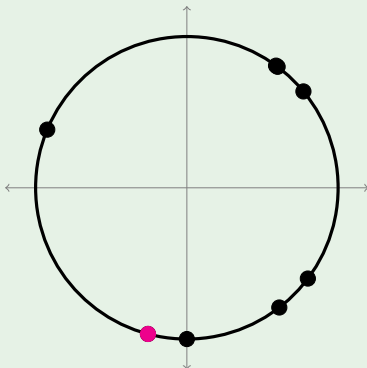


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

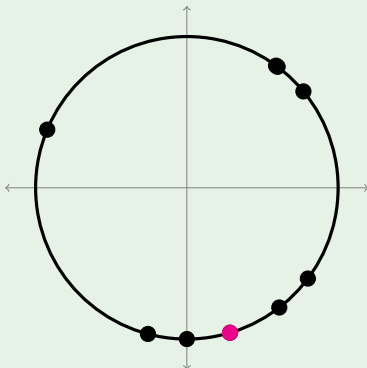


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

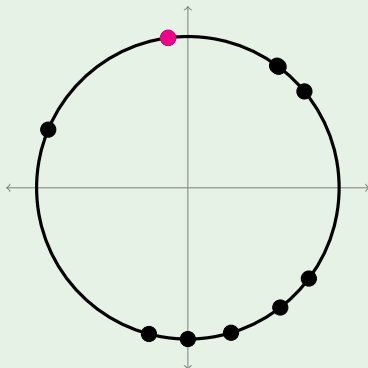


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

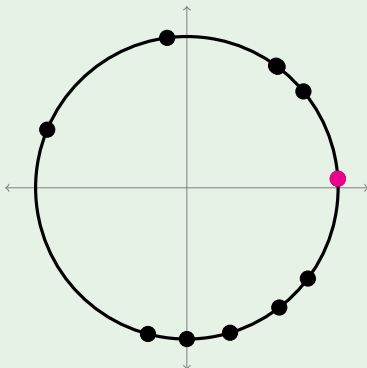


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

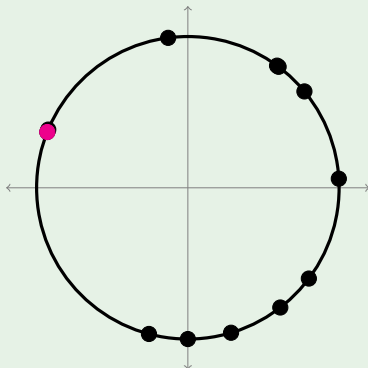


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

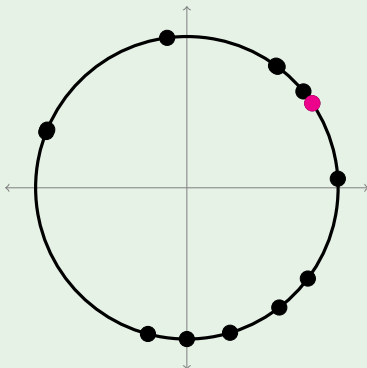


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

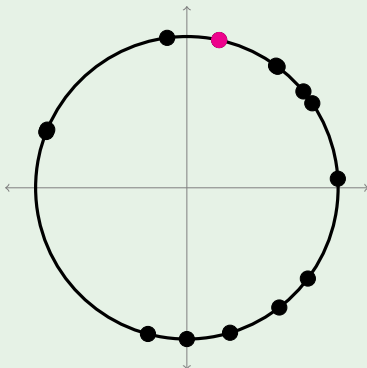


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

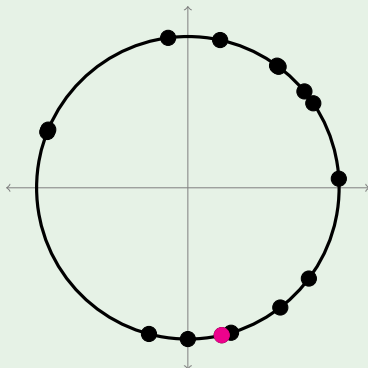


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

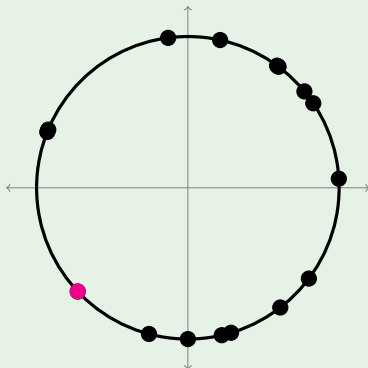


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

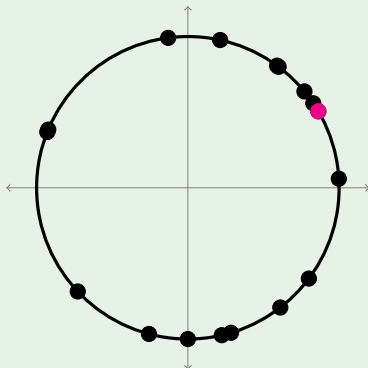


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

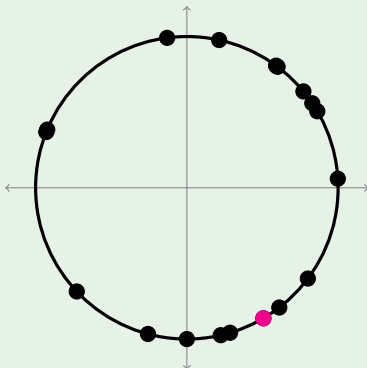


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

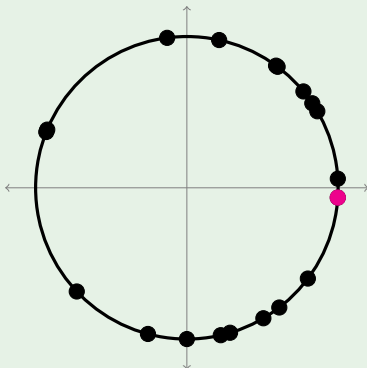


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

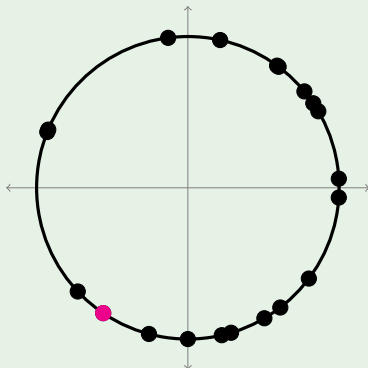


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

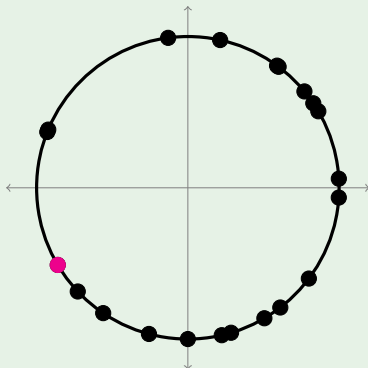


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

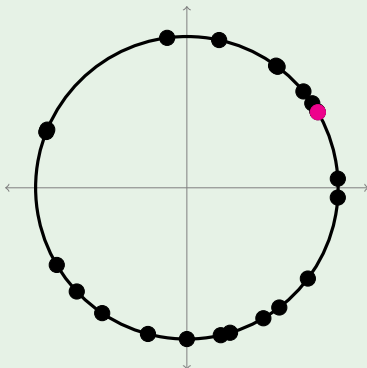


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

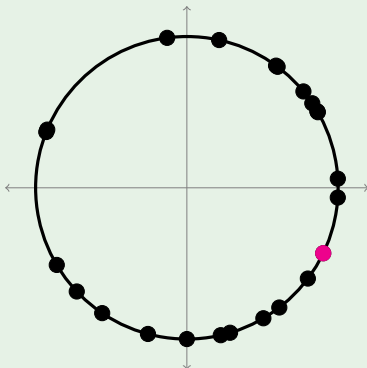


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

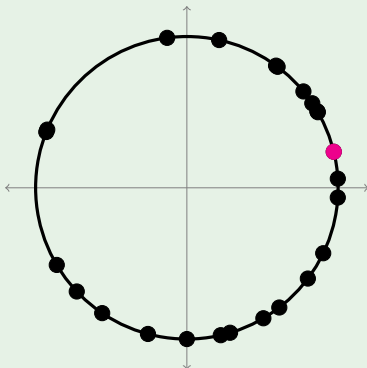


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

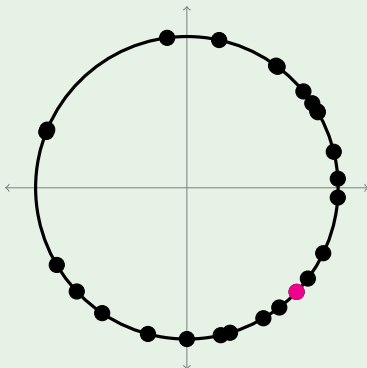


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

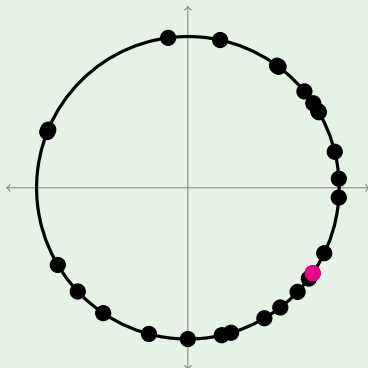


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

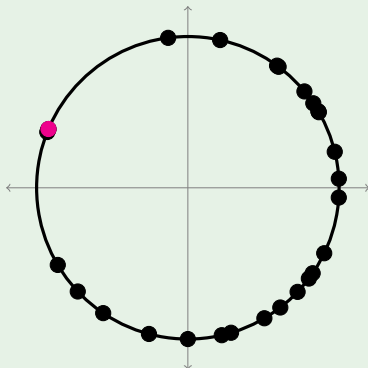


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

