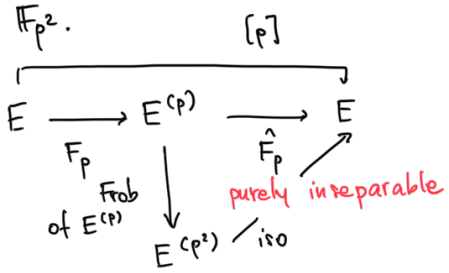
Counting supersingular curves

Recall: $p \geq 3$ prime, $\lambda \in \overline{\mathbb{F}_p}$

$y^2 = x(x-1)(x-\lambda)$ is supersingular $\iff$ $H_p(\lambda) = 0$

where $H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$ where $m = \frac{p-1}{2}$.

We want to count $j \in \overline{\mathbb{F}_p}$ such that elliptic curves E with $j(E) = j$ are singular. There only finitely many: if E supersingular, then $j(E) \in \mathbb{F}_{p^2}$.



$$E^{(p^2)} \xrightarrow[\text{iso}]{\sim} E \implies j(E^{(p^2)}) = j(E) = j(E)^{p^2}$$

$$\implies j(E) \in \mathbb{F}_{p^2}.$$

Exercise. Consider the differential operator

$$D = 4t(1-t)\frac{d^2}{dt^2} + 4(1-2t)\frac{d}{dt} - 1.$$

Show that $DH_p \equiv 0 \pmod{p}$.

Proof: $DH_p = \sum_{i=0}^{m} \binom{m}{i}^2 D(t^i)$.

$i = 0$: -1

$i = 1$: $4(1-2t) - t$

$i \geq 2$: $4(1-t)\, i(i-1)\, t^{i-1} + 4(1-2t)\, i\, t^{i-1} - t^i$.

$$= -t^i\left[4i(i-1) + 8i + 1\right] + t^{i-1}\left[4i(i-1) + 4i\right]$$

$4i^2 - 4i + 8i + 1 = 4i^2 + 4i + 1$ $\qquad$ $4i^2 - 4i + 4i = 4i^2$

$= (2i+1)^2$

$(2i+1)$ $\quad i=1 \quad [4 - \cdots$

$i=0 \quad -1$

$$= 4i^2 t^{i-1} - (2i+1)^2 t^i.$$

$$DH_p = -\binom{m}{0}^2 + \binom{m}{1}^2 [4(1-2t) - t] + \sum_{i=2}^{m} \left[4i^2 t^{i-1} - (2i+1)^2 t^i\right]\binom{m}{i}^2$$

$4 - 9t$

-1

$$\sum_{\substack{j=1 \\ j=i-1}}^{m-1} \binom{m}{j+1}^2 4(j+1)^2 t^j - \sum_{i=2}^{m} \binom{m}{i}^2 (2i+1)^2 t^i$$

$j=1 \quad \binom{m}{2}^2 4^2 t \qquad i=m \quad \binom{m}{m}^2 (2m+1)^2 t^m$

$$= \binom{m}{2}^2 4^2 t - (2m+1)^2 t^m + \sum_{i=2}^{m-1} \left[\binom{m}{i+1}^2 4(i+1)^2 - \binom{m}{i}^2 (2i+1)^2\right]$$

$$\binom{m}{i+1}^2 (i+1)^2 = \left(\frac{m!}{(i+1)!(m-(i+1))!}\right)^2 (i+1)^2 = \binom{m}{i}^2 \cdot (m-i)^2$$

$i!$

$$\longrightarrow \quad \text{(underbrace)} = \binom{m}{i}^2 \left[4(m-i)^2 - (2i+1)^2\right]$$

$$4\left(m^2 - 2im + i^2\right) - \left(4i^2 + 4i + 1\right)$$

$$= 4m^2 - 4i(1+2m) - 1$$

$m = \frac{p-1}{2}$

$$= (p-1)^2 - 4ip = p\left(p - 2 - 4i\right)$$

$2?$

$p^2 - 2p$

$$= \binom{m}{2}^2 4^2 t - p^2 t^m + \sum_{i=2}^{m-1} p(p-2-4i)\binom{m}{i}^2 t^i$$

$$DH_p = \sum_{i=0}^{m} \binom{m}{i}^2 \left[4it^{i-1} - (2i+1)^2 t^i\right] = -p^2 t^m + \sum_{i=0}^{m-1} p(p-2-4i)\binom{m}{i}$$

$$\equiv 0 \pmod{p}.$$

$\square$

Ex: Let $P(t) \in k[t]$ with k alg. closed $\mathrm{char}(k) = p$ be a polynomial s.t. $DP = 0$. If α is a multiple root of P then $\alpha = 0, 1$.

