Mordell-Weil and Billing-Mahler Theorems

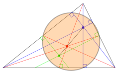
An Overview

Agniv Sarkar[1]

[1] Presenting author, agnivsarkar@proofschool.org

July 5, 2022

Table of Contents



Introduction

Why the Name?

First, ellipses are not elliptic curves.

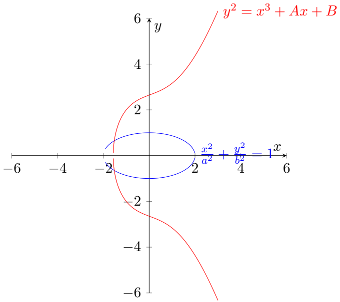


Figure: Example of Ellipse and Elliptic Curve

Ok but Why?

In order to find the circumference of an ellipse, people used elliptic integrals,

$$4a \int_0^1 \sqrt{\frac{1 - e^2 t^2}{1 - t^2}} dx.$$

The integrand $u(t)$ satisfies

$$u^2(1 - t^2) = 1 - e^2 t^2,$$

defining an elliptic curve.

Definition(s)

Definition

An elliptic curve E is a nonsingular projective curve over a field K given by the set

$$E = \{(x, y) : y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathbb{O}\}$$

for some constants a, b, c in K such that the discriminant is nonzero, and the point $\mathbb{O}$ is the point at infinity.

Definition(s)

Definition

An elliptic curve E is a nonsingular projective curve over a field K given by the set

$$E = \{(x, y) : y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathbb{O}\}$$

for some constants a, b, c in K such that the discriminant is nonzero, and the point $\mathbb{O}$ is the point at infinity.

Definition

A projective curve is the set of zeros of a homogeneous polynomial of three variables: $F(x, y, z) = 0$. We will assume that F has coefficients in $\mathbb{Z}$.

History

- Diophantus: Solved the earliest recorded elliptic curve $(Y(a - Y) = X^3 - X)$

History

- Diophantus: Solved the earliest recorded elliptic curve $(Y(a - Y) = X^3 - X)$
- Fermat: He conjectured some integer solutions for $y^2 = x^3 - 2$.

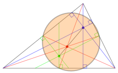
History

- Diophantus: Solved the earliest recorded elliptic curve $(Y(a-Y) = X^3 - X)$
- Fermat: He conjectured some integer solutions for $y^2 = x^3 - 2$.
- Weierstrass: Proved that all elliptic curves could take a much simpler form.

History

- Diophantus: Solved the earliest recorded elliptic curve $(Y(a-Y) = X^3 - X)$
- Fermat: He conjectured some integer solutions for $y^2 = x^3 - 2$.
- Weierstrass: Proved that all elliptic curves could take a much simpler form.
- Mordell: Studied curves of the form $y^2 = x^3 + n$, with n being a nonnegative integer.

History



- Diophantus: Solved the earliest recorded elliptic curve $(Y(a-Y) = X^3 - X)$
- Fermat: He conjectured some integer solutions for $y^2 = x^3 - 2$.
- Weierstrass: Proved that all elliptic curves could take a much simpler form.
- Mordell: Studied curves of the form $y^2 = x^3 + n$, with n being a nonnegative integer.
- Weil: Gave the first proof of the Mordell-Weil Theorem! Also chose ϕ as the empty set symbol

History

- Diophantus: Solved the earliest recorded elliptic curve $(Y(a-Y) = X^3 - X)$
- Fermat: He conjectured some integer solutions for $y^2 = x^3 - 2$.
- Weierstrass: Proved that all elliptic curves could take a much simpler form.
- Mordell: Studied curves of the form $y^2 = x^3 + n$, with n being a nonnegative integer.
- Weil: Gave the first proof of the Mordell-Weil Theorem! Also chose ϕ as the empty set symbol
- Billing, Mahler: Proved their own theorem about torsion points.

Abelian Group Structure

The Group Law

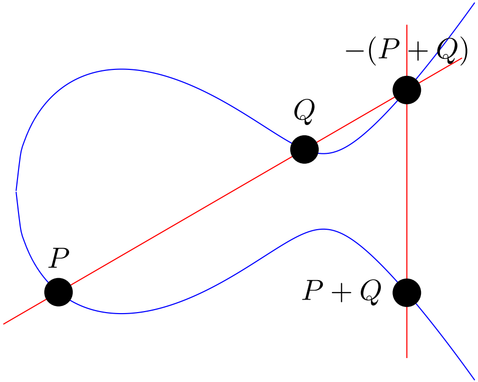
Definition

On a curve, we define the addition of any two given points, P and Q to be $P+Q$ such that it is the negative of the third intersection of the line drawn through P and Q and the cubic. The composition of P upon P, or $P+P=2P$, is the negative of the intersection of the tangent line to the curve at P to the curve.

