An Algebraic view on the Arithmetic of Elliptic Curves

Sachin Kumar
Faculty of Mathematics, University of Waterloo

Canadian Undergraduate Mathematics Conference (CUMC),
University of Toronto, June 21, 2023

Outline

About Me

I am an undergraduate student majoring in pure mathematics and combinatorics/optimization (Honours BMath) at the University of Waterloo's Faculty of Mathematics. I am primary research in the field of Algebra, Number Theory, Algebraic Geometry and Theoretical Cryptography.

Notation

Notation

We will follow the standard Bourbaki notations: $\mathbb{F}$ denotes a field, K denotes a number field, $\mathbb{Q}$ denotes the set of rational numbers, $\mathbb{C}$ denotes the set of complex numbers and $\mathbb{F}_p$ denotes the finite field.

What is an Elliptic Curve?

Let's assume that we have a smooth cubic equation $f(x,y)=0$ that has a point $P=(x_0,y_0)$ in a field F.

Definition (Elliptic curve)

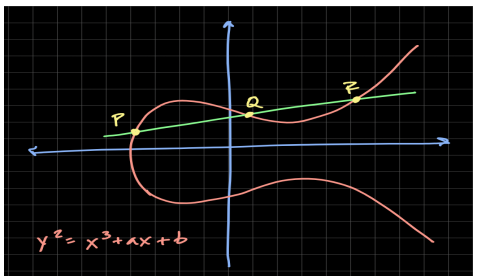
An elliptic curve over a field F is a non-singular curve E of the form,

$$E: y^2 = x^3 + Ax + B, \quad A,B \in \mathbb{Z} \tag{1}$$

with a discriminant,

$$\Delta = -4A^3 - 27B^2 \neq 0$$

The polynomial (1) has distinct roots. An elliptic curve E over a field F, denoted E/F. Also, there exists at point at infinity denoted as, O. So, E is the set $E=\{(x,y): y^2 = x^3+Ax+B\} \cup \{O\}$.



Why is (1) a non-singular curve?

Geometry of Elliptic Curves

Adding two points (distinct and non-distinct) and Reflection point

Let $P, Q \in E$.

We see that there is a vertical line passing through P and $-P$ on the curve E, but the line does not pass through a 3rd point, so what is,

$$P \oplus -P = ?$$

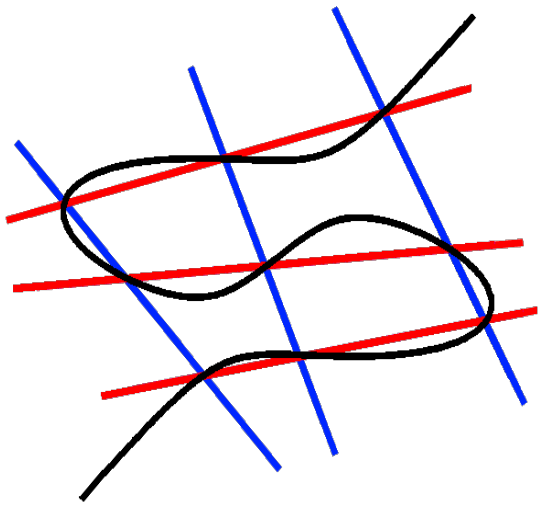
Group Structure

Theorem

A line intersects an elliptic curve at exactly three points, P, Q and R. If $P, Q \in \mathbb{Q}$, then $R \in \mathbb{Q}$.

Theorem (Cayley and Bacharach)

Suppose E_1, E_2 and E_3 are elliptic curves in the projective plane such that E_2 and E_3 intersect at 9 points. If E_1 passes through 8/9 intersection points of E_2 and E_3, then it must pass through the 9th one as well.



The set of projective points on an elliptic curve forms a group, with

$$\infty = [0:1:0]$$

$E(K)$ is a set of F-points of an elliptic curve E over a field F.

$$E(F) = \{(x,y) \in E/F : x,y \in F\} \cup \{\infty\}$$

Theorem (Group Law)

$E(\mathbb{Q})$ is an abelian *group* over addition (known as the Mordell-Weil group).

Is $E(\mathbb{Q})$ finite or infinite?

Something that cryptographers like!

Definition

An isogeny is a morphism ϕ of algebraic varieties between two elliptic curves, such that ϕ is a group homomorphism.

