MODULAR FORMS SEMINAR, TALK 7: FORMAL GROUP LAWS.

A. SALCH

1. Differential 1-forms on algebraic curves.

Let k be a field and let $C \subseteq \mathbb{P}^n_k$ be a smooth projective curve. Then the function field of C, written $\overline{k}(C)$, is the field of fractions of the ring of regular functions on $\mathbb{A}^n_k \cap C$ for any copy of $\mathbb{A}^n_k \subseteq \mathbb{P}^n_k$ which intersects C nontrivially. (Although this definition involves a choice of $\mathbb{A}^n_k \subseteq \mathbb{P}^n_k$, the function field of C is well-defined up to isomorphism.) Then Ω_C, the space of meromorphic differential 1-forms on C, is the $\overline{k}(C)$-vector space with basis the set of symbols $\left\{df : f \in \overline{k}(C)\right\}$ and with relations

- $d(x+y) = dx + dy$ for all $x, y \in \overline{k}(C)$,
- $d(xy) = xdy + ydx$ for all $x, y \in \overline{k}(C)$,
- $d(c) = 0$ for all $c \in \overline{k} \subseteq \overline{k}(C)$.

The $\overline{k}(C)$-vector space Ω_C is always one-dimensional.

Example 1.1.

- Suppose we consider the curve in $\mathbb{A}^1_k$ given by the vanishing of $x^2 + y^2 - 1$. Let C be the projectivization of this curve, i.e., C is the vanishing locus of $x^2 + y^2 - z^2$ in $\mathbb{P}^2_k$. The function field $\overline{k}(C)$ is the fraction field of the ring of functions of C's intersection with $\mathbb{A}^1_{\overline{k}}$, i.e., $\overline{k}(C)$ is the field of fractions of $\overline{k}[x,y]/(x^2+y^2-1)$. We have $d(y^2) = 2y\ dy$, so if k has characteristic $\neq 2$, then $dy = \frac{1}{2y}d(y^2) = \frac{1}{2y}d(1-x^2) = -\frac{x}{y}dx$, so you can see that Ω_C is a free $\overline{k}$-vector-space generated by, for example, dx; of course dy works just as well.

  What about when char $k = 2$? Then the Jacobian of our original affine curve is $\begin{bmatrix} 2x & 2y \end{bmatrix} = \begin{bmatrix} 0 & 0 \end{bmatrix}$, so the curve is singular (in fact, *every* point on the curve is singular), so the above discussion doesn't apply.
- Suppose we consider the curve in $\mathbb{A}^1_k$ given by the vanishing of $x^3 + x - y^2$. Let C be the projectivization of this curve, i.e., C is the vanishing locus of $x^3 + xz^2 - y^2z$ in $\mathbb{P}^2_k$. The function field $\overline{k}(C)$ is the fraction field of the ring of functions of C's intersection with $\mathbb{A}^1_{\overline{k}}$, i.e., $\overline{k}(C)$ is the field of fractions of $\overline{k}[x,y]/(x^3+x-y^2)$. We have $d(y^2) = 2y\ dy$, so if k has characteristic $\neq 2$, then $dy = \frac{1}{2y}d(y^2) = \frac{1}{2y}d(x^3+x) = \left(\frac{3}{2y}x^2 + \frac{1}{2y}\right)dx$, so you can see that Ω_C is a free $\overline{k}$-vector-space generated by, for example, dx.

  What about when char $k = 2$? Then the Jacobian of our original affine curve is $\begin{bmatrix} 3x^2+1 & -2y \end{bmatrix} = \begin{bmatrix} x^2+1 & 0 \end{bmatrix}$, so the curve is singular at the point $(1,0)$, so the above discussion doesn't apply.

Remember that a *divisor* on a curve C is simply a formal $\mathbb{Z}$-linear combination of points on C, and the divisor group of C, $\mathrm{Div}(C)$, is simply the free abelian group

Date: October 2018.

on the set of points of C. The purpose of $\mathrm{Div}(C)$ is to be a home for the divisors of functions: we have a map $div : \overline{k}(C)^\times \rightarrow \mathrm{Div}(C)$ which sends each function $f \in \overline{k}(C)^\times$ to the formal sum $\sum_{p \in C} \mathrm{ord}_p(f)p$, i.e., $div(f)$ simply records the orders of the poles and zeroes of f. The *degree* of a divisor is the sum of its coefficients.

Example 1.2. Again, let C be the projectivization of the affine curve given by the vanishing of $x^2 + y^2 - 1$. Assume char $k \neq 2$, so that C is smooth. The function $x - y \in \overline{k}(C)^\times$ vanishes when $x = y$, which happens on the affine curve when $x = y$ and $x^2 + y^2 = 1$, i.e., when $x = y = \pm\sqrt{1/2}$. The function $x - y$ clearly has no poles on the affine curve, but we need to check its behavior at the "points at infinity," i.e., the points in C which aren't in the affine curve. To do this, we intersect the vanishing locus of $x^2 + y^2 - z^2$ in $\mathbb{P}^2_k$ with a copy of $\mathbb{A}^2_k$ in $\mathbb{P}^2_k$ *other than* the $z \neq 0$ copy of $\mathbb{A}^2_k$ in $\mathbb{P}^2_k$; for example, if we choose the $y \neq 0$ copy of $\mathbb{A}^2_k$ in $\mathbb{P}^2_k$, then $C \cap \mathbb{A}^2_k$ is the vanishing locus of $x^2 + 1 - z^2$ in $\mathbb{A}^2_k$ and our function $x - y$ on C agrees with $\frac{x-1}{z}$ on this affine curve. We have poles at $x = \pm\sqrt{-1}$, $z = 0$. If k is algebraically closed, then $\sqrt{-1}$ and $\pm\sqrt{-1}$ exist and are distinct in k (remember we assumed char $k \neq 2$!), so

