Elliptic Curves

Sierra Woods
Mentor: Asimina Hamakiotes
University of Connecticut

December 10, 2022

Overview

Definitions

Definition (Elliptic Curves)

An *elliptic curve* $E/\mathbb{Q}$ is a smooth cubic projective curve E defined over $\mathbb{Q}$ with at least one rational point $\mathcal{O} \in E(\mathbb{Q})$ that is called the *origin*. Note that

- *smooth* means non-singular, there are no points on the graph where the tangent lines in the x, y, and z directions disappear
- *projective* means contained within the projective plane. We define the *projective plane* as

$$\mathbb{P}^2(\mathbb{R}) = \{[x, y, 1] : x, y \in \mathbb{R}\} \cup \{[a, b, 0] : a, b \in \mathbb{R}\}.$$

Geometrically

Elliptic Curves

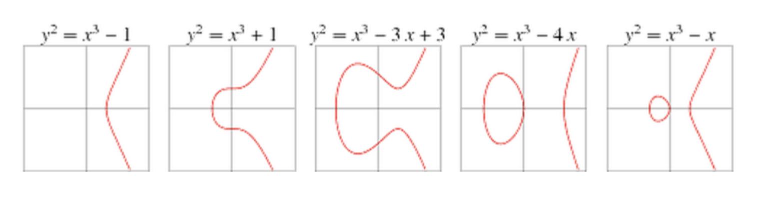


Figure: Some different elliptic curves.

Geometrically

Elliptic Curves

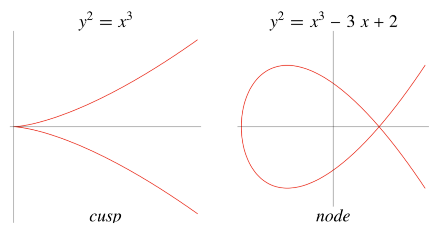


Figure: Two curves in affine coordinates with singularities.

Equation

Definition

This is how we define an elliptic curve over the rationals $E/\mathbb{Q}$ in the projective plane.

$$F(X,Y,Z) = aX^3+bX^2Y+cXY^2+dY^3+eX^2Z+fXYZ+gY^2Z+hXZ^2+jYZ^2+kZ^3 = 0$$

with coefficients $a, b, \ldots, k \in \mathbb{Q}$ such that E is smooth.

Definition

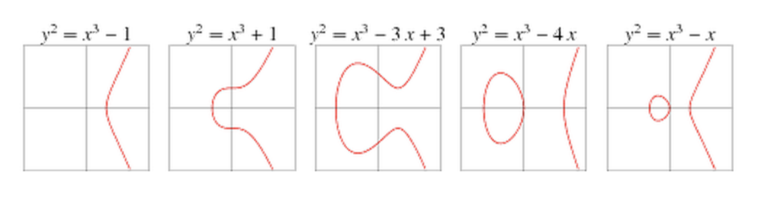
Sometimes we consider simply the affine charts of E, where we consider points of the form $[X, Y, 1]$ and study the curve given in affine coordinates by

$$aX^3 + bX^2 + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + jY + k = 0.$$

It is important to recognize that we are missing points of the form $[X, Y, 0]$ satisfying the projective equation, called the *points at infinity*.

Geometrically

Elliptic Curves



We can utilize the coordinate change from affine to projective by $x = X/Z$ and $y = Y/Z$.

1. $Y^2Z = X^3 - Z^3$
2. $Y^2Z = X^3 + Z^3$
3. $Y^2Z = X^3 - 3XZ^2 + 3Z^3$
4. $Y^2Z = X^3 - 4XZ^2$
5. $Y^2Z = X^3 - XZ^2$

Geometrically

Elliptic Curves

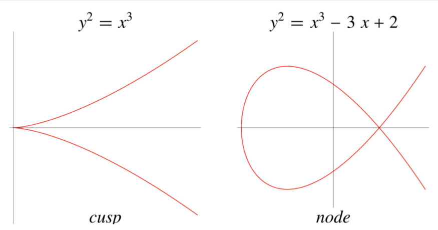


Figure: For the curve on the left, we can find a projective curve $D : x^3 - y^2 z$. After this, we can find the singularity as $\frac{\partial D}{\partial x} = \frac{\partial D}{\partial y} = \frac{\partial D}{\partial z} = 0$ at $[0, 0, 1]$ by

$$\frac{\partial D}{\partial x} = 3x^2 \qquad \frac{\partial D}{\partial y} = -2yz \qquad \frac{\partial D}{\partial z} = -y^2.$$

