Elliptic curves and modular forms

Jean-Stefan Koskivirta

October 21, 2023

Elliptic curves

An elliptic curve is given by an equation of the form

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

where a, b are two constants. For example, the following equations are equations of elliptic curves:

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

Elliptic curves

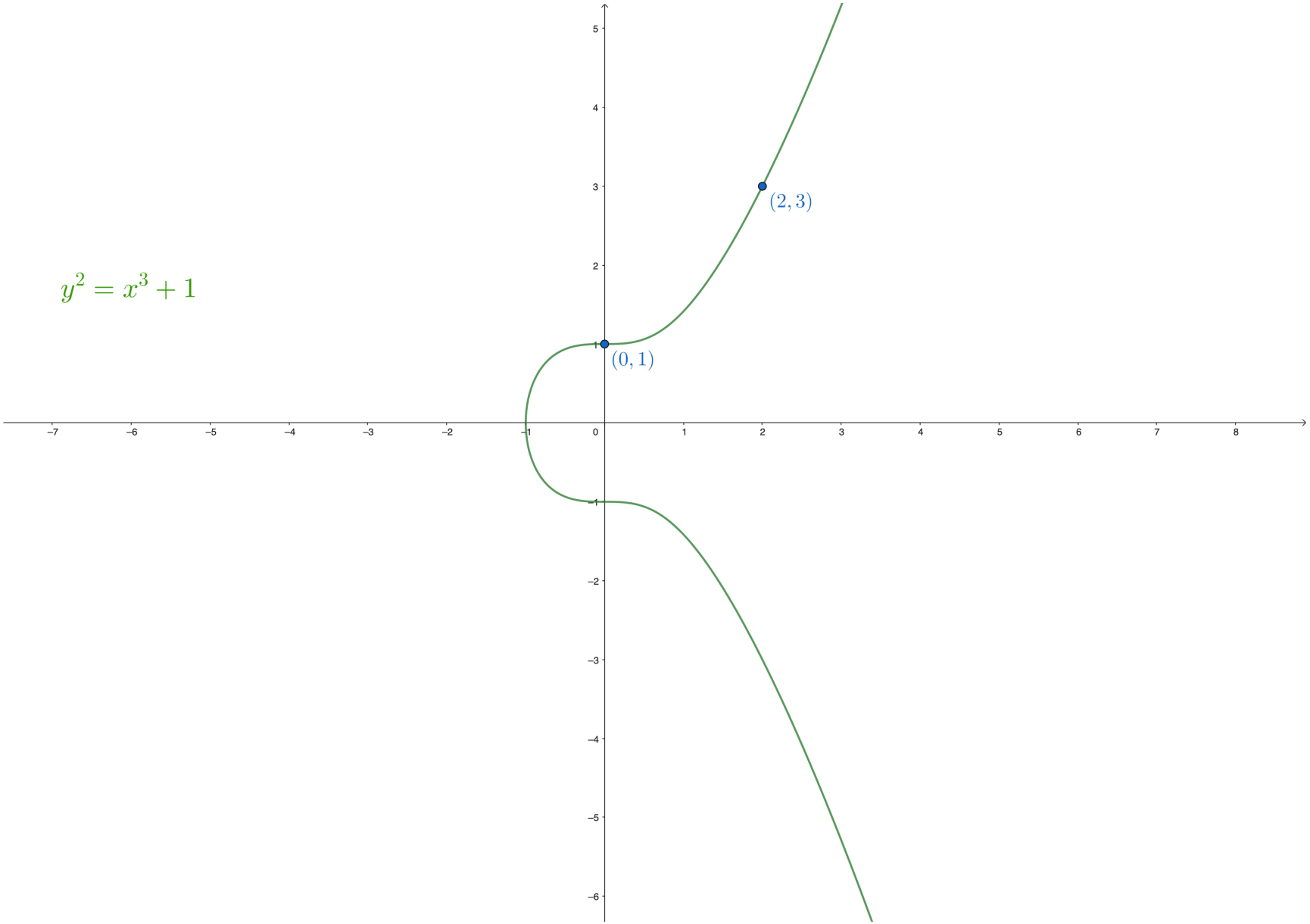
The elliptic curve defined by the equation $y^2 = x^3 + ax + b$ is the set of pairs (x, y) which satisfy this equation. For example, consider the equation

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

This equation is satisfied in the case $x = 0$, $y = 1$. It is also satisfied for $x = 2$, $y = 3$.
Thus, the graph of this equation in the xy-plane contains the points $(2, 3)$ and $(0, 1)$.

