ARIYAN (2) Shafarevich Theorem for ell. curves

k field

Def A pair (E,O) with E smooth proj geom connected curve $/k$ and $O = O_E \in E(k)$ is an ELLIPTIC CURVE $/k$ (with identity O) if genus $E = 1$ $\left(= h^0(E,\omega_E)\right)$

STRUCTURE

- Assume $k = \bar{k}$

$$\mathrm{Pic}^0_{E/k}(k) = \{ D : E(k) \to \mathbb{Z} \ : \ D \text{ divisor, } \deg D = 0 \} / \sim$$

$$\begin{array}{ccc} E(k) & \xrightarrow{\varphi} & \mathrm{Pic}^0_{E/k} \\ P & \longmapsto & [P] - [O_E] \end{array}$$

1) φ bijection
2) $E(k)$ is abelian group
3) group structure is compatible with algebraic structure

- $k = \mathbb{C}$

$E/\mathbb{C} \rightsquigarrow E^{an}$ compact R.S. connected

univ. cover $\mathbb{C} \longrightarrow E^{an} \cong \mathbb{C}/\Lambda \qquad \Lambda = \pi_1(E^{an})$

$\mathbb{C}/\Lambda \simeq \mathbb{R}^2/\mathbb{Z}^2 \simeq \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ ⊖

- $N \geq 1 \qquad H^0(E, NO_E) \qquad h^0(E, NO_E) = N$

$$\begin{array}{ccccccccc} H^0(E,O_E) & \subseteq & H^0(E,2O_E) & \subseteq & H^0(E,3O_E) & \subseteq & \cdots & \subseteq & H^0(E,6O_E) \\ \| & & \| & & \| & & & & \cup \\ k = k\cdot 1 & & \langle 1, x\rangle & & \langle 1, x, y\rangle & & & & \{1, x, x^2, x^3, y, \\ & & & & & & & & xy \end{array}$$

1. $E \longrightarrow k$

$x \in H^0(E,2O_E)$ $\quad y \in H^0(E,3O_E)$ $\quad x^2 \in H^0(E,4O_E)$

$x \notin H^0(E,O_E)$ $\quad y \notin H^0(E,2O_E)$ $\quad y^3 \in H^0(E,6O_E)$

7 elements in $H^0(E,6O_E)$ $\longrightarrow$ linearly dependent

If $6 \in k^*$ $\quad y^2 = x^3 + Ax + B$ $\quad A, B \in k$ Weierstraß equat.

$$E \longrightarrow \mathbb{P}^2_k$$

$$\searrow^{\sim} \quad C = \{ y^2 = x^3 + Ax + B \}$$

Rmk

E does not determine A, B

Ex : $E_t = \{ y^2 = x^3 + t \}$ / $k(t)$

is isomorphic to $y^2 = x^3 + 1$ over $k(\sqrt[6]{t})$

Def Let $y^2 = x^3 + Ax + B$ be a Weierstraß equation

$\Delta := -16(4A^3 + 27B^2)$ discriminant

$j := -1728 \dfrac{(4A)^3}{\Delta}$

PROP

1) the curve $y^2 = x^3 + Ax + B$ def /k is SINGULAR $\Leftrightarrow \Delta =$

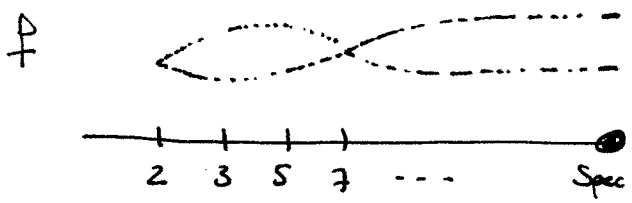
2) j only depends on isom class of the curve

Rmk :

Let $f(x) \in \mathbb{Z}[x]$ of degree 2 $f(x) = x^2 + bx + c$

$\Delta(f) = b^2 - 4c$

assume $\Delta \neq 0$, i.e. f has no double root / $\overline{\mathbb{Q}}$



if $2 | \Delta$ and $7 | \Delta$

in general $p | \Delta \rightsquigarrow \Delta \equiv 0 \mod p$

$\rightsquigarrow f$ has double root in $\overline{\mathbb{F}_p}$

ELLIPTIC CURVES OVER $\mathbb{Q}$

Def Given $E/\mathbb{C}$ ell curve, E can be defined over $\mathbb{Q}$ if $\exists$ weierstraß equation for E

$$y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Q}$

Lemma

E can be defined over $\mathbb{Q} \Longleftrightarrow j(E) \in \mathbb{Q}$

What about $\Delta(E)$?