Every isogeny is a group homomorphism and thus has a kernel,

$$\ker \phi : \{P \in E : \phi(P) = \infty\}$$

Given an elliptic curve E and a finite subgroup H on E, one can prove that there exists a unique up to isomorphism separable isogeny $\phi_H : E \to E/H$ such that $\ker_{\phi_H} = H$ and $\deg_{\phi_H} = |H|$.

Vélu;s Formula - Isogenies of degree 2

Let $E : y^2 = x^3 + ax + b$.

Suppose $H = \{\infty, P\}$. Then $P \oplus P = \infty$, so $P = (x_p, 0)$ with $x_p^3 + ax_p + b = 0$. We have,

$$E/H : y^2 = x^3 + (a - 5(3x_p^2 + a))x + (b - 7x_p(3x_p^2 + a))$$

$$\phi_H(x, y) = \left(x + \frac{3x_p^2 + a}{x - x_p}, y - \frac{y(3x_p^2 + a}{(x - x_p)^2} \right)$$

Rank of $E/\mathbb{Q}$

Theorem (Mordell)

The group $E(\mathbb{Q})$ of $\mathbb{Q}$-points is a finitely generated abelian group.

For some $r \in \mathbb{Z}_{\geq 0}$ and a finite abelian group T,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$$

The arithmetic measure r is called the rank of $E/\mathbb{Q}$ and finite abelian group T.

Arithmetic Rank

The arithmetic rank of an elliptic curve denoted as r, is an integer (not always!), which is the size of the smallest torsion-free subgroup of the Mordell-Weil group, $E(\mathbb{Q})$.

Can Mordell's theorem be more generalized? and can the rank, $r \notin \mathbb{Z}_{\geq 0}$?

The celebrated theorem

By Mazur 1977, we know that $E(\mathbb{Q})$ is isomorphic to only 15 groups.

What are the 15 groups?

$$\mathbb{Z}/n\mathbb{Z} \quad n \in \{1,\ldots,10,12\}$$
$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z} \quad n \in \{1,\ldots,4\}$$

Falting's Theorem a.k.a Mordell's conjecture

If $E/\mathbb{Q}$ is a elliptic curve over the rationals, with genus $g>1$, then $E(\mathbb{Q})$ is finite

This theorem can be generalized for any non-singular algebraic curve over a number field, with genus $g>1$.

When you don't know what you don't know!

There many natural fundamental questions that one can ask about the rank, but unfortunately they are still unsolved!

1. Does there exist any computational algorithm that can determine the rank of and elliptic curve?.
2. Is there a maximum rank of an elliptic curve? if yes, what is it?
3. What is the average rank of an elliptic curve?
4. Is the rank of an elliptic curve always 0 or 1? if no, what is the %?

Then what is Birch Swinnerton-Dyer conjecture?

What kind of solutions, do we need to care about?

Just like most of the number theoretic problems, the key idea is to analyze solutions in mod p, where p is a prime,

$$y^2 = x^3 + Ax + B \pmod{p} \tag{2}$$

Around 1960's, Birch and Swinnerton-Dyer did some computations of ranks of elliptic curves, and the number of solutions mod p on these elliptic curves, denoted by N_p. Let's take some random elliptic curve, then one can think that modulo p has p points, hence

$$\frac{N_p}{p} = 1$$

obviously, its not as easy as it looks! but why?

Let's think, if E has lot of rational points on it, then these points mod p, would give lots of points on (2).

Logically, one may think that if the rank of the elliptic curve E is large, then on average we can notice E having more than p points modulo p.

You know what, that's exactly what Birch and Swinnerton-Dyer hypothesized!

Birch Swinnerton-Dyer Conjecture

Let E be an elliptic curve, let r be its rank, and let N_p denote the number of points on $E \pmod p$. Then,

$$\prod_{p \leq X} \frac{N_p}{p} \sim c \cdot (\log X)^r$$

You **"just"** need to prove this to get a million dollar!

When algebra meets analysis! A modern formulation

But that was just the weak form of the conjecture!

Let E be an elliptic curve, and let N_p denote the number of points on $E \pmod p$. Let's set $a_p = p+1-N_p$, and define a incomplete L-function of E by,

$$L(E,s) = \prod_{p \nmid 2\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \tag{3}$$

$L(E,s)$ converges only for $s \in \mathbb{C}$ satisfying $\Re(s) > \frac{3}{2}$.