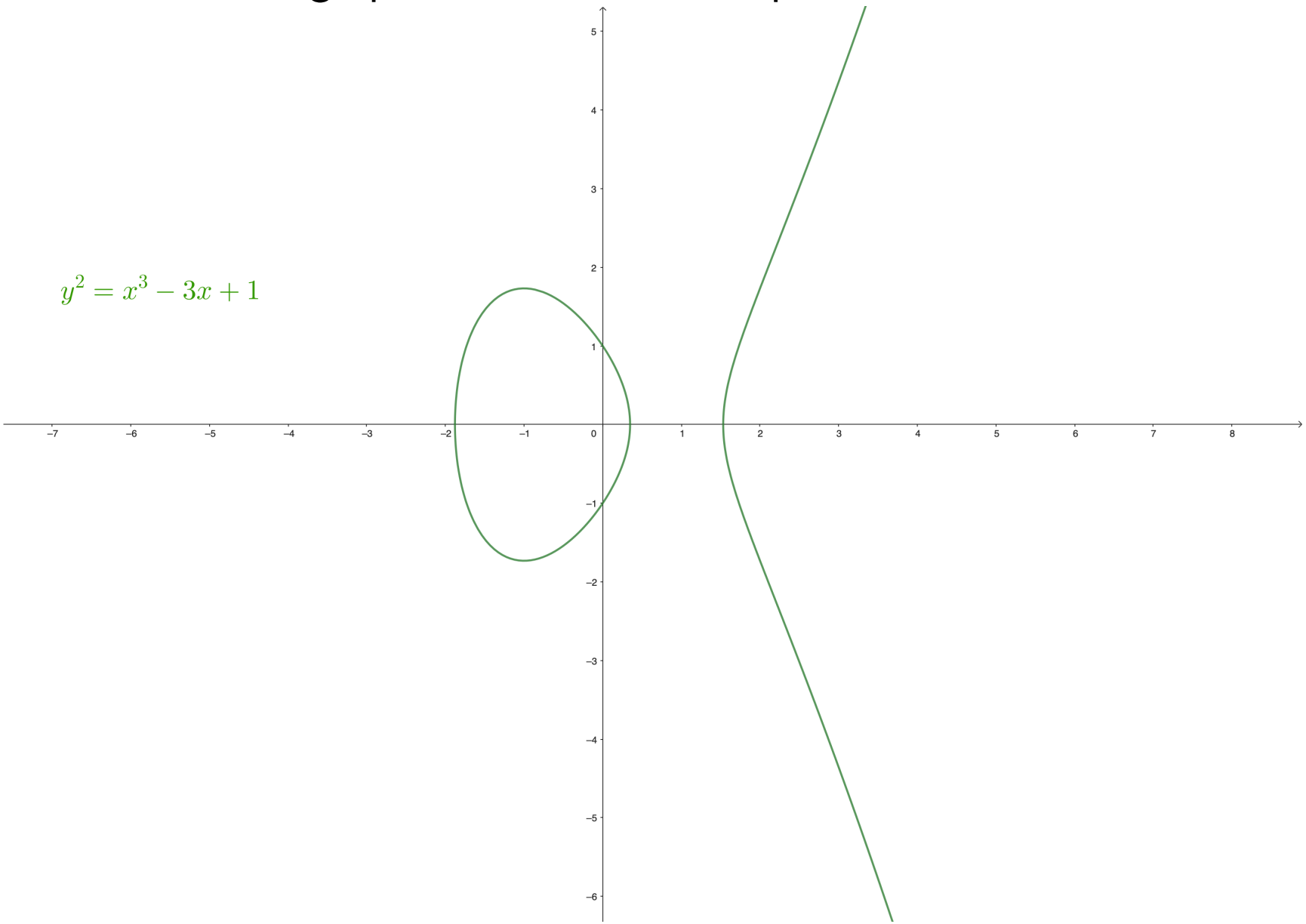
Graph

$y^2 = x^3 + 1$

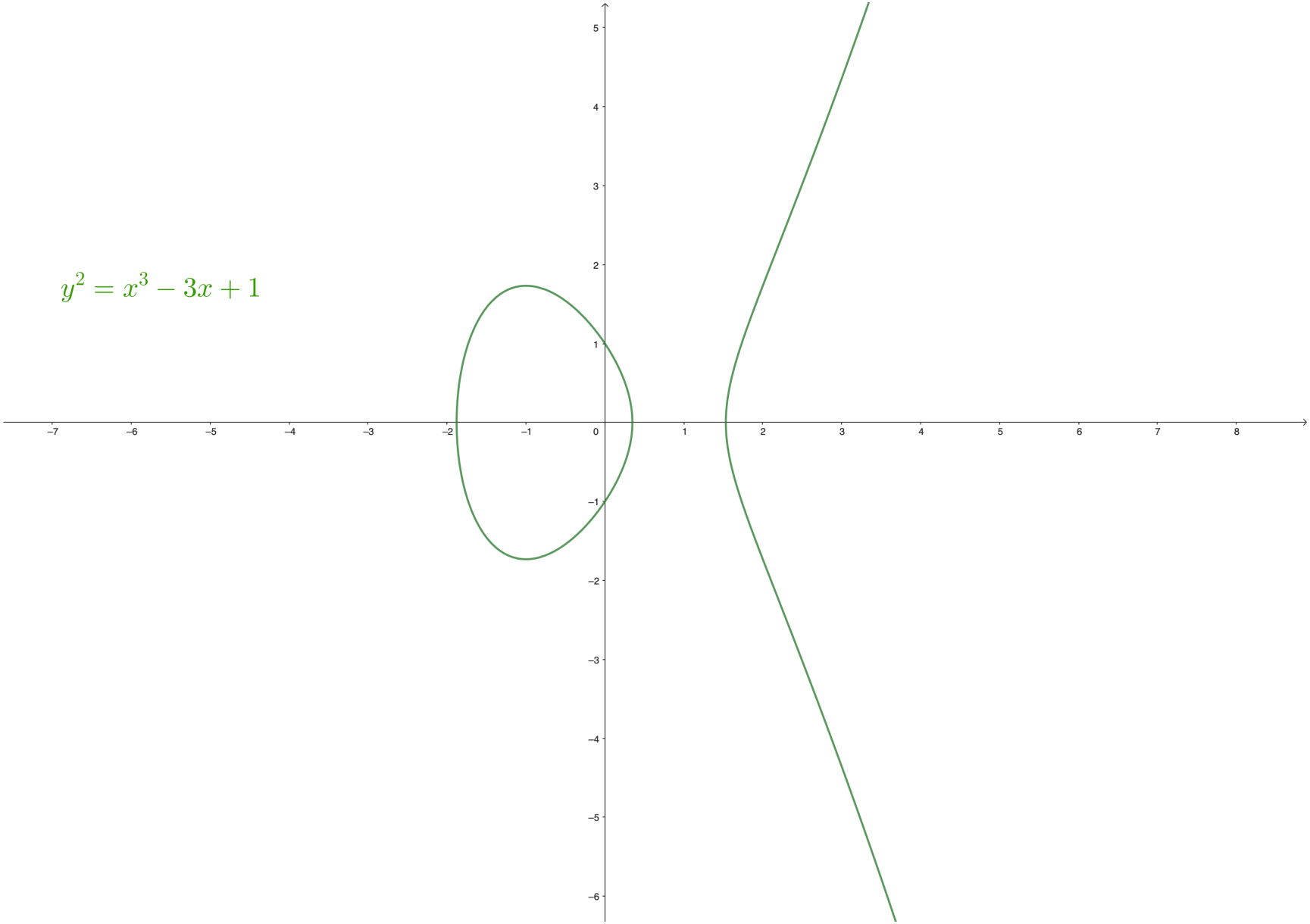


Graph

Sometimes, the graph can have two components:



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



Bezout's theorem

Theorem (Bezout)

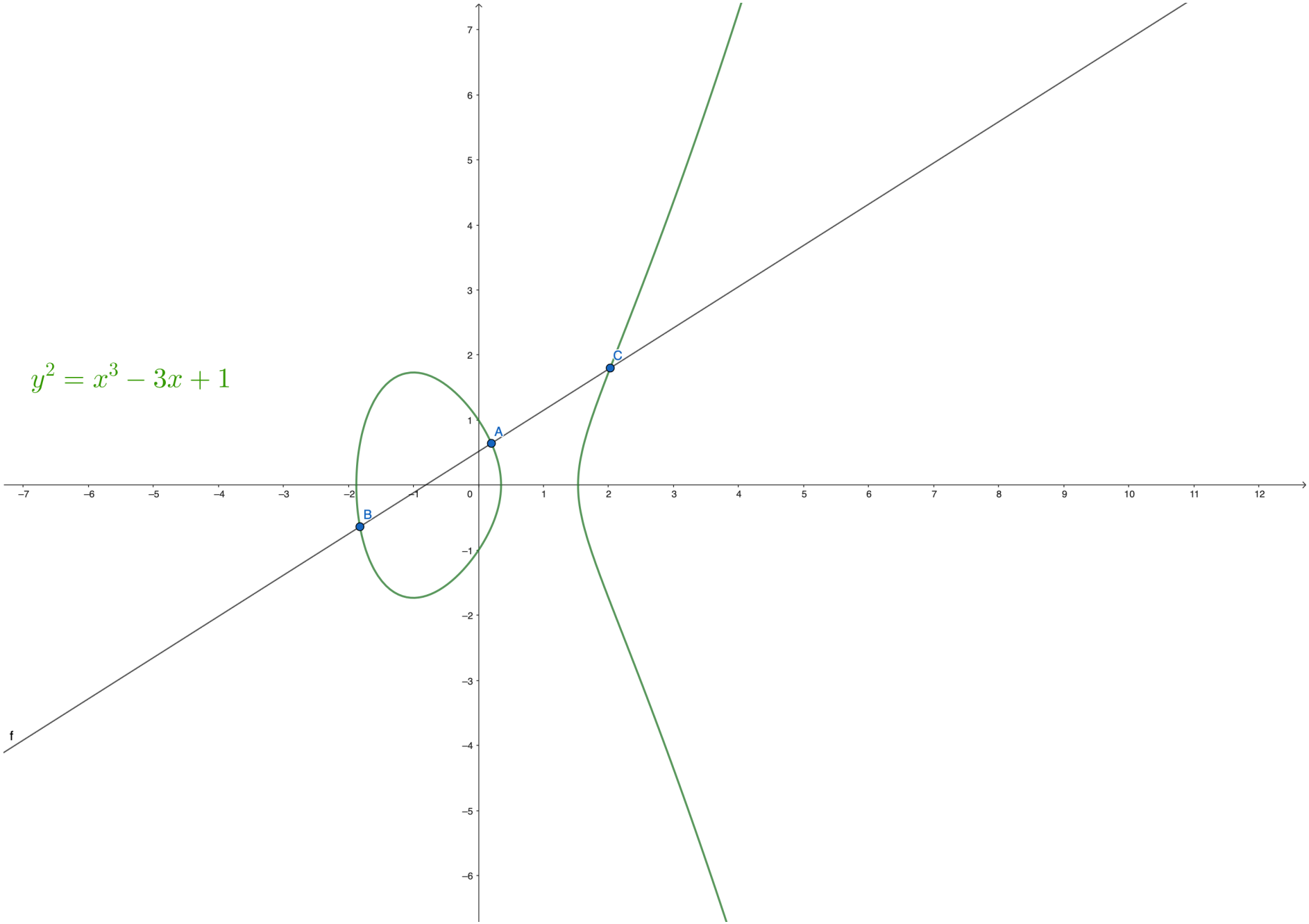
Let C_1 and C_2 be two distinct curves of degree d_1 and d_2 respectively. Then they intersect at exactly $d_1 \times d_2$ points.

Some caveats: One has to include points whose coordinates are "complex numbers" and one has to count multiplicities. Furthermore, one has to count "points at infinity".
Consider the case when C_1 is an ellitpic curve $y^2 = x^3 + ax + b$ and C_2 is a line. By Bezout's theorem there are $3 \times 1 = 3$ intersection points.

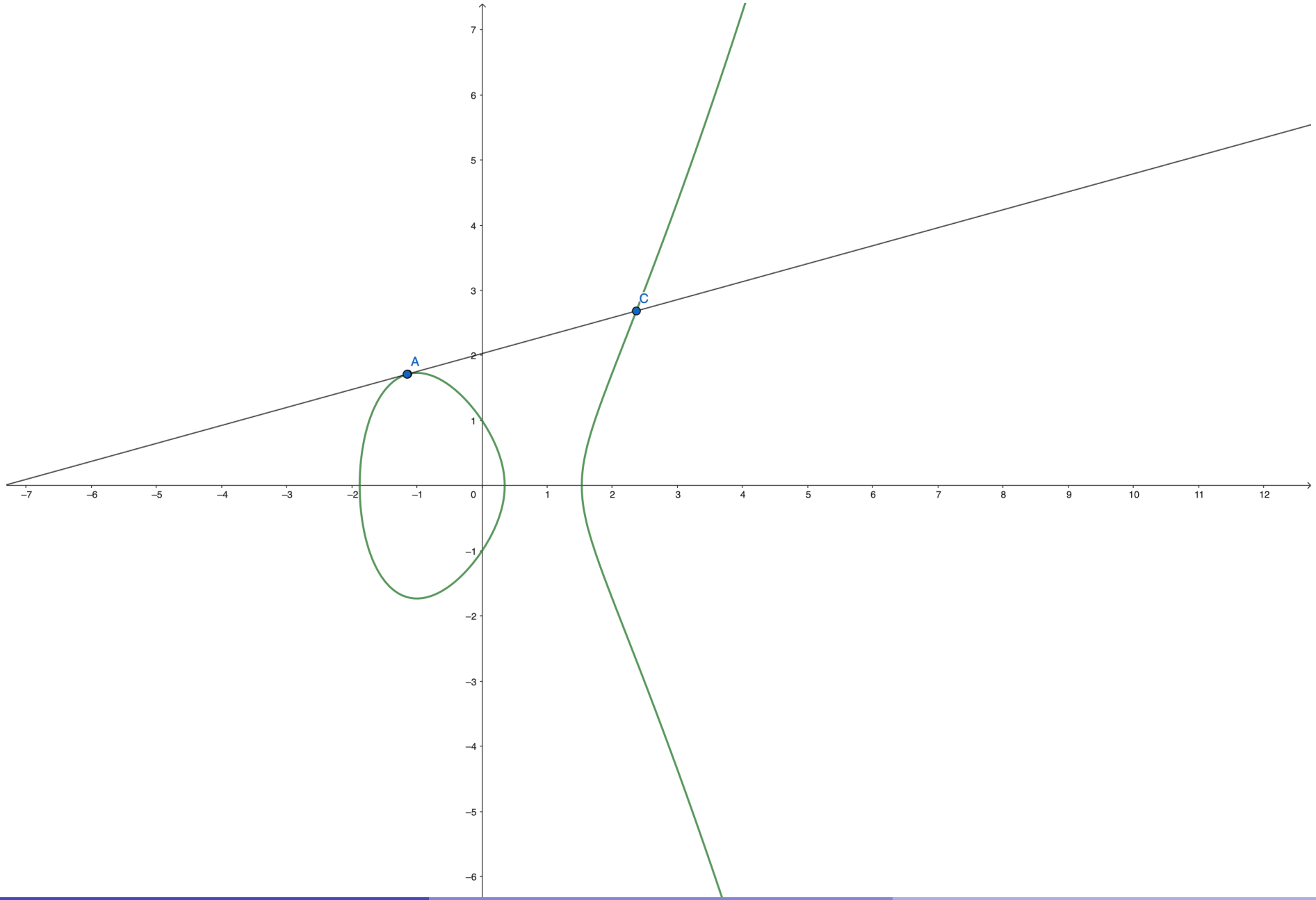
Corollary

If a line intersects an elliptic curve at two points A and B, it will intersect it at third point C.

