The Billing-Mahler Theorem

Crystal Xie

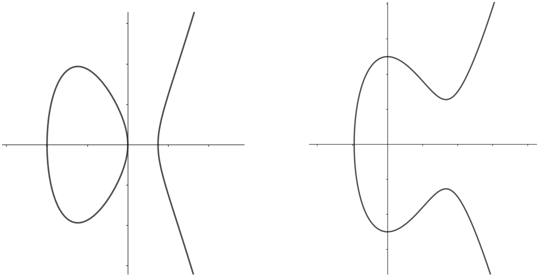
July 9, 2024

Elliptic Curve

An elliptic curve over $\mathbb{Q}$ is a non-singular curve given by

$$E = \left\{(x, y) \mid y^2 = f(x) = x^3 + ax^2 + bx + c\right\} \cup \{\mathcal{O}\},$$

where a, b, c are integers.



We want to find the rational points on curves like these.

The Group Law

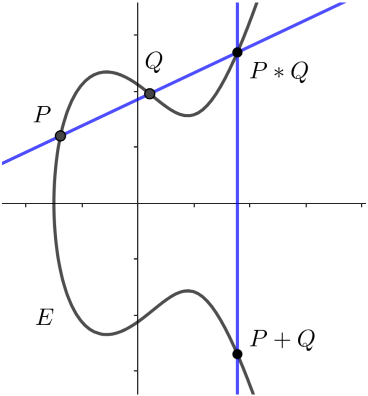
Let $P * Q$ be the third intersection with E of the line through P and Q.

The Group Law

Let $P * Q$ be the third intersection with E of the line through P and Q. Then let $P + Q$ be $\mathcal{O} * (P * Q)$.

The Group Law

Let $P * Q$ be the third intersection with E of the line through P and Q. Then let $P + Q$ be $\mathcal{O} * (P * Q)$.



The Group Law

Let $E(\mathbb{Q})$ denote the set of rational points (points with rational coordinates) on the elliptic curve E.

Proposition

The set $E(\mathbb{Q})$ is a group under the $+$ operation.

The Group Law

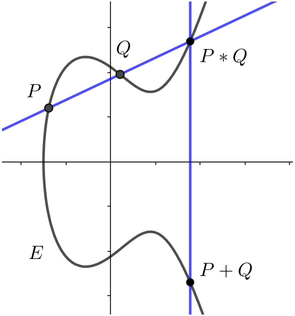
Let $E(\mathbb{Q})$ denote the set of rational points (points with rational coordinates) on the elliptic curve E.

Proposition

The set $E(\mathbb{Q})$ is a group under the $+$ operation.

Proof.

- Closure:
- Identity:
- Inverses:
- Associativity:



The Group Law

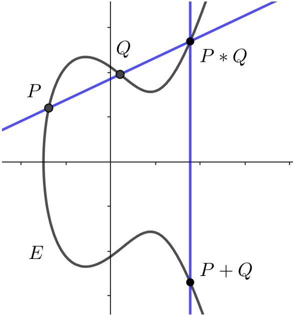
Let $E(\mathbb{Q})$ denote the set of rational points (points with rational coordinates) on the elliptic curve E.

Proposition

The set $E(\mathbb{Q})$ is a group under the $+$ operation.

Proof.

- Closure: From definition of $*$.
- Identity:
- Inverses:
- Associativity:



The Group Law

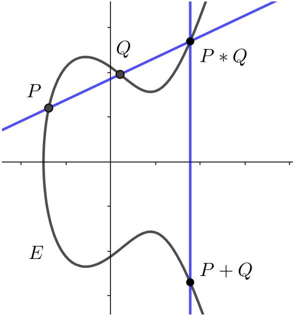
Let $E(\mathbb{Q})$ denote the set of rational points (points with rational coordinates) on the elliptic curve E.

Proposition

The set $E(\mathbb{Q})$ is a group under the $+$ operation.

Proof.