$$div(x - y) = [\sqrt{1/2}, \sqrt{1/2}, 1] + [-\sqrt{1/2}, -\sqrt{1/2}, 1] - [\sqrt{-1}, 1, 0] - [-\sqrt{-1}, 1, 0],$$

which has degree $1 + 1 - 1 - 1 = 0$, which is not a coincidence: $\deg(div(f)) = 0$ for all $f \in k(C)^\times$, again assuming that k is algebraically closed.

Differential 1-forms also have divisors, but this requires slightly more explanation. Assume $k = \overline{k}$. If $\omega \in \Omega_C$ and $P \in C$, we let $\mathrm{ord}_P(\omega)$ be the order of vanishing of g at P, where $g \in k(C)$ is the unique function such that $\omega = g\ dt$ for $t \in k(C)$ a uniformizer at P (i.e., t generates the maximal ideal of the ring of functions of C localized at P). While g depends on a choice of t, the order of vanishing of g at P doesn't, so $\mathrm{ord}_P(\omega)$ is well-defined. We let $div(\omega)$ be the divisor $\sum_P \mathrm{ord}_P(\omega) \cdot P$.

We say that a 1-form ω on a projective curve C is *holomorphic* if ω has nonnegative order at every point of the curve (i.e., no poles), and is *nonvanishing* if ω has nonpositive order at every point of the curve (i.e., no zeroes).

Example 1.3. Again, let C be the projectivization of the affine curve given by the vanishing of $x^2 + y^2 - 1$. Assume char $k \neq 2$, so that C is smooth. Let's compute the divisor of dx. Given a point $P = (x = a, y = b)$ on the affine curve, we have $(x - a, y - b)^2 = ((x - a)^2, (x - a)(y - b), (y - b)^2) = (x^2 - 2ax + a^2, (x - a)(y - b), 1 - x^2 - 2by + b^2) = (x^2 - 2ax + a^2, (x - a)(y - b), 1 - 2ax + a^2 - 2by + b^2)$, i.e., modulo $(x - a, y - b)^2$ we can rewrite every element of $k[x, y]/(x^2 + y^2 - 1)$ in terms of 1 and x, and in particular, the function $x - a$ generates the maximal ideal of the local ring of $k[C]$ at P, so we want to write dx as $g\ d(x - a)$. But since d vanishes on constants, we can simply let $g = 1$. So $\mathrm{ord}_P(dx) = 0$. For points at infinity, we intersect C with the $y \neq 0$ copy of $\mathbb{A}^2_k$ in $\mathbb{P}^2_k$: dx becomes $d(x/z)$ on the curve $x^2 + 1 = z^2$, the points at infinity with respect to the original affine curve are

$x = \pm\sqrt{-1}$ and $z = 0$, and

$$\begin{aligned} d(x/z) &= (1/z)\ dx - (x/z^2)\ dz \\ &= (1/z)\ dx - (x^2/z^3)\ dx \\ &= ((z^2 - x^2)/z^3)\ dx \\ &= 1/z^3\ dx \\ &= 1/z^3\ d(x \pm \sqrt{-1}), \end{aligned}$$

since $d(x/z)\ z + (x/z)\ dz = dx$ and $d(x^2+1) = 2xdx = 2zdz$. So the order of vanishing of $d(x/z)$ at each of the points at infinity is -3. So the divisor of dx on C is $-3[\sqrt{-1}, 1, 0] - 3[-\sqrt{-1}, 1, 0]$, and $div(dx)$ has degree 6, if I haven't managed to mess this calculation up. So dx is nonvanishing but not holomorphic.

Example 1.4. Again, let C be the projectivization of the affine curve given by the vanishing of $x^3 + x - y^2$. Assume char $k \neq 2$, so that C is smooth. The function y uniformizes every point P on the affine curve, and dx has divisor $[0, 0, 1] + [-\sqrt{-1}, 0, 1] + [\sqrt{-1}, 0, 1] - 3[0, 1, 0]$, the same divisor as $div(y)$. So $1/y\ dx$ has divisor 0. So $1/y\ dx$ is a nonvanishing holomorphic differential on C.

2. Formal group laws.

Given a commutative ring R, a *(one-dimensional, commutative) formal group law over* R is a power series $F(X,Y) \in R[[X,Y]]$ such that:

- $F(X, F(Y,Z)) = F(F(X,Y), Z)$,
- $F(X,Y) = F(Y,X)$,
- $F(0,X) = X = F(X,0)$, and
- there exists $i(X) \in R[[X]]$ such that $F(i(X), X) = F(X, i(X)) = 0$.