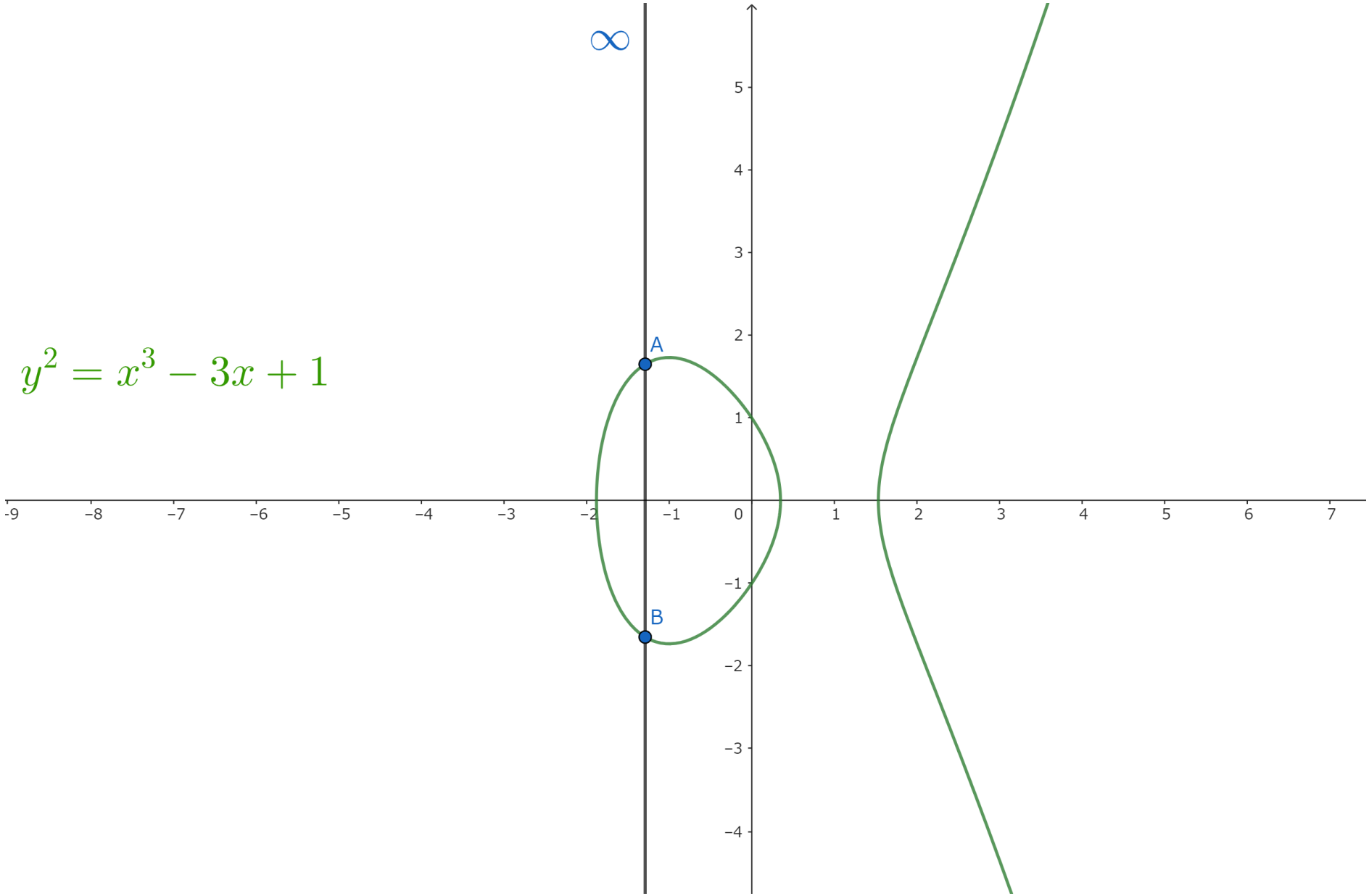
- We allow the case when $A = B$ and the line is tangent at A.
- The third point C can be the "point at infinity"


$y^2 = x^3 - 3x + 1$
A
B
C
f

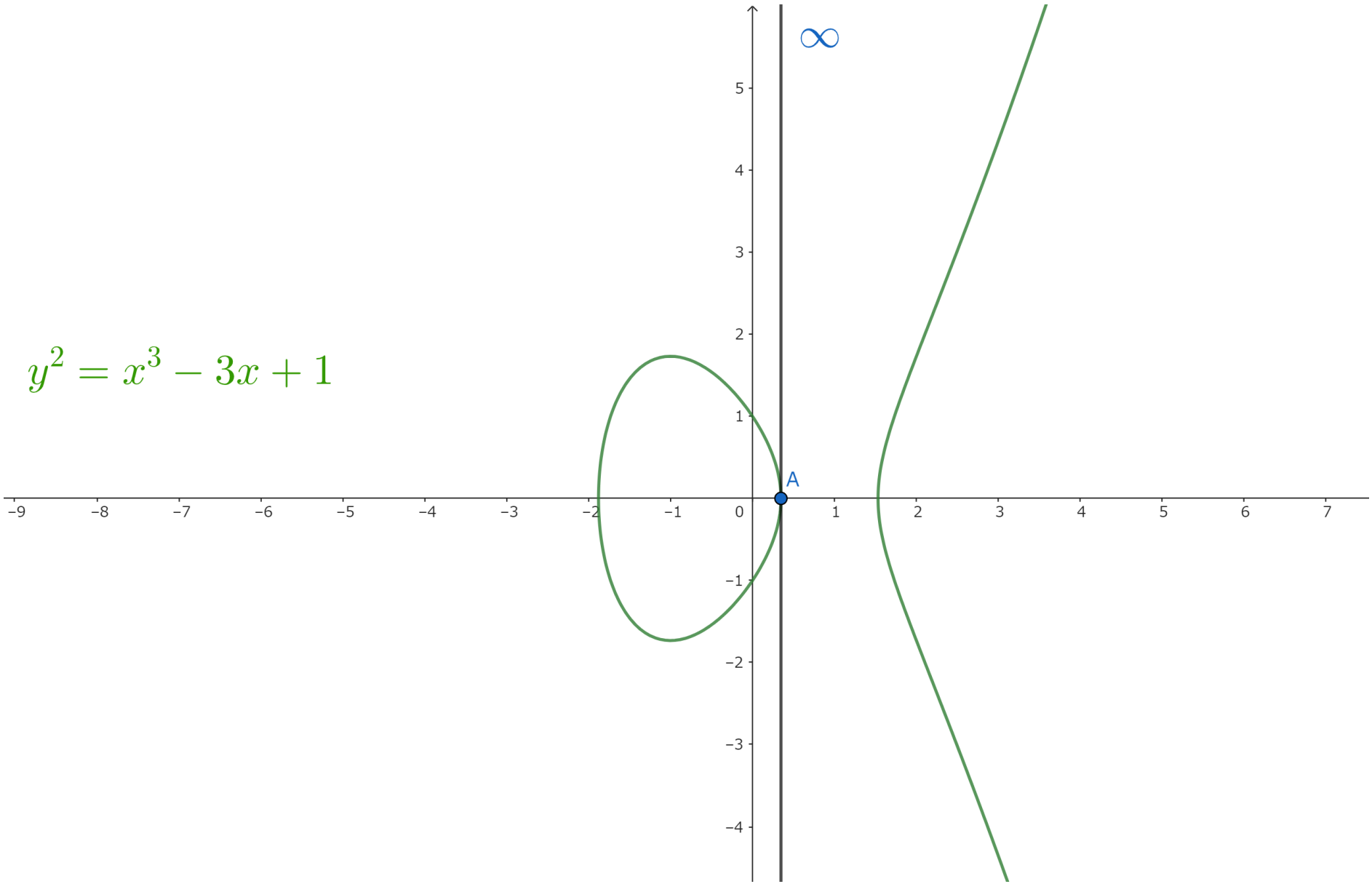
In this picture, the line intersects the curve at A with multiplicity 2, and at C with multiplicity 1.



In this picture, the line through A and B intersects the "point at infinity".



In this picture, the line intersects the curve at A with multiplicity 2 and the "point at infinity".



