PREVIOUSLY...

THM. (Riemann-Roch) Let C be a smooth curve, K_C a canonical divisor. Let $\mathcal{L}(D) = \{f \in \bar{K}(C)^* : \operatorname{div}(f) \geq -D\} \cup \{0\}$. Then, there is $g \geq 0$ s.t. for all $D \in \operatorname{Div}(C)$ we have $\boxed{\ell(D) - \ell(K_C - D) = \deg D - g + 1}$ where $\ell(D) = \dim_{\bar{K}} \mathcal{L}(D)$.

COR. (a) $\ell(K_C) = g$, (b) $\deg(K_C) = 2g-2$, (c) If $\deg D > 2g-2$, then $\ell(D) = \deg D - g + 1$.

THM. (Hurwitz) Let $\phi : C_1 \to C_2$ be a non-constant, separable, map of smooth curves. Then $\boxed{2g_1 - 2 \geq (\deg \phi) \cdot (2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1)}$ with equality if (i) char $K = 0$ or (ii) $\operatorname{char}(K) = p > 0$ and $p \nmid e_\phi(P)$ for all $P \in C$.

COR. Let E be a smooth curve of genus 1 over K, w/ $\mathcal{O} \in E(K)$. Then there is an iso$/K$ $\phi : E \longrightarrow C$ where $C: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$, $a_i \in K$

WEIERSTRASS MODEL. (smooth)

Example: Let $d \geq 1$, and let $E: x^3 + y^3 = d$

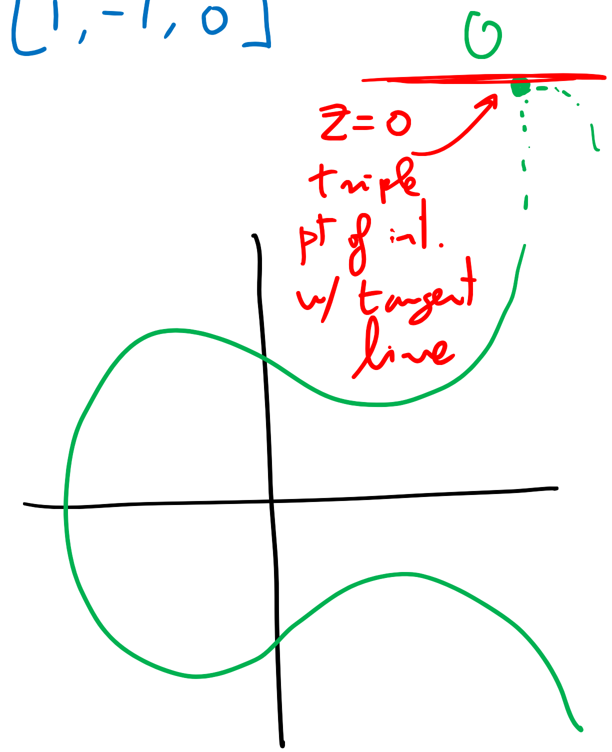
$$X^3 + Y^3 = dZ^3 \quad \ni \mathcal{O} = [1, -1, 0]$$

$$\psi : E \longrightarrow \hat{E} : ZY^2 = X^3 - 432 d^2 Z^3$$

$$[X, Y, Z] \longmapsto [12dZ, \ 36d(X - Y), \ X + Y]$$

$$\psi^{-1} : \hat{E} \longrightarrow E$$

$$[x, y, z] \longmapsto \left[\frac{36dz + y}{72d}, \ \frac{36dz - y}{72d}, \ \frac{x}{12d}\right]$$



$$\{x^3 + y^3 = d\} \longrightarrow \{y^2 = x^3 - 432 d^2\}$$

$$(x, y) \longmapsto \left(\frac{12d}{x+y}, \ \frac{36d(x-y)}{x+y}\right)$$

* From generic smooth cubic to Weierstrass form:
- Silverman/Tate
- Number Theory & Geometry §15.3

III. Elliptic Curves.

DEF. An elliptic curve E/K (defined over a field K) is a smooth curve of genus 1 together w/ a pt. $\mathcal{O} \in E(K)$.

$$E(K) = \{\text{points on } E \text{ defined over } K\}$$
$$E(\overline{K}) = \{\text{pts on } E \text{ defined over } \overline{K}\}$$

NOTE: E/K can be written in a Weierstrass model:

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

(LONG) WEIERSTRASS MODEL

for some $a_i \in K$.