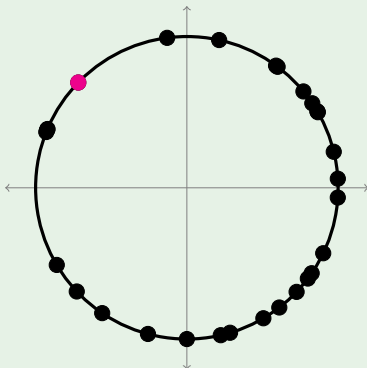


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

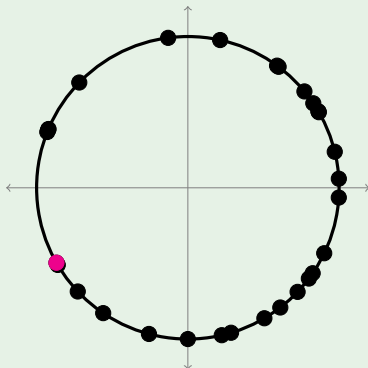


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

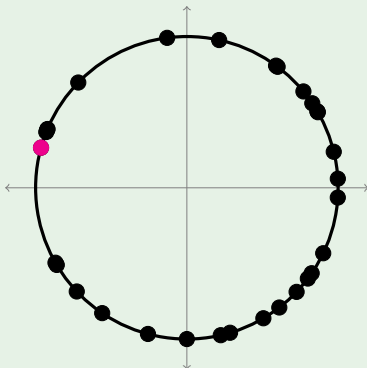


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

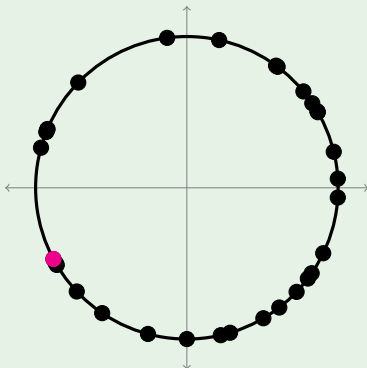


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

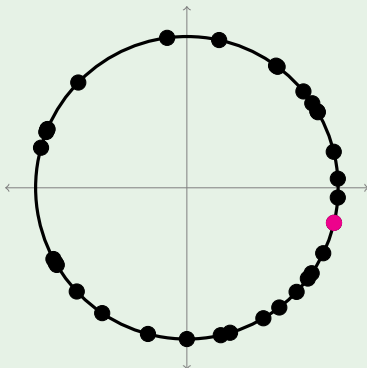


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

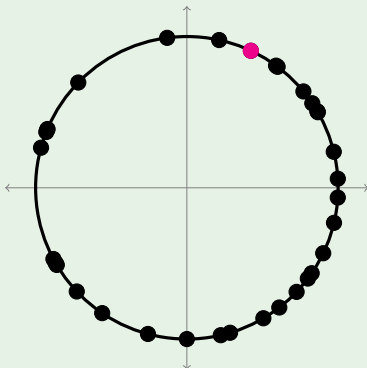


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

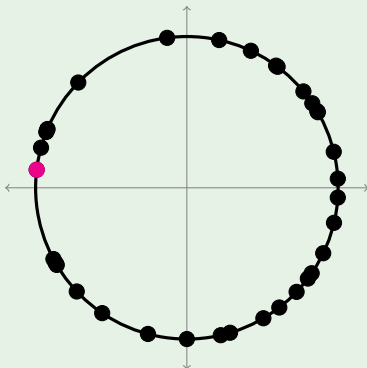


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

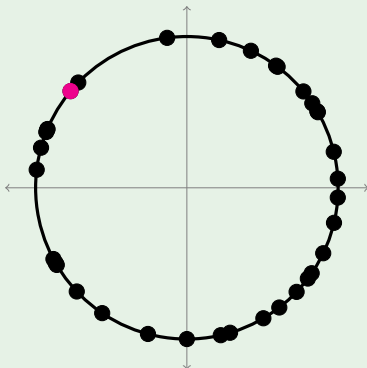


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

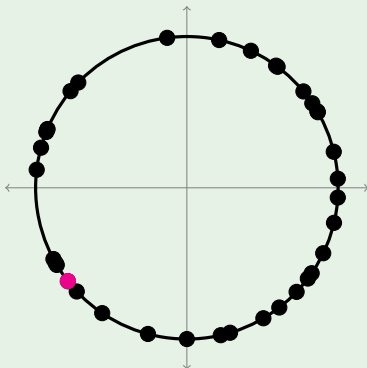


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

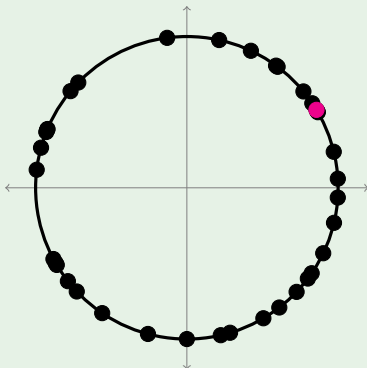


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

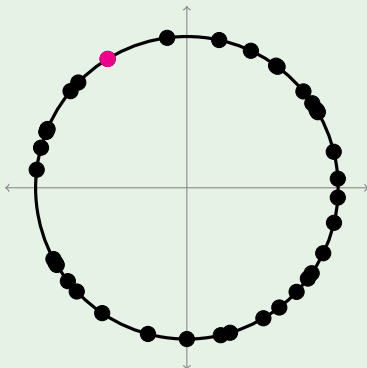


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

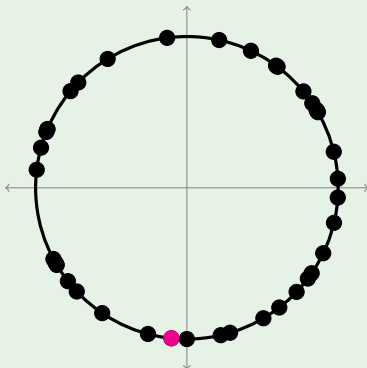


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

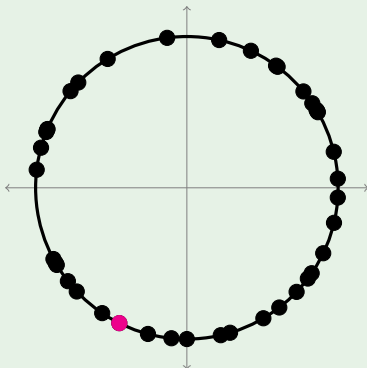


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

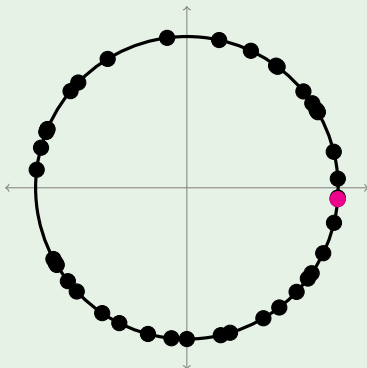


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

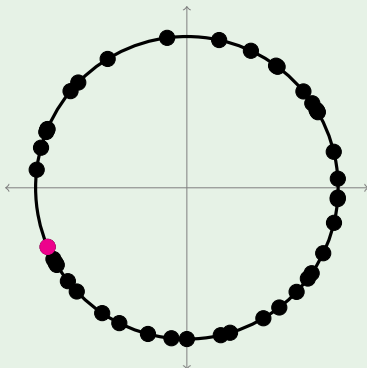


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

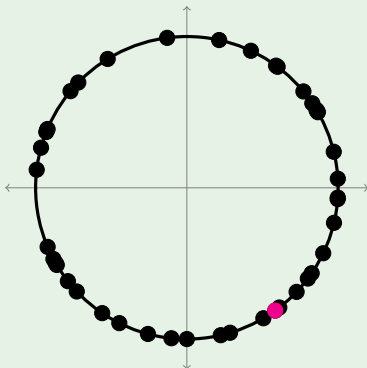


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

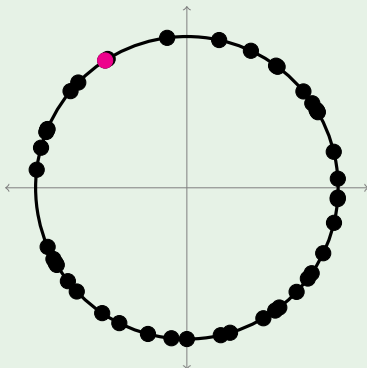


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

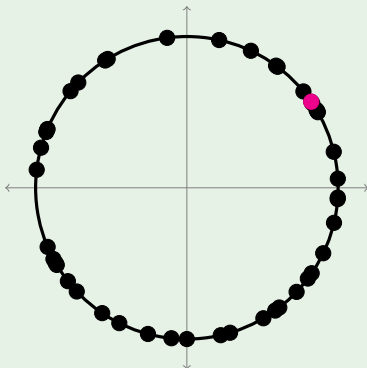


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

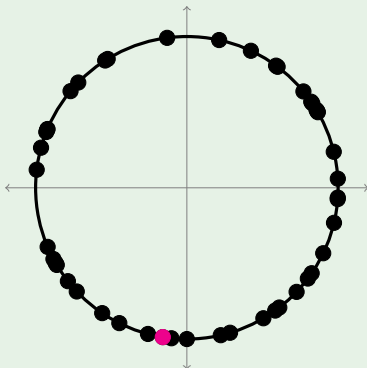


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

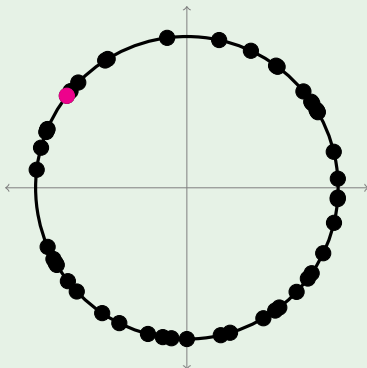