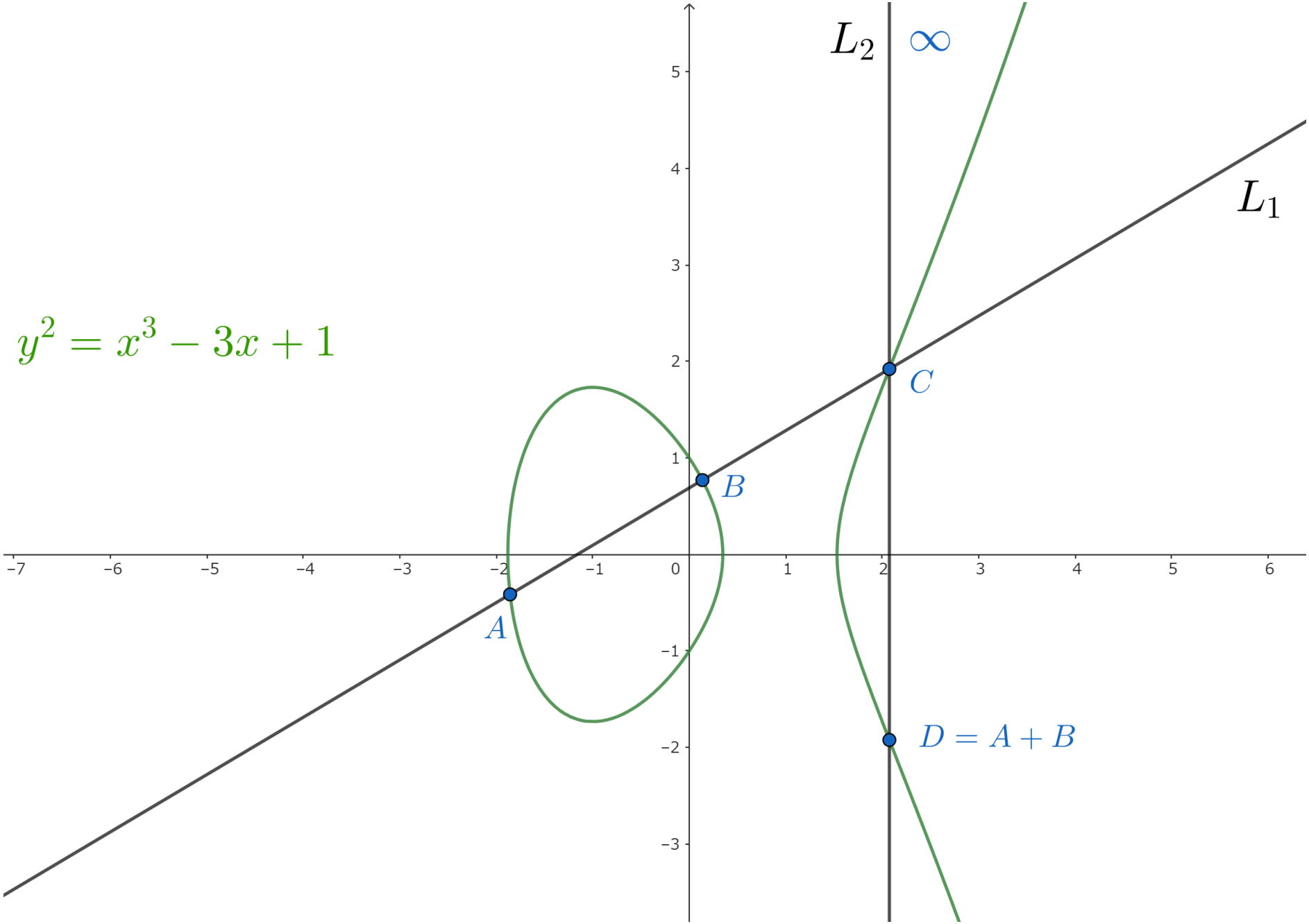
Addition law

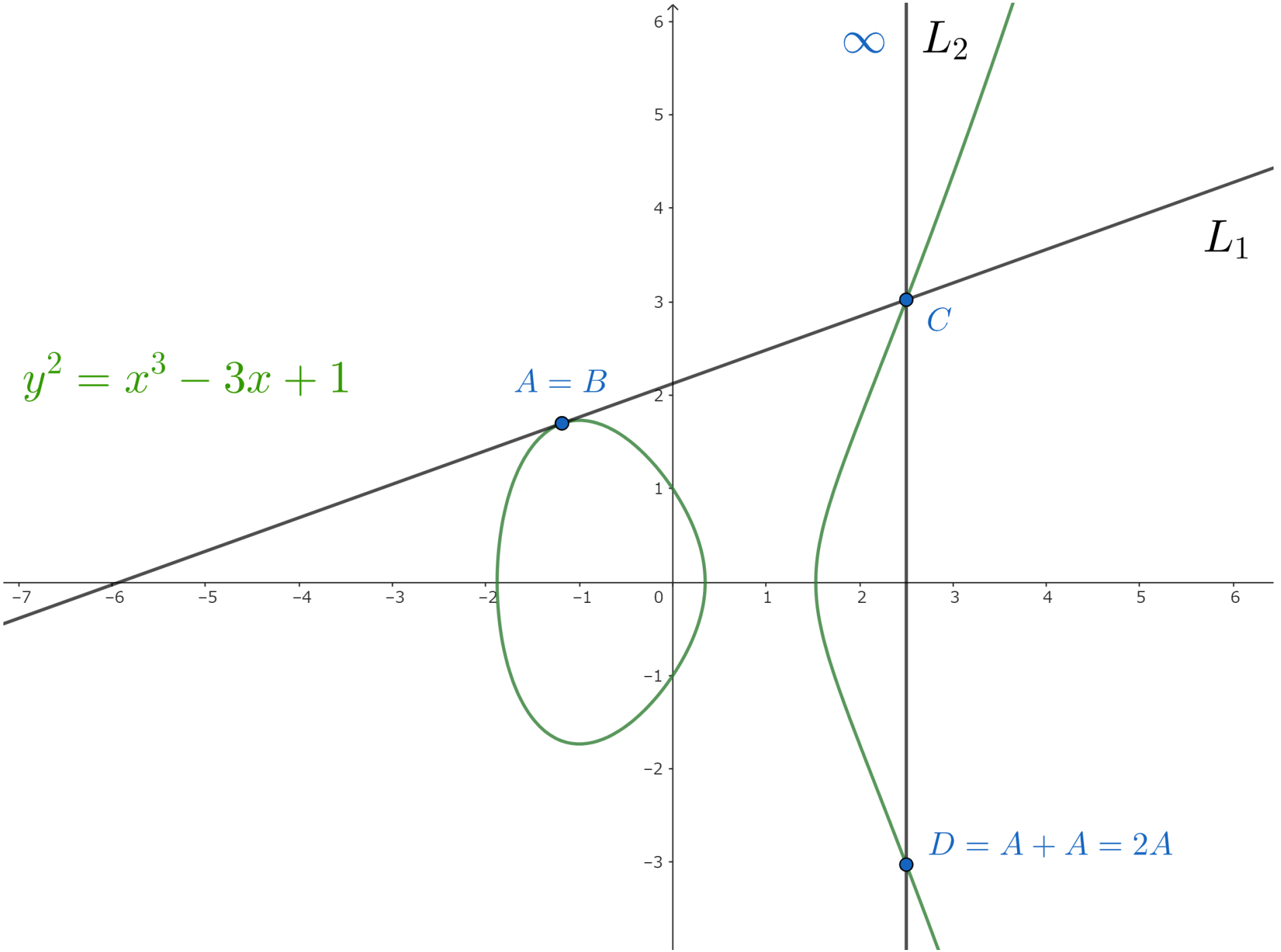
Let E be an elliptic curve, defined by the equation $y^2 = x^3 + ax + b$. Given two points A and B on this curve, we construct a third point C on the curve as follows:

Definition

- First, draw the line L_1 through A and B. It intersects the curve E at a third point C.
- Then, draw the line L_2 which passes through C which is parallel to the y-axis. This line also passes through the point at infinity.
- The line L_2 intersects E at a third point, say D.

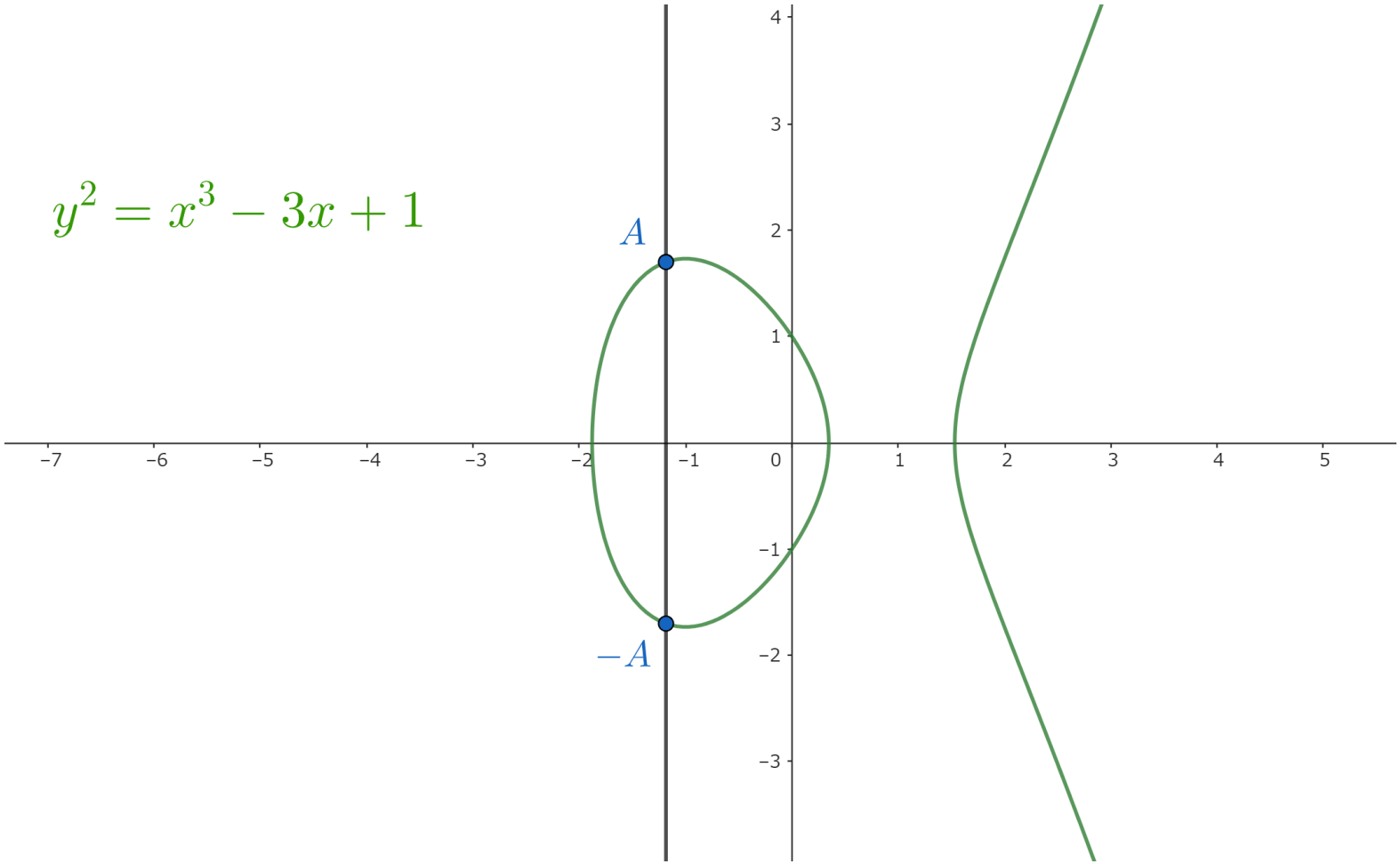
We define the sum of A and B to be the point D, and we denote it by $A + B$.


