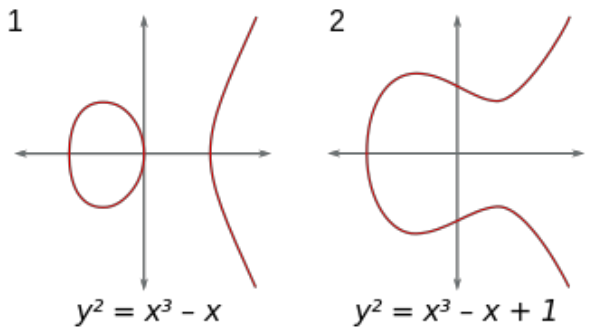
A Gentle Introduction to the Langlands Program

Jeremy Booher, University of Canterbury

Elliptic Curves



$y^2 = x^3 - x$ modulo 7

$\{ 0, (0,0), (1,0), (4,\pm 2), (5,\pm 1), (6,0) \}$

Elliptic Curves

References: Silverman-Tate: Rational Points on Elliptic Curves
Silverman: Arithmetic of Elliptic Curves
Diamond and Shurman: A First Course in Modular Forms

$E: y^2+y = x^3-x$ ☆ $\quad a_p(E) = p - \#\text{solutions to } ☆ \bmod p.$

p	2	3	5	7	11	13	17	19	23	29	31	37	41	...
$a_p(E)$	-2	-1	1	-2	-5	4	-2	0	-1	0	7	3	-8	...

Conjecture: $a_p(E) \equiv p+1 \bmod 5$ $\quad (p \neq 11)$

$a_p(E)$ is coefficient of ξ^p in q-expansion of modular form of weight 2 for $\Gamma_0(11)$.

Definition: An elliptic curve over a field k (or ring)
is a smooth projective genus 1 curve with a marked point.

Key Idea: The points of an elliptic curve form a group
with the marked point the identity element.

Starting Point: Understand the definition and key idea via examples:

$k = \mathbb{C}$, $k = \mathbb{R}$ $k = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

Elliptic Curves over the Complex Numbers

Complex Torus, Genus 1
Riemann Surface

smooth curve: Riemann surface

projective: Compact

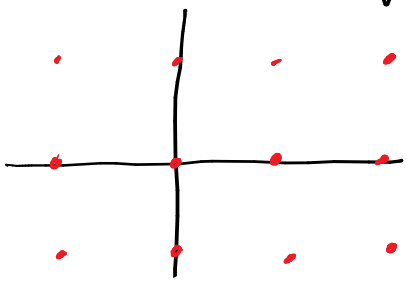
genus one: torus

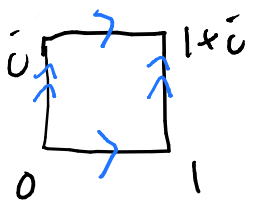
Group Law: Construct as $\mathbb{C}$ modulo a lattice

Lattice in $\mathbb{C}$: $\Lambda = \text{span}_{\mathbb{Z}}(v_1, v_2) = \{av_1 + bv_2 : a, b \in \mathbb{Z}\}$

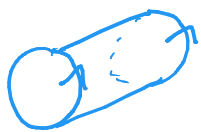
$v_1, v_2 \in \mathbb{C} \simeq \mathbb{R}^2$ lin. ind. over $\mathbb{R}$.

Example: $\Lambda = \mathbb{Z}^2 = \text{span}_{\mathbb{Z}}(1, i)$





$\mathbb{C}/\Lambda$: $z_1 \equiv z_2 \mod \Lambda$ if $z_1 - z_2 \in \Lambda$

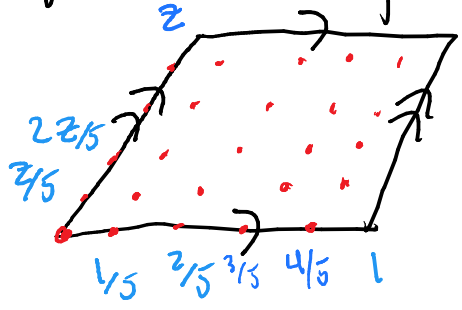


Group Law For Elliptic Curves over $\mathbb{C}$:

Realize as $\mathbb{C}/\Lambda$ (choice of origin arbitrary)

addition gives a group law identity is 0.