Rational points on the unit circle

Definition

A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)

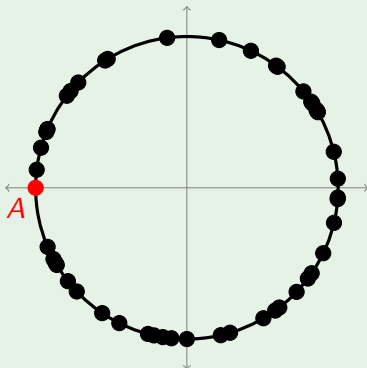


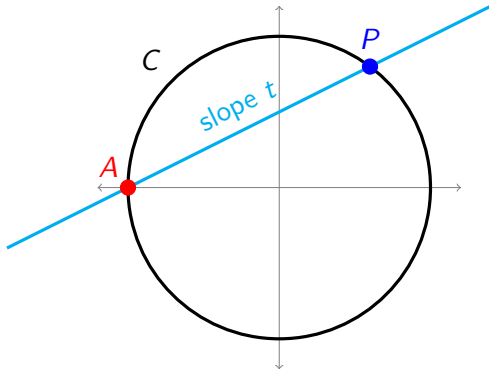
Rational points on the unit circle

Definition

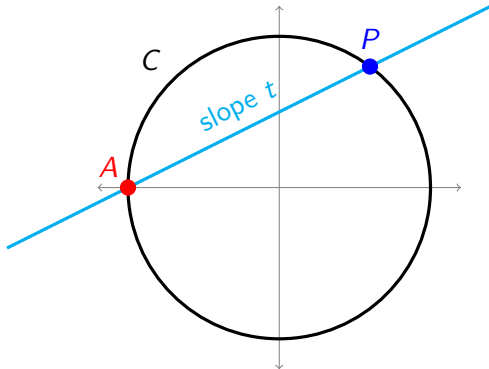
A **rational point** on a curve is a point whose coordinates are rational numbers (elements of $\mathbb{Q}$).

Example (The unit circle $x^2 + y^2 = 1$)



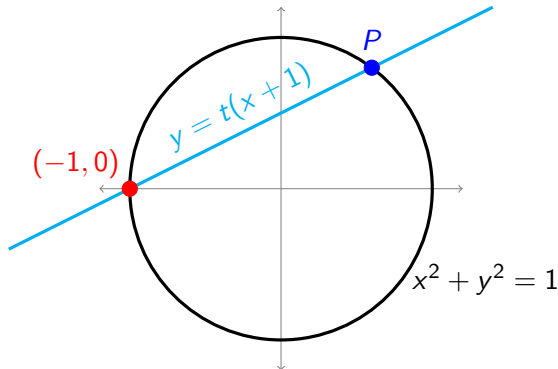


- Given $P \neq A$ on C , form $\overleftrightarrow{AP}$ and take its slope t .
If P is a rational point, then $t \in \mathbb{Q}$.
- Conversely, given t , draw the line L_t through A with slope t ;
then L_t intersects C in a second point P .
If $t \in \mathbb{Q}$, then must P be a rational point?



- Given $P \neq A$ on C , form $\overleftrightarrow{AP}$ and take its slope t .
If P is a rational point, then $t \in \mathbb{Q}$.
- Conversely, given t , draw the line L_t through A with slope t ;
then L_t intersects C in a second point P .
If $t \in \mathbb{Q}$, then must P be a rational point?

Yes!



To find the intersection, substitute $y = t(x + 1)$ into $x^2 + y^2 = 1$:

$$x^2 + t^2(x + 1)^2 = 1$$

$$(x + 1) ((1 + t^2)x - (1 - t^2)) = 0$$

$$x = -1 \text{ or } x = \frac{1 - t^2}{1 + t^2}.$$

Then use $y = t(x + 1)$ to get the corresponding y -coordinates:

$$(-1, 0) \quad \text{or} \quad \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right).$$

Theorem

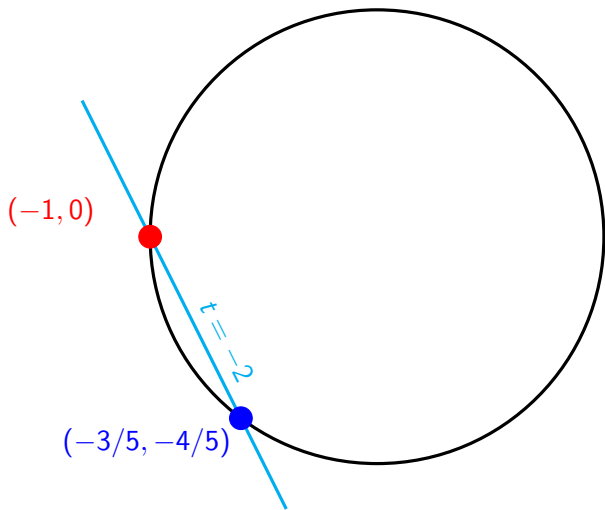
$$\left\{ \begin{array}{l} \text{rational points on } x^2 + y^2 = 1 \\ \text{other than } (-1, 0) \end{array} \right\} = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{Q} \right\}.$$

$(-1, 0)$



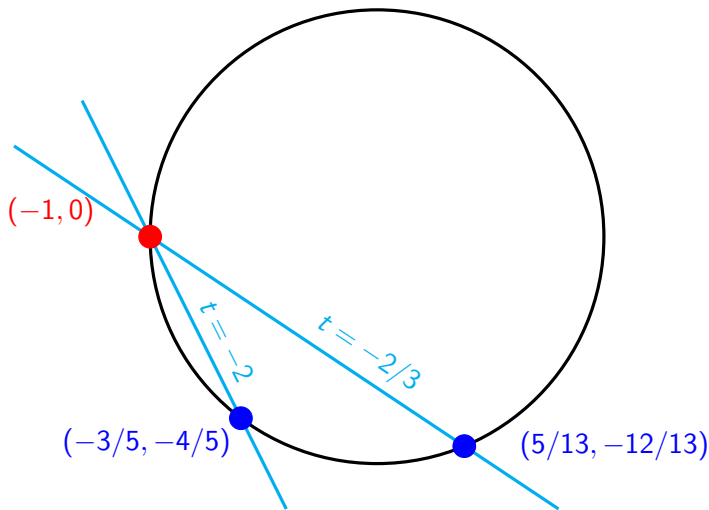
Theorem

$$\left\{ \begin{array}{l} \text{rational points on } x^2 + y^2 = 1 \\ \text{other than } (-1, 0) \end{array} \right\} = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{Q} \right\}.$$



