Lecture Notes:

Introduction: Elliptic curves: defining, minimals, L-functions, etc..

4.12: Defining elliptic curves

Defining elliptic variables:

$n \in \mathbb{N}$, $0 \in \Pi$ = the origin of the complex plane

$\mathcal{L}(n(0))$ denotes the $\mathbb{C}$-vector space of elliptic func. f attached to the lattice Λ with (at most) 1 pole at 0 of order $\leq n$, $\ell(n(0))$ is the dimension of the vector space

$\ell(n(0)) = n$, $\forall\, n \in \mathbb{N}$ — gamma

Generalizing: applying the above to a curve Γ defined over k

- assume $k(\Gamma)$ contains a simple point 0

  simple: as k.

- $k(\Gamma)$: function field: extension of k obtained by adjoining the coords of a generic point of Γ

Definition of an elliptic curve:

Let $\mathcal{L}(n(0))$ denote the k-vector space of functions on C which admit (at most) a pole at 0 of order $\leq n$ and let $\ell(n(0))$ denote the dimension. The pair $(\Gamma, 0)$ is an elliptic curve defined over k, if, for every $n \in \mathbb{N}$, we have $\ell(n(0)) = n$

(1) Every smooth cubic defined over k and with a rational point is an ell. curve

(2) Every curve which is birationally equiv. to an elliptic curve over k and with a rational point is an elliptic curve

An elliptic curve is a curve of genus one, defined over k, which has a rational point over k

4.12.2 Theorem: Let (Γ, O) be an elliptic curve defined over k, with function field $C = k(\Gamma)$. Then:

① There exist two functions x and $y \in C$, such that the map

phi ↓

$$\varphi \begin{pmatrix} \Gamma \to \mathbb{P}_2(k) \\ M \to (x(M), y(M), 1) \end{pmatrix}$$

is a birational map from (Γ, O) to a Weierstrass curve W of equation $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ defined over k, such that $\varphi(O) = (0,1,0)$

② Every other pair (x', y') can be written

$$\begin{cases} x' = u^2x + r \\ y' = u^3y + sx + t \end{cases}$$ with $u, r, s, t \in k$ and $u \neq 0$

↑ admissible change of coordinates

To show that a Weier... smooth cubic is an elliptic curve, you must show that it is of genus 1

① check that $\omega = dx/(2y + a_1 + a_3)$ (the differential) has no zeroes or poles

4.13: J-Invariant → $y^2 = x^3 + ax + b$

long Weierstrass → short: (completing the sq)

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, defined over K

$$\begin{cases} b_2 = a_1^2 + 4a_2 \\ b_4 = a_1a_3 + 2a_4 \\ b_6 = a_3^2 + 4a_6 \\ b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \end{cases}$$

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$$

$$\Delta = u^{12}\Delta'$$

Defining the j-variant: if $j = \frac{c_4^3}{\Delta} = 12^3\frac{c_4^3}{c_4^3 - c_6^2}$ is invariant under an admissable change of coords, j is the modular invariant of the curve E and is written $j(E)$

Every # $j \in K$ is the modular invariant of an elliptic curve over K

- if $j = 0$, $E: y^2 = x^3 + 1$
- if $j = 1728$, $E: y^2 = x^3 + x$
- else $E: y^2 + xy = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728}$

Theorem 4.13.1: A necessary + sufficient condition for 2 elliptic curves E and E' over K to be birationally equivalent over $\bar{K}$ is that they have the same j

Proof?

④

4.14 : Minimal Weierstrass eqs $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$

Defining minimal: The equation $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ is minimal at p if:

1) The eq is p-integral
2) $v_p(\Delta)$ cannot decrease because of a change of coords with coeffients in $\mathbb{Q}$ leading to a new p-integral eq

$v_p(\Delta)=0$

if $v_p=0$, then it is p-minimal

admissible change of coords:

$$\begin{cases} x=u^2x'+r \\ y=u^3y'+su^2x'+t \end{cases}$$

Proof 4.14.1

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

Assume the coefficients of equation f are p-integers. Then:

(i) If $|\Delta|_p \geq p^{-12}$ or $|c_4|_p \geq p^{-4}$ or $|c_6|_p \geq p^{-6}$, the equation is minimal