In other words: F puts the structure of a group object in formal schemes on $\operatorname{Spf} R[[X]]$. If you ask for just a group structure on $\hat{\mathbb{A}}^1_R$ without specifying an isomorphism $\hat{\mathbb{A}}^1_R \cong \operatorname{Spf} R[[X]]$, that's a *formal group over* R. FGs differ from FGLs only in that an FGL comes equipped with a canonical choice of coordinate for $\hat{\mathbb{A}}^1_R$.

Given FGLs F, G over R, a morphism $\phi : F \to G$ is a power series $\phi(X) \in R[[X]]$ such that $\phi(F(X,Y)) = G(\phi(X), \phi(Y))$. We say ϕ is *strict* if $\phi(X) \equiv X$ modulo X^2.

A *logarithm* for an FGL F over R is a power series $\log_F(X) \in R[[X]]$ such that $\log_F^{-1}(\log_F(X) + \log_F(Y)) = F(X,Y)$ and such that $\log_F(X) \equiv X$ modulo X^2. Every FGL is the reduction, modulo some ideal, of an FGL with a logarithm defined over a larger ring; so it usually does no harm to assume all FGLs have logarithms.

Here is the connection to elliptic curves: the Riemann-Roch theorem establishes that a smooth algebraic curve of genus g has a g-dimensional vector space of holomorphic 1-forms, and the degree of a holomorphic 1 form on a curve is $2g - 2$. So a smooth algebraic curve has a *nonvanishing* holomorphic 1-form if and only if its genus is 1, and every elliptic curve has a one-dimensional vector space of nonvanishing holomorphic 1-forms. In Example 1.4, we saw that $1/y\ dx$ generates this vector space, for the elliptic curve $y^2 = x^3 + x$; in fact $1/y\ dx$ generates this vector space for all elliptic curves with Weierstrass equations $y^2 = x^3 + Ax + B$.

If $\omega = g(X)\ dX$ is a holomorphic differential 1-form on an elliptic curve E over a ring R of characteristic zero, then the formal power series $\log_F(X) = \int\omega = \int g(X)\ dX \in R[[X]]$ is the logarithm of a formal group law $F(X,Y) = \log_F^{-1}(\log_F(X) + \log_F(Y))$, called the *formal group law of the elliptic curve E.* It is true, but not immediately obvious, that $F(X,Y)$ is defined over R. (The reason it isn't obvious is that formal integration introduces denominators, so unless R is a *field* of characteristic zero, the logarithm $\log_F(X) = \int\omega$ is only defined over $R \otimes_{\mathbb{Z}} \mathbb{Q}$. The "miracle"—not really a miracle, and explained nicely by Hazewinkel's functional equational lemma—is that these denominators disappear when you form $\log_F^{-1}(\log_F(X) + \log_F(Y))$, so that $\log_F^{-1}(\log_F(X) + \log_F(Y)) = F(X,Y) \in R[[X,Y]]$.)

There are other ways to construct and/or describe the formal group law of an elliptic curve; here is one other way. Elliptic curves are, a priori, smooth projective algebraic curves of genus 1; something that is true, but not obvious, is that every elliptic curve also has the additional structure of an *abelian variety,* that is, every elliptic curve E also admits a multiplication map $E \times E \to E$ and inverse map $E \to E$ which are both morphisms of varieties and which endow E with the structure of an abelian group. So elliptic curves are "like" Lie groups, in an algebraic (rather than simply smooth) setting; in fact when the ground field is $\mathbb{C}$, every elliptic curve *is* a Lie group, but it's a special kind of Lie group, one whose transition maps are not only smooth or analytic but actually *polynomial.* (As ordinary, smooth Lie groups, elliptic curves over $\mathbb{C}$ are all tori of the same dimension, so they are isomorphic to one another; it is only in the category of varieties (or abelian varieties), rather than the category of manifolds (or Lie groups), that any two elliptic curves can be non-isomorphic.) Over $\mathbb{R}$, a nice way to define the group structure on a Weierstrass elliptic curve E is by declaring any three (counting multiplicity) collinear points to sum to zero. This makes the (unique) point at infinity of the Weierstrass curve into the identity element of the group structure. A more conceptual approach to the group structure is to observe that every elliptic curve E is canonically isomorphic (via Abel-Jacobi) to the connected component $\mathrm{Pic}^0(E)$ of the identity in its Picard group scheme $\mathrm{Pic}(E)$, so transporting the group structure on $\mathrm{Pic}^0(E)$ along that isomorphism yields a canonical group structure on E.

