Last time: function fields of modular curves. Now, how can we make sense of isogenies $E \to E'$ algebraically and of Hecke operators?

For Hecke operators we already have $[\Gamma_1 \alpha \Gamma_2] : \mathrm{Div}(X_2) \to \mathrm{Div}(X_1)$. For $\Gamma_1(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ with (E, Q) an elliptic curve and Q its n-torsion we have

$$T_p : \mathrm{Div}(X_1) \to \mathrm{Div}(X_1)$$
$$T_p[E, Q] = \sum_C [E/C, Q + C]$$

where C is a subgroup of order p and $C \cap \langle Q \rangle = \{0\}$.

Now for elliptic curves over arbitrary fields

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

One cannot do a standard change of variables in arbitrary characteristic (namely $2, 3$). But one can define Δ, j. For $j \neq 0, 1728$ we can look at the curve

$$y^2 + xy = x^3 - \left(\frac{36}{j - 1728}\right) x - \frac{1}{j - 1728}.$$

It is still true that $E \hookrightarrow \mathbb{P}^2(\overline{k})$ and this forms an abelain group. The Group equations are defined over $k_{\text{prime}}(\{a_i\})$, where k_{prime} is $\mathbb{F}_p, \mathbb{Q}$ depending on the characteristic of k.

Theorem .0.1

The N-torsion for $N = \prod_p p^{e_p}$ can be described as

$$E[N] = \prod_p E[p^{e_p}],$$

Furthermore

- $E[p^e] \cong (\mathbb{Z}/p^e\mathbb{Z})^2$ if $\mathrm{char}(k) \neq p$.
- $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ for every e, or $E[p^e] \cong 0$ for every e provided that $\mathrm{char}(k) = p$. The first is called the ordinary case and the second is called the supersingular case.

The point, $E[p^e]$ is a finite affine scheme over k. Thus this is still $\mathrm{Spec}(A)$ for some k-algebra A, where $\dim_k A = p^{2e}$. The problem is how many points we have on the scheme.

Consider μ_p, well this is $\mathrm{Spec}\,(k[x]/(x^p - 1))$. In characteristic p this is $k[x]/(x-1)^p$. So then there's only one point on μ_p, this spectrum. This is exactly the sort of thing that is happening in general.

In the ordinary case, we have

$$E[p] \cong \mu_p \times \mathbb{Z}/p\mathbb{Z}$$

as a scheme.

We also need to study singular Weierstrass curves. That is when $\Delta = 0$. Suppose P is singular. We can change coordinates so that $P = (0, 0)$. We then get

$$C(x, y) = y^2 + a_1 xy - x^3 - a_2 x^2.$$

If $\text{char}(k) \neq 2$, this can be simplfied to

$$C(x, y) = y^2 - x^3 - a_2' x^2.$$

Check from these equations that $(0, 0)$ is the only singular point.

Then write $E(x, y) = (y - m_1 x)(y - m_2 x) - x^3$. There are two cases

- If $m_1 \neq m_2$, then there are two tangent directions and this is called a nodal singularity. In this case we can get a group structure on the points where you're nonsingular and this is isomorphic to $\overline{k}^\times$. Thus this is often called the multiplicative case.
- If $m_1 = m_2$, then we call this a cusp and the group is $\overline{k}$ additively, and this is called the additive case.

Now we'll look at more algebraic properties of curves in arbitrary characteristic.

Question: Finite fields, Galois groups?

Recall .0.1

For every p^n, there is a unique field $\mathbb{F}_{p^n}$, which is a degree n extension of $\mathbb{F}_p$ with Galois group $\mathbb{Z}/n\mathbb{Z}$. Furthermore it is generated by the Frobenius map $x \mapsto x^p$.

We have $\mathbb{F}_{p^n}$ embeds in $\mathbb{F}_{p^m}$ if and only if $n \mid m$. Also $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \widehat{\mathbb{Z}}$, the inverse limit of all the $\mathbb{Z}/n\mathbb{Z}$.

We get $\sigma_p : \mathbb{P}^n(\overline{\mathbb{F}}_p) \to \mathbb{P}^n(\overline{\mathbb{F}}_p)$ given by

$$[x_0 : \cdots : x_n] = [x_0^p : \cdots : x_n^p].$$

Suppose we have a curve C with an embedding $C \hookrightarrow \mathbb{P}^n(\overline{\mathbb{F}}_p)$ cut out by equations $\varphi_1, \ldots, \varphi_k$. We can then define

$$C^{\sigma_p} : \varphi_1^{\sigma_p}, \ldots, \varphi_k^{\sigma_p},$$

where $\varphi_i^{\sigma_p}$ tells us to act on the coefficients of φ_i via σ_p. Then σ_p gives a map $C \to C^{\sigma_p}$, since 0 is fixed by σ_p and σ_p is a Galois automorphism. Essentially for any field map $\varphi^\sigma(\sigma(x)) = \sigma(\varphi(x))$.

