Exercise: Let k be a field of characteristic 2. Consider the curve E given by the following equation

$$y^2 + xy = x^3 + ax + b.$$

1) Determine the (a,b) for which E is non-singular.

$0 = \frac{\partial}{\partial x}$: $y = 3x^2 + a = x^2 + a$

$0 = \frac{\partial}{\partial y}$: $x = 0$

$\Rightarrow \begin{cases} x = 0 \\ y = a \end{cases}$

Plug-in the equation of E:

$$a^2 = b.$$

The curve is non-singular iff $a^2 \neq b$.

Check that $[0:0:1]$ is non-s
$x = \frac{u}{v}$ $y = \frac{1}{v}$.
$v + uv = u^3 + auv^2 + bv^2$
$\frac{\partial}{\partial v}$: $1 + u = 0$
but we're interested i
$(u,v) = (0,0)$
then $\Rightarrow 1 + u \neq 0$.

2) Show that, for $p \in E(k)$, $p = (x_p, y_p)$

$$-p = (x_p, -x_p - y_p).$$

We have to consider the line joining $[1 : x_p : y_p]$ to $[0:0:1]$. This is the vertical line $x = x_p$. The intersection of E with the line $x = x_p$ will have three points (not necessarily distinct):

$$e = [0:0:1], \quad p, \quad -p.$$

Note that since p lies in $\{x_0 \neq 0\}$, the $-p$ also lies $\{x_0 \neq 0\}$
So the only point at ∞ will be e.

$$\begin{cases} y^2 + xy = x^3 + ax + b \\ x = x_p \end{cases}$$

$$v + uv - (u^3 + a uv^2 + bv^3) = F(u,v)$$

$$\frac{\partial F}{\partial u}(0,0)\, u + \frac{\partial F}{\partial v}(0,0)\, v = 0.$$

$\frac{\partial F}{\partial u}$: $v - (3u^2 + av^2) \overset{(u,v)=(0,0)}{=} 0.$

$\frac{\partial F}{\partial v}(0,0) = 1$

the tangent line is $v = 0$.

$$\begin{cases} F(u,v) = 0 \\ v = 0 \end{cases} \rightarrow \begin{cases} u^3 = 0 \\ v = 0. \end{cases}$$

Therefore $[0:0:1]$ is a flex. ∎

... look for the solutions of

We work [illegible]

$$G(y) = y^2 + x_p y - \underbrace{(x_p^3 + a x_p + b)}_{c} = 0$$

We know that $y = y_p$ is a solution. We divide $G(y)$ by $y - y_p$ in order to compute the other solution.

$$\begin{array}{r|l} y^2 + x_p y - c & y - y_p \\ \hline - \; y^2 - y_p y & y + (x_p + y_p) \\ \hline (x_p + y_p) y - c & \\ \hline 0 & \end{array}$$

Therefore the other solution is

$$y = -(x_p + y_p).$$

This is what we wanted to know.

3) Compute the 2-torsion points of E. Of course, e is 2-torsion point. The other 2-torsion points lie in $\{x_0 \neq 0\}$ and satisfy $P = -P$. This means

$$\begin{cases} x_P = x_P \\ y_P = -(x_P + y_P) \end{cases} \longleftrightarrow \underbrace{2y_P}_{\text{char}(k)=2} + x_P = 0 \to x_P = 0.$$

$$\begin{cases} y^2 + xy = x^3 + ax + b \\ x = 0 \end{cases} \longrightarrow \begin{cases} y^2 = b \\ x = 0. \end{cases} \leftarrow \text{this is a root of multip}$$

Suppose $k = \bar{k}$. Then $y^2 - b = 0$ has unique solution, write it $\sqrt{b}$. Therefore $E[2] = \{e, (0, \sqrt{b})\}$. In particular $\# E[2] = 2$.

[Rmk: $\mu_2 = \operatorname{Spm} k[t]/(t^2-1)$ This is an algebraic group with multiplication given by the ring homomorphism

$$\begin{array}{ccc} k[t]/(t^2-1) & \longrightarrow & k[v]/(v^2-1) \otimes k[u]/(u^2-1) \\ t & \longmapsto & v \otimes u. \end{array} \qquad \left| \begin{array}{l} \mu_2 \times \mu_2 \to \mu_2 \\ (t, u) \mapsto tu \end{array} \right.$$

μ_2 is not non singular in $\text{char}(k) = 2$.

$$(t^2-1)' = 0.$$

The only solution is $t=1$, but as an algebraic group it is different $k[t]/(t-1)$.]