Example: 5-torsion points: $5z \equiv 0 \bmod \Lambda$ ie $5z \in \Lambda$.

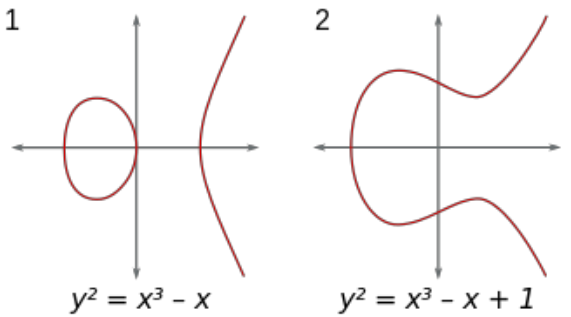


5-torsion is $\simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

$E[n]$ over $\mathbb{C}$
$\simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Elliptic Curves over the Real Numbers

$y^2 = x^3 + Ax + B$ plane curve $f(x,y) = x^3 + Ax + B - y^2 = 0$.



projective: add point "at infinity" $\mathcal{O}$

smooth: well-defined tangent line:

$\begin{bmatrix} \partial f/\partial x \\ \partial f/\partial y \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ on curve

genus 1 b/c degree 3

(Riemann-Hurwitz)

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

Relation with theory over $\mathbb{C}$

$\wp : \mathbb{C}/\Lambda \to \mathbb{C}$ Weierstrass $\wp$

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

Note: Smooth provided normal vector non-zero on curve.

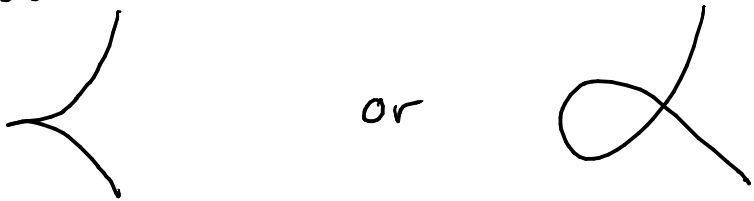
$\frac{\partial f}{\partial x} = 3x^2 + A = 0 \Rightarrow x = \sqrt{-A/3}$

$\frac{\partial f}{\partial y} = -2y = 0 \Rightarrow y = 0$

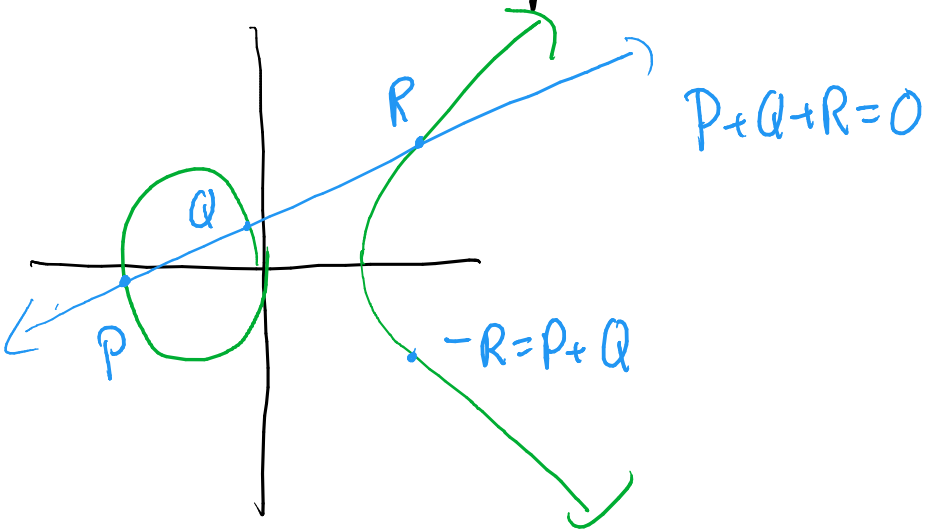
Solves $y^2 = x^3 + Ax + B$ iff $B^2 = -4/27\, A^3$.

ie $y^2 = x^3 + Ax + B$ smooth $\Leftrightarrow$ $27B^2 + 4A^3 \neq 0$.