- Closure: From definition of $*$.
- Identity: Is the point $\mathcal{O}$.
- Inverses:
- Associativity:



The Group Law

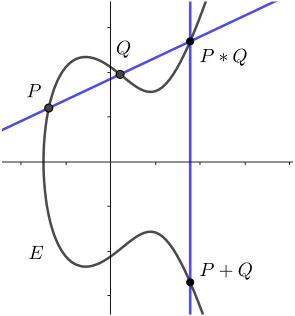
Let $E(\mathbb{Q})$ denote the set of rational points (points with rational coordinates) on the elliptic curve E.

Proposition

The set $E(\mathbb{Q})$ is a group under the $+$ operation.

Proof.

- Closure: From definition of $*$.
- Identity: Is the point $\mathcal{O}$.
- Inverses: Reflection over x-axis.
- Associativity:



The Group Law

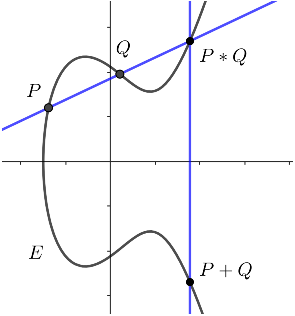
Let $E(\mathbb{Q})$ denote the set of rational points (points with rational coordinates) on the elliptic curve E.

Proposition

The set $E(\mathbb{Q})$ is a group under the $+$ operation.

Proof.

- Closure: From definition of $*$.
- Identity: Is the point $\mathcal{O}$.
- Inverses: Reflection over x-axis.
- Associativity: Can be checked using explicit formulas for the $+$ operation. □



The Group Law

One way that the group law is useful, is that given an initial set of rational points, we can obtain more rational points using the group law.

Example

Let E be the elliptic curve given by

$$y^2 = f(x) = x^3 - 4x + 4.$$

Plugging in $x = 0$ and $x = 1$ gives solutions $(0, \pm 2)$ and $(1, \pm 1)$.

The Group Law

One way that the group law is useful, is that given an initial set of rational points, we can obtain more rational points using the group law.

Example

Let E be the elliptic curve given by

$$y^2 = f(x) = x^3 - 4x + 4.$$

Plugging in $x = 0$ and $x = 1$ gives solutions $(0, \pm 2)$ and $(1, \pm 1)$. Let $A = (0, -2)$ and $B = (1, 1)$. Let's add these two.

The Group Law

One way that the group law is useful, is that given an initial set of rational points, we can obtain more rational points using the group law.

Example

Let E be the elliptic curve given by

$$y^2 = f(x) = x^3 - 4x + 4.$$

Plugging in $x = 0$ and $x = 1$ gives solutions $(0, \pm 2)$ and $(1, \pm 1)$. Let $A = (0, -2)$ and $B = (1, 1)$. Let's add these two.
The line through A and B is $y = 3x - 2$, so we plug back into $y^2 = f(x)$ to get $0 = x^3 - 9x^2 + 8x$. Then we factor to find that $x = 0$, $x = 1$, or $x = 8$.

The Group Law

One way that the group law is useful, is that given an initial set of rational points, we can obtain more rational points using the group law.

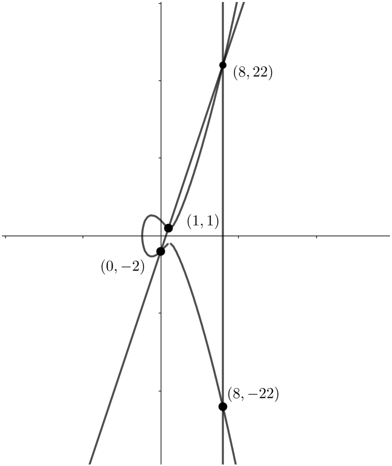
Example

Let E be the elliptic curve given by

$$y^2 = f(x) = x^3 - 4x + 4.$$

Plugging in $x = 0$ and $x = 1$ gives solutions $(0, \pm 2)$ and $(1, \pm 1)$. Let $A = (0, -2)$ and $B = (1, 1)$. Let's add these two.
The line through A and B is $y = 3x - 2$, so we plug back into $y^2 = f(x)$ to get $0 = x^3 - 9x^2 + 8x$. Then we factor to find that $x = 0$, $x = 1$, or $x = 8$.
Plugging $x = 8$ into $y^2 = f(x)$, we get $A * B = (8, 22)$, and $A + B = (8, -22)$.