Ex. [$\text{char}(k) \neq 2$.] Consider the algebraic curve E with equation

$$y^2 + y = x^3 + ax + b.$$

[illegible] the couples (a,b) for which E is non-singular.

c) Determine the [illegible]

$0 = \frac{\partial}{\partial x}: \quad 3x^2 + a = 0.$

$0 = \frac{\partial}{\partial y}: \quad 1 + \underbrace{2y}_{0} = 0$ never happens.

Check at infinity: $x = \frac{u}{v} \qquad y = \frac{1}{v}.$

$$\begin{cases} v + v^2 = u^3 + auv^2 + bv^3 \\ v = 0 \rightarrow u = 0. \end{cases}$$

$$\begin{cases} \frac{\partial}{\partial u}: \quad 3u^2 + auv = 0 \quad (u=0) \\ \frac{\partial}{\partial v}: \quad 1 + \underbrace{2v}_{0} - \left(\underbrace{2auv}_{0} + 3bv^2 \right) = 1 - 3bv^2 = 0. \quad (v=0) \end{cases}$$

This says that $[0:0:1]$ is non-singular with tangent line $v = 0$.

Remark that $[0:0:1]$ is a flex.

2) Given $P = (x_P, y_P)$ compute $-P$. By the same argument as before, it suffices to find the other point of intersection with the line $x = x_P$ lying in $\{x_0 \neq 0\}$.

$$G(y) = y^2 + y - \underbrace{\left(x_P^3 + ax_P + b \right)}_{c} = 0.$$

We know that one solution is y_P. We want to find the other.

$$\begin{array}{r|l} y^2 + y - c & y - y_P \\ \hline -\left(y^2 - y_P y \right) & y + (1 + y_P) \\ \hline (1+y_P)y - c & \\ \hline 0 & \end{array}$$

The solution we are looking for is $y = -(1 + y_P)$.

Therefore

$$-P = (x_P, -(1+y_P)).$$

3) Compute the 2-torsion points of E. (Suppose $k = \bar{k}$). The 2-torsion points are, satisfy $P = -P$ and lie in $\{x_0 \neq 0\}$.

$$P = -P \iff \begin{cases} x_P = x_P \\ y_P = -(1 + y_P) \rightarrow \cancel{2y_P} + 1 = 0 \end{cases}$$

This never happens. Therefore $E[2] = \{e\}$.

[illegible] non-singular

This curves are called supersingular.

Let k be a perfect field of characteristic $p>0$.

Ex. Let $X \subseteq \mathbb{P}^2$ a smooth projective curve given by the equation $f=0$, with $f(x,y) = \sum_{i,j} a_{ij} x^i y^j$. Then the first Frobenius twist $X^{(p)}$ of X is the curve with equation $\sum_{i,j} a_{ij}^p x^i y^j = 0$.

The first Frobenius twist of X is the smooth projective curve with function field $K(X)^p$ where $K(X)$ is the function field of X.

$$K(X) = \operatorname{Frac} A \qquad A = k[x,y]/(f(x,y)).$$

$$\begin{array}{ccc} A & \xrightarrow[\sim]{\cdot^p} & A^p \\ \cap & & \cap \\ K(X) = K & \xrightarrow[\sim]{p} & K^p \end{array} \qquad K^p = \operatorname{Frac}(A^p).$$

$$A^p = k[x^p, y^p]/(f(x,y)^p) \quad \text{because}$$

$$\begin{array}{ccccccc} 0 & \longrightarrow & k[x,y] & \xrightarrow{f} & k[x,y] & \longrightarrow & A \longrightarrow 0. \\ & & \wr\downarrow \cdot^p & & \wr\downarrow \cdot^p & & \downarrow \cdot^p \\ 0 & \longrightarrow & k[x^p,y^p] & \xrightarrow{f^p} & k[x^p,y^p] & \longrightarrow & A^p \longrightarrow 0. \end{array}$$

$$f(x,y)^p = \Big(\sum_{i,j} a_{ij} x^i y^j\Big)^p = \sum_{i,j} a_{ij}^p x^{ip} y^{jp}$$

$t := x^p \qquad u = y^p$

$$\longrightarrow \quad A^p = k[t,u]/(g(t,u)) \quad \text{where } g(t,u) = \sum_{i,j} a_{ij}^p t^i u^j.$$

Exercise: check that the curve defined by $g=0$ is smooth. □

Ex. Let E be an elliptic curve over $\overline{\mathbb{F}_p}$. Show that E is defined over $\mathbb{F}_q$ for some power q of p and F_q is an endomorphism of E. If $p=q$, show that F_p is not the multiplication by an integer.