Pf: $P = (t-\alpha)^r Q(t)$, $r \geq 2$ $\quad (t-\alpha) \nmid Q$.

$$\longrightarrow \quad \mathrm{ord}_\alpha(P') = r-1$$

$$\mathrm{ord}_\alpha(P'') = r-2.$$

$DP = 0 \Rightarrow P = 4t + (t-1)P'' + 4(1-2t)P'$

$\alpha \neq 0,1$, $p \geq 5$: $\operatorname{ord}_\alpha(t(t-1)P'') = r-2$, $\operatorname{ord}_\alpha((1-2t)P') \geq r-1$ $\longrightarrow$ $\operatorname{ord}_\alpha P = r-2$. ↓

□

Exercise: Show that the number of supersingular elliptic curves is

$$\frac{1}{6}\left(\frac{p-1}{2} - 2\varepsilon_p(0) - 3\varepsilon_p(1728)\right) + \varepsilon_p(0) + \varepsilon_p(1728)$$ where

$$\varepsilon_p(0) = \begin{cases} 0 & \text{if } p \equiv 1 \ (3) \\ 1 & \text{if } p \equiv 2 \ (3) \end{cases}$$

$$\varepsilon_p(1728) = \begin{cases} 0 & \text{if } p \equiv 1 \ (4) \\ 1 & \text{if } p \equiv 3 \ (4) \end{cases}$$

Pf. Because of the previous exercises, the only possible multiple roots of H_p are 0 and 1.

$H_p(0) = 1 \neq 0$

$$H_p(1) = \sum_{i=1}^{m} \binom{m}{i}^2 = \binom{2m}{m} = \binom{p-1}{(p-1)/2} \not\equiv 0 \mod p.$$

$\left[(1+x)^a (1+x)^b = (1+x)^{a+b} \right]$ actually $(-1)^{\frac{p-1}{2}}$

In particular, there are no multiple roots.

j is a map of degree 6

Hurwitz formula: $-2 = 6(-2) + \deg R_j$. $\deg R_j = 10$

-12

$$j = 256 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (\lambda - 1)^2}$$

$R_j = [\infty] + [0] + [1] + 2[\omega] + 2[\eta] + [a] + [b] + [c]$

with $j(a) = j(b) = j(c) = 1728$.

ω, η solutions of $\lambda^2 - \lambda + 1 = 0$

Therefore j is $6:1$ except in ω, η, a, b, c

∞ with multiplicity 3

$j=0$ 2 points with [illegible]

$j=1728$ 3 ——————— 2.

Recall: • $Y^2 = X^3+1$ has $j=0$ $\begin{cases} p\equiv 1 \ (3) & \text{ordinary} \\ p\equiv 2 \ (3) & \text{supersingular} \end{cases}$

• $Y^2 = X^3 - X$ has $j=1728$ $\begin{cases} p\equiv 1 \ (4) & \text{ordinary} \\ p\equiv 3 \ (4) & \text{supersingular.} \end{cases}$

All in all:

$$\frac{1}{6}\left(\frac{p-1}{2} - 2\varepsilon_p(0) - 3\varepsilon_p(1728)\right) + \varepsilon_p(0) + \varepsilon_p(1728)$$

p mod 12	1	5	7	11
$\varepsilon_p(0)$	0	1	0	1
$\varepsilon_p(1728)$	0	0	1	1
	$\frac{p-1}{12}$	$\frac{p-5}{12}+1$	$\frac{p-7}{12}+1$	$\frac{p-11}{12}+2$.

look at $p=5$: $H_p(t) = 1 + \binom{2}{1}^2 t + \binom{2}{2}^2 t^2 = t^2 - t + 1.$

$Y^2 = X^3 + X$ is the unique supersingular curve.

Where does the operator D come from?