The Group Law



Mordell's Theorem

Theorem (Mordell)

The group $E(\mathbb{Q})$ of rational points on E is finitely generated.

Mordell's Theorem

Theorem (Mordell)

The group $E(\mathbb{Q})$ of rational points on E is finitely generated.

So, for any elliptic curve E (defined over $\mathbb{Q}$), there is a finite set of rational points such that we can find all other rational points on E by adding points from the starting set in various ways.

Points of Finite Order

Mordell's theorem says we have a way of finding all the rational points on E. But what if we want to narrow our search to some special rational points, say just the rational points that have finite order?

Points of Finite Order

Mordell's theorem says we have a way of finding all the rational points on E. But what if we want to narrow our search to some special rational points, say just the rational points that have finite order?

Definition

A point of finite order is a point P such that

$$\underbrace{P + P + \cdots + P}_{n \text{ times}} = nP = \mathcal{O}$$

for some non-negative integer n. We may also say that P is a *torsion point*.

Points of Finite Order

Before we look at another interesting result, we will need to know about a certain important value associated with polynomials:

Points of Finite Order

Before we look at another interesting result, we will need to know about a certain important value associated with polynomials:

Definition

The discriminant of a cubic $x^3 + ax^2 + bx + c$ is

$$D_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Points of Finite Order

Before we look at another interesting result, we will need to know about a certain important value associated with polynomials:

Definition

The discriminant of a cubic $x^3 + ax^2 + bx + c$ is

$$D_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

We can check that this is $(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$, where x_1, x_2, x_3 are the roots of the cubic, so the discriminant is nonzero if and only if the roots are all distinct.

Points of Finite Order

Theorem (Nagell-Lutz)

If $P = (x, y)$ is a rational torsion point (rational point of finite order) on elliptic curve E given by

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

then:

- *x and y are both integers*
- *either $y = 0$ or y divides the discriminant of f.*

Points of Finite Order

Theorem (Nagell-Lutz)

If $P = (x, y)$ is a rational torsion point (rational point of finite order) on elliptic curve E given by

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

then:

- *x and y are both integers*
- *either $y = 0$ or y divides the discriminant of f.*

So, through the Nagell-Lutz theorem we can obtain a complete list of the rational points of finite order in a finite number of steps.

Points of Finite Order

Example

Find the rational torsion points on the elliptic curve E given by

$$y^2 = f(x) = x^3 - 4x + 3.$$

Points of Finite Order

Example

Find the rational torsion points on the elliptic curve E given by

$$y^2 = f(x) = x^3 - 4x + 3.$$

The discriminant is $D_f = 13$, so assuming $y \neq 0$, we have $y \mid 13$ due to the Nagell-Lutz theorem.

Points of Finite Order

Example

Find the rational torsion points on the elliptic curve E given by

$$y^2 = f(x) = x^3 - 4x + 3.$$

The discriminant is $D_f = 13$, so assuming $y \neq 0$, we have $y \mid 13$ due to the Nagell-Lutz theorem. We can then test $y^2 = 1$ and $y^2 = 169$.

Points of Finite Order

Example

Find the rational torsion points on the elliptic curve E given by

$$y^2 = f(x) = x^3 - 4x + 3.$$

The discriminant is $D_f = 13$, so assuming $y \neq 0$, we have $y \mid 13$ due to the Nagell-Lutz theorem. We can then test $y^2 = 1$ and $y^2 = 169$.