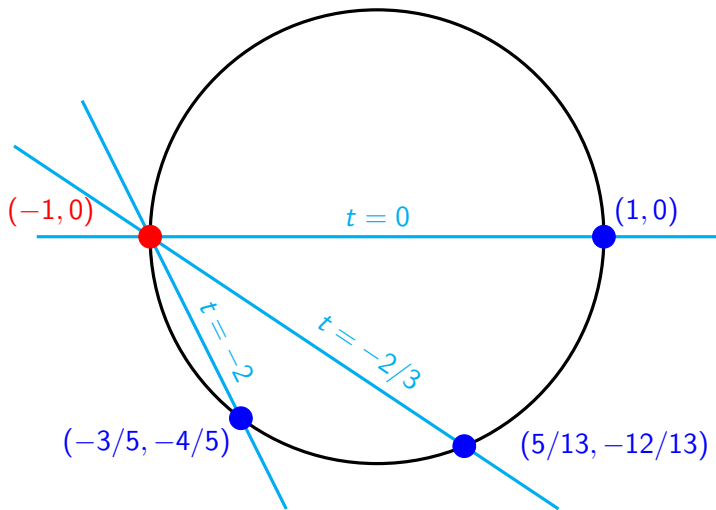
Theorem

$$\left\{ \begin{array}{l} \text{rational points on } x^2 + y^2 = 1 \\ \text{other than } (-1, 0) \end{array} \right\} = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{Q} \right\}.$$



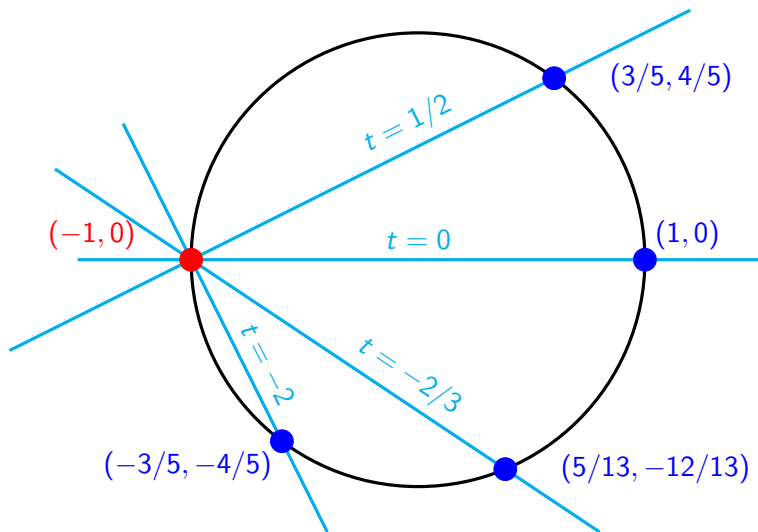
Theorem

$$\left\{ \begin{array}{l} \text{rational points on } x^2 + y^2 = 1 \\ \text{other than } (-1, 0) \end{array} \right\} = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{Q} \right\}.$$



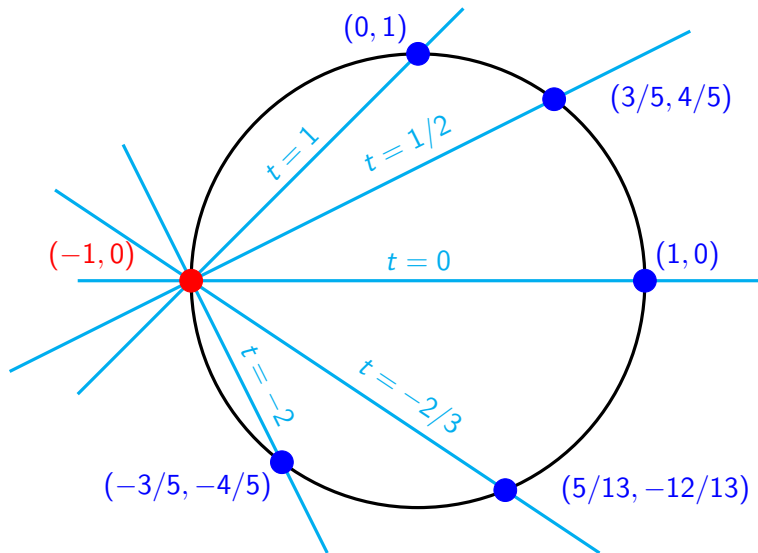
Theorem

$$\left\{ \begin{array}{l} \text{rational points on } x^2 + y^2 = 1 \\ \text{other than } (-1, 0) \end{array} \right\} = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{Q} \right\}.$$



Theorem

$$\left\{ \begin{array}{l} \text{rational points on } x^2 + y^2 = 1 \\ \text{other than } (-1, 0) \end{array} \right\} = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{Q} \right\}.$$



Rational points on other conics (and other shapes)

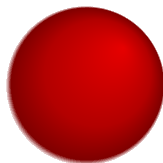
- The same method parametrizes the rational points on any conic, *provided that one rational point is known*.
 - There is also a test, based on checking congruences, for deciding whether a conic has a rational point.
-

Challenge: Parametrize the rational points on

1. the ellipse $x^2 + 5y^2 = 1$



2. the sphere $x^2 + y^2 + z^2 = 1$



Challenge: Use congruences to show that the circle $x^2 + y^2 = 3$ has no rational points.

The projective line $\mathbb{P}^1$

Definition

The **projective line** $\mathbb{P}^1$ is the set of all lines in $\mathbb{R}^2$ through $(0,0)$.

Why is this set being called a **line**?

The projective line $\mathbb{P}^1$

Definition

The **projective line** $\mathbb{P}^1$ is the set of all lines in $\mathbb{R}^2$ through $(0, 0)$.

Why is this set being called a **line**?



The projective line $\mathbb{P}^1$

Definition

The **projective line** $\mathbb{P}^1$ is the set of all lines in $\mathbb{R}^2$ through $(0,0)$.

Why is this set being called a **line**?

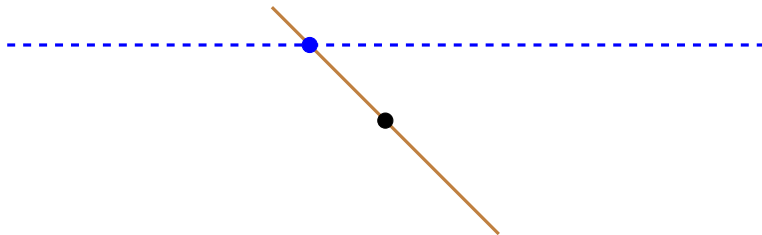
•
(0,0)

The projective line $\mathbb{P}^1$

Definition

The **projective line** $\mathbb{P}^1$ is the set of all lines in $\mathbb{R}^2$ through $(0,0)$.

Why is this set being called a **line**?



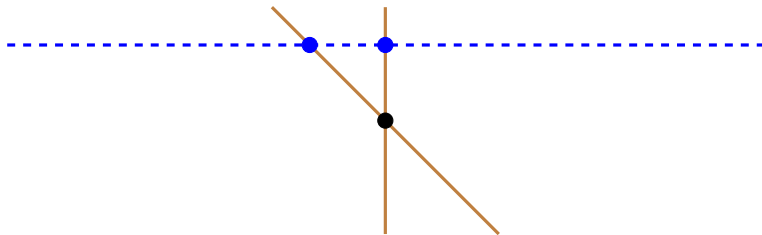
each non-horizontal line $\longleftrightarrow$ **some point on the blue line**

The projective line $\mathbb{P}^1$

Definition

The **projective line** $\mathbb{P}^1$ is the set of all lines in $\mathbb{R}^2$ through $(0,0)$.

Why is this set being called a **line**?



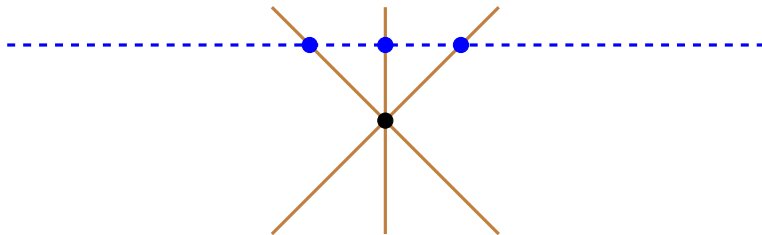
each non-horizontal line $\longleftrightarrow$ **some point on the blue line**

The projective line $\mathbb{P}^1$

Definition

The **projective line** $\mathbb{P}^1$ is the set of all lines in $\mathbb{R}^2$ through $(0,0)$.