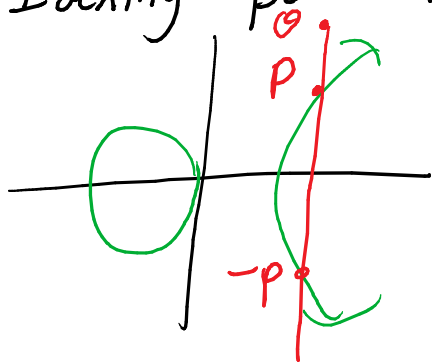
non-smooth



Group Law over $\mathbb{R}$

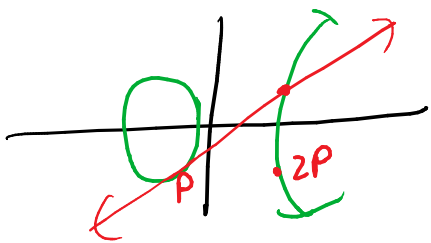


Identity: Point at infinity



Inverse: Reflect over x-axis

Doubling:



Associativity: !?!

Elliptic Curves Algebraically

The theory over $\mathbb{R}$ can be rephrased algebraically

Get complicated algebraic formula for group law.

[derivatives of polynomials don't need limits]

or

Define it to be smooth projective curve of genus 1 over k with a marked point. [Use that point to embed and get group law $E \xrightarrow{\sim} \mathrm{Jac}(E)$, $P \mapsto [P]-[O]$]

Example: $y^2+y = x^3-x^2$ $(=)$ $\left(y+\frac{1}{2}\right)^2 = x^3-x^2+\frac{1}{4}$

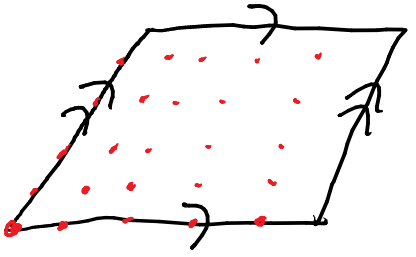
real solutions: curve

rational numbers: $(0,0)$ $(0,-1)$, $(1,0)$, $(1,-1)$, $\mathcal{O}$

(Could be infinite - see Daniel's talks)

Example: $y^2+y = x^3 - x^2$ elliptic curve E

Over Complex Numbers: 5-torsion points $E[5]$



$E[5](\mathbb{C}) \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$

$E(\mathbb{C})$ infinite

Over $\mathbb{Q}$: $E(\mathbb{Q}) \simeq E[5](\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$ $\{(0,0)\ (0,-1),\ (1,0),\ (1,-1),\ \mathcal{O}\}$

Over Finite Field: $E(\mathbb{F}_7) = \{\mathcal{O}, (0,0), (0,-1), (1,0), (1,-1),$
$(4,2), (4,4), (5,1), (5,5), (6,3)\}$

ten of them

$E: y^2+y = x^3 - x$ ✓

$a_p(E) = p+1 - \#E(\mathbb{Z}/p\mathbb{Z})$ includes point at infinity

p	2	3	5	7	11	13	17	19	23	29	31	37	41	...
$a_p(E)$	-2	-1	1	-2	-5	4	-2	0	-1	0	7	3	-8	...

Conjecture: $a_p(E) \equiv p+1 \mod 5$

$p \neq 11$

$(0,0)$ sol.

Explanation: There is a 5-torsion point on E with integer coordinates

This gives a 5-torsion point on E with coordinates in $\mathbb{F}_p$

$\Rightarrow \#E(\mathbb{F}_p)$ is a multiple of 5

What goes wrong for $p=11$: $y^2+y = x^3-x$ not smooth over $\mathbb{F}_{11}$.

Modularity of Elliptic Curves

Definition: If E is an elliptic curve defined by an equation with integer (or rational) coefficients, let $a_p(E) = p+1 - \#E(\mathbb{F}_p)$

Definition: E is modular if there exists a modular form f of wt 2 for $\Gamma_0(N)$ such that $a_p(E) = a_p(f)$ for every prime p.