Over $\mathbb{C}$ (x,λ) $\mathcal{E} = \{ (\overbrace{[x_0 : x_1 : x_2]}^{x}, \lambda) \in \mathbb{P}^2(\mathbb{C}) \times \mathbb{C}\setminus\{0,1\} :$

$x_0 x_2^2 = x_1 (x_1 - x_0)(x_1 - \lambda x_0)\}$

$\downarrow \quad \downarrow \pi$

$\lambda \quad \mathbb{C}\setminus\{0,1\}$

$E_\lambda = \pi^{-1}(\lambda) = \mathbb{C} / \mathbb{Z} \oplus \mathbb{Z}\tau(\lambda)$

How does $\tau(\lambda)$ vary with λ?

$D = 4t(t-1)\frac{d^2}{dt^2} + 4(1-2t)\frac{d}{dt} - 1.$ lin. indep ↓

The differential equation $\mathcal{D}=0$ has two solution:

$$F\left(1, \tfrac{1}{2}, \tfrac{1}{2}, \lambda\right) \qquad F\left(1, \tfrac{1}{2}, \tfrac{1}{2}, 1-\lambda\right) \quad ? \text{ (Check!)}$$

$$\tau(\lambda) = \frac{F\left(1, \frac{1}{2}, \frac{1}{2}, \lambda\right)}{F\left(1, \frac{1}{2}, \frac{1}{2}, 1-\lambda\right)}$$

↑ Gauss hypergeometric.

Exercise: $p \geq 5 \longrightarrow \sum_{\substack{\text{isom. class.} \\ \text{supersing. } [E]}} \frac{1}{\#\mathrm{Aut}(E)} = \frac{p-1}{24}$.

Pf: $j \neq 0, 1728$ $\quad \mathrm{Aut}(E) = \{\pm \mathrm{id}\}$

$j = 0$ $\quad \#\mathrm{Aut}(E) = 6$

$j = 1728$ $\quad \#\mathrm{Aut}(E) = 4$.

$$\sum_{\#\mathrm{Aut}(E)} \frac{1}{\#\mathrm{Aut}(E)} = \frac{1}{6}\left(\frac{p-1}{2} - 2\varepsilon_p(0) - 3\varepsilon_p(0)\right)\cdot\frac{1}{2} + \varepsilon_p(0)\cdot\frac{1}{6} + \varepsilon_p(1728).$$

$$= \frac{1}{12}\cdot\frac{p-1}{2} - \underbrace{\varepsilon_p(0)\left[-\frac{8}{6}\cdot\frac{1}{2}+\frac{1}{6}\right]}_{0} - \underbrace{\varepsilon_p(1728)\left(-\frac{3}{12}+\frac{1}{4}\right)}_{0}$$

$$= \frac{p-1}{24}. \qquad \square$$

Singular Weierstrass equations

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Suppose that the associated curve in $\mathbb{P}^2$ is singular.

Exercise: Then there is only one singular point.

Rmq: the point at infinity is always non singular.

$$\begin{cases} \frac{\partial}{\partial y}: & 2y + a_1 x + a_3 = 0. \longrightarrow y = -\frac{a_1 x + a_2}{2} \\ \frac{\partial}{\partial x}: & a_1 y = 3x^2 + 2a_2 x + a_4 \longrightarrow a_1 y = 3x^2 + 2a_2 x + a_4. \end{cases}$$

Up to linear change of coordinates we may assume that $(0,0)$ is a singular point. Therefore the equation

has to be of the form

$$y^2 + a_1 xy = x^3 + a_2 x^2 \qquad a_3 = a_4 = a_6 = 0.$$

$$\begin{cases} 2y + a_1 x = 0 \\ a_1 y = 3x^2 + 2a_2 x. \end{cases} \qquad y = -\frac{a_1}{2} x.$$

$$\boxed{-\frac{a_1^2}{2} x = 3x^2 + 2a_2 x}$$

$$\longrightarrow \left(\frac{a_1}{2}\right)^2 x^2 - \frac{a_1^2}{2} x^2 = x^3 + a_2 x^2$$

$$\xrightarrow[x \neq 0]{} \quad x = a_1^2 \left(\frac{1}{4} - \frac{1}{2}\right) - a_2 = -\frac{a_1^2}{4} - a_2.$$

$x \neq 0$

$$-\frac{a_1^2}{2} - 2a_2 = 3x. \longrightarrow x = -\frac{1}{3}\left(\frac{a_1^2}{2} + 2a_2\right)$$

$$x = -\left(\frac{a_1^2}{4} + a_2\right).$$

$$\longrightarrow \frac{a_1^2}{2} + 2a_2 = 0. \longrightarrow x = 0 \quad \lightning. \qquad \square$$

We consider an equation of the form

$$y^2 + a_1 xy = x^3 + a_2 x^2 \longrightarrow y^2 + a_1 xy - a_2 x^2 = x^3$$

Let k'/k be a splitting field of $t^2 + a_1 t - a_2 = 0$.