Why is this set being called a **line**?



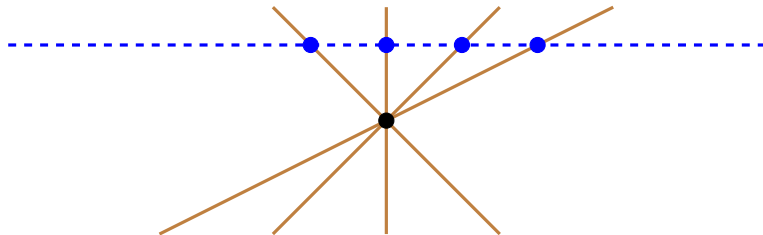
each non-horizontal line $\longleftrightarrow$ **some point on the blue line**

The projective line $\mathbb{P}^1$

Definition

The **projective line** $\mathbb{P}^1$ is the set of all lines in $\mathbb{R}^2$ through $(0,0)$.

Why is this set being called a **line**?



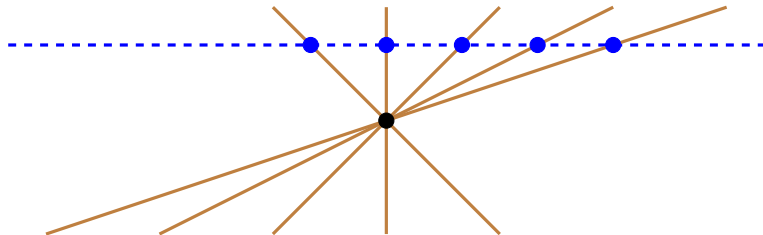
each non-horizontal line $\longleftrightarrow$ **some point on the blue line**

The projective line $\mathbb{P}^1$

Definition

The **projective line** $\mathbb{P}^1$ is the set of all lines in $\mathbb{R}^2$ through $(0,0)$.

Why is this set being called a **line**?



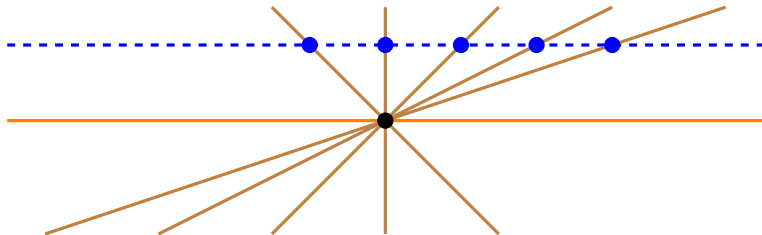
each non-horizontal line $\longleftrightarrow$ **some point on the blue line**

The projective line $\mathbb{P}^1$

Definition

The **projective line** $\mathbb{P}^1$ is the set of all lines in $\mathbb{R}^2$ through $(0,0)$.

Why is this set being called a **line**?



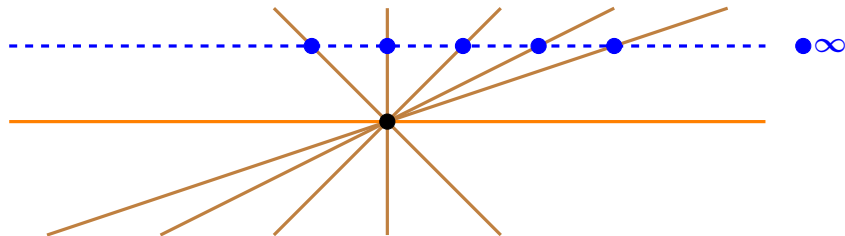
each non-horizontal line $\longleftrightarrow$ some point on the blue line
the horizontal line $\longleftrightarrow$

The projective line $\mathbb{P}^1$

Definition

The **projective line** $\mathbb{P}^1$ is the set of all lines in $\mathbb{R}^2$ through $(0,0)$.

Why is this set being called a **line**?



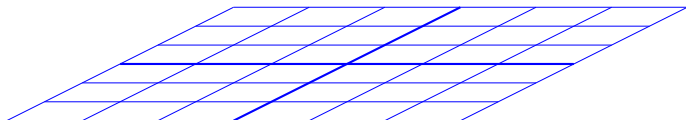
each non-horizontal line $\longleftrightarrow$ **some point on the blue line**

the horizontal line $\longleftrightarrow$ **a new point ∞**

The projective plane $\mathbb{P}^2$

$$\mathbb{P}^1 := \{\text{lines through } (0,0) \text{ in } \mathbb{R}^2\} \longleftrightarrow \text{line} \cup \{\infty\}$$

$$\mathbb{P}^2 := \{\text{lines through } (0,0,0) \text{ in } \mathbb{R}^3\} \longleftrightarrow \text{plane} \cup (\quad)$$

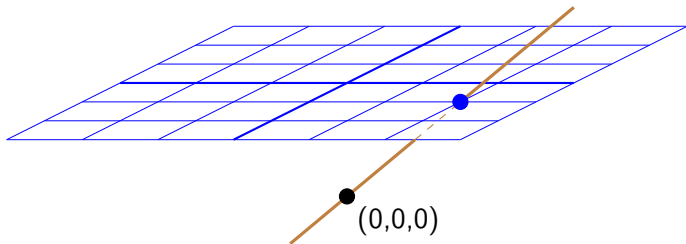


●
(0,0,0)

The projective plane $\mathbb{P}^2$

$$\mathbb{P}^1 := \{\text{lines through } (0,0) \text{ in } \mathbb{R}^2\} \longleftrightarrow \text{line} \cup \{\infty\}$$

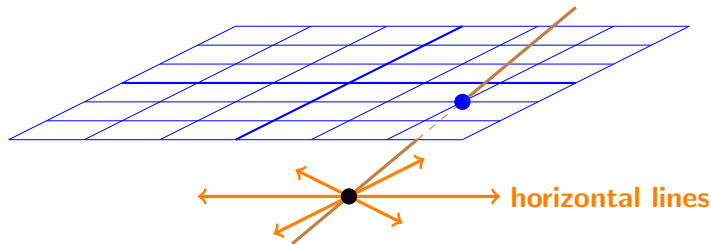
$$\mathbb{P}^2 := \{\text{lines through } (0,0,0) \text{ in } \mathbb{R}^3\} \longleftrightarrow \text{plane} \cup ($$



The projective plane $\mathbb{P}^2$

$$\mathbb{P}^1 := \{\text{lines through } (0,0) \text{ in } \mathbb{R}^2\} \longleftrightarrow \text{line} \cup \{\infty\}$$

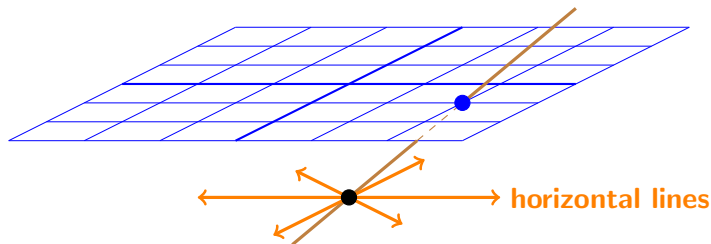
$$\mathbb{P}^2 := \{\text{lines through } (0,0,0) \text{ in } \mathbb{R}^3\} \longleftrightarrow \text{plane} \cup (\text{many points at } \infty)$$



The projective plane $\mathbb{P}^2$

$$\mathbb{P}^1 := \{\text{lines through } (0,0) \text{ in } \mathbb{R}^2\} \longleftrightarrow \text{line} \cup \{\infty\}$$

$$\mathbb{P}^2 := \{\text{lines through } (0,0,0) \text{ in } \mathbb{R}^3\} \longleftrightarrow \text{plane} \cup (\text{many points at } \infty)$$

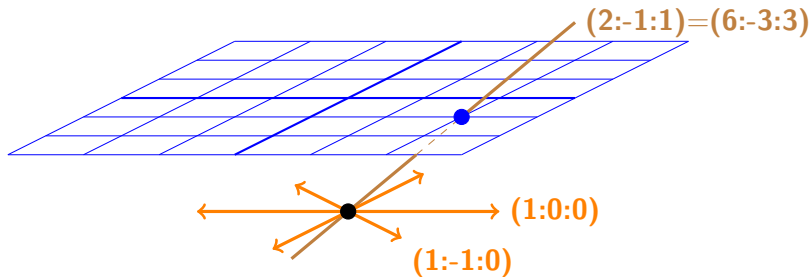


Questions:

- What coordinates can we use on $\mathbb{P}^2$?
- How can we label each line in $\mathbb{R}^3$ through $(0,0,0)$?