Simplify the model: • If char $K \neq 2$, then $y \mapsto \frac{1}{2}(y - a_1x - a_3)$

gives
$$\boxed{y^2 = \underbrace{4x^3 + b_2x^2 + 2b_4x + b_6}_{\Delta = \text{the discriminant of this polynomial.}}}$$
for some $b_i \in K$.

• If $\mathrm{char}(K) \neq 2,3$, then $(x,y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right)$

gives $y^2 = x^3 - 27c_4 x - 54c_6$

for some $c_4, c_6 \in K$. $\rightsquigarrow$ $y^2 = x^3 + Ax + B$ (SHORT) WEIERSTRASS MODEL

• changes of variables? that preserve short W. models?

$$\begin{cases} x = u^2 x' \\ y = u^3 y' \end{cases}$$

on a LONG WEIER. MODEL $y^2 + a_1xy + \dots = x^3 + a_2x^2 \dots$

$\downarrow$

$y^2 - \frac{a_1}{u}xy + \dots = x^3 + \frac{a_2}{u^2}x^2 \dots + \frac{a_4}{u^4}x + \frac{a_6}{u^6}$

E $\quad y^2 = x^3 + Ax + B \longleftrightarrow$ E' $\quad y'^2 = x'^3 + \frac{A}{u^4}x' + \frac{B}{u^6}$

We can give a unique model for $E/\mathbb{Q}$ w/ $A, B \in \mathbb{Z}$ and no $u \in \mathbb{Z}$ s.t. $u^4 \mid A$, $u^6 \mid B$.

In (short) Weierstrass:

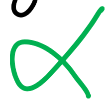
$$\boxed{\Delta = \text{discriminant of } E/\mathbb{Q}} = -16(4A^3 + 27B^2), \quad \boxed{c_4 = -48A}$$

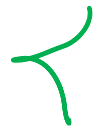
$$\boxed{j = j\text{-invariant of } E/\mathbb{Q}} = \frac{-1728(4A)^3}{\Delta} = \frac{(c_4)^3}{\Delta}$$

$\Delta' = \frac{\Delta}{u^{12}}$, $j' = j$, $c_4' = \frac{c_4}{u^4}$

PROP. III.1.4 Let E be a curve given by a Weierstrass eq'n.

(a) (i) It is non-singular $\iff \Delta \neq 0$.

(ii) Has a node  $\iff \Delta = 0,\ c_4 \neq 0$

(iii) Has a cusp  $\iff \Delta = 0,\ c_4 = 0$.

(b) Two elliptic curves are isomorphic (over $\overline{K}$, not nec. $/K$) iff they have the same j-invariant.

(c) Let $j_0 \in \overline{K}$. Then there exists an elliptic curve over $K(j_0)$ with j-invariant equal to j_0.

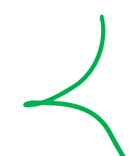
is singular if $\begin{cases} y^2 = f(x) \\ \partial F/\partial x = 0 \rightsquigarrow f'(x)=0 \\ \partial F/\partial y = 0 \rightsquigarrow y = 0 \\ \partial F/\partial z = 0 \end{cases}$ $\left.\begin{matrix} f(x)=0 \\ f'(x)=0 \end{matrix}\right\}$ $f(x)$ has a double root.

(ASSUME char $k \neq 2,3$)

__Proof.__ (a) Δ is the discriminant of $y^2 = f(x)$.

and $\Delta = 0 \iff f(x)$ has a double root $\iff$ the model is singular. (i) ✓

(ii) + (iii) $y^2 = x^3 + Ax + B$, $c_4 = 0 \iff A = 0$

$c_4 = 0$, $\underset{-16(4A^3+27B^2)}{\Delta \overset{\shortparallel}{}} = 0 \iff A=0, B=0 \Rightarrow y^2 = x^3$  cusp

$c_4 \neq 0$
$\Delta = 0$  node.

(b) E, E' two elliptic curves $/K$, both in Weierstrass models

- If $E \cong E'$ are isom., then isom is a linear change of variables and these leave j unchanged, i.e., $j = j'$.