Lemma $E/\mathbb{Q}$ ell curve. Then $\exists$ Weierstraß Eq

$$y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{Q}$$

$$\star \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad a_i \in \mathbb{Z}$$

Finally, for all prime numbers p

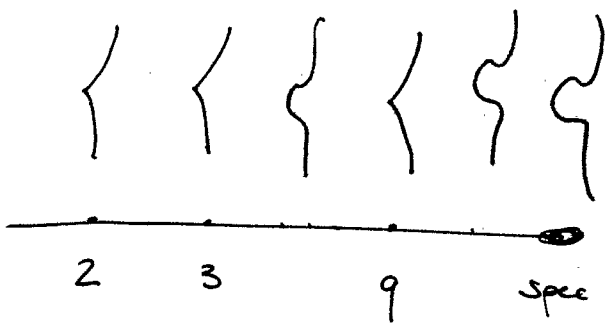
$$\mathrm{ord}_p(\Delta(*)) = \min\{ v_p(\Delta) \mid \text{Weierstraß eq for } E \text{ with coeff in } \mathbb{Z} \}$$

$$\Delta(*) = \Delta_{min}(E)$$

minimal discriminant of $E/\mathbb{Q}$

Let $E/\mathbb{Q}$, $\Delta = \Delta_{min}(E)$

example: $y^2 = x^3 + q$ q prime $\qquad \Delta_{min} = -2^4 3^3 q^2 \neq 0$



2, 3 and q are the primes of bad reduction for E over $\mathbb{Z}$

Def E has bad reduction at p if $p \mid \Delta_{min}(E)$

clearly: $\Delta \in \mathbb{Z} \setminus \{0\} \Rightarrow S_{bad} = S = \{p : E \text{ bad reduct at } p\}$ IS FINITE!

note: E extends to an elliptic curve $/\mathbb{Z}[S^{-1}]$

NUM FIELD	FUN FIELD
$S \subset \{$primes in $\mathbb{Z}\}$	$S = \{p_1 - p_n\} \subseteq \mathbb{A}^1_{\mathbb{C}}$
$d > 1$	$d > 1$
$\{K$ # fields : deg $\leq d$ ramif over $S\}$	$\left\{ \begin{array}{c} X \\ \downarrow \\ \mathbb{A}^1_{\mathbb{C}} \end{array} \right.$ degree $\leq d$, Ramified only over S $\}$
$\{ \begin{array}{c} X \\ \downarrow \\ \mathrm{Spec}\,\mathbb{Z} \end{array}$: deg $\leq d$ ramif over $S\}$	
IS FINITE	IS FINITE

Spec $\mathbb{Z}$ is simp conn.	$\mathbb{A}^1_{\mathbb{C}}$ is simply connected i.e. no non-trivial finite étale cover of $\mathbb{A}^1_{\mathbb{C}}$
There are no elliptic curves over Spec $\mathbb{Z}$ (TATE)	There are no non-isotrivial ell. curve over $\mathbb{A}^1_{\mathbb{C}}$

Thm (Shafarevich 1962)
S finite set of pants of Spec $\mathbb{Z}$
Then the set of isomorphism classes of ell. curves/$\mathbb{Q}$ with bad reduction at S only, is FINITE.

Aim: prove an eff. version of Shaf Thm.

UNIT EQUATION: A ring of finite type / $\mathbb{Z}$ $A \subseteq \mathbb{C}$ ex $A = \mathbb{Z}[\frac{1}{2}]$

unit equation: $x + y = 1$ $\quad x, y \in A^*$

Thm (Györy-yu, Siegel-Mahler-Lang, Evertsee-Györy)
$\{(x,y) : x+y=1,\ x,y \in A^*\}$ is Finite and effectively computable

Rmk:
$$\{(x,y) : x+y=1 \quad x,y \in A^*\} \subset A^2$$
$$\| $$
$$\{(x,y) : x(x-1)y - 1 = 0\} \subset A^2$$
$$\| $$
$$\mathrm{Spec}\left(\mathbb{Z}\left[x, \tfrac{1}{x}, \tfrac{1}{x-1}\right]\right)(A)$$
$$\| $$
$$(\mathbb{A}^1_{\mathbb{Z}} - \{0,1\})(A) = (\mathbb{P}^1_{\mathbb{Z}} - \{0,1,\infty\})(A)$$

proof Let $E/\mathbb{Q}$ be an elliptic curve with good reduction outside $S \subseteq$ Spec $\mathbb{Z}$

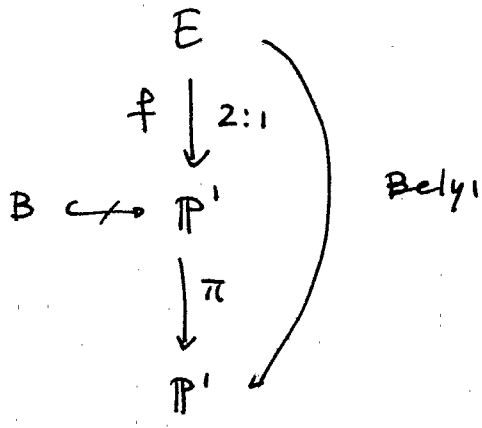
For simplicity: assume E: $y^2 = x(x-1)(x-\lambda)$ with $\lambda \in$ 4/7

$\lambda \in \mathbb{Q}$, but since E has good reduction outside S

can choose $\lambda \in \mathbb{Z}[S^{-1}]$ $\rightsquigarrow$ $\lambda \neq 0$ $\lambda \neq 1$ mod $p \notin S$

$\Leftrightarrow$ λ and $\lambda^{-1} \in \mathbb{Z}[S^{-1}]^*$ so λ solve the unit equation.

The result follows from Evertse-Győry $\square$



$h(E) \leq \deg(X) \leq 2 \deg \pi$
$\leq c \cdot \text{Height}(B)$