Weierstrass Equation

Definition (Weierstrass Equation)

A Weierstrass equation is an elliptic curve E of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in \mathbb{Q}$. Typically however, we write a Weierstrass equation in projective coordinates as $y^2z = x^3 + Axz^2 + Bz^3$ or in affine coordinates as $y^2 = x^3 + Ax + B$. Any Weierstrass equation of this form is non-singular iff $4A^3 + 27B^2 \neq 0$ and has a unique point at infinity called the origin $\mathcal{O} = [0, 1, 0]$.

Example

Looking back at our equations from earlier, we see $E : y^2 = x^3 + 1$ is non-singular because $4(0) + 27(1) = 27 \neq 0$. Similarly, $y^2 = x^3$ is singular because $4(0) + 27(0) = 0$ and we found the point of singularity at (0,0) in affine or $[0, 0, 1]$ in projective.

Isomorphisms

Definition

Let $E : f(x, y) = 0$ be an elliptic curve with origin $\mathcal{O}$, and let $E' : g(X, Y) = 0$ be an elliptic curve with origin $\mathcal{O}'$. We say E is isomorphic to E' over $\mathbb{Q}$ if there is an invertible change of variables $\psi : E \to E'$, defined by rational functions with coefficients in $\mathbb{Q}$, such that $\psi(\mathcal{O}) = \mathcal{O}'$.

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Then E has only a finite number of integral points.

Change of Coordinates

Proposition

Let $E/\mathbb{Q} : y^2 + a_1xy + a_3y = x^3 + a^2x^2 + a_4x + a_6$ be an elliptic curve for $a_i \in \mathbb{Q}$. We can find a map by $(x, y) \to (u^{-2}x, u^{-3}y)$, we can find the equation of an elliptic curve isomorphic to E given by

$$E' : y^2 + (a_1u)xy + (a_3u^3)y = x^3 + (a_2u^2)x^2 + (a_4u^4)x + (a_6u^6)$$

with coefficients $a_iu^i \in \mathbb{Z}$ for $i = 1, 2, 3, 4, 6$.

Example

Let $E : y^2 = x^3 + \frac{x}{2} + \frac{5}{3}$. We may change variables by $x = \frac{X}{6^2}$, and $y = \frac{Y}{6^3}$ to obtain

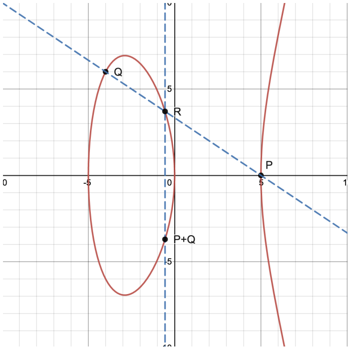
$$Y^2 = X^3 + 648X + 77760.$$

Addition of Points

$P + Q$

Let E be given by a Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$. Let P and Q be two rational points in $E(\mathbb{Q})$ such that $P \neq Q$ and let $\mathcal{L} = \bar{PQ}$ be the line that goes through P and Q. If R is the third intersection point on $\mathcal{L}$, then the sum of P and Q, denoted by $P + Q$ is the second point of intersection with E of the vertical line that goes through R, or in other words, the reflection of R across the x-axis.

Addition of Points



Let E be elliptic curve $y^2 = x^3 - 25x$. We can find $P, Q \in E(\mathbb{Q})$ by $P = (5, 0)$ and $Q = (-4, 6)$. In order to find $P + Q$, we find $\mathcal{L} = \overline{PQ}$. We can find $m = \Delta y / \Delta x = -2/3$ and thus we find the line between them to be $\mathcal{L} : -\frac{2}{3}(x - 5)$. We can find the third point of intersection by solving a systems of equation and thus we receive $R = (-\frac{5}{9}, \frac{100}{27})$. Now we reflect R across the x-axis, so $P + Q = (-\frac{5}{9}, -\frac{100}{27})$.