Homogeneous coordinates on $\mathbb{P}^2$

Write $(a:b:c)$ to mean **the line through $(0,0,0)$ and (a,b,c)** .



$$\mathbb{P}^2 = \frac{\mathbb{R}^3 - \{(0,0,0)\}}{\text{scaling}}$$

Curves in $\mathbb{P}^2$

Each curve in $\mathbb{R}^2$ can be “completed” to a curve in $\mathbb{P}^2$ by adding points at infinity.

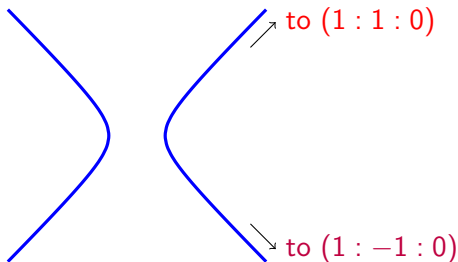
Example

The hyperbola $x^2 - y^2 = 5$ becomes $x^2 - y^2 = 5z^2$.
Points in $\mathbb{R}^2$ like $(3, 2)$ correspond to $(3 : 2 : 1)$ in $\mathbb{P}^2$.

To find the points at infinity, set $z = 0$:

We get $x^2 - y^2 = 0$, which leads to $y = x$ or $y = -x$,

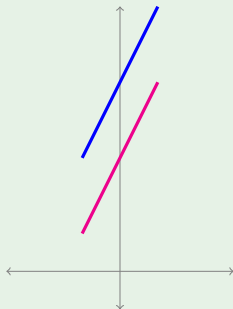
that is, $(x : x : 0) = \boxed{(1 : 1 : 0)}$ or $(x : -x : 0) = \boxed{(1 : -1 : 0)}$.



Intersecting lines in $\mathbb{P}^2$

Example

The lines $y = 2x + 3$ and $y = 2x + 5$ do not intersect.



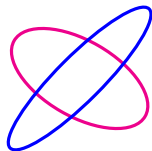
But their projective versions $y = 2x + 3z$ and $y = 2x + 5z$ intersect at the point where $y = 2x$ and $z = 0$, which is $(1 : 2 : 0)$.

Intersecting two curves in $\mathbb{P}^2$

Bézout's theorem

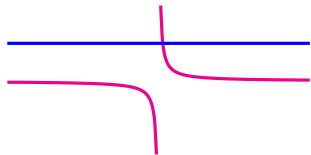
Two plane curves $f(x, y) = 0$ and $g(x, y) = 0$ of degrees m and n intersect in *mn points*, **if**

1. $f(x, y)$ and $g(x, y)$ have no common factor,
2. we include intersections at infinity (work in $\mathbb{P}^2$),
3. we include intersections with complex number coordinates, and
4. points of tangency count as two or more points.

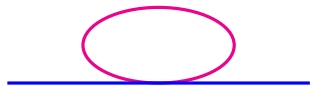


$$2 \cdot 2 = 4$$

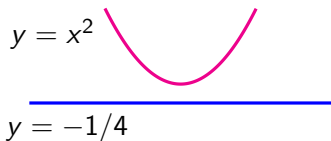
More instances of Bézout's theorem



$2 \cdot 1 = 2$ (one intersection is at infinity)



$2 \cdot 1 = 2$ (tangency counts as 2)



$2 \cdot 1 = 2$ (complex intersection points)

Elliptic curves

Definition

An **elliptic curve** is the completion in $\mathbb{P}^2$ of the curve

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

where A and B are numbers

such that $x^3 + Ax + B$ has no double roots.

Example

Let E be the completion in $\mathbb{P}^2$ of $y^2 = x^3 - 25x$.

This is an elliptic curve, since the polynomial

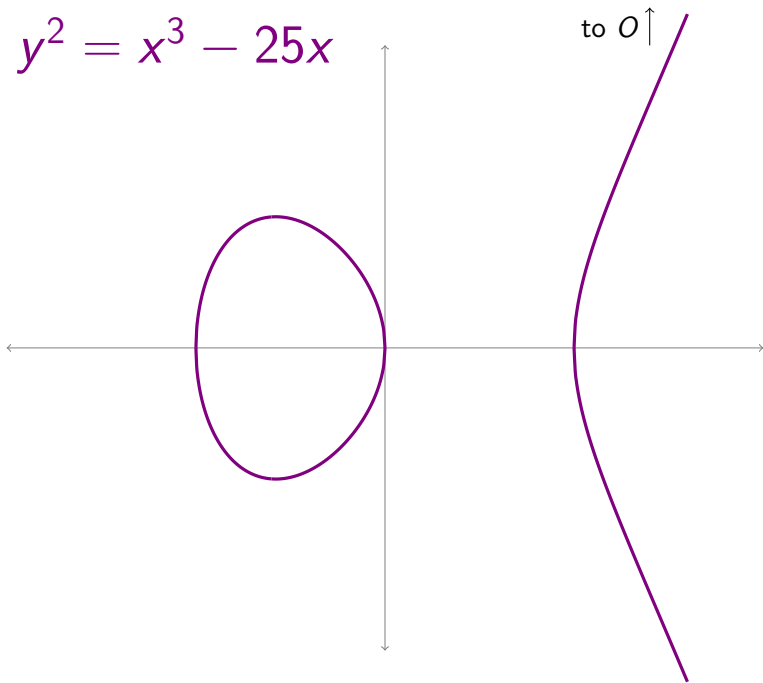
$x^3 - 25x = x(x + 5)(x - 5)$ has no double roots.

The projective version is $y^2z = x^3 - 25xz^2$.

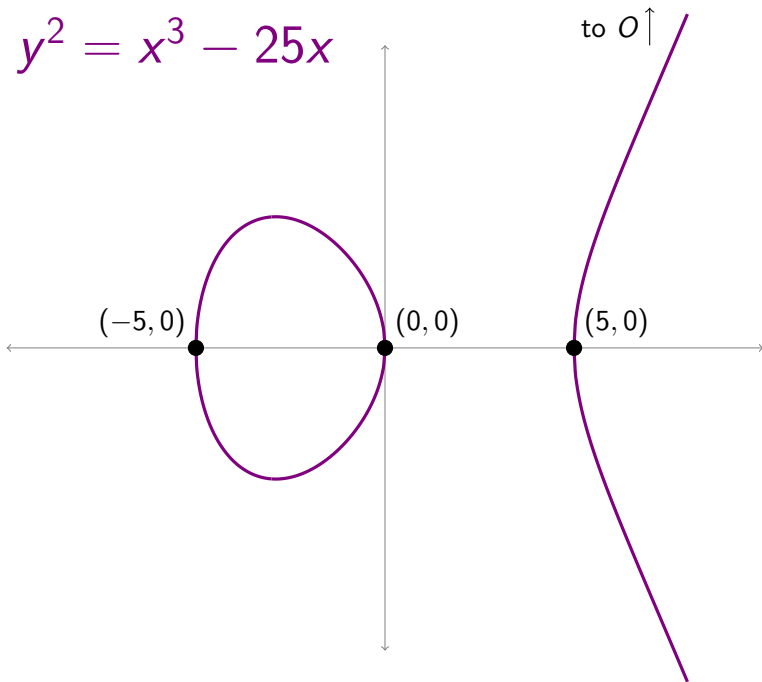
To find the points at infinity, set $z = 0$; get $0 = x^3$.

Conclusion: The only point at infinity is $(0 : 1 : 0)$. Call it O .

