What is this thing called an 'Elliptic Curve?'

Claire Frechette

9/23/19

SNTS 1

I. Definitions

II. Some History & Uses

~~III. Modern Uses~~ III. Other Uses

Sources/ Reference:

- Silverman & Tate, "Rational Points on Elliptic Curves"
- Silverman, "The Arithmetic of Elliptic Curves" GTM
- lecture notes for 2006 Summer School on Computational Number Theory at U. Wyoming.

Section 1 : Definitions

Def: a $\boxed{\text{curve}}$ is a set of solutions to an algebraic equation over a given field K; ex: $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$, etc.

Intuitively: an elliptic curve is a curve that's also a group, where gp law is constructed geometrically

Note: not a curve that is an ellipse.

Def: an $\boxed{\text{elliptic curve}}$ is a curve given by an equation $y^2 = x^3 + Ax + B$, where $\Delta = 4A^3 + 27B^2 \neq 0$.

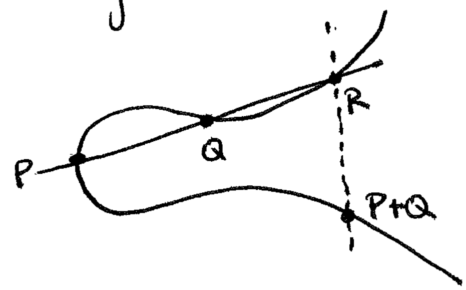
$$E = \{(x,y) : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

"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

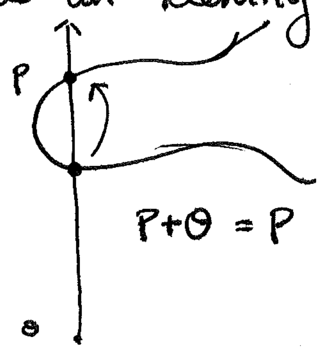
Ex: $E: y^2 = x^3 - 5x + 8 \ / \mathbb{R}$



1. take two pts $P, Q \in E$
2. draw line through P, Q, also intersects E at R
3. draw vertical through R, also intersects E at another pt. Let that pt be $P+Q$.

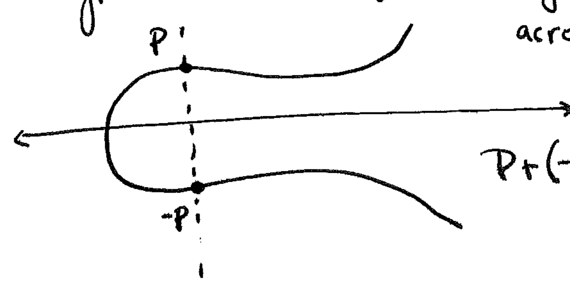
Are you sure this is a gp?

- gp needs an identity: $\mathcal{O}$



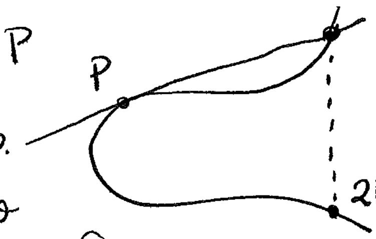
$P + \mathcal{O} = P$

- gp needs inverses: to get $-P$, reflect across x-axis



$P + (-P) = \mathcal{O}$.

- 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 fancier algebraic or analytic methods

  you can make explicit formulas for addition; they're messy, though

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

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 $E(K)$ = pts w/ coords in $K = \{(x,y) \in E : x, y \in K\} \cup \{\Theta\}$.

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

Section 2: some uses

As Andy mentioned in his 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 $/\mathbb{R}$ (or $\mathbb{C}$...)

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

x	y^2
0	1 ✓
1	4 ✓
2	6
3	6
4	3
5	3
6	5

Squares mod 7 are $\{0, 1, 2, 4\}$

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

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

So we have $E(\mathbb{F}_7) \cong C_5$, cyclic gp of order 5.

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

start running sideboard

Ex: ~~for~~ For our E, $E(\mathbb{F}_{37}) \cong C_3 \times C_{15}$.

~~squares~~ By this method, $\#E(\mathbb{F}_p) \leq 2p+1$ points

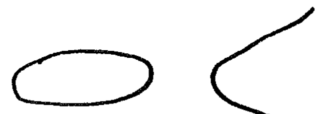
Given that about $1/2$ of # are squares mod p, we might then expect $\#E(\mathbb{F}_p) \approx p+1$ points

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  ?