Once you have a group structure on E, the tangent space to the identity of E inherits a Lie algebra structure, from taking the commutator of tangent vectors using the multiplication on E. You can tell this isn't a very useful thing to do, because in the smooth category every elliptic curve is just a torus, and the Lie algebra of an analytic (or algebraic) Lie group only depends on its underlying Lie group in the smooth category, which is an abelian Lie algebra for a torus. So for elliptic curves the Lie bracket is just zero. The purpose of studying an elliptic curve's formal group law is that, since an elliptic curve E is not just a Lie group but is an *analytic* Lie group, you have a well-defined multiplication not only of tangent vectors to the identity element on E, you also have some algebraic structure defined on higher-order (quadratic, cubic, etc.) infinitesimal data near the identity element. Scheme-theoretically, if E is an elliptic curve over a field k, we let $\eta : \mathrm{Spec}\, k \to E$ be the map sending the point $\mathrm{Spec}\, k$ to the identity element of E, and we take a formal completion of E along the inclusion map η to get an affine formal scheme $\hat{E}_\eta$. Since E is smooth, $\Gamma(\hat{E}_\eta)$ is a regular, adically-complete local k-algebra whose unit map $k \to \Gamma(\hat{E}_\eta)$ admits a left inverse in k-algebras, so by the Cohen structure theorem, $\Gamma(\hat{E}_\eta) \cong k[[x_1, \dots, x_n]]$ for some n; since E is a curve, $n = 1$. The group structure on E induces a group structure $\hat{E}_\eta \times \hat{E}_\eta \to \hat{E}_\eta$ on $\hat{E}_\eta$, and on taking global sections, a cogroup structure $\Delta : \Gamma(\hat{E}_\eta) \cong k[[z]] \to k[[x, y]] \cong \Gamma(E \mathbin{\hat{\times}} E_\eta)$, i.e., the structure of a Hopf algebra on $k[[x]]$. The formal power series $\Delta(z) \in k[[x, y]]$ is the formal group law of the elliptic curve E: it agrees with the one you can get by integrating a nonvanishing holomorphic differential.

3. Height, supersingularity.

Given a prime p, an FGL with a logarithm is called *p-typical* if $\log_F(X) = \sum_{n \geqslant 0} \ell_i X^{p^i}$, i.e., all the coefficients in $\log_F(X)$ vanish except the ones for powers of p. If R is a $\mathbb{Z}_{(p)}$-algebra, then every formal group law is canonically strictly isomorphic to a p-typical one (its *Cartier typicalization*), so if we p-localize, it again usually do no harm to assume that our formal group laws are p-typical. The *p-height* of a p-typical FGL is the least n such that the coefficient ℓ_n in the logarithm $\sum_{n \geqslant 0} \ell_n X^{p^n}$ is nonzero modulo p. Over $\overline{\mathbb{F}}_p$, FGLs are classified up to isomorphism by their height $\in \{1, 2, \dots, \infty\}$.

If E is an elliptic curve over $\mathbb{Q}$, we can clear denominators in a Weierstrass equation presenting E to get a set of defining equations for E over $\mathbb{Z}$, and regard E as an "elliptic curve over $\mathbb{Z}$." (Note that we didn't really define elliptic curves over rings that aren't fields, hence the scare quotes.) But really there are many possible proper schemes over $\mathbb{Z}$ with generic fibre (i.e., $\mathbb{Q}$-points) isomorphic to E, and some may have nicer properties than others. Let's call such a proper scheme over $\mathbb{Z}$ an *integral model for E.* For a given prime p, there are four possibilities for what happens when you reduce modulo p the equations for an integral model for E:

- You might get a singular curve over $\mathbb{F}_p$ in which the singularity is a cusp. This happens when the formal group law of the integral model has infinite p-height, i.e., its reduction modulo p is isomorphic to the additive formal group law $F(X, Y) = X + Y$. We then say that this integral model for E has *additive reduction at p.*
- You might get a singular curve over $\mathbb{F}_p$ in which the singularity is a node. When this happens, the formal group law of the integral model has p-height 1, i.e., its reduction modulo p is isomorphic to a multiplicative formal group law $F(X, Y) = X + Y + uXY$ with u a unit. We then say that this integral model for E has *multiplicative reduction at p.*
- You might get a smooth curve over $\mathbb{F}_p$, and the (Cartier p-typicalization of the) formal group law has p-height 2. We then say that this integral model for E *has good reduction at* p and is *supersingular at p.* (This terminology isn't good: supersingular curves aren't singular! But it has the weight of tradition behind it.)

- You might get a smooth curve over $\mathbb{F}_p$, and the (Cartier p-typicalization of the) formal group law of E has p-height 1[1]. We say that E *has good reduction at* p and is *ordinary at* p.

Whether a Weierstrass equation over $\mathbb{Q}$ with good reduction at p is ordinary or supersingular is determined by the vanishing of the Hasse invariant, E_{p-1}, which is a polynomial in the Weierstrass coefficients; however, this polynomial E_{p-1} is a different polynomial for each prime p, so we can't conclude that the vanishing locus of E_{p-1} (i.e., the set of Weierstrass curves which are supersingular at p) is a finite subset of $\mathbb{Z}$ by some easy argument about Zariski-closed subsets of $\mathbb{Z}$. Instead, what happens is that, for a CM elliptic curve E (i.e., an elliptic curve over $\mathbb{Q}$ whose endomorphism ring contains the ring of integers in a quadratic extension of $\mathbb{Q}$), the asymptotic density of supersingular primes for E is 0.5, so "half the primes are supersingular," while for a non-CM elliptic curve E over $\mathbb{Q}$, a deep theorem of Elkies is that there are infinitely many supersingular primes for E, but that set of primes has asymptotic density 0.