Comments: Can determine N based on E

Omitted correct definition of $a_p(E)$ if $p \mid N$.

Problems with p such that E is not smooth mod. p

$E: y^2+y = x^3-x$ $\qquad a_p(E) = p+1 - \#E(\mathbb{F}_p)$

p	2	3	5	7	11	13	17	19	23	29	31	37	41	
$a_p(E)$	-2	-1	1	-2	-5	4	-2	0	-1	0	7	3	-8	...

Modular form wt 2 $\Gamma_0(11)$ $\qquad f(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = \sum a_n(f)q^n = q-2q^2-q^3+\dots$

n	2	3	5	7	11	13	17	19	23	29	31	37	41	
$a_n(f)$	-2	-1	1	-2	1	4	-2	0	-1	0	7	3	-8	...

Observed that $a_n(f) = a_p(E)$ for $p \neq 11$ ie E is modular.

(We have named this, not explained it)

Problem with 11: it's conductor/level. $y^2+y=x^3-x$ not smooth over $\mathbb{F}_{11}$

Theorem: Every elliptic curve defined over $\mathbb{Q}$ is modular.

Cor: There are no nontrivial solutions to $x^n + y^n = z^n$ with $n > 2$.

↑ Fermat's Last Theorem 1637

Taniyama and Shimura conjectured it 1957

Wiles, Taylor-Wiles proved for "many" ell curves '93-'95

Breuil-Conrad-Diamond-Taylor all ell. curves late 90's

Relationship: If $a^n + b^n = c^n$, $n > 2$, Frey curve $y^2 = x(x - a^n)(x + b^n)$ would have weird properties (not modular - Ribet '90)

Notes: Proof based on Galois representations (next talk)

Modularity theorem proven for elliptic curves over $\mathbb{Q}$

Siksek, Freitas, Le Hung: coefficients in real quadratic field like $\mathbb{Q}(\sqrt{5})$.
Use gen. of mod form

Open problem: coefficients in imaginary quadratic field like $\mathbb{Q}(\sqrt{-5})$.

See Quanta Article

"Amazing Math Bridge Extended Beyond Fermat's Last Theorem"

Why consider $a_p(E) = p+1 - \#E(\mathbb{F}_p)$?

1) Hasse-Weil: $\left|\#E(\mathbb{F}_p) - (p+1)\right| \leq 2\sqrt{p}$

2) Trace of Frobenius

Observe: $(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \dots + b^p$

$\equiv a^p + b^p \mod p$

i.e. Frobenius $F(x) = x^p$ is ring homomorphism in char p.

fixes $\mathbb{F}_p$, automorphism of $\mathbb{F}_{p^r}$ or $\overline{\mathbb{F}_p}$.

Consider $E: y^2 = x^3 + Ax + B$ w/ $A, B \in \mathbb{F}_p$. (x, y) point on curve.

Then $(F(x), F(y))$ also on curve: $F(y)^2 \stackrel{?}{=} F(x)^3 + AF(x) + B = F(x^3 + Ax + B)$

$E: y^2 = x^3 + Ax + B$ $\quad A, B \in \mathbb{F}_p$ $\quad$ obtain Frobenius $F_E : E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p)$

group isomorphism.

Fix $\ell \neq p$

Obtain: linear transformation of $E[\ell] \cong \mathbb{Z}/(\ell) \oplus \mathbb{Z}/\ell$

linear transformation of $E[\ell^2] \cong \mathbb{Z}/(\ell^2) \oplus \mathbb{Z}/(\ell^2)$

etc.

Definition: Tate module $T_\ell E = \varprojlim \left(\cdots \to E[\ell^3] \xrightarrow{[\ell]} E[\ell^2] \xrightarrow{[\ell]} E[\ell] \right)$

$\cong \mathbb{Z}_\ell^2 = \varprojlim \left(\cdots \to \left(\mathbb{Z}/(\ell^3)\right)^{\oplus 2} \to \left(\mathbb{Z}/(\ell^2)\right)^{\oplus 2} \to \left(\mathbb{Z}/(\ell)\right)^{\oplus 2} \right)$

linear transformation given by Frobenius.