$y^2 = x^3 - 3x + 1$
L_2
∞
L_1
C
B
A
$D = A + B$


$y^2 = x^3 - 3x + 1$
$A = B$
C
$D = A + A = 2A$
∞
L_1
L_2

Inverse

For any point A of the curve E, we define the inverse of $A = (x, y)$, denoted by $-A$, as the symmetric of A with respect to the x-axis. In other words, $-A$ is the point $(x, -y)$.



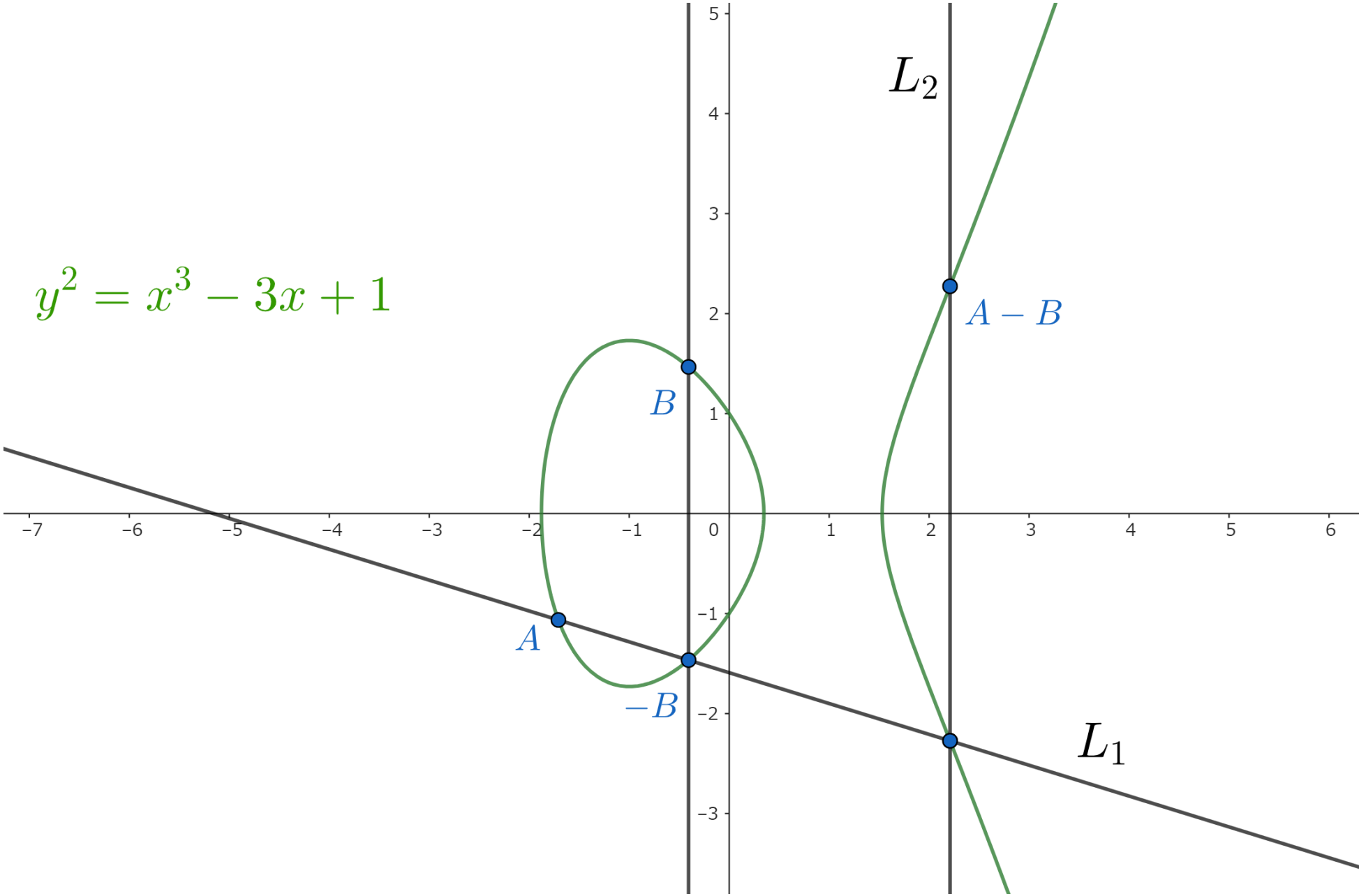
Subtraction

For two points A and B on the curve, we can define the subtraction $A - B$ as follows:

Definition

- We first construct the point $-B$.
- We add A and $-B$ to produce $A + (-B)$.

We define $A - B$ as the point $A + (-B)$.


$y^2 = x^3 - 3x + 1$
L_2
$A - B$
B
A
$-B$
L_1

Addition Law

Theorem

The addition and inverse operations make E a abelian group. This means the following:

- *For any points A, B, C, one has $(A + B) + C = A + (B + C)$. We say that addition is associative.*
- *For any points A, B, one has $A + B = B + A$. We say that addition is commutative.*
- *For each point A, one has $A + 0 = 0 + A = A$, where 0 denotes the point at infinity. We say that the point at infinity is the identity element.*
- *For any point A, there exists a point $-A$ such that $A + (-A) = (-A) + A = 0$. We say that $-A$ is the inverse of A.*

Abelian groups

Let G be a nonempty set. Assume that G is endowed with an operation $(x, y) \mapsto x + y$, which attaches to any two elements $x, y \in G$ an element $x + y$ in G. For example, the usual "addition" is an operation on the set of integers.

Definition

We say that G is an abelian group if it satisfies the following:

- For all x, y, z in G, we have $(x + y) + z = x + (y + z)$ (associativity),
- For all x, y in G, we have $x + y = y + x$ (commutativity),
- There exists an element $0 \in G$ such that for all x in G, we have $x + 0 = 0 + x = x$ (identity element),
- For each x in G, there exists an element $-x$ in G such that $x + (-x) = (-x) + x = 0$ (inverse element).

Examples

- Let $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ denote the integers. Then $\mathbb{Z}$ is an abelian group with respect to the addition $(x, y) \mapsto x + y$. The identity element is 0, and the inverse of x is $-x$.
- Let $\mathbb{R}$ denote the real numbers. Then $\mathbb{R}$ is also a group with respect to addition.
- For an integer n, write $\mathbb{Z}^n$ for the set of tuples $(k_1, \dots, k_n)$ consisting of n integers. We can define an addition on $\mathbb{Z}^n$ by

$$(k_1, \dots, k_n) + (k_1', \dots, k_n') = (k_1 + k_1', \dots, k_n + k_n').$$

  Then $\mathbb{Z}^n$ is also an abelian group.

Rank

Definition

If G is an abelian group, we can define the rank of G. It can be intuitively understood as the number of "degrees of liberty" in G.

- For example, the rank of $\mathbb{Z}$ is 1.
- Then rank of $\mathbb{Z}^n$ is n.
- For some abelian groups, the rank can be infinite. For example $\mathbb{R}$ has infinite rank.

Here is a precise definition of rank:

- Say that elements $x_1, \ldots, x_n$ in G are free if one can never reach 0 by adding and subtracting the x_i's.
- Define the rank of G as the maximal n such that there exists free elements $x_1, \ldots, x_n$.

Mordell-Weil theorem

Consider an elliptic curve

$$y^2 = x^3 + ax + b \qquad (E)$$

where a, b are rational numbers. If $A = (x_1, y_1)$ and $B = (x_2, b_2)$ are two solutions to this equation, we have defined a third point $A + B = (x_3, y_3)$. One can show that if the coordinates of A, B are rational numbers, then so are the coordinates of $A + B$. Therefore, if we write $E(\mathbb{Q})$ for the solutions in rational numbers of this equation, then addition preserves $E(\mathbb{Q})$. Hence $E(\mathbb{Q})$ is also an abelian group.

Theorem (Mordell 1922, Weil 1929)

The rank of $E(\mathbb{Q})$ is finite.

This means that $E(\mathbb{Q})$ looks like $\mathbb{Z}^n$ for some $n \geq 1$ (plus some finite part).

Rank of elliptic curves

- Is the rank of $E(\mathbb{Q})$ bounded by a fixed number, or are there elliptic curves with arbitrary large ranks ?
  The answer to this question is not known. So far, the world record for the highest rank was discovered by N. Elkies:

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 344816117950305564670329856903907203748559443593191803612660082962919394487322434 29$$

  which has rank 28.
- However, the "average rank" of an elliptic curve is quite small. This is the rank one would obtain on average if we chose an elliptic curve randomly.