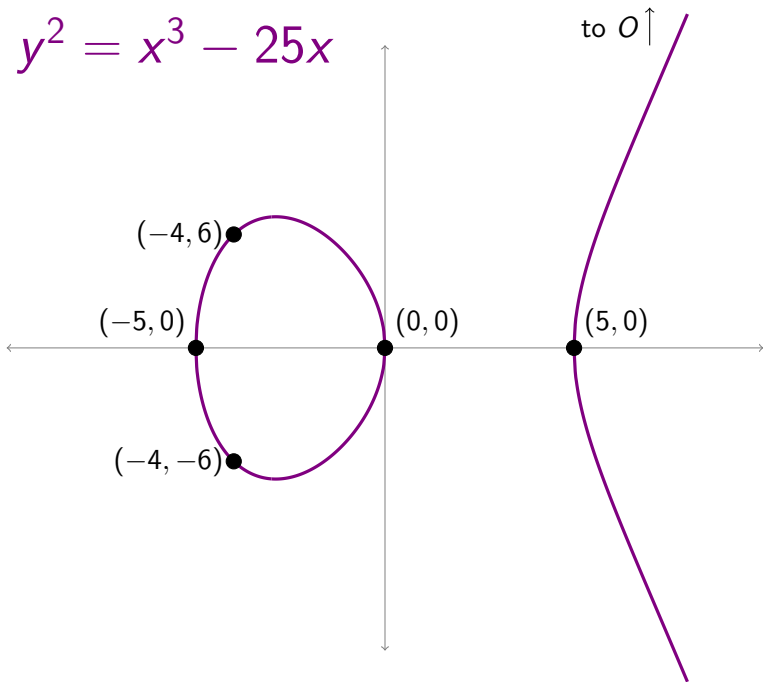
$$y^2 = x^3 - 25x$$



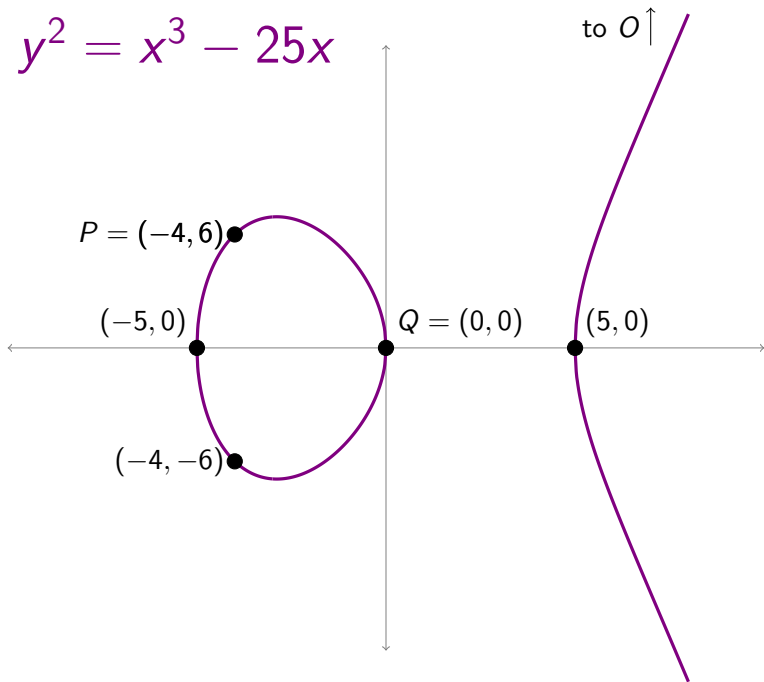
$$y^2 = x^3 - 25x$$



$$y^2 = x^3 - 25x$$

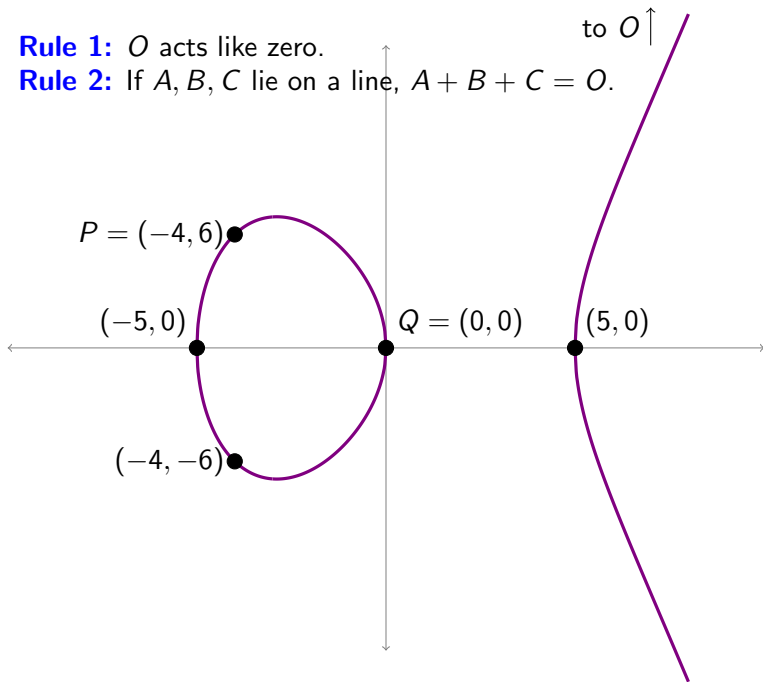


$$y^2 = x^3 - 25x$$



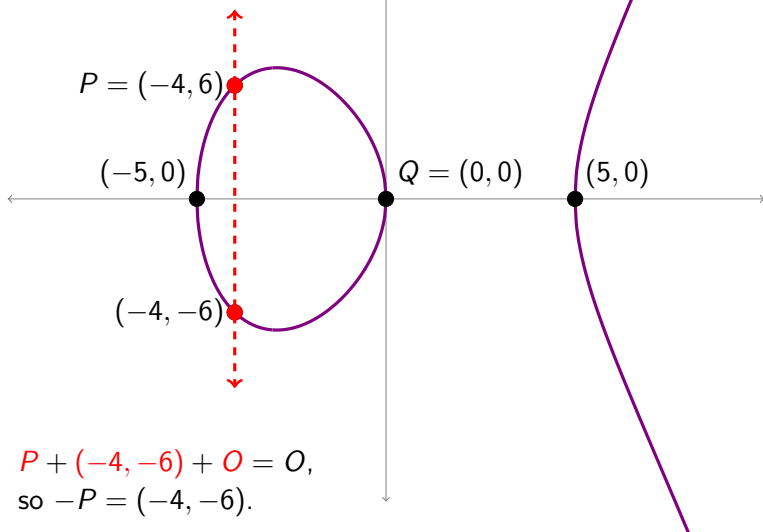
Rule 1: O acts like zero.

Rule 2: If A, B, C lie on a line, $A + B + C = O$.



Rule 1: O acts like zero.

Rule 2: If A, B, C lie on a line, $A + B + C = O$.

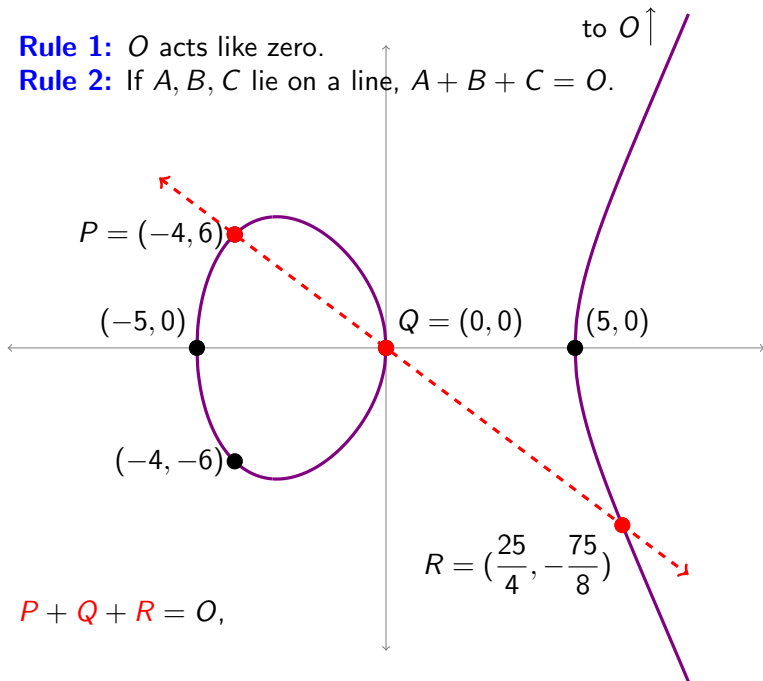


$$P + (-4, -6) + O = O,$$

so $-P = (-4, -6)$.

Rule 1: O acts like zero.

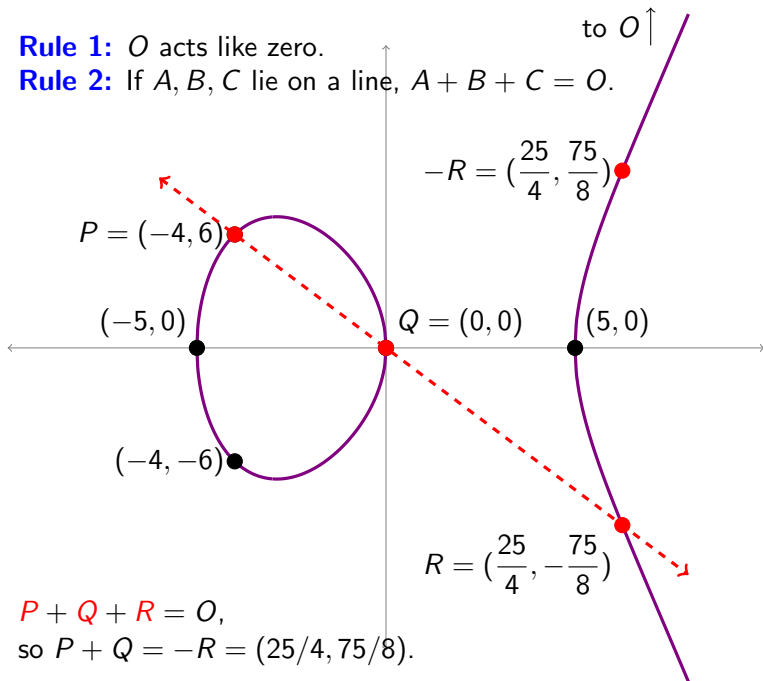
Rule 2: If A, B, C lie on a line, $A + B + C = O$.



$$P + Q + R = O,$$

Rule 1: O acts like zero.