Proposition: The characteristic polynomial of F_E on $T_\ell E$ is

$$X^2 - (p+1 - \#E(\mathbb{F}_p))X + p.$$

In particular, trace of Frobenius is $p+1-\#E(\mathbb{F}_p)$

Notes: Char poly of F_E ind. of ℓ; can mostly ignore $\mathbb{Z}_\ell$ vs $\mathbb{Z}$ at first glance

Tate module $T_\ell E$ is a concrete substitute for a cohomology theory for curves over finite fields

this perspective is really important

$a_p(E)$ and $p+1-\#E(\mathbb{F}_p)$ reflected Frobenius action on cohomology of E.

$H^1(E, \mathbb{Z}_\ell)$ dual to $T_\ell E$

↑ étale cohomology

An Interlude on L-functions (Time Permitting)

The Riemann Zeta Function: $\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ prime}} (1-p^{-s})^{-1}$ $\quad \mathrm{Re}(s) > 1$

Study to get prime number theorem

Riemann hypothesis

Dirichlet Series $\uparrow$

$\prod_{p} (1 + p^{-s} + p^{-2s} + \dots)$

$\downarrow$

Dirichlet L-function: $L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = \prod_{p \text{ prime}} (1 - \chi(p) p^{-s})^{-1}$

χ Dirichlet character

χ homomorphism $(\mathbb{Z}/m\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ extend by zero to $\mathbb{Z}$

$\zeta(s)$ defined for $\mathrm{Re}(s) > 1$. Riemann hypothesis about $\mathrm{Re}(s) = \frac{1}{2}$.

How to extend the zeta function: Reminder: extension results for holomorphic...

1) Find an alternative definition on a larger domain $\mathrm{Re}(s) > 0$

2) Prove a functional equation

If $\xi(s) = \pi^{-s/2}\,\Gamma(s/2)\,\zeta(s)$ then $\xi(1-s) = \xi(s)$

Extend to meromorphic function on $\mathbb{C}$ using ↗

L-Functions for Modular Forms

Definition: Let $f(q) = \sum_{n=1}^{\infty} a_n(f) q^n$ be a cusp form of weight k for $\Gamma_0(N)$.

if an eigenfunction for Hecke operators etc for forms in Langlands program

$$L_f(s) := \sum_{n=1}^{\infty} a_n(f) n^{-s} \qquad \mathrm{Re}(s) > 1 + k/2$$

$$= \prod_{p \nmid N} \left(1 - a_p(f) p^{-s} + p^{k-1} p^{-2s}\right)^{-1} \prod_{p \mid N} (\dots)$$

Mellin transform

$$\int_0^{\infty} f(ix) x^s \frac{dx}{x}$$

Functional Equation: $\overline{L}_f(s) = N^{s/2} (2\pi)^{-s} \Gamma(s) L_f(s)$

$$\overline{L}_f(s) = \pm \overline{L}_f(k-s) \quad (\text{all } s)$$

L-functions for Elliptic Curves

Let E be an elliptic curve defined over $\mathbb{Q}$.

Definition: $$L_E(s) = \prod_{p \nmid N_E} \left(1 - a_p(E)p^{-s} + p \cdot p^{-2s}\right)^{-1} \prod_{p \mid N_E} (\dots)$$

Converges $\mathrm{Re}(s) > 3/2$

Question: Extension? Functional equation?

no Dirichlet series directly

L-functions for Elliptic Curves

Let E be an elliptic curve defined over $\mathbb{Q}$.

Definition: $$L_E(s) = \prod_{p \nmid N_E} \left(1 - a_p(E)p^{-s} + p \cdot p^{-2s}\right)^{-1} \prod_{p \mid N_E} (\dots)$$

Converges $\mathrm{Re}(s) > 3/2$

no Dirichlet series directly

Question: Extension? Functional equation?

As E is modular, $\exists$ f weight 2 level N_E cusp form $a_p(E) = a_p(f)$

phrasing closer to Langlands

$$L_E(s) = L_f(s) = \prod_{p \nmid N_E} \left(1 - a_p(f)p^{-s} + p^{2-1}p^{-2s}\right)^{-1}$$ ← BSD about $s = 1$.