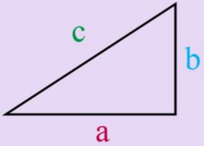
Properties of Elliptic Curves

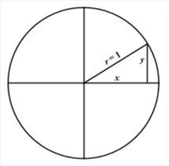
Anuj Sakarda, Jerry Tan, and Armaan Tipirneni

December 11, 2020

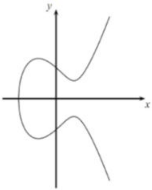
What are Elliptic Curves?



$a^2 + b^2 = c^2$



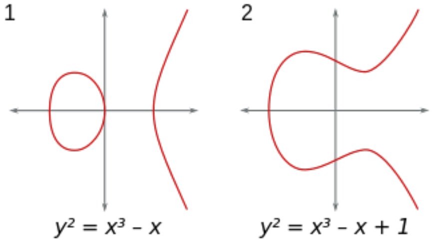
$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$



What are Elliptic Curves?

Definition (Elliptic Curve)

An elliptic curve is any curve that is birationally equivalent to a curve with the equation $y^2 = f(x) = x^3 + ax^2 + bx + c$.



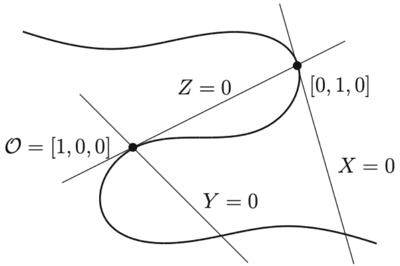
Weierstrass Normal Form

Theorem

The equation of any cubic curve with a rational point can be written in the form

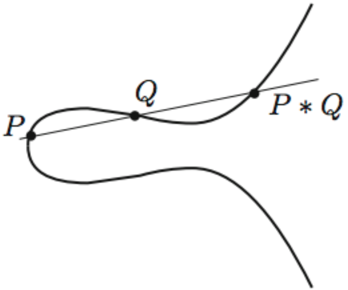
$$y^2 = 4x^3 - g_2 x - g_3.$$

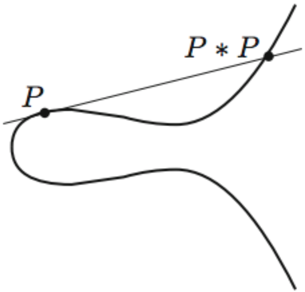
where a rational point is a point with rational coordinates.



Definition

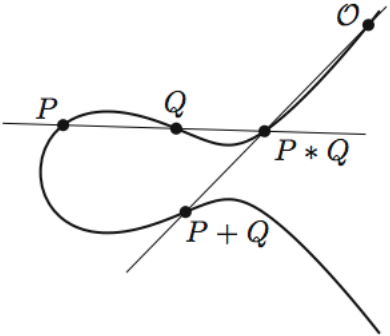
Given two points P and Q, denote $P * Q$ as the third point of intersection of the line through P and Q and the cubic.





Definition

Define $P + Q = O * (P * Q)$



What is a Group?

Definition

An abelian group *is a set of elements with an operation that satisfying the following 5 axioms*

(1) Closure.

(2) Associativity.

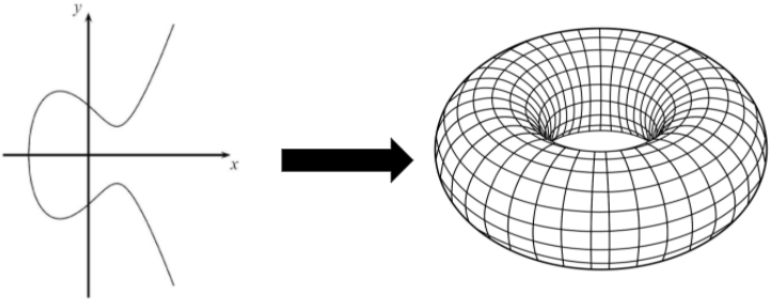
(3) Identity.