Addition of Points

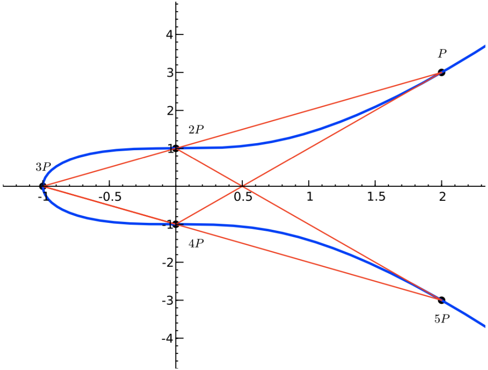


Figure: The rational points on $y^2 = x^3 + 1$ for $P = (2, 3)$. Notice $5P = -P$ so $6P = 5P + P = \mathcal{O}$.

Moreover, notice $3P + 2P = 5P = 2P + 3P$.

Review of Groups

Definition

A group $(G, \cdot)$ is a set G associated with a binary operation $\cdot$ where the following conditions are satisfied:

1. Closure: $\forall g, h \in G$, $g \cdot h \in G$ and $h \cdot g \in G$.
2. Identity: $\exists e \in G$ such that $\forall g \in G$, $e \cdot g = g = g \cdot e$.
3. Inverses: $\forall g \in G$, $\exists g^{-1} \in G$ such that $g \cdot g^{-1} = e = g^{-1} \cdot g$.
4. Associativity: $\forall g, h, k \in G$, $g \cdot (h \cdot k) = (g \cdot h) \cdot k$.

If a group also satisfies commutativity, so $\forall g, h \in G$, $g \cdot h = h \cdot g$, then we say G is an abelian group. An abelian group is called finitely generated if $\exists H \subset G$ subset such that H generates G.

Mordell-Weil Theorem

Example

Going back to our equation, $E/\mathbb{Q} : y^2 = x^3 + 1$, the point $P = (2,3) \in E(\mathbb{Q})$ has order 6. Given that $E(\mathbb{Q})$ has order 6, we can find that $E(\mathbb{Q}) = \{\mathcal{O}, P, 2P, 3P, 4P, 5P\}$ is a finitely generated abelian group. We can see closure, inverses by $-P = 5P$, $-2P = 4P$, and $-3P = 3P$. This implies the identity is $\mathcal{O} \in E(\mathbb{Q})$, and we can see commutativity by geometry.

Theorem (Mordell-Weil)

There are points $P_1, \ldots, P_n$ such that any other point $Q \in E(\mathbb{Q})$ can be expressed as a linear combination $Q = a_1P_1 + a_2P_2 + \cdots + a_nP_n$ for some $a_i \in \mathbb{Z}$. Thus $E(\mathbb{Q})$ is a finitely generated abelian group.

Mordell-Weil Cont.

Theorem (Weak Mordell-Weil)

$E(\mathbb{Q})/mE(\mathbb{Q})$ *is a finite group* $\forall m \geq 2$.

Corollary

We find

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^{R_E}.$$

The Torsion Subgroup

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^{R_E}$$

Definition

We define the torsion subgroup to be

$$E(\mathbb{Q})_{\text{torsion}} = \{P \in E(\mathbb{Q}) : \exists n \in \mathbb{N} \ \text{ such that } \ nP = \mathcal{O}\}.$$

Definition

We define $\mathbb{Z}^{R_E}$ as an abelian group where R_E represents the order of the set $F = \{P \in E(\mathbb{Q}) : nP \neq \mathcal{O} \ \ \forall n \in \mathbb{Z} \ \ s.t. \ \ n \neq 0\}$. And $\mathbb{Z}^{R_E} = \mathbb{Z} \times \cdots \times \mathbb{Z}$ for R_E times.