There is another perspective on the distinction between ordinary and supersingular primes for an elliptic curve. Given an elliptic curve E over $\mathbb{Q}$ and a prime p of good reduction for E, choose a prime $\ell \neq p$, and write $(E/p)_{\mathrm{et}}$ for the small étale site on E reduced modulo p, i.e., the category of affine schemes over $E \otimes_{\mathbb{Z}} \mathbb{F}_p$ that are members of some étale covering family of $E \otimes_{\mathbb{Z}} \mathbb{F}_p$, equipped with the Grothendieck topology given by étale covers. Let $\mathbb{Z}/\ell^m\mathbb{Z} : (E/p)_{\mathrm{et}}^{\mathrm{op}} \to \mathrm{Ab}$ be the sheafification of the constant presheaf of abelian groups taking the value $\mathbb{Z}/\ell^m\mathbb{Z}$. We can take the right-derived functors $R^n\Gamma$ of the functor of global sections Γ on the category of sheaves of abelian groups on $(E/p)_{\mathrm{et}}$, and we define $H^n_{\mathrm{et}}(E;\mathbb{Q}_\ell)$ as

$$H^n_{\mathrm{et}}(E;\mathbb{Q}_\ell) = \mathbb{Q}_\ell \otimes_{\hat{\mathbb{Z}}_\ell} \lim_m (R^n\Gamma)(\mathbb{Z}/\ell^m\mathbb{Z}).$$

Grothendieck's de Rham theorem identifies the dimension of the $\mathbb{Q}_\ell$-vector space $H^n_{\mathrm{et}}(E;\mathbb{Q}_\ell)$ with the dimension of the $\mathbb{R}$-vector space of the de Rham cohomology $H^n_{dR}(E \otimes_{\mathbb{Z}} \mathbb{C})$, regarding $E \otimes_{\mathbb{Z}} \mathbb{C}$ as an ordinary, classical manifold. So, since de Rham cohomology agrees with singular cohomology and $E \otimes_{\mathbb{Z}} \mathbb{C}$ is topologically just a torus, we have

$$H^n_{\mathrm{et}}(E;\mathbb{Q}_\ell) \cong \begin{cases} \mathbb{Q}_\ell & \text{if } n = 0, 2 \\ \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell & \text{if } n = 1 \\ 0 \text{ otherwise.} & \end{cases}$$

[1] Note that, if the FGL has p-height 1, this doesn't immediately tell you whether the given integral model for your curve has multiplicative reduction, or ordinary good reduction: for that, you also need to know if the curve has singular reduction modulo p. You might ask: is there a way of augmenting the FGL with additional "FGL-like" data, such that we can tell whether an integral model for E has multiplicative reduction or ordinary good reduction, just from the FGL with that extra data? The answer is yes: this is what the *p-divisible group* of an integral model, also called its *Barsotti-Tate group*, provides. Without defining what p-divisible groups are, here is how the story plays out: the p-divisible group of an integral model for E with multiplicative reduction is isomorphic (over $\overline{\mathbb{F}}_p$) to $\mathbb{G}_1$, the slope 1 indecomposable p-divisible group in the Dieudonné-Manin classification, while the p-divisible group of an integral model for E with ordinary good reduction is $\mathbb{G}_0 \oplus \mathbb{G}_1$, a direct sum of indecomposable slope 0 and an indecomposable slope 1. The formal group of a p-divisible group (over $\overline{\mathbb{F}}_p$) captures just the positive-slope summands, which is one way of saying why the FGL alone doesn't distinguish between multiplicative reduction and ordinary good reduction. For what it's worth, integral models with supersingular reduction have p-divisible group isomorphic to $\mathbb{G}_{1/2}$, an indecomposable slope 1/2 p-divisible group.

So the $\mathbb{Q}_\ell$-vector space dimension of $H^n_{\mathrm{et}}(E;\mathbb{Q}_\ell)$ actually does not depend on the choice of prime p, as long as $p \neq \ell$.

The reason to use étale cohomology in this setting, and not simply de Rham cohomology, is that étale cohomology has a special operator acting on it: every object in $(E/p)_{\mathrm{et}}$ is, in particular, a scheme over $\mathbb{F}_p$, so there is a well-defined Frobenius (pth power) morphism Fr_p on the étale cohomology of E/p. In particular, we have an $\mathbb{Q}_p$-linear operator Fr_p on $H^1_{\mathrm{et}}(E;\mathbb{Q}_\ell) \cong \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell$. That operator is known to be semisimple, i.e., after base-change to $\overline{\mathbb{Q}}_\ell$, it's diagonalizable, even when its two eigenvalues coincide. (More generally, this is conjectured to be true even when E isn't an elliptic curve: the action of Fr_p on $H^n_{\mathrm{et}}(X;\mathbb{Q}_\ell)$ is expected to be semisimple for all smooth varieties over $\mathbb{Z}$ with good reduction at p (this is Tate's conjecture), and it's known to be true for X an abelian variety, e.g. when X is an elliptic curve.

