Elliptic curve $E: Y^2Z = X^3 + aXZ^2 + bZ^2$, $a, b \in \mathbb{Q}$, $\Delta = 4a^3 + 27b^2 \neq 0$

~~Change variables~~ $\cancel{X \mapsto \frac{X}{c^2}, Y \mapsto \frac{Y}{c^3}, Z \mapsto Z}$, ~~assume~~ $\cancel{a, b \in \mathbb{Z}}$

Look at them mod p, curve E over $\mathbb{F}_p$

1) Algebraic groups of dim. 1 · Assume k is a separable field (every finite extension is separable)

i) ~~Elliptic curves: only irreducible projective curves having a group~~ structure defined by poly maps

ii) · Additive group $\mathbb{G}_a$

$\mathbb{A}^1(k) = k$, $(x, y) \mapsto x + y : k \times k \to k$

iii) · Multiplicative group $\mathbb{G}_m$

$\mathbb{A}^1(k) \setminus \{0\} = k^\times$, $(x, y) \mapsto xy : k^\times \times k^\times \to k^\times$

$\cancel{(x \mapsto (x, x^{-1}) \Rightarrow \mathbb{G}_m \leftrightarrow \text{affine } XY = 1}$

iii) Twisted multiplicative groups, a nonsquare in $k^\times$, $L := k(\sqrt{a})$

~~Claim~~ ~~∃ alg.~~ $\cancel{\mathbb{G}_m\{a\}}$ ~~(this is definition) over k s.t.~~

$\cancel{\mathbb{G}_m\{a\}(k) = \{\gamma \in L^\times \mid N_{L/k}(\gamma) = 1\}}$

· Define $\alpha = \sqrt{a}$ s.t. $\{1, \alpha\}$ basis

$(x + \alpha y)(x' + \alpha y') = xx' + ayy' + \alpha(xy' + x'y)$

$N_{L/k}(x + \alpha y) = (x + \alpha y)(x - \alpha y) = x^2 - ay^2$

~~· Define~~ $\cancel{\mathbb{G}_m\{a\}}$ ~~to be~~ $\cancel{X^2 - aY^2 = 1}$ ~~w/ group structure~~

$(x, y) \cdot (x', y') = (xx' + ayy', xy' + x'y)$

Invertible change of variables transforms $\mathbb{G}_m\{a\} \to \mathbb{G}_m\{ac^2\}$, $c \in k^\times$

$\Rightarrow \mathbb{G}_m\{a\}$ only depends on $k(\sqrt{a})$

~~When a is square in k,~~ $\cancel{X^2 - aY^2 = (X + \alpha Y)(X - \alpha Y) = X'Y' = 1}$

$\Rightarrow \mathbb{G}_m\{a\} \cong \mathbb{G}_m$ over $k(\sqrt{a}) = k$, ~~hence the~~ ~~twists~~ $\cancel{\mathbb{G}_m\{a\}}$

C, D projective plane curves, no comp. component in common
m n

C and D intersect over k^{al} at exactly mn pts $\sum_{p \in C(k^{al}) \cap D(k^{al})} I(p, C \cap D) = mn$

$X^2 - aY^2 = 0$
$\left(\frac{X}{Y}\right)^2 = a$

Ex. $k = \mathbb{F}_q \Rightarrow |G_a(k)| = q$, $|G_m(k)| = q-1$, $|G_m[a](k)| = q+1$ for any nonsquare a in k

~~From field theory~~, $\cancel{\mathbb{F}_q(\sqrt{a}) = \mathbb{F}_{q^2}}$

~~$\Rightarrow \exists$ exact sequence~~ $\cancel{0 \xrightarrow{\phi} G_m[a](\mathbb{F}_q) \xrightarrow{\varphi} \mathbb{F}_{q^2} \xrightarrow{\chi} \mathbb{F}_q^{x} \to 0}$ $\quad \varphi = N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\ )$

$\therefore \varphi$ is surjective, and by 1st isomorphism thm, $|G_m[a](k)| = \frac{q^2-1}{q-1} = q+1$

Q: In previous talk, if nonsingular projective curve has genus 1, then it has a group structure A: Converse is true - pf uses Lefschetz fixed pt theorem

Singular Cubic curves E singular plane projective curve over perfect k, char$(\,) \neq 2$