(1) First of all, there is a power q of such that E is defined over $\mathbb{F}_q$. Indeed, take an embedding of E in $\mathbb{P}^2$ and take q so big that $\mathbb{F}_q$ contains the coefficients of the equation (and so that the image of e is $\mathbb{F}_q$-rational).

(2) Suppose E is defined over $\mathbb{F}_q$. By iteration of the previous exercise, we see that $E^{(q)} = E$. Embed E in $\mathbb{P}^2_{\mathbb{F}_q}$ via $i_{3[e]}$, and let $f(x,y) = \sum a_{ij} x^i y^j$ be the equation of E. Then, by iteration of the previous exercise we see that $E^{(q)}$ is given by the equation

$$\sum a_{ij}^q x^i y^j = 0$$

Since $a_{ij} \in \mathbb{F}_q$, we have $a_{ij}^q = a_{ij}$. Therefore $E^{(q)} = E$.

Addendum to the previous exercise

$$\begin{array}{ccccc} X \subseteq \mathbb{P}^2 & \{ f = \sum a_{ij} x^i y^j = 0 \} = X & & (x,y) \\ F_p \downarrow & & & \downarrow \\ X^{(p)} \subseteq \mathbb{P}^2 & \{ \sum a_{ij}^p x^i y^j = 0 \} = X^{(p)} & & (x^p, y^p) \end{array}$$

(3) In particular $F_q : E \to E^{(q)} = E$ is an endomorphism of E.

Suppose $p = q$. The multiplication by $[p]$ is not a separable isogeny and it factors through F_p as follows:

$$\begin{array}{ccccc} E & \xrightarrow{F_p} & E^{(p)} & \xrightarrow{\hat{F}_p} & E \\ & \searrow & & & \nearrow \\ & & [p] & & \end{array}$$

Now, since E is defined over $\mathbb{F}_p$, we have $E = E^{(p)}$.

Moreover $\deg F_p = p$ since $\deg [m] = m^2$ for each $m \in \mathbb{Z}$, F_p cannot be the multiplication by an integer. □

Ex: Consider the elliptic curves

$E_1 \quad y^2 = x^3 + 1$ over $\mathbb{F}_5$.

$E_2 \quad y^2 = x^3 - x$

[There are curves that have "complex multiplication".]

- The curve E_2 has automorphisms (4 automorphisms)

$(x,y) \mapsto (x,y)$

$(x,y) \mapsto (x,-y)$

$(x,y) \overset{2}{\mapsto} (-x, \pm 2y)$ because $2^2 \equiv -1 \quad (5)$

"multiplication by $\sqrt{-1}$".

- The curve E_1 has automorphisms (6 automorphisms)

$(x,y) \mapsto (x,y)$

$(x,y) \mapsto (x,-y)$

$(x,y) \overset{2}{\mapsto} (ux, \pm y)$ $\quad u^3 = 1$, $u \neq 1$ over $\mathbb{F}_{5^2}$.

It is not defined over $\mathbb{F}_5$ but only over $\mathbb{F}_{5^2}$.

Show that F_5 commutes with the automorphisms of E_2, but does not commute with the automorphisms of E_1. In particular, in the statement $\mathrm{End}(E_1)$ is not commutative.

E_2) $x, y \in E(\overline{\mathbb{F}_5})$

$$(x,y) \overset{\alpha}{\longmapsto} (-x, 2y) \overset{F_5}{\longmapsto} (-x^5, 2^5 y^5)$$

$$\overset{F_5}{\longmapsto} (x^5, y^5) \overset{\alpha}{\longmapsto} (-x^5, 2y^5)$$

($2^5 = 2$)

so they commute.

[Rule: Let $f, g : X \to Y$ be morphism of alg varieties over a field k (Y separated)

Suppose $\overline{X} = X \times_k \bar{k}$, $\overline{Y} = Y \times_k \bar{k}$ are reduced and irreducible

and that $f(x) = g(x)$ for all $x \in X(\bar{k})$.

Then $f = g$ as morphism of alg varieties.]