This should then induce a map of function fields!

Example .0.2

Conisder

$$\sigma_p : \mathbb{P}^1(\overline{\mathbb{F}}_p) \to \mathbb{P}^1(\overline{\mathbb{F}}_p)$$

This then gives us

$$\begin{aligned} \overline{\mathbb{F}}_p(t) &\leftarrow \overline{\mathbb{F}}_p(t) \\ t^p &\leftarrow\!\shortmid t, \end{aligned}$$

and we can consider $\overline{\mathbb{F}}_p(t^p) = \overline{\mathbb{F}}_p(s)$. Then $t^p = s$, and the minimal polynomial is $x^p - s = x^p - t^p = (x-t)^p$. Furthermore, this map above is a bijection, but we *really* should not think of it as an isomorphism.

Then $\mathbb{F}_p(t)/\mathbb{F}_p(s)$ is an inseperable extension (separable extension is when the minimal polynomial has no repeated roots).

For any algebraic extension $k \subseteq K$, we can factor this as

$$k \hookrightarrow k^{\text{sep}} \to K,$$

where the first is separable, and the second is purely inseperable. Thus if we have $h : C \to C'$, we get a factoring as follows

$$C \hookrightarrow C_{\text{sep}} \to C',$$

where the first is inseparable and looks like σ_p^e, and the second is separable. Thus we get a factorization $h = h_{\text{sep}} \circ \sigma_p^e$.

Then $\deg(h) = \deg[K(C) : K(C')]$. Then $\deg(h) = \deg(h)_{\text{sep}} \deg(h)_{\text{inseparable}}$. It is still true that

$$\sum_{P \in h^{-1}(Q)} e_P(h) = \deg h,$$

where the ramification inseparable piece is ramified *everywhere* which is quite strange. In particular one thing that will be true is if $\varphi : E \to E'$, then

$$\deg(\varphi)_{\text{sep}} = |\ker \varphi| .$$

Example .0.3

The isogeny $[p] : E \to E$. The kernel is the p-torsion. Fact: $\deg[p] = p^2$ always. But the p-torsion may be smaller than p^2! This is because the inseperable piece is taking over.

We'll have $\deg[p]_{\text{sep}} = p$ in the ordinary case and $\deg[p]_{\text{sep}} = 1$ in the supersingular case.

Why do we care about this? Well if we have an elliptic curve with coefficients over $\mathbb{Z}$, we can reduce all the coefficents modulo p to get a curve over $\mathbb{F}_p$. This is called the reduction at p of this elliptic curve.

It turns out, sometimes when you reduce a nonsingular elliptic curve E over $\mathbb{Z}$ then sometimes it can become singular in the reduction. Here we'll fix $E/\mathbb{Q}$ and define

$$v_p(E) = \min(v_p(\Delta(E)) : E' \sim E),$$

where E' has integral coefficients via a change of coordinates from E. We also define

$$\Delta(E)_{\min} = \prod_p p^{v_p(E)}.$$

Fact: $\Delta(E)_{\min}$ can be achieved via a change of coordinates with a Weierstrass curve. We call such an integral curve achieving the minimal discriminant a "minimal Weierstrass model." From now on assume E is given in this form.

We then may reduce E to E_p. There are two reduction types

1) Good reduction, we get a nonsingular elliptic curve
   a) Ordinary $|E_p[p]| = p$.
   b) Supersingular $|E_p[p]| = 1$.
2) Bad reduction, there are many subtypes
   a) Multiplicative, $m_1 \neq m_2$.
      i) Split, $m_1, m_2 \in \mathbb{F}_p$

ii) Nonsplit, $m_1, m_2 \notin \mathbb{F}_p$, in fact $m_1, m_2 \in \mathbb{F}_{p^2}$.

b) Additive, $m_1 = m_2$.

HW: find an example of each reduction type, due next Tuesday.

Algebraic Conductor. This will be $N_E = \prod_p p^{f_p}$ where

$$f_p = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if multiplicative reduction} \\ 2 & \text{if additive reduction } p \neq 2, 3 \\ 2 + \delta_p & \text{if additive reduction } p \in \{2, 3\} \end{cases}.$$

δ_p is something we'll look at later. We can be assured from the book that δ_p is no more than 6. Recall in the modularity theorem we wanted a map $X_0(N) \to E$. It turns out the N we need is N_E.