→ · Bezout's thm / in Adam's talk only 1 singular pt

· Assume $E(k)$ has pt $O \neq S$: then $E^{ns}_{(k)} := E(k) \setminus \{S\}$ is a group w/ zero O

· Consider line through two nonsingular pts P, Q; by Bezout, it will only intersect at one additional pt, PQ, which can't be singular

~~$P+Q := $ 3rd pt of~~ intersection ~~b/w line through~~

PQ and O and cubic Two cases:

1) Cubic curves w/ cusps:

(1.12) $E: Y^2Z = X^3$ has a cusp at $S = (0:0:1)$ b/c $y^2 = x^3$ has a cusp at $(0,0)$

· S only pt on curve w/ Y-coord. 0, so $E(k) \setminus \{S\} = E \cap \{Y \neq 0\}$

$= E_1 : Z = X^3$

$Z = aX + \beta$ intersects E_1 at $P_i = (x_i, z_i)$, $1 \leq i \leq 3$, x_i roots of $X^3 - aX - \beta$

$x_1 + x_2 + x_3 = 0$, by Vieta

~~$\Rightarrow$ When $P_1 + P_2 + P_3 = 0$ (i.e. all lie on same line)~~,

$x(P_1) + x(P_2) + x(P_3) = 0$

$Y^2 = X^3 + aX^2$ tangent $y = \pm\sqrt{a}x$ define $\Leftrightarrow$ a is square

singularity $a \neq 0 \Rightarrow$ node
$a = 0 \Rightarrow$ cusp

$O = (0,0) \Rightarrow P \mapsto -P$ is $(x,z) \mapsto (-x,-z)$ so $P \mapsto x(P)$ satisfies $x(-P) = -x(P)$

~~$\Rightarrow P \mapsto x(P) : E_1(k) \to k$ is a homomorphism~~

$\underset{E \setminus \{S\}}{\overset{\shortparallel}{}}$ $\quad \underset{G_a}{\overset{\shortparallel}{}}$

$P \mapsto \frac{x(P)}{y(P)} : E \setminus \{S\} \to G_a$ is an isomorphism of algebraic groups

2) Cubic Curve w/ a node:

~~$(t,6) \to$ $Y^2Z = X^3 + cX^2Z$, $c \neq 0$ has node at $(0:0:1)$ b/c $Y^2 = X^3 + cX^2$ has~~

a node at $(0,0)$

· Tangent lines at $(0,0)$ given by $y^2 - cx^2 = 0$
$\shortparallel$
~~$(y - \sqrt{c}x)(y + \sqrt{c}x)$ when c is a square~~

rational over k

$\Rightarrow E^{ns} = E \setminus \{\text{singular pt}\}$
$\cong G_m$

· c not a square $\Rightarrow$ tangent lines not rational over $k \Rightarrow \cong G_m[c]$

Criterion $E : Y^2Z = X^3 + aXZ^2 + bZ^3$, $a, b \in k$, $\Delta = 4a^3 + 27b^2 = 0$

Q: Which of the above cases does E fall into? Assume char$(k) \neq 2, 3$

· $(0:1:0)$ always nonsingular $\Rightarrow$ only need to study

~~$\to Y^2 = X^3 + aX + b$~~

· We wish to find a t s.t. $y^2 = (x-t)^2(x+2t) = x^3 - 3t^2x + 2t^2$

$\Rightarrow$ need to choose t s.t. $t^2 = -a/3$, $t^3 = b/2 \Rightarrow t = \frac{b/2}{-a/3} = -\frac{3}{2}\frac{b}{a}$

Rewrite as

$y^2 = 3t(x-t)^2 + (x-t)^3$

· Has singularity at $(t, 0)$ → 1) cusp if $3t = 0$

2) node w/ rational tangents if $3t$ is square in k

3) node w/ irrational tangents if $3t$ is nonsquare in $k^\times$

$-2ab = -2(-3t^2)(2t^3) = (2t^2)^2\, 3t$

$\Rightarrow$ ~~$3t$ is nonzero / square / nonsquare, according to $-2ab$~~

$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Reduction of an elliptic curve