Let $\lambda, \mu \in k'$ be solutions.

$$(y - \lambda x)(y - \mu x) = x^3.$$

$$\begin{cases} (y - \lambda x)(y - \mu x) = x^3 \\ y = tx \end{cases}$$

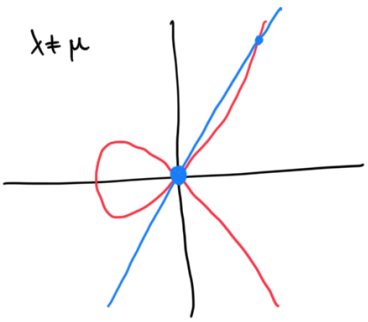
$$(tx - \lambda x)(tx - \mu x) = x^3$$

$$x^2 (t - \lambda)(t - \mu) = x^3$$

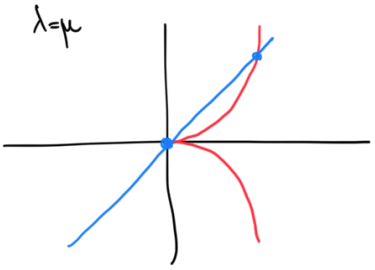
$$\xrightarrow[x \neq 0]{} \quad x = (t - \lambda)(t - \mu)$$

$$y = t(t - \lambda)(t - \mu).$$

$\lambda \neq \mu$



$\lambda = \mu$



This gives an isomorphism

$\lambda \neq \mu$ $\quad \mathbb{P}^1 \smallsetminus \{\lambda, \mu\} \xrightarrow{\sim}$ Creg = non singular points of $C: (y-\lambda x)(y-\mu) = x^3$.

$\lambda = \mu$ $\quad \mathbb{P}^1 \smallsetminus \{\lambda\} \xrightarrow{\sim}$ Creg

By changing coordinates, we get isomorphisms

$\lambda \neq \mu$ $\quad \varphi : \mathbb{P}^1 \smallsetminus \{0, \infty\} = \mathbb{G}_m \longrightarrow$ Creg

$$t \longmapsto \left[\frac{(t-1)^3}{(\lambda-\mu)^2 t} : t-1 : \mu t - \lambda\right]$$

$\lambda = \mu$ $\quad \psi : \mathbb{P}^1 \smallsetminus \{\infty\} = \mathbb{A}^1 \longrightarrow$ Creg

$$u \longmapsto [u^3 : u : 1+\lambda u].$$

Exercise: Show that

1) $\varphi(t_1), \varphi(t_2), \varphi(t_3)$ lie on a line iff $t_1 t_2 t_3 = 1$. $\quad t_i \in \mathbb{G}_m$

2) $\psi(t_1), \psi(t_2), \psi(t_3)$ ——— $u_1 + u_2 + u_3 = 0$, $u_i \in \mathbb{A}^1$

Pf. 1) Take a line with equation $a X_0 + b X_1 + c X_2 = 0$.

Suppose that $[1:0:0]$ does not belong to the line, i.e. $a \neq 0$. We may assume $a = 1$.

$\varphi(t_i) \in L \iff t_1, t_2, t_3$ are the solutions of the deg 3 equations for $i = 1, 2, 3$

$$\frac{(t-1)^3}{(\lambda-\mu)^2 t} + b(t-1) + c(\mu t - 1) = 0.$$

$$\iff (t-1)^3 + \underbrace{b(\lambda-\mu)^2 (t-1) + c(\lambda-\mu)^2 (\mu t - 1)}_{\text{terms in here have degree } 1, 2} = 0.$$

this is a monic polynomial in t of degree 3 with constant term -1

$$\Longrightarrow t_1 t_2 t_3 = 1.$$

2) Consider the line $L: X_0 + b X_1 + c X_2 = 0$.

Then the degree 3 polynomial:

u_1, u_2, u_3 are the solutions of the [illegible]

$$u^3 + bu + c(1+\lambda u) = 0.$$

the equation is monic of degree 3 and there is no term of degree 2.

$$\Longrightarrow \quad u_1 + u_2 + u_3 = 0.$$