Conjecture (Hasse)

$L(E,s)$ has a holomorphic continuation as a function of s to the entire complex plane.

Guess, who proved this?

Since, we introduced the L-function of an elliptic curve, it makes sense for us to speak about the value and order of the vanishing of this holomorphic function at $s = 1$.

Notice anything?

BSD Conjecture

The rank of E is equal to $\text{ord}_{s=1} L(E, s)$.

Theorem (Wiles, 1995)

For any elliptic curve E, the L-function $L(E, s)$ has a holomorphic continuation to the entire complex plane.

Hasse conjecture, was a consequence of the modularity conjecture.

How does all this connect to the algebraic structure of E?

Let E be an elliptic curve, and let r be its rank. By Wiles, we know there exists and integer r' such that the Taylor expansion of $L(E,s)$ at $s=1$ is of the form,

$$L(C,s) = c(s-1)^r + \text{ higher order terms}$$

with $c \neq 0$ and $r = \text{rank}(E(\mathbb{Q}))$.

What is c? Can it be defined? Yes!

Modern BSD Conjecture

The arithmetic rank of E is equal to its analytic rank of E, ie.,

$$r = r'$$

Let's be happy!

Theorem (Coates-Wiles, 1977)

If E is an elliptic curve of form $y^2 = x^3 + Ax$ or $y^2 = x^3 + B$, and if $r' = 0$, then the BSD conjecture is true for E.

Why those elliptic curves in specific?

Theorem (Gross, Zagier, and Kolyvagin, 1789)

If $r' = 0$ or 1 for an elliptic curve E, then the BSD conjecture is true for E.

Till now, we have always been thinking about, whether

$$r' = 0 \text{ or } 1 \implies r = 0 \text{ or } 1$$

But what about the converse! Is it true? Does

$$r = 0 \text{ or } 1 \implies r' = 0 \text{ or } 1$$

hold?

Surprisingly, it does bit with a lot of restrictions! So combining the proof techniques of the previous theorems, as well as Kato, Mazur-Wiles, and Wiles:

Skinner-Urban-Zhang 2013

If $r = 0$ or 1 for an elliptic curve E, and if E satisfies some technical conditions, like for some $p \geq 5$, E has a p-selmer rank 0 or 1, E has a good ordinary or multiplicative reduction at p, etc...), then $r' = 0$ or 1.

After all these ridiculous conditions, a natural question may arise,

Can such an elliptic curve even exist?

The height of an elliptic curve

Recall that $E/\mathbb{Q}$ is of the form,

$$E_{A,B} : y^2 = x^3 + Ax + B$$

where $A, B \in \mathbb{Z}$.

Height

The height of E is the size of the coefficients of the defining equation.

If $E_{A,B}/\mathbb{Q}$, then $H(E_{A,B}) := \max\{4|A|^3, 27B^2\}$, this is called the naive height of the elliptic curve.

List all elliptic curves $E/\mathbb{Q}$ in order of increasing height.

Let's get realistic, if we can't prove it, we can at least check the probability of BSD being satisfied by these curves and ask statistical questions about the rank.

Previously, we asked whether most elliptic curves have small rank? Yeah somewhat! We at least know most elliptic curves have rank 0 or 1.

Theorem (Bhargava-Shankar, 2013)

At least 83% of all elliptic curves have rank 0 or 1.

In fact, the proof method of Bhargava and Shankar helped in establishing some of the technical conditions that skinner, Urban, and Zhang required to deduce:

Corollary

A positive proportion of elliptic curves satisfy BSD conjecture.

What happens if we combine all the result we saw till now? Can we really get anything out of it?

Boooom!

Theorem (Bhargava-Skinner-Zhang)

The BSD conjecture is true for more than 66% of all elliptic curves.

What is left to be done?

- What about curves with rank, $r > 1$? Even though it is conjectured that 100% curves have rank 0 or 1 (not all!)
- The complicated conditions of skinner-Urban-Zhang must be removed? At least we will know 100% of the curves satisfy BSD conjecture.
- There are elegant extensions of the BSD conjecture, like the bloch-Kato conjecture, p-adic analogues, over general number fields, etc...

Book Recommendations for Undergraduates

1. Rational Points on Elliptic Curves by John Tate and Joseph Silverman.
2. An Introduction to Mathematical Cryptography by Joseph Silverman.

Other advanced books by Joseph Silverman, Alfred Menezes, David Jao etc.

Thank You!