(4) Invertibility.

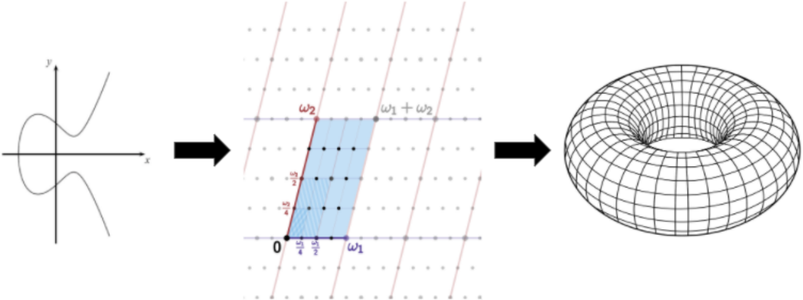
(5) Commutativity.

The "+" operation over an elliptic curve satisfies the abelian group axioms.

Visualizing Elliptic Curves



Visualizing Elliptic Curves



Lattices and Curves

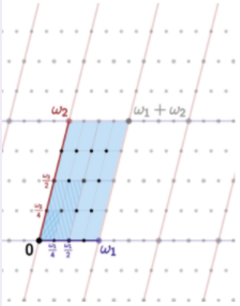
There is a bijective correspondence between lattices and complex elliptic curves.

The Weierstrass normal form of E_L (the corresponding elliptic curve) is $y^2 = 4x^3 - g_2(L)x - g_3(L)$ where $g_2(L) = 60\sum_{L^*} \frac{1}{\omega^4}$ and $g_3(L) = 140\sum_{L^*} \frac{1}{\omega^6}$ where L^* is L without the element 0.

An inverse map called the j-invariant exists

Addition works by modding out by the lattice

E.g. $(0.5\omega_1 + 0.5\omega_2)$
$+(0.5\omega_1 + 0.75\omega_2) \equiv 0.25\omega_2$



Animation can be found at
`https://en.wikipedia.org/wiki/Torus#/media/File:Torus_from_rectangle.gif`

Mordell-Weil

We are now ready to present the main subject of our study of rational points on elliptic curves, the Mordell-Weil Theorem.

Theorem (Mordell-Weil)

If a non-singular rational cubic curve has a rational point, then the group of rational points is finitely generated. In particular, if C is a non-singular cubic curve given by

$$C : y^2 = x^3 + ax^2 + bx,$$

where a, b are integers, then the group of rational points $C(\mathbb{Q})$ is a finitely generated abelian group.

Mordell-Weil

Definition

We define the height function H for a rational number $x = \dfrac{a}{b}$ as

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

where a and b are relatively prime integers.
Further, $h(x) = \log H(x)$. The height of a point is the height of its $x-$coordinate.

Proof of Mordell-Weil

We will break the proof down into four main lemmas.

Mordell-Weil

Lemma (Lemma 1)

For every real number M, the set

$$\{P \in C(\mathbb{Q}) : h(P) \leq M\}$$

is finite.

Proof Outline

- Height of x-coordinate of P is bounded
- Finite number of choices for numerator and denominator

Mordell-Weil

Lemma (Lemma 2)

Let P_0 be a fixed rational point of C. There is a constant κ_0 that depends on P_0 and on a, b, and c, so that

$$h(P + P_0) \leq 2h(P) + \kappa_0 \quad \textit{for all } P \in C(\mathbb{Q})$$

Proof Outline

- Use explicit formula for x-coordinate of $P + P_0$:

$$\xi + x + x_0 = \lambda^2 - a \text{ with } \lambda = \frac{y - y_0}{x - x_0}$$

- Work with height function, equation of curve, and triangle inequality

Mordell-Weil

Lemma (Lemma 3)