The reason this matters is that the Hasse-Weil zeta-function of E is

$$\zeta_E(s) = \prod_{p \text{ good red.}} \prod_{n \geqslant 0} \det\left(\mathrm{id} - p^{-s}\,\mathrm{Fr}_p \mid |_{H^n_{\mathrm{et}}(E;\mathbb{Q}_\ell)}\right)^{(-1)^{n+1}} \cdot \prod_{p \text{ bad red.}} ??, \tag{3.1}$$

which converges for complex s with sufficiently large real part, and which *conjecturally* admits meromorphic continuation to $\mathbb{C}$. (Perhaps the meromorphic continuation is known now: the modularity theorem relates the good-reduction factors in (3.1) to the L-function of modular forms, which are known to be admit meromorphic continuations to $\mathbb{C}$.) In (3.1) I have left off the Euler factors at primes of bad reduction of E, because I don't remember what you're supposed to do there (sorry, I'm writing these notes from memory; you get degree 0 and 1 Euler factors[2] at primes of bad reduction, rather than degree 2.). It's not hard to see that E can have only finitely many primes of bad reduction: for example, if you write E in the form of a Weierstrass equation, then its Jacobian is a one-by-two matrix of polynomials, so bad reduction of E is equivalent to simultaneous vanishing of Weierstrass equation and the two (polynomial) entries in the Jacobian, for some (x, y), i.e., bad reduction of E happens in a Zariski-closed subset of $\mathbb{Z}$, so E has either finitely many primes of bad reduction, or *all* primes are primes of bad reduction for E. With a bit more you can rule out the second possibility, and E consequently has only finitely many primes of bad reduction, so (3.1) gives you $\zeta_X(s)$ up to finitely many factors corresponding to the primes of bad reduction.

One part of the (now proven) Weil conjectures was that the eigenvalues of the action of Fr_p on $H^n_{\mathrm{et}}(E;\mathbb{Q}_\ell)$ have complex norm $p^{n/2}$, under a fixed choice of embedding of fields $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$. In particular, if $H^n_{\mathrm{et}}(E;\mathbb{Q}_\ell)$ is a one-dimensional $\mathbb{Q}_\ell$-vector space, then Fr_p acts on $H^n_{\mathrm{et}}(E;\mathbb{Q}_\ell)$ simply by multiplication by $p^{n/2}$.

The previous two paragraphs actually apply equally well to all smooth curves E over $\mathbb{Q}$, after clearing denominators to get a curve over $\mathbb{Z}$—E doesn't actually have to be elliptic. (Of course, the relationship between Frobenius semisimplicity and the height of the formal group relies on E being elliptic: if E is a non-elliptic curve, it's not even clear what kind of formal group we can associate to E, much less that there is one whose p-height governs the semisimplicity of action of Fr_p on $H^1_{\mathrm{et}}(E;\mathbb{Q}_\ell)$. But the stuff on p-height was more than two paragraphs ago.) Those ideas are enough to let us calculate the Hasse-Weil zeta-function of the projective line, $\mathbb{P}^1$:

[2] The *degree* of an Euler factor $\left(a_0 + a_1p^{-s} + a_2p^{-2s} + \cdots + a_np^{-ns}\right)^{(-1)^m}$ with $a_n \neq 0$ is defined to be n. In other words: if you treat an Euler factor as a polynomial in p^{-s}, the degree of an Euler factor is just the degree of that polynomial.

by Grothendieck's de Rham theorem, $\dim_{\mathbb{Q}_\ell} H^n_{\mathrm{et}}(\mathbb{P}^1;\mathbb{Q}_\ell) = \dim_{\mathbb{R}}(H^n_{dR}(\mathbb{C}P^1))$, which is 1 if $n = 0, 2$ and which is zero otherwise. So Weil's description of the norm of the Frobenius eigenvalues actually determines the Frobenius eigenvalues:

$$\begin{aligned}\zeta_{\mathbb{P}^1}(s) &= \prod_p \frac{1}{(1-p^{-s})(1-p^{1-s})}\\ &= \zeta(s)\zeta(s-1),\end{aligned}$$

so the meromorphic continuation of the Riemann zeta-function $\zeta(s)$ to $\mathbb{C}$, with its only pole at $s = 1$, gives you the meromorphic continuation of $\zeta_{\mathbb{P}^1}(s)$ to $\mathbb{C}$ as well, with its only poles at $s = 1$ and $s = 0$. Notice that the nice formula $\zeta(1-n) = \frac{-B_n}{n}$ for the values of the Riemann zeta-function at negative integers gets totally lost when you pass to $\zeta_{\mathbb{P}^1}(s)$, since $\zeta(1-n)$ vanishes for odd n, so in the product $\zeta(s)\zeta(s-1)$, whenever s is an integer < -1, one of the two factors is necessarily zero. So the only nonvanishing special value of $\zeta_{\mathbb{P}^1}(s)$ at a negative integer is $\zeta_{\mathbb{P}^1}(-1) = \zeta(-1)\zeta(0) = \frac{-1}{12}\frac{-1}{2} = \frac{1}{24}$.