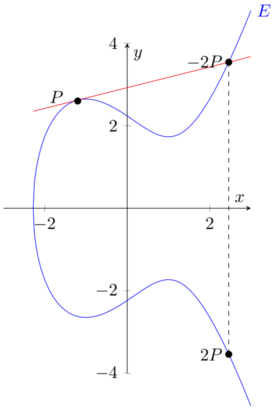
Group Law:

1. Identity Element, $P+\mathbb{O}=\mathbb{O}+P=P$
2. Inverse Element, $P+(-P)=\mathbb{O}$
3. Associativity, $P+(Q+R)=(P+Q)+R$
4. Commutativity, $P+Q=Q+P$

Example of Addition



Example of $2P$



Closed Formula

Because of this geometric definition, one can find a closed formula for the addition law.

Closed Formula

Because of this geometric definition, one can find a closed formula for the addition law. We simply look at the line between two points (or the tangent), and look for the third intersection with the line and the curve.

Closed Formula

Because of this geometric definition, one can find a closed formula for the addition law. We simply look at the line between two points (or the tangent), and look for the third intersection with the line and the curve. Let

$$y = mx + b$$

be the line of intersection of points $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$. We can find m through the slope formula or derivatives. The closed formula for addition is then

$$P_1 + P_2 = (x_1, y_1) + (x_2, y_2) = (m^2 - x_1 - x_2, -mx_3 - b) = (x_3, -y_3).$$

Quick Definition!

Definition

Let E be an elliptic curve over K in the form $y^2 = f(x)$. The set of K-*rational points* on E is the set

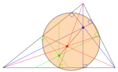
$$\{(x, y) \in K \times K | y^2 = f(x)\},$$

which we will denote as $E(K)$.

The set of $\mathbb{Q}$-rational points on E is equivalent to saying the set of rational points on E.

Mordell-Weil

Mordell Weil Theorem



Theorem

(Mordell-Weil) For elliptic curves over the rationals $\mathbb{Q}$, the group of rational points is always finitely generated.

Mordell Weil Theorem Definitions

Definition

For a rational number $x = \frac{a}{b}$, the height of x is given by

$$\mathcal{H}(x) = \max(|a|, |b|).$$

Elliptic Curve Height

Definition

For an elliptic curve E over $\mathbb{Q}$, the height of a rational point $P = (x, y)$ on E is

$$\mathcal{H}(P) = \mathcal{H}(x), \mathcal{H}(\mathbb{O}) = 1.$$

The small height of a point is simply

$$h(P) = \log \mathcal{H}(P),$$

or it is 0 if $\mathcal{H}(P) = 0$.

Mordell Weil Theorem Assumptions

In order to prove Mordell-Weil, we would normally need to prove 4 different things.

- Finiteness Property of $\mathcal{H}$ on $E(\mathbb{Q})$
- Height of P and P_0 where P_0 is some given point on E satisfies $h(P+P_0) \leq 2h(P) + \kappa_0$ where κ_0 depends on a, b, c, P_0.
- Doubling the point increases the height, or $h(2P) \geq 4h(P) - \kappa$ where κ is dependent on a, b, and c.
- Denote $2E(\mathbb{Q})$ to be the subgroup of $E(\mathbb{Q})$ which contains only points of the form $2P$ where $P \in E(\mathbb{Q})$. Then, $E(\mathbb{Q})/2E(\mathbb{Q})$ is a finite group.

Mordell Weil Theorem Proof

Let $Q_1, Q_2, Q_3, \ldots Q_n$ be a finite number of coset representatives. So, there is some index $1 \leq i_1 \leq n$ dependent on P such that $P - Q_{i_1} = 2P_1, P_1 \in E(\mathbb{Q})$.

Mordell Weil Theorem Proof

Let $Q_1, Q_2, Q_3, \ldots Q_n$ be a finite number of coset representatives. So, there is some index $1 \leq i_1 \leq n$ dependent on P such that $P - Q_{i_1} = 2P_1, P_1 \in E(\mathbb{Q})$.We can recursively expand on P_i to get

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \ldots + 2^{m-1}Q_{i_m} + 2^m P_m.$$

Mordell Weil Theorem Proof

Let $Q_1, Q_2, Q_3, \ldots Q_n$ be a finite number of coset representatives. So, there is some index $1 \leq i_1 \leq n$ dependent on P such that $P - Q_{i_1} = 2P_1, P_1 \in E(\mathbb{Q})$.We can recursively expand on P_i to get

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \ldots + 2^{m-1}Q_{i_m} + 2^m P_m.$$

Set $P = -Q_i$. By the second property, we get

$$h(P - Q_i) \leq 2h(P) + \kappa_i, \forall P \in E(\mathbb{Q}).$$

We can do this for each coset and get n different κ_i. Denote κ' as the largest.

Cool Equation Time

$$
\begin{aligned}
4h(P_j) &\leq h(2P_j) + \kappa \\
&= h(P_{j-1} - Q_{i_j}) + \kappa \\
&\leq 2h(P_{j-1}) + \kappa' + \kappa
\end{aligned}
$$

Cooler Equation Time

$$
\begin{aligned}
h(P_j) &\leq \frac{h(P_{j-1})}{2} + \frac{\kappa' + \kappa}{4} \\
&= \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa)) \\
&\leq \frac{3}{4}h(P_{j-1}) \\
&\vdots \\
h(P_m) &\leq \kappa' + \kappa
\end{aligned}
$$

What the Cool Equations Mean

So, starting with $h(P_{j-1}) \geq \kappa' + \kappa$, as $h(P_j) \leq \frac{3}{4}h(P_{i-1})$. As j gets larger, $h(P_j)$ trends to 0. There must be an m such that $h(P_m) \leq \kappa' + \kappa$.

