PREVIOUSLY...

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

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1$$

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

$$2g_1 - 2 \geq (\deg \phi)\cdot(2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1)$$

with equality if (i) $\mathrm{char}\, K = 0$ or (ii) $\mathrm{char}(K) = p > 0$ 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

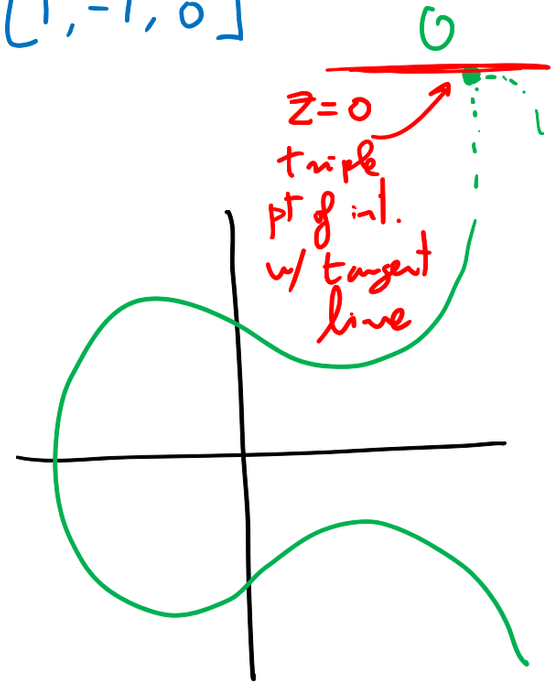
$$\phi : E \longrightarrow C$$

where C: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in K$ (Smooth)

WEIERSTRASS MODEL.

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

$X^3 + Y^3 = d Z^3 \Rightarrow O = [1, -1, 0]$



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

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

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

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

or

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

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

* 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:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad \left(\begin{array}{c}\text{(LONG)}\\ \text{WEIERSTRASS}\\ \text{MODEL}\end{array}\right)$$

for some $a_i \in K$.

Simplify the model: • If $\operatorname{char} K \neq 2, t$