I shouldn't forget to mention the formula

$$\prod_{n\geqslant 0} \det\left(\mathrm{id} - p^{-s}\operatorname{Fr}_p \mid |_{H^n_{\mathrm{et}}(E;\mathbb{Q}_\ell)}\right)^{(-1)^{n+1}} = e^{\sum_{m\geqslant 0}\frac{\#(E(\mathbb{F}_{p^m}))}{m}p^{-ms}},$$

which holds at primes p of good reduction for E. Here $\#(E(\mathbb{F}_{p^m})$ is the number of points on E over $\mathbb{F}_{p^m}$, i.e., the number of solutions to the defining equations for E over the field $\mathbb{F}_{p^m}$. This tells you why people actually care about Hasse-Weil zeta-functions: if p is a prime of good reduction for E, then the p-local Euler factor of $\zeta_E(s)$ records some very concrete and important arithmetic data, the number of points on E over each finite field of characteristic p. So the Hasse-Weil zeta-function relates arithmetic data (points counts of a variety over finite fields) to topological data (de Rham cohomology of the complex points of the variety) and to analytic number-theoretic data (factorizations of the resulting Hasse-Weil zeta-function into copies of Riemann, Dirichlet, etc. zeta- and L-functions, and resulting asymptotics).

That whole train of thought about the Hasse-Weil zeta-function of $\mathbb{P}^1$—using the topology of the complex points to make a cohomological calculation, deducing something about the Frobenius action, then rewriting the Hasse-Weil zeta-function as a product of L-functions of a number-theoretic origin (e.g. the Riemann zeta-function), and drawing conclusions about meromorphic continuation and behavior in the left half-plane—is all a pretty standard train of thought for Hasse-Weil zeta-functions of more general varieties, too. Let's try it for an elliptic curve. If α, β are the eigenvalues of Fr_p, then of course $\det\left(\mathrm{id} - p^{-s}\operatorname{Fr}_p \mid |_{H^n_{\mathrm{et}}(E;\mathbb{Q}_\ell)}\right)$ is just

$$(1-\alpha p^{-s})(1-\beta p^{-s}) = 1 - (\alpha+\beta)p^{-s} + \alpha\beta p^{-2s} = 1 - (\alpha+\beta)p^{-s} \pm p^{1-2s},$$

with the last equality due to the complex norm of each eigenvalue being $\sqrt{p}$. (More about that below.) The number $\alpha + \beta$ is, of course, the trace of Fr_p; this number is often called a_p. If $p > 2$, there aren't many ways a sum of two complex numbers of norm $\sqrt{p}$ can be divisible be p, so if p is a prime of good reduction with $p \mid a_p$, then the p-local Euler factor in $\zeta_E(s)$ is just $\frac{1-p^{1-2s}}{1-p^{-s}}1 - p^{1-s}$, i.e., it's the same as in the p-local Euler factor of $\frac{\zeta(2s)}{\zeta(s)\zeta(s-1)}$. The primes p of good reduction for E for which $p \mid a_p$ turn out to be exactly the supersingular primes for E! That's the relationship between supersingular primes and $\zeta_E(s)$.

Now if you've done some number theory in the past, maybe you're thinking you might be able to write $\zeta_E(s)$ as a product of degree 1 L-functions: classically that's what you do with the Dedekind zeta-functions of abelian number fields, using class field theory to rewrite the Artin L-functions of the characters of the Galois group of the number field as Dirichlet (or at least Hecke) L-functions:

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{m} \subseteq \mathcal{O}_K} \frac{1}{\#(\mathcal{O}_K/\mathfrak{m})^s} \tag{3.2}$$

$$= \prod_{\rho : G_{K/\mathbb{Q}} \to GL_n(\mathbb{C})} \frac{1}{\left(\det\left(\mathrm{id} - p^{-s}\,\mathrm{Fr}_p \mid_\rho\right)\right)^{\deg(\rho)^2}} \tag{3.3}$$

$$= \prod_{\rho : G_{K/\mathbb{Q}} \to \mathbb{C}^\times} \frac{1}{\det\left(\mathrm{id} - p^{-s}\,\mathrm{Fr}_p \mid_\rho\right)} \tag{3.4}$$

$$= \prod_{\chi_1, \chi_2, \dots, \chi_n} \frac{1}{1 - \chi(p)p^{-s}} \tag{3.5}$$

where (3.2) is a definition, (3.3) is an Euler product expansion combined with Artin's factorization, (3.4) is because we assumed K is abelian so its Galois group has only one-dimensional representations, and (3.5) is a consequence of global class field theory: the splitting of primes in (a representation of) an abelian number field is governed by a reciprocity law, and the reciprocity law can be encoded by a Dirichlet character of modulus equal to the modulus of the reciprocity law.