Ogg's Conjecture

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{torsion}$ is isomorphic to exactly one of the following groups:

$$\begin{array}{rll} \mathbb{Z}/N\mathbb{Z} & \textit{with} & 1 \leq N \leq 10 \textit{ or } N = 12, \quad \textit{or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \textit{with} & 1 \leq M \leq 4 \end{array}$$

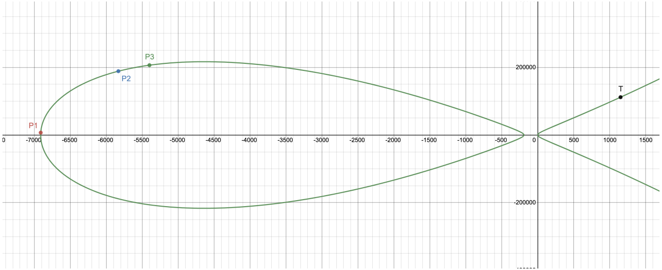
Example

Remembering our previous example, $E/\mathbb{Q} : y^2 = x^3 + 1$, we saw $E(\mathbb{Q})_{\text{torsion}} = \{\mathcal{O}, P, 2P, 3P, 4P, 5P\}$ was a group with order 6. Thus we can apply Ogg's Conjecture and say $E(\mathbb{Q})_{\text{torsion}} \cong \mathbb{Z}/6\mathbb{Z}$. Given there are only 6 rational points and we have found them all, we see $R_E = 0$ thus $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}} \cong \mathbb{Z}/6\mathbb{Z}$.

More Examples

Example

Consider the curve $E/\mathbb{Q} : y^2 = x^3 + 7105x^2 + 1327104x$. We can find the torsion subgroup to be generated by $T = (1152, 111744)$ with order 4 (so $4T = \mathcal{O}$). We can also find three points of infinite order: $P_1 = (-6912, 6912)$, $P_2 = (-5832, 188568)$, and $P_3 = (5400, 206280)$. We see $E(\mathbb{Q})_{\text{torsion}} \cong \mathbb{Z}/4\mathbb{Z}$ and because $R_E = 3$, we have $E(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}^3$. But what about the rank?



Rank

Theorem

For any $N \geq 1$, let $\nu(N)$ be the number of distinct positive prime divisors of N. Let $E/\mathbb{Q}$ be an elliptic curve given by $E : y^2 = x^3 + Ax^2 + Bx$ for $A, B \in \mathbb{Z}$. We have:

$$R_E \leq \nu(A^2 - 4B) + \nu(B) - 1.$$

Example

Going back to $E/\mathbb{Q} : y^2 = x^3 + 7105x^2 + 1327104x$, we have $A = 7105$ and $B = 1327104$. So $A^2 - 4B = 45172609$ which has prime factorization $97^2 \cdot 4801$ so we find $\nu(45172609) = 2$. Furthermore, 1327104 has prime factorization $2^{14} \cdot 3^4$, thus $\nu(1327104) = 2$, and by the formula, $R_E \leq 2 + 2 - 1 = 3$. Since we found 3 points of infinite order and $R_E \leq 3$, we can clearly see $R_E = 3$ and once again conclude $E(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}^3$.

Why?

Applications

- Fermat's last theorem
- Cryptography

Cryptography

- Recall point addition
- Point on curve called public point. Some number $pr \in \mathbb{Z}$ called private key, and we find the public key by multiplying public point by pr many times.
- Discrete Logarithmic Problem, so computationally difficult that there is no known algorithm to determine the answer or simplify the problem
- Elliptic curves are symmetric on both sides so we only consider x value and parity of y value, making it efficient for data-usage

Bitcoin

- Apple
- US Government
- Bitcoin uses the curve **Secp256k1** known as $y^2 = x^3 + 7$

References

Judson, Thomas W. "Abstract Algebra: Theory and Applications." AATA, 9 Aug. 2021, http://abstract.ups.edu/aata/aata.html

Lozano-Robledo, Álvaro. Elliptic Curves, Modular Forms, and Their L-Functions. Vol. 58, American Mathematical Society Institute for Advanced Study, 2009.

Saqan, Suhail. "Explanation of Bitcoin's Elliptic Curve Digital Signature Algorithm." Medium, Medium, 26 Feb. 2022, https://suhailsaqan.medium.com/explanation-of-bitcoins-elliptic-curve-digital-signature-algorithm-6603f951863a.

Weisstein, Eric W. "Elliptic Curve." Wolfram MathWorld, Wolfram Research, https://mathworld.wolfram.com/EllipticCurve.html.

The End