Theorem (Bhargava–Shankar, 2015)

The average rank of elliptic curves is less that $\frac{7}{6}$.

Problem

Question

What is the significance of the rank of $E(\mathbb{Q})$? What information does it provide about E ?

Integer solutions

Consider an elliptic curve

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

where a, b are integers. In general, there are very few solutions to this equation in integers x, y. For example, consider the equation:

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

The only solution to this equation with integer coefficients (x, y) is $(0, 0)$.

Solution : Look for solutions in other "number systems" !

Number systems

There are many "number systems" that we may consider:

- The rationals $\mathbb{Q} = \{\frac{a}{b} \mid a, b : \text{integers}\}$
- The real numbers $\mathbb{R}$: The numbers that "fill in the gaps" between rational numbers. They have an infinite decimal expansion:

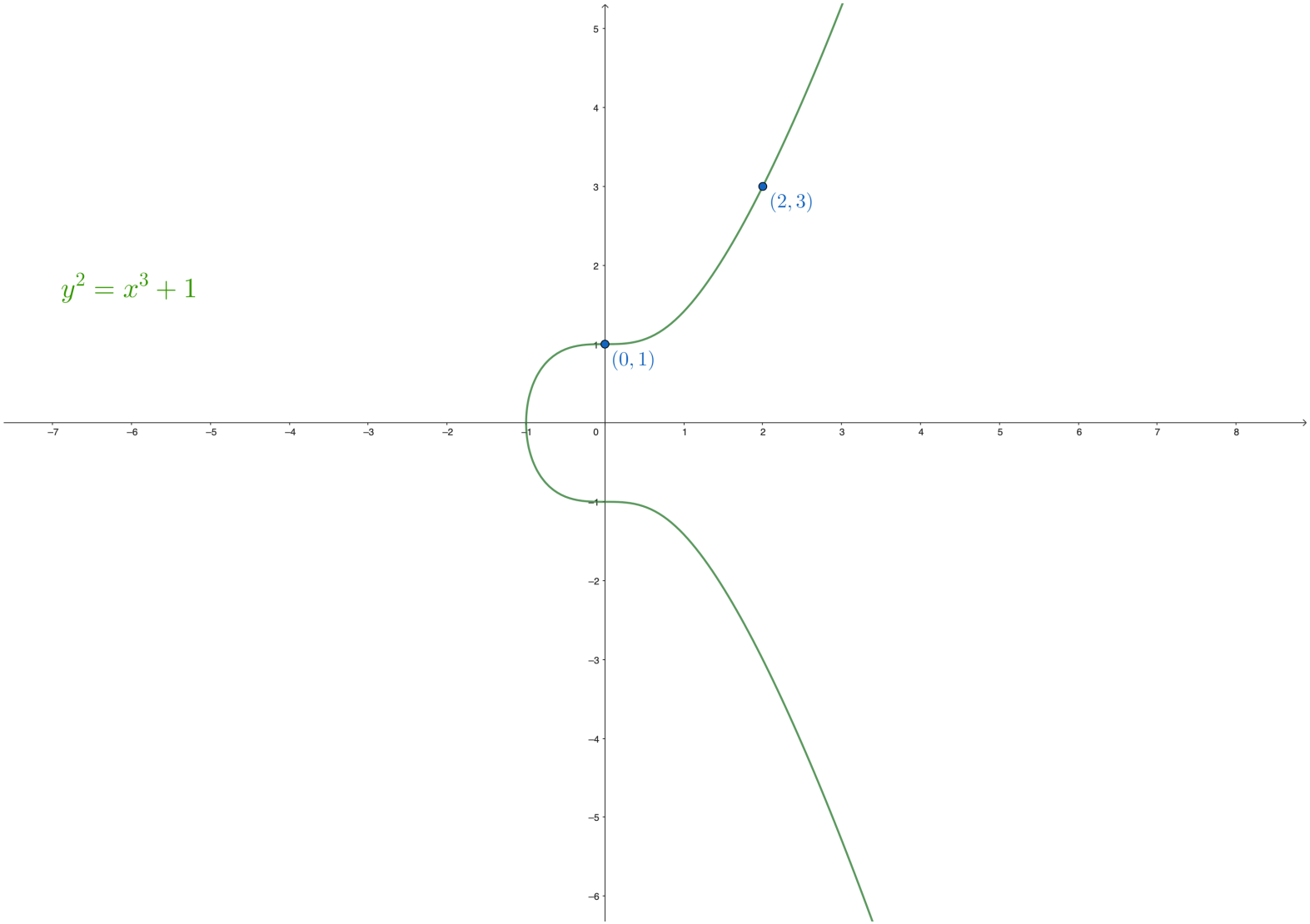
$$\pi = 3.14159265358979323846264338327950288419716939...$$

- The complex numbers $\mathbb{C}$: They can be written $a + ib$ where a, b are real numbers and i is "the square root of -1". They can be added, multiplied and divided as follows:

$$(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2)$$
$$(a_1 + ib_1) \times (a_2 + ib_2) = (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1)$$
$$\frac{1}{a + ib} = \frac{a - ib}{a^2 + b^2}.$$

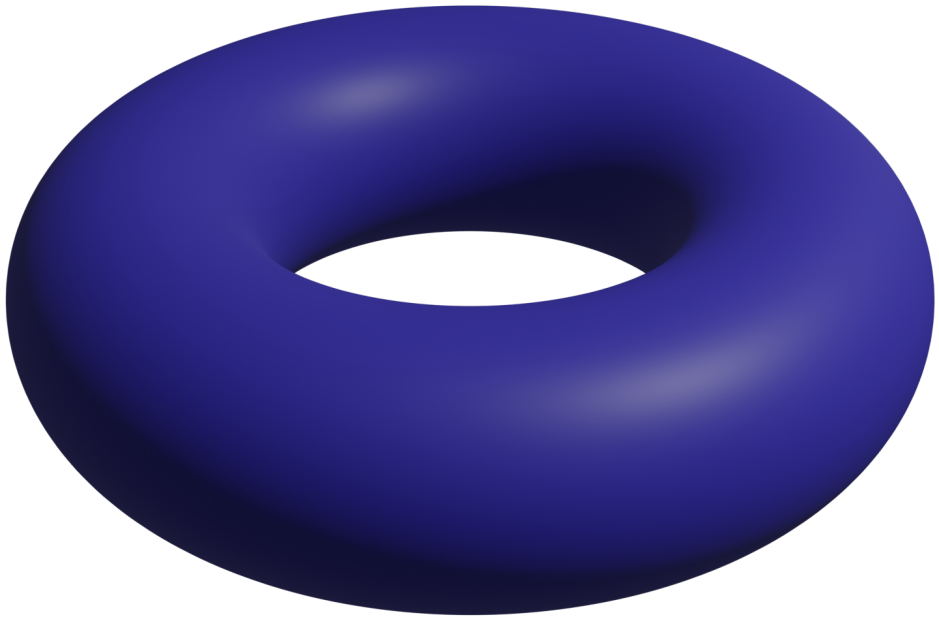
Solutions in $\mathbb{R}$

For example, if we look at solutions of the equation $y^2 = x^3 + ax + b$ in real numbers x, y, we get the kind of curve we are already familiar with:



Solutions in $\mathbb{C}$

Now, consider solutions of the equation $y^2 = x^3 + ax + b$ in complex numbers x, y. If we plot the solutions, we obtain the following kind of shape:



This geometric shape is called "a torus".

Integers modulo p

We fix a prime number p, i.e. a number only divisible by 1 and itself. For example $2, 3, 5, 7, 11, 13, \ldots$ are prime numbers. We are going to identify two integers a, b when they differ by a multiple of p, and we write

$$a \equiv b \pmod{p}.$$

For example, take $p = 7$. Then, in this number system, we have $11 \equiv 4 \pmod{7}$, hence 4 and 11 represent the same number. Therefore, the integers modulo 7 are:

$$\mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$$

Any integer a will be equal to one of the above up to a multiple of 7. More generally

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, ..., p-1\}.$$

Addition, multiplication, division

We can define addition, multiplication, division for elements of $\mathbb{Z}/p\mathbb{Z}$. For example, if $p = 5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

We also have inverses (i.e. "$\frac{1}{x}$") and divisions: For example $2 \times 3 \equiv 1 \pmod 5$, so 3 is the inverse of 2 modulo 5.

Solutions modulo p

Let $y^2 = x^3 + ax + b$ (with a, b integers) be an elliptic curve. Fix a prime number p. We can look for solutions "modulo p". For example, consider the equation:

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

and take $p = 7$. There are exactly 7 solutions in $\mathbb{Z}/7\mathbb{Z}$, which are:

$$(x, y) = (0, 0), (1, 3), (1, 4), (3, 3), (3, 4), (5, 2), (5, 5).$$

We write N_p for the number of solutions modulo p of the equation.