- If $j(E) = j(E')$, and char $k \neq 2, 3$, then $E: y^2 = x^3 + Ax + B$

$E': y^2 = x^3 + A'x + B'$

$$j = j' \Rightarrow \frac{A^3}{4A^3 + 27B^2} = \frac{A'^3}{4A'^3 + 27B'^2} \Longrightarrow \boxed{A^3 B'^2 = A'^3 B^2}$$

$\boxed{\text{CASE 1}}$. $A = 0$ (so $j = 0$), $B \neq 0$ (b/c $\Delta \neq 0$) $\Rightarrow A' = 0$, change $u = \left(B/B'\right)^{1/6}$

$(x, y) \overset{*}{\longmapsto} (u^2 x', u^3 y')$

$\boxed{\text{CASE 2.}}$ $B = 0$ (so $j = 1728$), $A \neq 0$ $\Rightarrow B' = 0$, change $u = \left(A/A'\right)^{1/4}$

Recall: $y^2 = x^3 + Ax + B \overset{*}{\rightsquigarrow} y^2 = x^3 + \frac{A}{u^4} x + \frac{B}{u^6}$

$\boxed{\text{CASE 3}}$ $AB \neq 0$, $\left(\frac{A}{A'}\right)^3 = \left(\frac{B}{B'}\right)^2$, $u = \left(\frac{A}{A'}\right)^{1/4} = \left(\frac{B}{B'}\right)^{1/6} \rightsquigarrow E \cong E'$. $\blacksquare$

- $j_0 \in \overline{K}$
  - $j_0 \neq 0, 1728$, take

$$\boxed{E_{j_0} : \; y^2 + xy = x^3 - \frac{36}{j_0 - 1728}\, x - \frac{1}{j_0 - 1728}}$$

has $\Delta = \dfrac{j_0^2}{(j_0 - 1728)^3} \neq 0$ and $j(E_{j_0}) = j_0$.

  - $j_0 = 0$, take $y^2 + y = x^3$, $\Delta = -27$, $j = 0$
  - $j_0 = 1728$, take $y^2 = x^3 + x$, $\Delta = -64$, $j = 1728$. $\blacksquare$