$E: Y^2Z = X^3 + aXZ^2 + bZ^3$; $a, b \in \mathbb{Q}$, $\Delta = 4a^3 + 27b^2 \neq 0$

change $X \mapsto X/c^2$, $Y \mapsto Y/c^3$ w/ c chosen s.t. $a, b \in \mathbb{Z}$, $|\Delta|$ minimal

equation is minimal

$\bar{E}: Y^2 Z = X^3 + \bar{a}XZ^2 + \bar{b}Z^3$, $\bar{a}, \bar{b} \equiv a, b \bmod p$ is reduction mod p

3 cases:

(a) Good reduction: $p \neq 2$ and $p \nmid \Delta$, then $\bar{E}$ is an e.c. over $\mathbb{F}_p$

$P = (x:y:z) \in E \Rightarrow$ can choose rep. (x,y,z) for P w/ $x, y, z \in \mathbb{Z}$

and having $\gcd(x,y,z) = 1$, then $\bar{P} := (\bar{x} : \bar{y} : \bar{z})$ well-defined

As $(0:1:0) \equiv (0:1:0)$ and lines reduce to lines,

$E(\mathbb{Q}) \to E(\mathbb{F}_p)$ homo

(b) Cusp reduction: $\bar{E}$ has cusp, i.e. $p \mid 4a^3 + 27b^2$ and $p \mid -2ab$

$\Rightarrow \bar{E}^{ns} \cong G_a$

(c) Node reduction: $\bar{E}$ has node, i.e. $p \mid 4a^3 + 27b^2$ and $p \nmid -2ab$

- Split reduction: tangents at nodes are rational over $\mathbb{F}_p$

$$\Updownarrow$$

$$-2ab \text{ is square in } \mathbb{F}_p$$

$$\Updownarrow$$

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)^{(p^2+4p-5)/8} = (-1)^{(p+1)(p+3)/8}$$

$\Rightarrow \bar{E}^{ns} \cong G_m$

- Nonsplit reduction: $-2ab$ not a square in $\mathbb{F}_p$

$$\Downarrow$$

$$\bar{E}^{ns} \cong G_m\{\sqrt{-2\bar{a}\bar{b}}\}$$

$$= G_m\{3t\} = G_m\left\{\frac{9}{-2}\frac{\bar{b}}{\bar{a}}\right\}$$

Type	Tangents	$\Delta \bmod p$	$-2ab \bmod p$	E^{ns}	N
good		$\not\equiv 0$		E	?
cusp		0	0	G_a	p
node	rational	0	$\square$	G_m	$p-1$
node	not rational	0	$\neq \square$	$G_m\{\sqrt{-2ab}\}$	$p+1$

KdV equation ~~Recall $(w')^2 = 4w^3 - k_1 w - k_2$~~

~~soln. $w(z) = \wp(z+\gamma; k_1, k_2)$~~

$$\frac{\partial u}{\partial t} - \frac{3}{2}u\frac{\partial u}{\partial x} + \frac{1}{4}\frac{\partial^3 u}{\partial x^3} = 0$$

Suppose soln. is of the form $u(x,t) = w(x+ct)$

$$\Rightarrow c w' = \frac{3}{2} w w' + \frac{1}{4} w'''$$

We may integrate this equation

$$\Rightarrow c w = \frac{3}{4} w^2 + \frac{1}{4} w'' + \gamma_1$$

Multiply by w' $\Rightarrow c w w' = \frac{3}{4} w' w^2 + \frac{1}{4} w' w'' + \gamma_1 w'$

$$\Rightarrow \frac{c}{2} w^2 = \frac{1}{4} w^3 + \frac{1}{8}(w')^2 + \gamma_1 w + \gamma_2$$

$$\Rightarrow (w')^2 = -2w^3 + 4cw^2 - 8\gamma_1 w - 8\gamma_2$$

The general solution to this equation can be written in terms of a Weierstrass $\wp$-function; specifically

$$w_1(z) = -2\wp(z + \omega; k_1, k_2) + \frac{2c}{3} \quad \forall \text{ constant } \omega \text{ and with}$$

$$k_1 = \frac{4}{3}(c^2 - 3\gamma_1), \quad k_2 = \frac{8c^3}{27} - \frac{4c\gamma_1}{3} - 2\gamma_2$$

$$\Rightarrow u_{ell}(c, \omega, k_1, k_2) = -2\wp(x + ct + \omega; k_1, k_2) + 2c/3 \quad \text{soln. } \forall\, \omega \in \mathbb{C},\ k_1, k_2, c$$