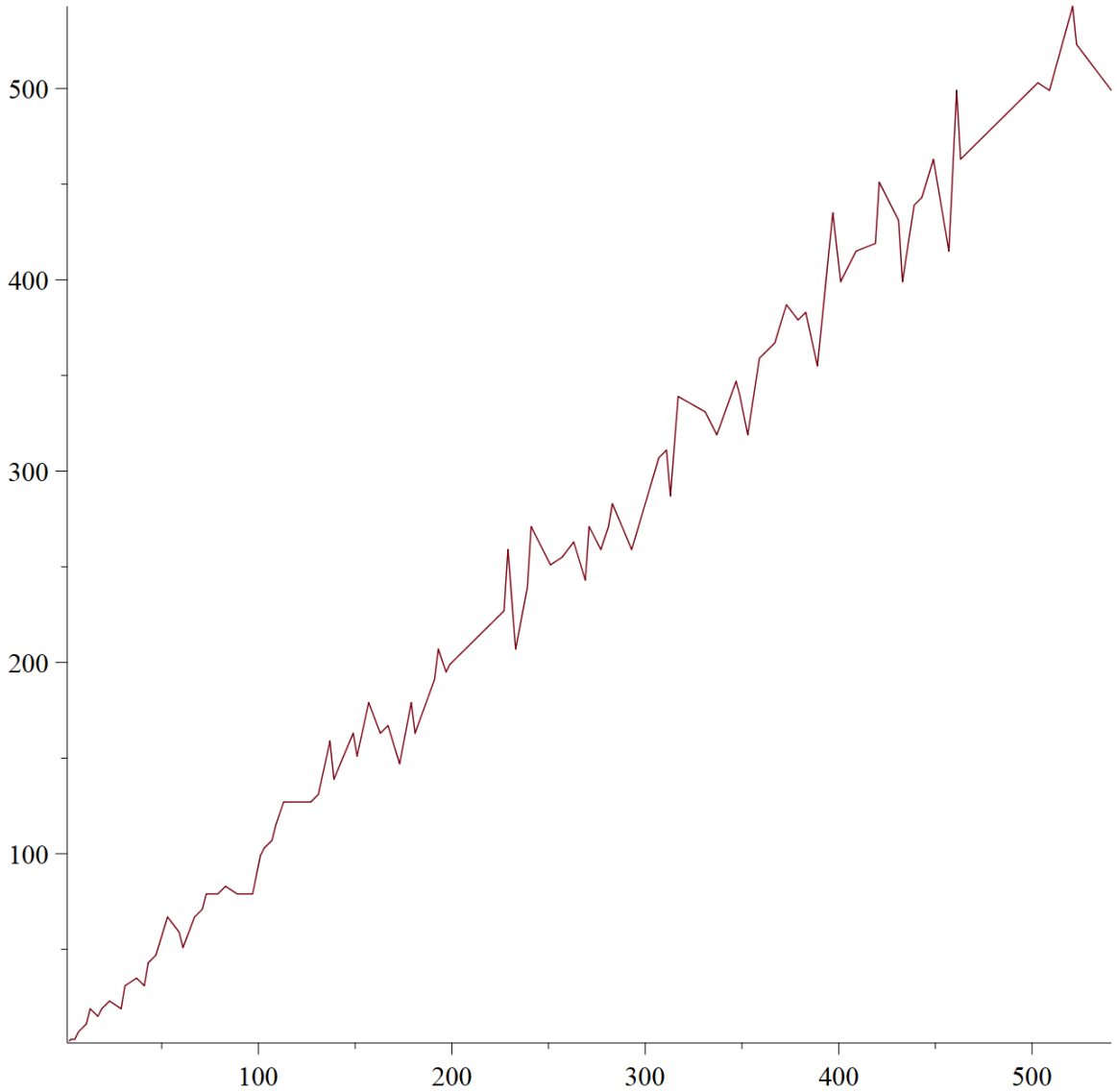
```
solutions := proc(p)
local x, y, R;
R := [ ];
for x from 0 to p - 1 do
for y from 0 to p - 1 do
if y^2 - x^3 - x mod p = 0 then
R := [op(R), [x, y]]
end if;
end do;
end do;
R;
end proc:

solutions(7)
```

$$[[0, 0], [1, 3], [1, 4], [3, 3], [3, 4], [5, 2], [5, 5]]$$

```
solutions(11)
```

$$[[0, 0], [5, 3], [5, 8], [7, 3], [7, 8], [8, 5], [8, 6], [9, 1], [9, 10], [10, 3], [10, 8]]$$

Graph of N_p



The number of solutions modulo p seems to be roughly equal to p

Approximation of N_p

In general, it is true that N_p is "roughly equal to p". More precisely:

Theorem

One has $|p - N_p| \leq 2\sqrt{p}$.

The number $a_p = p - N_p$ is an important quantity that will apear later.

Finite fields

We can go beyond $\mathbb{Z}/p\mathbb{Z}$ and consider more general "finite systems of numbers". Let p be a prime number and $n \geq 1$ an integer. There is a unique way to define addition, multiplication, division on a set with p^n elements. This system of numbers is denoted by $\mathbb{F}_{p^n}$. For example, for $p = 2$ and $n = 2$, $\mathbb{F}_4$ consists of four elements

$$\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$$

and addition and multiplication are defined as follows:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Solutions in $\mathbb{F}_{p^n}$

Again, we may look for solutions to the equation $y^2 = x^3 + ax + b$ in this new system of numbers $\mathbb{F}_{p^n}$. For example, the solutions of

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

in $\mathbb{F}_4$ are:

$$(0,0), (1,0), (\alpha, \alpha), (\beta, \beta).$$

In $\mathbb{Z}/2\mathbb{Z}$ we could only see the solutions $(0,0)$ and $(1,0)$. By extending our system of numbers to $\mathbb{F}_4$, we found two more solutions.

Zeta function

Consider an elliptic curve E defined by $y^2 = x^3 + ax + b$ (a, b integers). Let p be a prime number and write N_{p^n} for the number of solutions of this equation in $\mathbb{F}_{p^n}$.

Definition

Define the Zeta function of E at p as follows:

$$\zeta_{E,p}(t) = \exp\left(\sum_{n\geq 1} \frac{N_{p^n}}{n} t^n\right).$$

where exp is the exponential function $\exp(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \ldots$

This function knows about all the different numbers N_{p^n} for $n \geq 1$.

Weil conjectures

Grothendieck (1965) and Deligne (1974) proved the "Weil conjectures". In the case of elliptic curves, it says the following:

Theorem (Grothendieck 1965, Deligne 1974)

$\zeta_{E,p}(t)$ is a rational function. More precisely:

$$\zeta_{E,p}(t) = \frac{pt^2 - a_p t + 1}{(1-t)(1-pt)},$$

where $a_p = p - N_p$.

A similar result holds for any polynomial equation $P(x_1, \ldots, x_n) = 0$ with integer coefficients.

L-function

For each prime number p, we have defined a function $\zeta_{E,p}(t)$. Its denominator $pt^2 - a_p t + 1$ is the important part. We define a new function $L(E, s)$ by making the change of variable $t = p^{-s}$ and taking the product over all primes:

Definition

For any complex number s, we define

$$L(E, s) := \prod_p \frac{1}{p(p^{-s})^2 - a_p(p^{-s}) + 1}.$$

This function is called the Hasse–Weil Zeta function of E.

This function encapsulates all the different numbers N_{p^n} for all primes p and all $n \geq 1$ in a single object.

Riemann Zeta function

Why this definition? The function $L(E, s)$ is modeled on the famous "Riemann Zeta function" $\zeta(s)$, defined by

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

It shows up in several fields of mathematics, and has interesting properties. For example:

Theorem (Basel problem, Euler 1734)

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \frac{\pi^2}{6}.$$

Euler also showed that $\zeta(s)$ can be written as a product:

Theorem (Euler)

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

Analytic continuation

Furthermore, we can make sense (in a unique and rigorous way) of the value $\zeta(s)$ for any complex number s, except for $s = 1$. For example,

$$\zeta(-1) = -\frac{1}{12},\ \zeta(-2) = 0,\ \zeta(-3) = \frac{1}{120},\ \zeta(-4) = 0, \ldots$$

Around the point $s = 1$, $\zeta(s)$ looks like the function $\frac{1}{s-1}$, and the value at 1 is infinite:

$$\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots = \infty$$

Question

Can the function $L(E, s)$ also be extended to (almost) any value of s ?

Since the usual Riemann ζ function takes many interesting values, we can similarly expect that the values and coefficients of $L(E, s)$ will give useful information about E.

Taniyama–Shimura Conjecture

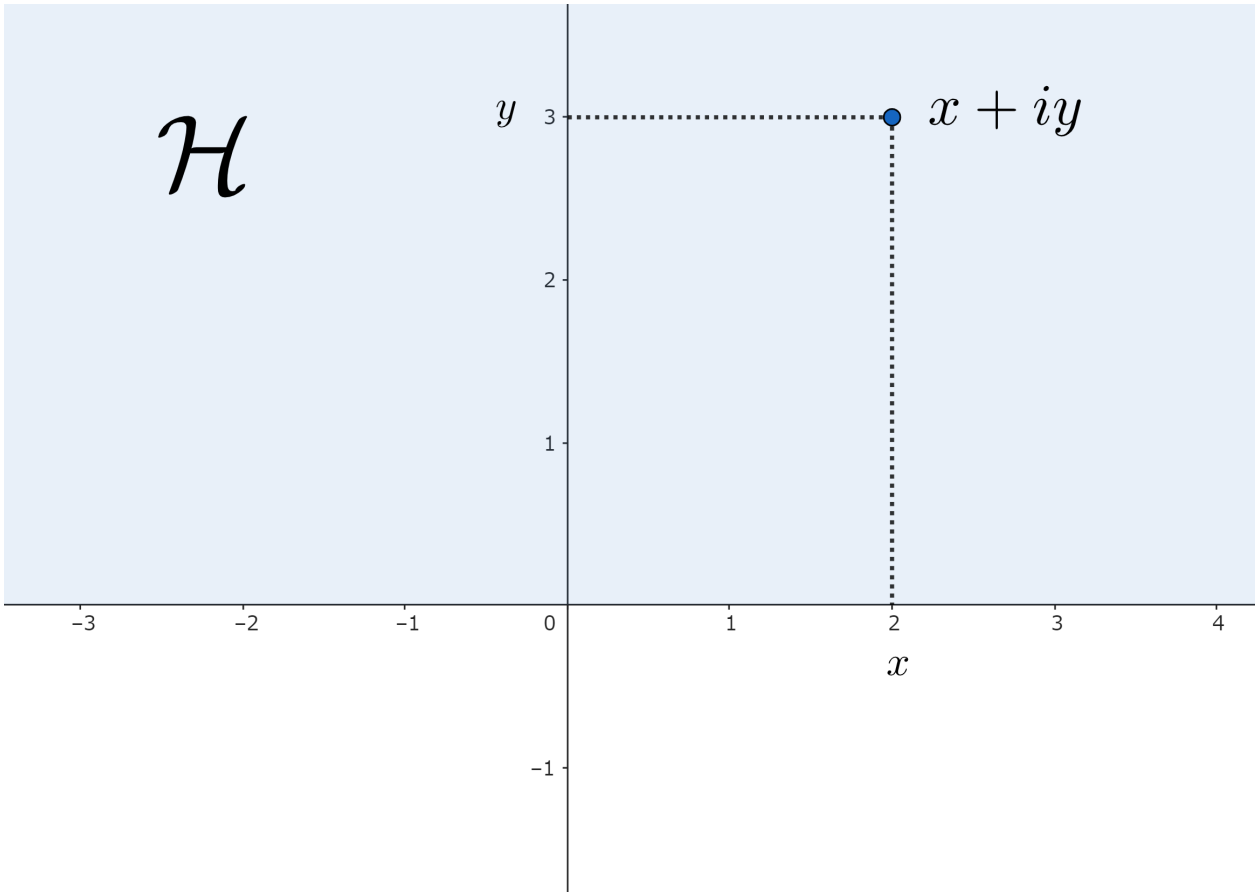
In 1955 at a conference in Tokyo, Taniyama–Shimura proposed the following conjecture (later proved by A. Wiles):