ex

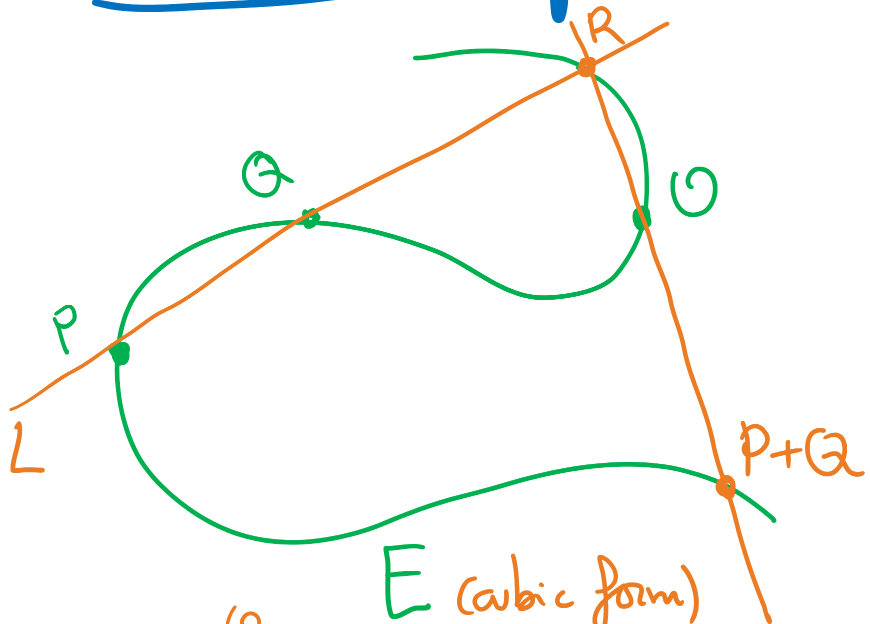
$j = 0 \quad y^2 + y = x^3$

$j = 1 \quad y^2 + xy = x^3 + 36x + 3455$

$j = 2 \quad y^2 = x^3 + x^2 + 288x + 55264$

$j = -\dfrac{2^{12}}{11} \quad y^2 + y = x^3 - x^2$

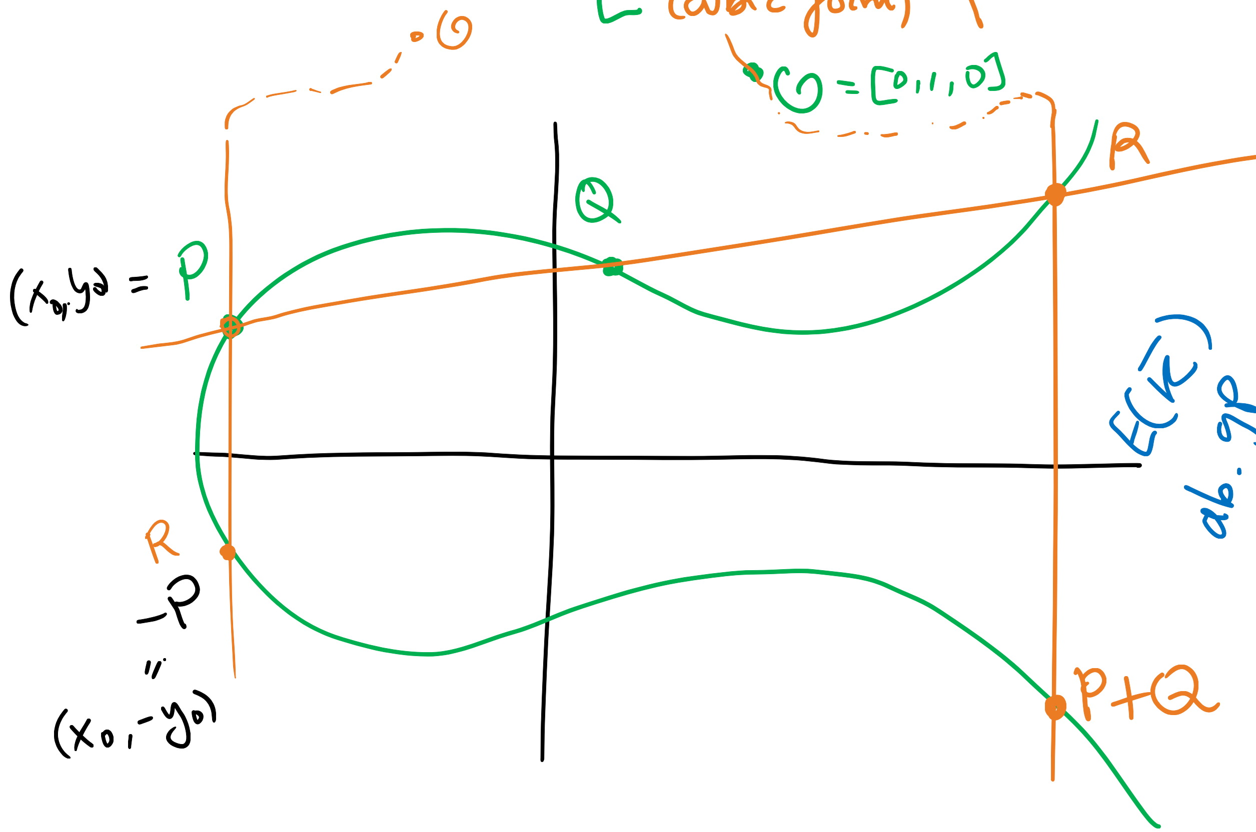
§2. The Group Law



L : line thru P, Q, and R

L' : line thru R, $\mathcal{O}$, and P+Q.

KEY: Tangent line at $\mathcal{O}$ in a Weier. model is $\{Z=0\}$ and it has a <u>triple</u> point of intersection at $\mathcal{O}$. (exercise)



PROP.

(a) If $\mathcal{O}$ is an inflection pt, and if L intersects E on P, Q, R, then $(P+Q)+R=\mathcal{O}$.

E(K) ab. gp

(b) $P+\mathcal{O}=P$ for all $P\in E$.

(c) $P+Q=Q+P$ for all $P,Q\in E$.

(d) $\forall P\in E$, $\exists\,(-P)\in E$ s.t. $P+(-P)=\mathcal{O}$.

(e) $(P+Q)+R=P+(Q+R)$ $\forall P,Q,R\in E$

(f) $(E(K),+)$ is a subgp of E.