For $y^2 = 1$, any potential rational solutions will have an x-coordinate satisfying $0 = x^3 - 4x + 2$. The rational roots of $x^3 - 4x + 2$ must divide 2, so they would be in $\{\pm 1, \pm 2\}$. Checking each possibility $\implies$ no rational roots in this case.

Points of Finite Order

Example

Find the rational torsion points on the elliptic curve E given by

$$y^2 = f(x) = x^3 - 4x + 3.$$

The discriminant is $D_f = 13$, so assuming $y \neq 0$, we have $y \mid 13$ due to the Nagell-Lutz theorem. We can then test $y^2 = 1$ and $y^2 = 169$.

For $y^2 = 1$, any potential rational solutions will have an x-coordinate satisfying $0 = x^3 - 4x + 2$. The rational roots of $x^3 - 4x + 2$ must divide 2, so they would be in $\{\pm 1, \pm 2\}$. Checking each possibility $\implies$ no rational roots in this case.

We can do the same thing for the case $y^2 = 169$, but we also get no rational roots in this case.

Points of Finite Order

Example

Find the rational torsion points on the elliptic curve E given by

$$y^2 = f(x) = x^3 - 4x + 3.$$

The discriminant is $D_f = 13$, so assuming $y \neq 0$, we have $y \mid 13$ due to the Nagell-Lutz theorem. We can then test $y^2 = 1$ and $y^2 = 169$.

For $y^2 = 1$, any potential rational solutions will have an x-coordinate satisfying $0 = x^3 - 4x + 2$. The rational roots of $x^3 - 4x + 2$ must divide 2, so they would be in $\{\pm 1, \pm 2\}$. Checking each possibility $\implies$ no rational roots in this case.

We can do the same thing for the case $y^2 = 169$, but we also get no rational roots in this case.

So, the only possibility is when $y = 0$. Rational roots to $0 = x^3 - 4x + 3$ would divide 3, and checking each possibility, we get $(1, 0)$ as the only rational torsion point on E.

Possible Orders

It turns out that we can write down elliptic curves with rational points that have order 2, 3, 4, 5, 6, 7, 8, 9, 10, and 12, but never an elliptic curve with a rational point of order 11. This is what is known as the Billing-Mahler theorem (proven in 1940):

Possible Orders

It turns out that we can write down elliptic curves with rational points that have order 2, 3, 4, 5, 6, 7, 8, 9, 10, and 12, but never an elliptic curve with a rational point of order 11. This is what is known as the Billing-Mahler theorem (proven in 1940):

Theorem (Billing-Mahler)

There are no rational points of order 11 on any elliptic curve E defined over $\mathbb{Q}$.

Possible Orders

It turns out that we can write down elliptic curves with rational points that have order 2, 3, 4, 5, 6, 7, 8, 9, 10, and 12, but never an elliptic curve with a rational point of order 11. This is what is known as the Billing-Mahler theorem (proven in 1940):

Theorem (Billing-Mahler)

There are no rational points of order 11 on any elliptic curve E defined over $\mathbb{Q}$.

In fact, orders of 1 through 10, as well as 12, are the *only* orders possible for an elliptic curve E over $\mathbb{Q}$. This is Mazur's theorem, proven in 1970.

Possible Orders

It turns out that we can write down elliptic curves with rational points that have order 2, 3, 4, 5, 6, 7, 8, 9, 10, and 12, but never an elliptic curve with a rational point of order 11. This is what is known as the Billing-Mahler theorem (proven in 1940):

Theorem (Billing-Mahler)

There are no rational points of order 11 on any elliptic curve E defined over $\mathbb{Q}$.

In fact, orders of 1 through 10, as well as 12, are the *only* orders possible for an elliptic curve E over $\mathbb{Q}$. This is Mazur's theorem, proven in 1970.

Theorem (Mazur)

If $E(\mathbb{Q})$ has a point of finite order m, then either $1 \leq m \leq 10$ or $m = 12$.