Conjecture

The function $L(E, s)$ is the L-function of a modular form.

Modular forms

Set $\mathcal{H} = \{z = x + iy \in \mathbb{C} \mid y > 0\}$ be the set of complex numbers with positive imaginary part.



Modular forms are certain functions defined on $\mathcal{H}$ that have "many symmetries".

Definition

Specifically, a function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight k (k is a positive integer) if it satisfies

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all integers a, b, c, d such that $ad - bc = 1$. In particular, if we take $a = b = d = 1$ and $c = 0$, we find that

$$f(z+1) = f(z)$$

hence f is periodic of period 1. This implies that we can write f as an infinite series:

$$f(z) = \sum_{n \geq 0} a_n q^n$$

where $q = e^{2i\pi z} = \cos(2\pi z) + i \sin(2\pi z)$.
When $a_0 = 0$, it is called a cusp form.

Elliptic curves and modular forms

- For an elliptic curve E over $\mathbb{Q}$, we have defined the L-function

$$L(E, s)$$

- On the other hand, if f is a cusp form $f(z) = \sum_{n \geq 1} a_n q^n$, we can define the L-function of f by

$$L(f, s) := \sum_{n \geq 1} \frac{a_n}{n^s}.$$

Theorem (A. Wiles, Breuil–Conrad–Diamond–Taylor 2001)

Let E be an elliptic curve over $\mathbb{Q}$. Then there exists a cusp form of weight 2 satisfying

$$L(E, s) = L(f, s).$$

We say that "any elliptic curve over $\mathbb{Q}$ is modular".

Fermat's Last Theorem

One of the most celebrated results that came out of these developments is the famous Theorem of Fermat, that he claimed to have proved in 1637 in his book *Arithmetica*:

Theorem (Fermat's Last Theorem)

For $n > 2$, the only integer solutions to the equation

$$z^n = x^n + y^n$$

are the trivial ones, i.e. $x = 0$ or $y = 0$.

This Theorem is a consequence of the modularity of elliptic curves. It was proved by Andrew Wiles in 1995 (with the help of his student Richard Taylor).

Langlands correspondence

This correspondence between elliptic curves over $\mathbb{Q}$ and modular forms is an example of a general philosophy proposed by Langlands in 1967.

In particular, this philosophy implies that any information about an elliptic curve E can be read on the "analytic" side, i.e. on the L-function $L(E, s)$.

Question

How is the rank of $E(\mathbb{Q})$ related to $L(E, s)$?

Order

Let $f(s)$ be a function defined in a neighborhood of a point s_0. If the function

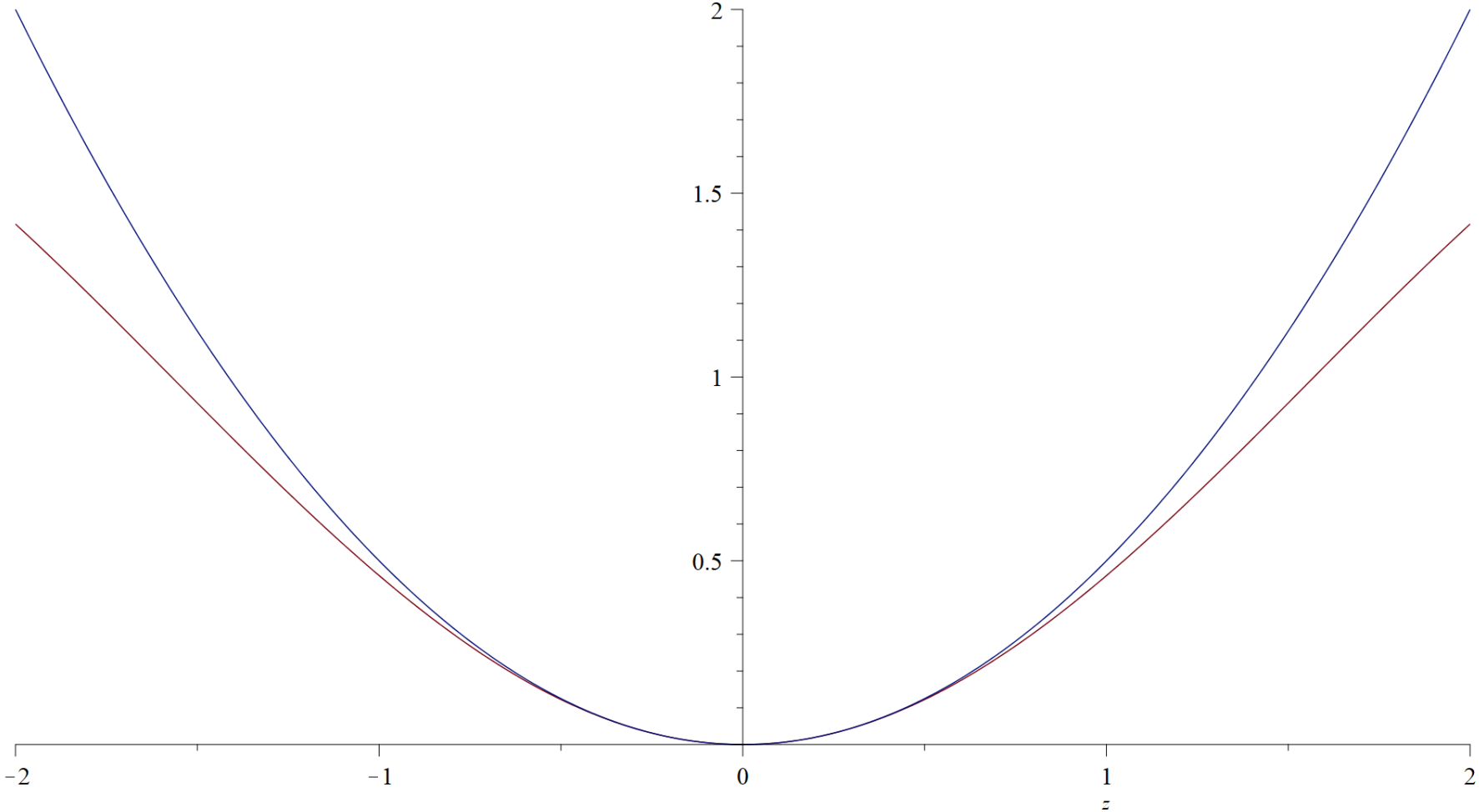
$$\frac{f(s)}{(s-s_0)^k}$$

converges to a nonzero value when s approaches s_0, then we say that $f(s)$ has a zero of order k at $s = s_0$. This means that $f(s)$ converges "as fast as" $(s-s_0)^k$ when s is close to s_0. For example, consider the function

$$f(s) = 1 - \cos(s)$$

When $s = 0$, we have $f(0) = 1 - 1 = 0$. If we plot this function, we get the following graph:

$f(s) = 1 - \cos(s)$ $\quad$ $g(s) = \frac{s^2}{2}$



Close to $s = 0$, we have $f(s) \approx \frac{s^2}{2}$. Therefore, $f(s)$ has a zero of order 2 at the point $s = 0$.

Birch–Swynnerton–Dyer Conjecture

Conjecture (Birch–Swynnerton–Dyer)

The rank of $E(\mathbb{Q})$ is equal to the order of the zero of the function $L(E, s)$ at the point $s = 1$.

Only certain special cases of this conjecture are known, but the general case is out of reach.

Consequence

This conjecture gives a way to "guess" the rank of an elliptic curve. Indeed, it has the following consequence:

$$\prod_{p \leq x} \frac{N_p}{p} \approx C \log(x)^r \quad \text{as } x \to \infty$$

where r is the rank of $E(\mathbb{Q})$ and N_p is the number of solutions modulo p.

Example

For the elliptic curve $y^2 = x^3 + x$, the function $F(x) = \prod_{p \leq x} \frac{N_p}{p}$ takes the following values at different values of x:

```
check(30)
```
0.5069433609

```
check(50)
```
0.3625797934

```
check(100)
```
0.2998054644

```
check(200)
```
0.4097726227

```
check(500)
```
0.2824604455

Hence, it appears that the function $F(x)$ is bounded. Since

$$F(x) \approx C \log(x)^r$$

this would indicate that the rank of $y^2 = x^3 + x$ is zero.