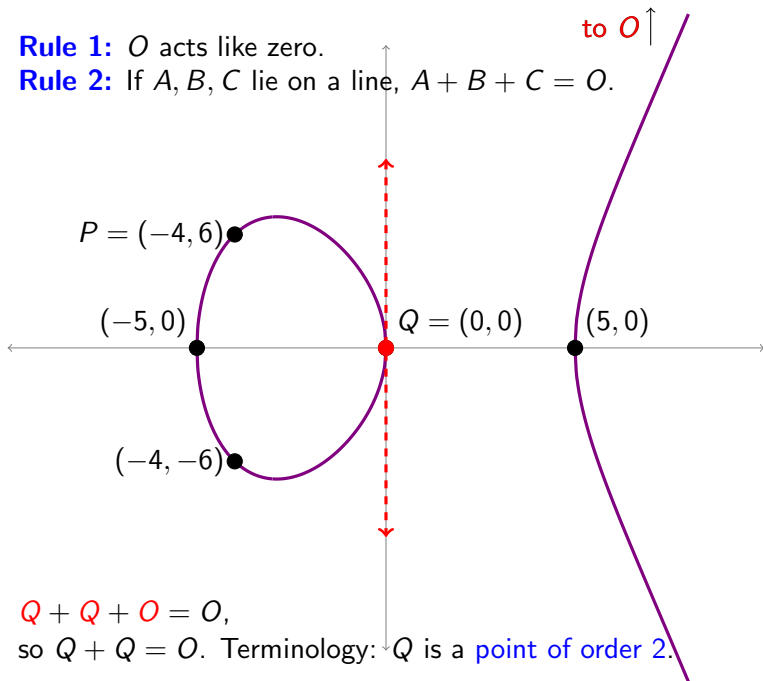
Rule 2: If A, B, C lie on a line, $A + B + C = O$.



$$P + Q + R = O,$$
$$\text{so } P + Q = -R = (25/4, 75/8).$$

Rule 1: O acts like zero.

Rule 2: If A, B, C lie on a line, $A + B + C = O$.



$$Q + Q + O = O,$$

so $Q + Q = O$. Terminology: Q is a **point of order 2**.

Generating all rational points from a few starting points

Remark

It turns out that for

$$y^2 = x^3 - 25x,$$

if we start with $P = (-4, 6)$

*(and the points of finite order $(-5, 0)$, $(0, 0)$, $(5, 0)$),
then all other rational points can be generated from these!*

There are infinitely many rational points; in fact,

$$\dots \quad -3P \quad -2P \quad -P \quad \textcolor{violet}{O} \quad P \quad 2P \quad 3P \quad \dots$$

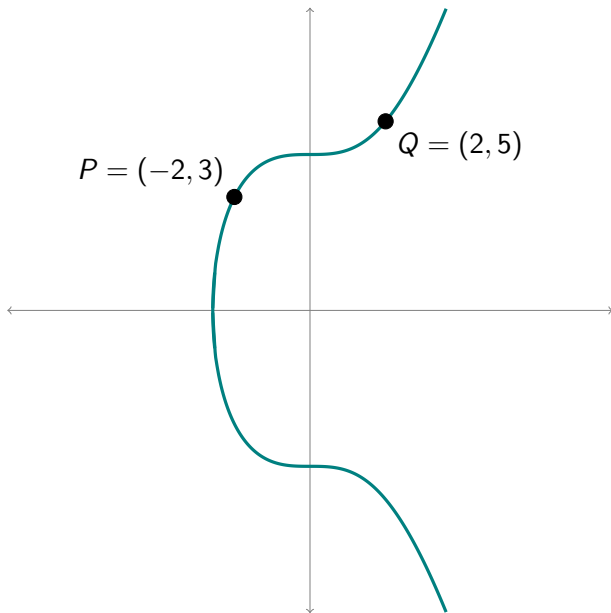
are all distinct.

Because only **one** starting point P was needed

(not counting the points of finite order),

the elliptic curve is said to have **rank 1**.

The elliptic curve $y^2 = x^3 + 17$



The elliptic curve $y^2 = x^3 + 17$, continued

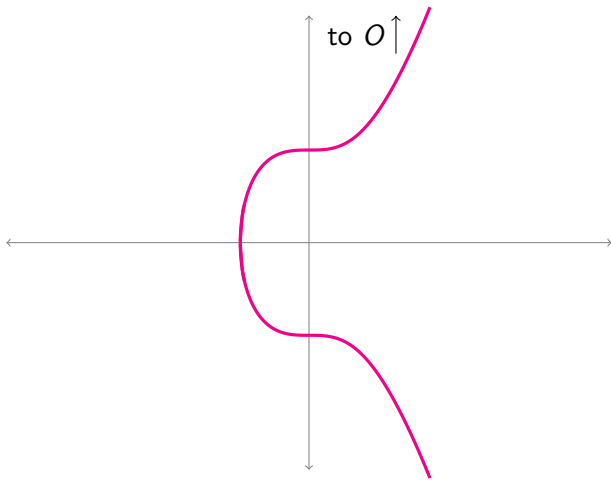
Let $P = (-2, 3)$ and $Q = (2, 5)$. Then the rational points

	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\dots$	$-2P + 2Q$	$-P + 2Q$	$2Q$	$P + 2Q$	$2P + 2Q$	$\dots$
$\dots$	$-2P + Q$	$-P + Q$	Q	$P + Q$	$2P + Q$	$\dots$
$\dots$	$-2P$	$-P$	O	P	$2P$	$\dots$
$\dots$	$-2P - Q$	$-P - Q$	$-Q$	$P - Q$	$2P - Q$	$\dots$
$\dots$	$-2P - 2Q$	$-P - 2Q$	$-2Q$	$P - 2Q$	$2P - 2Q$	$\dots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

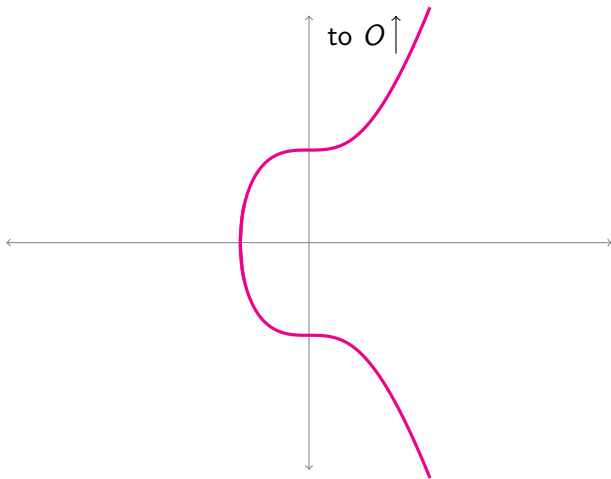
are all distinct, and they are all the rational points on this curve.

Conclusion: $y^2 = x^3 + 17$ has rank 2.

The elliptic curve $y^2 = x^3 + 6$



The elliptic curve $y^2 = x^3 + 6$



The only rational point is O ! So $y^2 = x^3 + 6$ has rank 0.

Mordell's theorem (1922)

For each elliptic curve E , there is a finite list of rational points $P_1, P_2, \dots, P_n$ such that every other rational point on E can be generated from these.

The number of starting points required
(not including points of finite order, which count as free)
is called the **rank** of E .

Rank of $y^2 = x^3 + n$

n	rank
1	0
2	1
3	1
4	0
5	1
6	0
7	0
8	1
9	1
10	1
11	1
12	1
13	0
14	0
15	2
16	1
17	2

Unsolved problems

Problem

Find a method for computing the rank of any given elliptic curve E .

Problem

Find a method for listing points that are guaranteed to generate E .

There is an elliptic curve of rank **at least 28** (the record since 2006).

Problem

*Is there an elliptic curve whose rank is **> 28** ?*

If you want to know more:

Silverman & Tate, *Rational points on elliptic curves*.