E_1)

$$(x,y) \overset{\alpha}{\longmapsto} (ux, y) \overset{F_5}{\longmapsto} (u^5 x^5, y^5)$$

$$\overset{F_5}{\longmapsto} (x^5, y^5) \longmapsto (ux^5, y^5)$$

$u^5 \neq u$ (otherwise $u^2 = 1$)

u is not fixed under Frobenius because it does not belong to $\mathbb{F}_5$

We will see: $\mathrm{End}(E)$ is commutative $\iff$ E is not supersingular ($\#E[p](\bar{k}) = 1$)

supersingular

MORPHISMS

AUTOMORPHISMS

Let k be an algebraically closed field. Let E/k be an elliptic curve with neutral element e.

Suppose $\mathrm{char}(k) \neq 2,3$. Let $x \in H^0(2[e]) \setminus H^0([e])$

$y \in H^0(3[e]) \setminus H^0(2[e])$ s.t.

$$y^2 = x^3 + \lambda x + \mu. \qquad (*)$$

Let $\varphi : E \to E$ an automorphism s.t. $\varphi(e) = e$. Thus

$$\varphi^* : H^0(d[e]) \xrightarrow{\sim} H^0(d[e]) \quad \text{isomorphism.}$$

$(*)$ is the unique linear relation in $H^0(6[e])$.

$$(**) \qquad \left[(\varphi^* y)^2 - \left(\varphi^* x^3 + \lambda \varphi^* x + \mu \right) \right] = u \left[y^2 - (x^3 + \lambda x + \mu) \right]$$

$$\varphi^* 1 = 1$$

$$\varphi^* x = ax + b \qquad a \neq 0$$

$$\varphi^* y = cy + dx + e$$

Because of $(**)$,

$d = 0$ otherwise the coefficient xy is $\neq 0$.

$e = 0$ ——— y ———

$b = 0$ ——— x^2 ———

$$\varphi^* x = ax \qquad \varphi^* y = cy$$

$$c^2 y^2 - \left(a^3 x^3 + \lambda a x + \mu \right) = \left[y^2 - (x^3 + \lambda x + \mu) \right] u$$

- $u = c^2 = a^3$
- $\lambda a = \lambda u$
- $\mu a = \mu$.

$\boxed{\lambda \mu \neq 0}$ $\quad u = 1. \quad a = 1 \quad c^2 = 1.$

$\Rightarrow c = \pm 1.$

The possible automorphisms are

$(x, y) \mapsto (x, y)$ identity $\qquad (x, y) \mapsto (x, -y)$ inverse.

$\boxed{\lambda = 0}$ $\quad y^2 = x^3 - \mu.$

$u = 1 \quad c^2 = 1, \ a^3 = 1$

$\mu \neq 0$

a is a 3^{rd} of unity
$c = \pm 1$

Automorphisms
$(x, y) \mapsto (\zeta^2 x, \zeta^3 y)$
ζ is a primitive 6^{th} root of 1

$\Longrightarrow \quad \# \mathrm{Aut}(E) = 6.$

$\lambda \neq 0$
$\mu = 0$

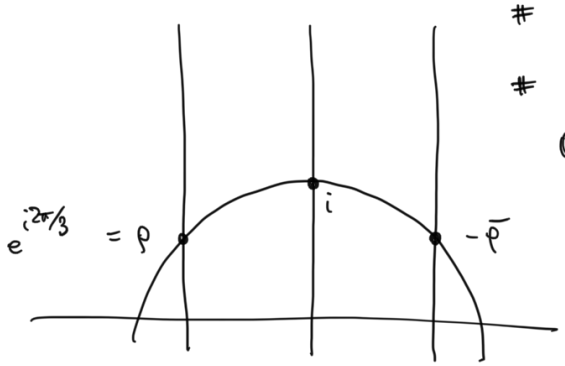
$y^2 = x^3 - \lambda x.$

$a = u \Rightarrow a^2 = 1.$
$c^2 = a^3.$

$a = 1$: $(x, y) \mapsto (x, y)$ identity
$(x, y) \mapsto (x, -y)$ -1

$a = -1$: $(x, y) \mapsto (-x, iy)$

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



$\# \mathrm{Stab}_{SL_2(\mathbb{Z})}(i) = 4.$

$\# \mathrm{Stab}_{SL_2(\mathbb{Z})}(\rho) = 6.$

Over the complex numbers
$\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}i$ has
4 automorphisms.

$\mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\rho$ has
6 automorphisms.