Section 1: Definitions

Def: a **curve** is a set of solutions to an algebraic equation over a given field; e.g. \( K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p \), etc.

Intuitively: an **elliptic curve** is a curve that’s also a group, where group law is constructed geometrically.

Note: not a curve that is an ellipse.

Def: an **elliptic curve** is a curve given by an equation \( y^2 = x^3 + Ax + B \), where \( \Delta = 4A^3 + 27B^2 \neq 0 \).

\[ E = \{(x,y) : y^2 = x^3 + Ax + B \} \cup \{ \theta \} \]

"point at infinity"

- have to add in pt at infinity to make gp law work

Fact: an EC has a gp structure given by geometry; easiest to show with an example

Ex: \( E: y^2 = x^3 - 5x + 8 / \mathbb{R} \)

- take two pts \( P, Q \in E \)
- draw line through \( P, Q \), also intersects \( E \) at \( R \)
- draw vertical through \( R \), also intersects \( E \) at another pt; let that pt be \( P + Q \).

- gp needs inverses: to get \(-P\), reflect across x-axis

\[ P + \theta = P \]

\[ P + (-P) = \theta \]
how do I add $P + P$? take tangent line at $P$

Thm: the addition law above makes $E$ a comm. gp.

- need to check associativity, which you can do
  algebraically using addition formula, or using functor algebraic or
  analytic methods
  
  You can make explicit formulas for
  addition; they’re messy, though

Ex: if $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, $x(P_1 + P_2) = \frac{(y_2 - y_1)^2 - x_1 - x_2}{x_2 - x_1}.

Fact: for a given equation $E: y^2 = x^3 + Ax + B$, we can also ask for
solutions in different fields. In particular, if $P_1 \neq P_2$ are both in $E(K)$,
so is $P_1 + P_2$, by formula above.

Thm (Poincaré, ~1900) Let $K$ be a field and $E: y^2 = x^3 + Ax + B$, $A, B \in K$

Let $E(K) = \{ (x, y) \in E : x, y \in K \} \cup \{(0, 0)\}$.

Then $E(K)$ is a subgroup of all the points in $E$.

Section 2: some uses

At Andy's mention of this Intro to Number Theory talk, studying $E(K)$

for different fields $K$ has been a major part of number theory—there's
a lot of structure and information here.

Ex: looking back at our example from earlier:

$E: y^2 = x^3 - 5x + 8$, which we defined (for $\mathbb{C}$).

We can ask: what does $E(\mathbb{Q})$ look like? What about $E(\mathbb{F}_p)$ for
$p$ prime?

- for $\mathbb{F}_p$ is easier: plug in each possible value of $x$ and check if
$x^3 - 5x + 8$ is a square mod $p$

\[
\begin{array}{c|c|c|c|c}
 x & y^2 & 1 & 4 & 6 \\
 0 & 1 & 4 & 6 & 3 \\
 1 & 6 & 3 & 3 & 1 \\
 2 & 6 & 3 & 3 & 1 \\
 3 & 6 & 3 & 3 & 1 \\
 4 & 6 & 3 & 3 & 1 \\
 5 & 6 & 3 & 3 & 1 \\
\end{array}
\]

So we get 4 points $(0, 1), (0, 6), (1, 2), (1, 5)$

You can check: $2(0, 1) = (1, 5)$, $3(0, 1) = (1, 2)$,
$4(0, 1) = (0, 6)$, $5(0, 1) = (0, 6)$.

So we have $E(\mathbb{F}_7) \cong \mathbb{C}_5$ cyclic gp of order 5.

Thm: $E(\mathbb{F}_p)$ is either a cyclic group or the product of two cyclic
groups

Ex: for our $E$, $E(\mathbb{F}_{37}) \cong C_3 \times C_{15}$.
By this method, \( \#E(\mathbb{F}_p) \leq 2p+1 \) points.

Given that about \( \frac{1}{2} \) of \( \# \) are squares mod \( p \), we might then expect \( \#E(\mathbb{F}_p) \approx p+1 \) points.

Thm (Hasse, 1922) \( E: y^2 = x^3 + Ax + B \) w/ \( A, B \in \mathbb{F}_p \).

Then \( |\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p} \).
What about \( E(\mathbb{R}) \)? Is it always a blob \( \bigcirc \)?

No! We can also have

\[
E : y^2 = x^3 - 5x + 2
\]

Thm: analytically, \( E(\mathbb{R}) \) is isom to \( S^1 \) or to two copies of \( S^1 \)

What about \( E(\mathbb{C}) \)? A bit more complicated

Note that \( y^2 = x^3 + Ax + B \) can be rewritten by subbing \( y \rightarrow \frac{1}{2} y \)

to get \( y^2 = 4x^3 + 4Ax + 4B \)

Weierstrass form

How is this better? It looks like something else.

Complex analysts (in particular Karl Weierstrass) were studying fins

with similar properties: let \( \mathcal{L} \) be a lattice in the \( \mathbb{C} \) plane.

We pick \( \omega, \omega_1, \omega_2 \in \mathbb{C} \) and set \( \mathcal{L} = \{ n_1 \omega + n_2 \omega_2 : n_1, n_2 \in \mathbb{Z} \} \)

Then we want a \( f \) that has poles at all the lattice points

\[
g(z) = \frac{1}{z^2} + \sum_{w \in \mathcal{L}} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right)
\]

Which actually has double pole \( w/ \) \( \nabla \) at all lattice pts

and is holomorphic on \( \mathbb{C} \setminus \mathcal{L} \).