(ii) If $p>3$ and if $|\Delta_p| \leq p^{-12}$ and $|c_4|_p \leq p^{-4}$, not minimal

Suppose f is not minimal. $\Rightarrow \exists$ an admissible change of coords with coefficients in $\mathbb{Q}$ s.t. the new equation has coefficients a_i' in $\mathbb{Z}_p$ such that $|\Delta'_p|_p > |\Delta|_p$

$|\Delta|_p = |\Delta'|_p |u|_p^{12} \Rightarrow |u|_p^{12} < 1$, so $u_p \in \mathbb{Z}_{(p)}$

$\Rightarrow |\Delta|_p > p^{-12}$ and $\Delta' \in \mathbb{Z}$ so $|\Delta'|_p \leq 1$

$$\Rightarrow |u|_p^{12} = \frac{|\Delta|_p}{|\Delta'|_p} > p^{-12}$$

$\Rightarrow |u|_p = 1$ But that is a contradiction!

(ii) $p > 3$, $|\Delta|_p \leq p^{-12}$, $|c_4|_p \leq p^{-4}$

Since $1728\Delta = c_4^3 - c_6^2 \Rightarrow |c_6|_p \leq p^{-6}$

$\Rightarrow$ adm. change of coords

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$$

$$\begin{cases} x = p^2 x' \\ y = p^3 y' \end{cases} \Rightarrow y^2 = x^3 - \frac{c_4}{48p^4}x - \frac{c_6}{864p^6}$$

coefficients are p-integers,

discriminant $\Delta' = \Delta p^{-12} \Rightarrow |\Delta'|_p > |\Delta|_p$

$\therefore$ the existence of this curve shows it is <u>not</u> minimal

Define <u>globally minimal</u>:

① The eq has coefficients in $\mathbb{Z}$

② At every prime p, the equation is minimal

Neron's Theorem:

(i) Given elliptic curve E defined over $\mathbb{Q}$ by a Weierstrass eq, $\exists$ an admissible change of coords, w/ coeff. $\in \mathbb{Q}$ st. the new eq is globally minimal

(ii) 2 globally minimal eq for the same curve E, are related by an admissible change of coords st. $u = \pm 1$, $r, s, t \in \mathbb{Z}$

defining semi-stable:

Let E be an elliptic curve defined over $\mathbb{Q}$ and birationally equiv. over $\mathbb{Q}$ to a Weier. cubic W whose equation is minimal. The curve E is semi-stable $\Leftrightarrow$ if W has good reduction or multiplicate reduction ~~additive~~ at every prime

In order for E to be semi-stable, it is necessary and sufficient that Δ and c_4 be relatively prime

(7)(16)

4.15: Hasse-Weil Functions

Brief Overview of the Riemann Zeta function

defined over $\mathbb{C}$, for $Re(s) > 1$, by $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$

which can be decomposed into an Euler product

Zeta $\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$

- this means that every $n \in \mathbb{N} \geq 1$ can be uniquely written as a product of primes

from the Riemann zeta function, we can say $\Lambda(s) = -\Lambda(-s)$ for the rings of p-adic integers $\mathbb{Z}_p$ (whose non-zero ideals are of the form (p^v))

Artin Zeta Function

Define an elliptic curve E, over the finite fields $\mathbb{F}_p$

$E: Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6)$

associated to the Dedekind domain $A = \mathbb{F}_p[X,Y]/(E)$

- this being the quotient of the polynomial ring $\mathbb{F}_p[X,Y]$ by the ideal generated by E

zeta function of A:

$$\zeta_A(s) = \sum_{\substack{\text{ideal of } A \\ a \neq 0}} \frac{1}{N(a)^s}$$

Euler product:

$$\zeta_A(s) = \prod_{\substack{p \text{ prime ideal of } A \\ p \neq 0}} \frac{1}{1 - N(p)^{-s}}$$

$\Rightarrow$ for $s \in \mathbb{C}$ s.t. $Re(s) > 1$,

$$\zeta_E(s) = \frac{1}{1-p^{-s}} \zeta_A(s)$$

Artin's Theorem: $T = p^{-s}$, let N_E^n be the cardinal of the group of points of E in $\mathbb{F}_p$