What the Cool Equations Mean

So, starting with $h(P_{j-1}) \geq \kappa' + \kappa$, as $h(P_j) \leq \frac{3}{4}h(P_{i-1})$. As j gets larger, $h(P_j)$ trends to 0. There must be an m such that $h(P_m) \leq \kappa' + \kappa$. Since $h(P_m) \leq \kappa' + \kappa$, there are a finite number of possible P_m. So,

$$\{Q_1, Q_2, \ldots, Q_n\} \cup \{P_m \in E(\mathbb{Q}) : h(P_m) \leq \kappa' + \kappa\}$$

finitely generate $E(\mathbb{Q})$.
This proves that the group of rational points on an elliptic curve are finitely generated.

Billing-Mahler

Billing Mahler Theorem

Theorem

(Billing-Mahler) An elliptic curve defined over $\mathbb{Q}$ does not have a rational torsion point of order 11.

Billing Mahler Definitions

Definition

A point $P \in E : y^2 = f(x) = x^3 + ax^2 + bx + c$ with finite order m means that there exists a positive integer m such that

$$mP = P + P + \ldots + P = \mathbb{O}.$$

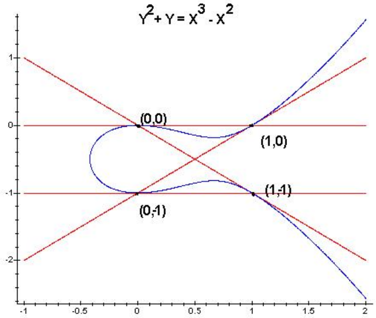
Definition

The set of points $E[m]$ is the set of m-torsion points, meaning

$$E[m] = \{P \in E(\overline{\mathbb{Q}}) | mP = \mathbb{O}\}.$$

The set of all rational torsion points on a curve E will be denoted as $E(\mathbb{Q})_{tors}$.

An example of $E[2]$



It may be interesting to some that $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$. A further proof of this is within [1].

Billing Mahler Proof Outline

Assume to the contrary that there is an 11-torsion point on some curve E.

Billing Mahler Proof Outline

Assume to the contrary that there is an 11-torsion point on some curve E. We can then look at multiples of this point in the projective plane and lines between points. Multiples of rational points on a curve are rational, so we can show with the assumption there are more than 5 rational points.

Billing Mahler Proof Outline

Assume to the contrary that there is an 11-torsion point on some curve E. We can then look at multiples of this point in the projective plane and lines between points. Multiples of rational points on a curve are rational, so we can show with the assumption there are more than 5 rational points. Through remapping of coordinates, we can then try to find the number of rational points on

$$E : y^2 = x^3 - 4x^2 + 16.$$

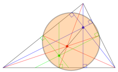
Billing Mahler Proof Outline

Assume to the contrary that there is an 11-torsion point on some curve E. We can then look at multiples of this point in the projective plane and lines between points. Multiples of rational points on a curve are rational, so we can show with the assumption there are more than 5 rational points. Through remapping of coordinates, we can then try to find the number of rational points on

$$E : y^2 = x^3 - 4x^2 + 16.$$

By [2], the solution set $E(\mathbb{Q})$ has order 5. So, we would need to show that the rank of this is 0, as then it would mean that there are exactly 5 rational points on E, and no more.

Billing Mahler Proof Outline



This now becomes an algebraic number theory problem. Due to time constraints, I will not actually prove this in the talk. Sorry!

Billing Mahler Proof Outline

This now becomes an algebraic number theory problem. Due to time constraints, I will not actually prove this in the talk. Sorry! However, there are only 5 rational points on that curve, contradicting the original claim of there being any 11-torsion points! People spent a long time searching for one ...

Elliptic Curves in the Real World

Elliptic Curve Cryptography

ECC, or Elliptic Curve Cryptography, is an extremely powerful form of cryptography used today. This is a lot more secure than RSA, because elliptic curves on their own are much harder to understand. By applying it to a finite field, the group law still holds, providing a pretty strong encryption service.

Elliptic Curve Cryptography

ECC, or Elliptic Curve Cryptography, is an extremely powerful form of cryptography used today. This is a lot more secure than RSA, because elliptic curves on their own are much harder to understand. By applying it to a finite field, the group law still holds, providing a pretty strong encryption service. The reason torsion points are interesting is because of how ECC determines what secret code to send. It takes the secret message, a, and some original point P, and sends the message aP.

Conclusion

Conclusion

I hope that gives a healthy synopsis on elliptic curves and at least one of their uses!

References I

J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106. Springer, 2009.

T. Nagell, "Sur les propriétés arithmétiques des cubiques planes du premier genre," *Acta mathematica*, vol. 52, pp. 93–126, 1929.

Thank you!

Thank you for listening! Questions?