Crazy thing:

\[
\left( \frac{\partial g}{\partial z} \right)^2 = 4 \frac{g(z)^3}{g'(z)} - g_5 g(z) - g_3
\]

where \( g_2, g_3 \) depending on the lattice we picked.

Then we get a map \( \mathcal{L} \xrightarrow{\sigma : (g(z), \frac{1}{2}g'(z))} E(\mathbb{C}) \)

But \( g(z) \) is periodic, so to make map isom, we need

\( g(z + \omega) = g(z) \forall \omega \in \mathcal{L} \)

So in fact \( \mathbb{C} \xrightarrow{\sigma : (g(z), \frac{1}{2}g'(z))} E(\mathbb{C}) \)

So \( E(\mathbb{C}) \simeq S^1 \times S^1 \)

One nice extension of this isomorphism is that it's easy to describe pts

with finite order
for $N \geq 1$, $E(C)_N = \{ p \in E(C) : NP = \Theta \}$

Prop: $\forall N \geq 1$, $E(C)_N \cong C_N \times C_N$.

But what about $E(\mathbb{Q})$? Hard, still a bit fuzzy...

Quest for description birthed an entire subfield: Diophantine equations, study of polynomial equations w/ integral or rational solutions, in 1922 when Mordell proved:

Thm (Mordell, 1922): $E(\mathbb{Q})$ is a finitely generated abelian group.

Algebra tells us, then, that $E(\mathbb{Q}) \cong \text{finite gp} \times \mathbb{Z}^r \leftarrow \text{rank of } E(\mathbb{Q})$.

$E(\mathbb{Q})_{\text{tors}} = \text{torsion subgroup of } E(\mathbb{Q})$

We know a little more.

Thm (Mazur, 1977): $E(\mathbb{Q})_{\text{tors}}$ is one of the following groups:

- $C_N$ for $1 \leq N \leq 10$ or $N = 12$
- $C_2 \times C_{2N}$ for $1 \leq N \leq 4$.

description is relatively simple, pf is extremely difficult

What about the rank?

Conjecture (folklore): $\exists$ elliptic curves of arbitrarily large rank.

- 2000: martens-McMillan found curve w/ rank $\geq 24$
- 2006: Elkies w/ rank $\geq 28$.

What next? Well, when number theorists get stuck, they start looking for someone else's hammer to borrow! $L$-functions (and talked a little about this)

For a curve $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, we study all of the subgps $E(\mathbb{F}_p)$ at the same time.

We expected $\# E(\mathbb{F}_p) \sim p + 1$; let $a_p = p + 1 - \# E(\mathbb{F}_p)$.

Def: the $L$-series of $E$ is

$$L(E, s) = \prod_{p \text{ prime}} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1} \quad s \in \mathbb{C}$$

- converges for Re$(s) > \frac{3}{2}$

Thm (Wiles): $L(E, s)$ extends to an analytic fn on all of $\mathbb{C}$. Furthermore, $\exists N \in \mathbb{Z}$, called conductor of $E$, s.t. $L(E, s) = N^{-\frac{s}{2}} (2\pi)^{-s} \Gamma(s) L(E, s)$.

satisfies mod eqn

$$\hat{L}(E, 2-s) = \pm L(E, s).$$
Technically, what happens is you rewrite $L(E,s)$ in sum form to get

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

and then set $s(E,s) = \sum a_n e^{2\pi int}$

Then $s(E,s)$ is a modular form (weight 2 cusp form for $\Gamma_0(N)$).

This Thm + ideas of Frey, Serre, & Ribet $\Rightarrow$ Fs of Fermat's Last Thm.

"It is a truth universally acknowledged that "$E$-series with $a$ in possession of a finite equation" must have interesting behavior at the center of its critical strip."

For us, that's $s=1$.

If we could plug in, we'd have "formal and completely unjustified"

$$L(E,1) = \prod_{p} \left( 1 - \frac{a_p}{p^2} + \frac{1}{p} \right)^{-1} = \prod_p \frac{1}{p - \#E(\mathbb{F}_p)}$$

which suggests that if $\#E(\mathbb{F}_p)$ is large for $p$, then $L(E,1) = 0$.

Conj's (Birch & Swinnerton-Dyer)

$$L(E,1) = 0 \iff \#E(\mathbb{Q}) = 0$$

or, famously

\[ \text{ord}_{s=1} L(E, s) = \text{rank} E(\mathbb{Q}) \]

Clay millenium problem

-Current question: do most curves have rank 0 or 1? Another talk in and of itself.

---

**Section 3: Other Uses**

So, EC show up in hard pure number theory; are they good for anything else?

"Yes! Cryptography!"

Modern cryptosystems are based on trapdoor problems: things that are hard to compute brute force but easy to compute if you have an extra piece of info.

One of these is Discrete Log Problem: for $g \in G$, $g \in G$; given $h \in G$,

Find me $m$ s.t. $h = g^m$.

-What $G$ you pick determines how hard this is:
  - $(\mathbb{Z}/m\mathbb{Z}, +)$ is easy (Euclidean algm)
  - $(\mathbb{R}^*, \cdot)$ or $(\mathbb{C}^*, \cdot)$ easy (usual log)
  - $(\mathbb{F}_p^*, \cdot)$ is harder $\Rightarrow$ has subexponential algm Index Calculus
  - $(E, +)$ is fastest known algm is Pollard's P-1 method, which isn't that fast, also requires smaller key space blocks for ease of transmission.