Then $\zeta_E(s) = \frac{1 - a_E T + pT^2}{(1-T)(1-pT)}$

where $a_E = p + 1 - N_E$

Defining the L-function of E:

$L_E(s) = (1 - a_E p^{-s} + p \cdot p^{-2s})^{-1}$

by changing s to s-1 we get:

(i) $p^{-s} L_E = p^{s-1} L_E(1-s)$

(ii) $\zeta_E(s) = \zeta_E(1-s)$

Hasse-Weil L-function:

take an elliptic curve over $\mathbb{Q}$ by a globally minimum eq

$E = O$

$$L_E(s) = \prod_p L_p(s)$$ where

$$L_p(s) = \begin{cases} L_{\tilde{E}_p}(s) & \text{if } E \text{ has good reduction at } p \\ (1-p^{-s})^{-1} & \text{if } E \text{ has multiplicative reduction w/ rational tangent} \\ (1+p^{-s})^{-1} & \text{if } E \text{ has multiplicative reduction w/ irrational tangent} \\ 1 & \text{if } E \text{ has additive reduction at } p \end{cases}$$

The three cases only occur for prime numbers that divide the discriminant of E

- $\tilde{E}_p$ is the elliptic curve over $\mathbb{F}_p$ deduced from E (mod p)

$L_{\tilde{E}_p}(s) = (1 - \theta_p p^{-s})^{-1} (1 - \bar{\theta}_p p^{-s})^{-1}$, θ_p is an arbitrary root of $1 - a_{\tilde{E}_p} T + pT^2$

Hasse and Weil conjecture: the functions L_E associated to elliptic curves E defined over $\mathbb{Q}$ possess meromorphic continuations to the whole complex plane

In order to show that the function L_E satisfies a functional eq, we must define the conductor

Let E be a globally minimal eq of an elliptic curve over $\mathbb{Q}$

The conductor $N_E = \prod_{p \text{ prime}} p^{f_p}$

where $f_p = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative} \\ 2+\delta_p \text{ with } \delta_p \geq 0 & \text{if } E \text{ has additive reduction} \end{cases}$

limiting ourself to $\delta_p = 0$ when $p > 3$ (delta)

the functional equation of L_E:

$$\Lambda_E(s) := \left(\frac{\sqrt{N_E}}{2\pi}\right)^s \Gamma(s) L_E(s)$$

$$\Lambda_E(s) = w \Lambda_E(2-s), \quad w = \pm 1$$

Birch-Swinnerton-Dyer conjecture:

the rank r of the Mordell-Weil group of an elliptic curve E defined over $\mathbb{Q}$ is equal to the order of the zero of $L_E(s)$ when $s = 1$

or: $$\prod_{\substack{p \leq R \\ p \nmid \Delta}} \frac{\text{card}(\tilde{E}_p(\mathbb{F}_p))}{p} \sim C(\log R)^r$$

Consider an e curve E defined over $\mathbb{Q}$ and prime p.

(i) eq of E can be made minimal at p by an admissible change of coords

(ii) if the coeff of E are already p-integers, then the coeffs are also p-integers

(iii) 2 minimal eq at p coming from E are related by an admissible change of coords for which $|u|_p = 1$, i.e., $r, s, t \in \mathbb{Z}_p$

Proof for $p > 3$

(i) Assume E has integral coeff. $|\Delta|_p \leq 1$. Since $|\Delta|_p > 0$, there are only a finite # of possible $|\Delta'|_p$ between $|\Delta|_p$ and $1 \Rightarrow \exists$ a minimal eq.

(ii) if the new eq is minimal, the eq. of $u^{12}\Delta' = \Delta$ shows $v_p \leq 1$. Since $a_i' \in \mathbb{Z}_p \Rightarrow s, r, t \in \mathbb{Z}_p$

(iii) if eq of E' is min. we saw that $|u|_p \leq 1$
$|u^{-1}|_p \leq 1 \Rightarrow |u|_p \geq 1 \Rightarrow |u|_p = 1$