When it comes to the zeta-function of an elliptic curve, that same logic applies to the supersingular primes (as above, since the Euler factor for every supersingular prime is just $\frac{\zeta(2s)}{\zeta(s)\zeta(s-1)}$), but not very well to the ordinary primes. Here is an example: let E be the projectivization of the curve $y^2 = x^3 + x$, and let $p \geqslant 5$. Then E is supersingular at p if and only if $p \equiv 3$ modulo 4. (That's not supposed to be an obvious fact, but it's true: section 4.6 in Washington's book on elliptic curves is a nice reference.) So, at ordinary primes $p \geqslant 5$, the p-local Euler factor of $\zeta_E(s)$ is $\frac{1 - a_p p^{-s} \pm p^{1-2s}}{(1-p^{-s})(1-p^{1-s})}$, while at supersingular primes $p \geqslant 5$, the p-local Euler factor of $\zeta_E(s)$ is $\frac{1-p^{1-2s}}{(1-p^{-s})(1-p^{1-s})}$. So the Euler factors of $\zeta_E(s)$ at supersingular primes are easily expressed in familiar terms. But the Euler factors of $\zeta_E(s)$ at ordinary primes are much harder to express in terms of degree 1 L-functions, like the Riemann zeta-function or Dirichlet L-functions. For example, take a look at this table of values of a_p, for the curve $y^2 = x^3 + x$, that I produced in SAGE (very easily—this is good software!):

```
print "p, p mod 4, a_p"
for p in range(3,500):
    if is_prime(p):
        E = EllipticCurve(GF(p),[1,0])
        print p, p % 4 , E.cardinality() - p - 1
```

```
Output:

p, p mod 4, a_p
3 3 0
5 1 -2
```

```
7 3 0
11 3 0
13 1 6
17 1 -2
19 3 0
23 3 0
29 1 -10
31 3 0
37 1 -2
41 1 -10
43 3 0
47 3 0
53 1 14
59 3 0
61 1 -10
67 3 0
71 3 0
73 1 6
79 3 0
83 3 0
89 1 -10
97 1 -18
101 1 -2
103 3 0
107 3 0
109 1 6
113 1 14
127 3 0
131 3 0
137 1 22
139 3 0
149 1 14
151 3 0
157 1 22
163 3 0
167 3 0
173 1 -26
179 3 0
181 1 -18
191 3 0
193 1 14
197 1 -2
199 3 0
211 3 0
223 3 0
227 3 0
229 1 30
233 1 -26
```

```
239 3 0
241 1 30
251 3 0
257 1 -2
263 3 0
269 1 -26
271 3 0
277 1 -18
281 1 -10
283 3 0
293 1 -34
307 3 0
311 3 0
313 1 -26
317 1 22
331 3 0
337 1 -18
347 3 0
349 1 -10
353 1 -34
359 3 0
367 3 0
373 1 14
379 3 0
383 3 0
389 1 -34
397 1 38
401 1 -2
409 1 6
419 3 0
421 1 30
431 3 0
433 1 -34
439 3 0
443 3 0
449 1 14
457 1 -42
461 1 38
463 3 0
467 3 0
479 3 0
487 3 0
491 3 0
499 3 0
```

So:

$$\zeta_E(s) = \frac{1-3^{1-2s}}{(1-3^{-s})(1-3^{1-s})}\frac{1+2\cdot 5^{-s}-5^{1-2s}}{(1-5^{-s})(1-5^{1-s})}\frac{1-7^{1-2s}}{(1-7^{-s})(1-7^{1-s})}\frac{1-11^{1-2s}}{(1-11^{-s})(1-11^{1-s})}$$
$$\frac{1-6\cdot 13^{-s}-13^{1-2s}}{(1-13^{-s})(1-13^{1-s})}\frac{1+2\cdot 17^{-s}-17^{1-2s}}{(1-17^{-s})(1-17^{1-s})}\frac{1-19^{1-2s}}{(1-19^{-s})(1-19^{1-s})}\dots.$$

You can see how a_p is vanishing for the primes congruent to 3 modulo 4: those are the supersingular primes for this curve! But you can also see that the value of a_p, for $p \equiv 1 \mod 4$, is hard to predict: a_p isn't a root of unity in general, so there's no way $\zeta_E(s)$ could be equal to a product of Dirichlet L-functions. If it's periodic like how Dirichlet L-functions and degree 1 Artin L-functions are **(in other words: if there is a reciprocity law which says that $a_p = a_\ell$ whenever $p \equiv \ell$ modulo N for some particular N; this is precisely the analogue, for $\zeta_E(s)$, of what quadratic and cubic and Jacobi and Hilbert etc. etc. reciprocity says about $\zeta_K(s)$ for abelian number fields K)**, then it must be periodic of very long period.

In fact I think we find that this function $p \mapsto a_p$ isn't periodic; the methods for proving this are something that I am just now learning myself, so I won't say I'm positive that it's true. However, it happens that there is a modular form $\mathcal{E}$ of weight 2 and level 64 (the numerology here is that 64 is the *conductor* of E) such that the q-expansion of $\mathcal{E}$ is $a_1q + a_2q^2 + a_3q^3 + \dots$, i.e., the coefficients a_p appearing in $\zeta_E(s)$ are the prime-degree Fourier coefficients of a modular form! In fact, this *always* happens, by Wiles' proof of the Shimura-Taniyama conjecture, now called the modularity theorem: the factor $\prod_{p\ good\ red.}(1 - a_p p^{-s} + p^{-2s}) = \sum_{n\geqslant 1}\frac{a_n}{n^s}$ in $\zeta_E(s)$ coming from H^1_{et}, for E an elliptic curve of conductor N, is always the L-series of a cusp form of weight 2 and level N, i.e., the cusp form has q-expansion $a_1q + a_2q^2 + a_3q^3 + \dots$.