There is a constant κ, depending on a, b, and c, so that

$$h(2P) \geq 4h(P) - \kappa \quad \text{for all } P \in C(\mathbb{Q}).$$

Proof Outline

- Equivalent to fact about polynomials P and Q: Let $d = \max\{\deg(P), \deg(Q)\}$. There are constants κ_1 and κ_2, so that for all rational m/n that are not roots of Q,

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{P(m/n)}{Q(m/n)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2.$$

- Work with height function, equation of curve, and triangle inequality

Mordell-Weil

Lemma (Weak Mordell-Weil Theorem)

Denote $\Gamma = C(\mathbb{Q})$.
Let the notation 2Γ *denote the subgroup of* Γ *consisting of points that are twice other points.*
Then $(\Gamma : 2\Gamma)$, *the index of the subgroup* 2Γ *in* Γ, *is finite.*

Proof Outline

- Let $\overline{C}$ be given by $y^2 = x^3 + \overline{a}x^2 + \overline{b}x$ where $\overline{a} = -2a, \overline{b} = a^2 - 4b$
- Consider maps $\phi : C \to \overline{C}$ and $\psi : \overline{C} \to C$
- $\phi \circ \psi$ and $\psi \circ \phi$ are both multiplication by two maps.

Mordell-Weil

Theorem (Descent Theorem)

Let Γ be an abelian group, and suppose that there is a function $h : \Gamma \longrightarrow [0, \infty)$ with the following properties:

1. *For every real number M, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite.*
2. *For every $P_0 \in \Gamma$ there is a constant κ_0 so that*
$$h(P + P_0) \leq 2h(P) + \kappa_0 \quad \text{for all } P \in \Gamma.$$
3. *There is a constant κ so that*
$$h(2P) \geq 4h(P) - \kappa \quad \text{for all } P \in \Gamma.$$
4. *The subgroup 2Γ has finite index in Γ.*

Then Γ is finitely generated.

Galois Representation

Notation

Let the n-torsion

$$C[n] = \{\mathcal{O}, (x_1, y_1), (x_2, y_2), \dots, (x_m, y_m)\}$$

be the points P on the curve C such that $nP = \mathcal{O}$.
Let $\mathbb{Q}(C[n]) = \mathbb{Q}(x_1, y_1, \dots, x_m, y_m)$.

Galois Representation

Theorem

$$C[n] \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z}).$$

Proof Outline

Each of ω_1 and ω_2 in lattice representation represents one of the groups in the direct sum.

Galois Representation

Theorem

$K = \mathbb{Q}(C[n])$ *is a Galois extension of* $\mathbb{Q}$.

Proof Outline

- $\sigma : K \to C$
- If $P_i \in C[n]$, $\sigma(P_i) \in C[n]$
- $\sigma(K) \subseteq K \implies \sigma(K) = K$.

Galois Representation

Theorem (Galois Representation Theorem)

Let C be an elliptic curve given by a Weierstrass equation with rational coefficients, and let $n \geq 2$ be an integer. Fix generators P_1 and P_2 for $C[n]$. Then the map

$$\rho_n : \mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}), \rho_n(\sigma) = \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}$$

where

$$\sigma\left(P_1\right) = \alpha_\sigma P_1 + \gamma_\sigma P_2$$
$$\sigma\left(P_2\right) = \beta_\sigma P_1 + \delta_\sigma P_2$$

is an injective group homomorphism.

References

[1] Joseph H. Silverman and John T. Tate *Rational Points on Elliptic Curves*. Addison-Wesley, Reading, Massachusetts, 1993.

[2] AJ Bull: Galois Representations and Elliptic Curves, `http://www.math.utah.edu/~moss/AJ_Bull_Galois_Representations_and_Elliptic_Curves.pdf`

[3] Drew Sutherland: Elliptic Curves Over $\mathbb{C}$, `http://math.mit.edu/classes/18.783/2017/LectureNotes16.pdf`

[4] Images - Wikipedia and `https://slideplayer.com/slide/12970423/79/images/7/Computations+on+Elliptic+Curves.jpg`