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

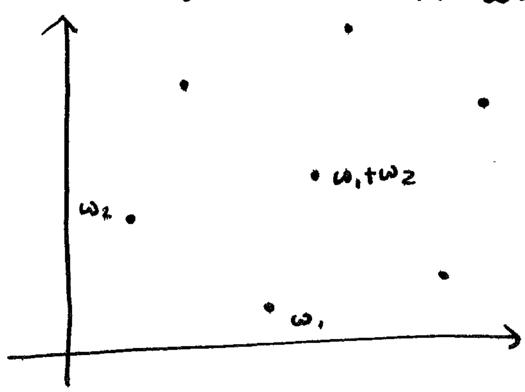
~~Note~~ Note that $y^2 = x^3 + Ax + B$, can be rewritten by subbing $y \mapsto \frac{1}{2}y$

to get $\underbrace{y^2 = 4x^3 + 4Ax + 4B}_{\text{Weierstrass form}}$

How is this better? It looks like something else.

Complex analysts (in particular Karl Weierstrass) were studying fcns ~~on~~ w/ similar properties: let L be a lattice in the $\mathbb{C}$ plane:

We pick ~~2~~ $\omega_1, \omega_2 \in \mathbb{C}$ and set $L = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}$



Then we want a fcn that has poles at all the lattice points

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

actually has double pole w/ res 0 at all lattice pts, and is holomorphic on $\mathbb{C} \setminus L$.

Crazy thing:

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3.$$

where g_2, g_3 are constants depending on the lattice we picked.

Then we get a map $\mathbb{C} \setminus L \xrightarrow{(\wp(z), \frac{1}{2}\wp'(z))} E(\mathbb{C})$

But ~~the~~ $\wp(z)$ is periodic, so to make map isom, we need to take fundamental domain for L.

$$\wp(z+\omega) = \wp(z) \quad \forall \omega \in L$$

So in fact $\mathbb{C}/L \xrightarrow[\cong]{(\wp(z), \frac{1}{2}\wp'(z))} E(\mathbb{C})$

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

One nice ~~extension~~ use of this isomorphism is that it's easy to describe pts with finite order:

for $N \geq 1$, $\in \mathbb{Z}$, $E(\mathbb{C})_N = \{P \in E(\mathbb{C}) : NP = \Theta\}$

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

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 $E(\mathbb{Q}) \simeq \underbrace{\text{finite gp}}_{E(\mathbb{Q})_{tors} = \boxed{\text{torsion subgp}} \text{ of } E(\mathbb{Q})} \times \mathbb{Z}^r \leftarrow \boxed{\text{rank}}$ of $E(\mathbb{Q})$

Weil + generalized

We know a little more

Thm (Mazur, 1977): $E(\mathbb{Q})_{tors}$ is always 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 Marten-McMillen found curve w/ rank ≥ 24
- 2006 Elkies " " " rank ≥ 28.

What now? Well, when number theorists get stuck, they start looking for someone else's hammer to borrow! $\mathcal{L}$-functions (Andy 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 $a_p = p+1 - \#E(\mathbb{F}_p)$ $\leftarrow$ $\boxed{\text{trace of Frobenius}}$

Def: the $\boxed{\mathcal{L}\text{-series of } E}$ is
$$\mathcal{L}(E,s) = \prod_{p \text{ prime}} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1} \quad s \in \mathbb{C}$$

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

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

$$\xi(E, 2-s) = \pm\, \xi(E,s).$$

gamma fcn from Joe's talk

Technically, what happens is you rewrite $L(E,s)$ in sum form to get $L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ and then set $f(E,\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n \tau}$

Then $f(E,\tau)$ is a modular form (wt 2 cusp form for $\Gamma_0(N)$).
this Thm + ideas of Frey, Serre, & Ribet $\Rightarrow$ pf of Fermat's Last Thm.

"It is a truth universally acknowledged that any L-series ~~with~~ in possession of a fcnl 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"

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

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

Conj.s (Birch & Swinnerton-Dyer)

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

or, famously $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}\, E(\mathbb{Q})$ ← 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 gp G, $g \in G$; given $h \in \langle g \rangle$, find $m \in \mathbb{Z}$ s.t. $h = g^m$.

- what gp 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 ← has subexponential algm Index Calculus
  - $(E, +)$ ← fastest known algm is Pollard's ρ method, which isn't that fast
    ← also requires smaller keys & blocks for same level of difficulty