Gross-Zagier reading seminar notes:
Modular curves over the integers
Lecture 8 • Wei Ho • November 4, 2014

1 Introduction

In previous lectures, we introduced modular curves over $\mathbb{C}$ (first constructed as quotients of the upper half plane by congruence subgroups) and then over $\mathbb{Q}$. We recall the modular interpretation of the open modular curves $\mathscr{Y}_0(N)$ and $\mathscr{Y}_1(N)$ over $\mathbb{Q}$ (or any field k of characteristic not dividing N): for any k-algebra R,

- R-points of $\mathscr{Y}_0(N)$ correspond to elliptic curves E over R with a subgroup D of order N, also defined over R; or equivalently, cyclic degree N isogenies $\varphi : E \to E'$ of elliptic curves E and E' over R [where $\ker \varphi$ corresponds to the subgroup D]
- R-points of $\mathscr{Y}_1(N)$ correspond to elliptic curves E over R with an R-rational point P of order N.

The usual notation $Y_0(N)$ and $Y_1(N)$ refer to the coarse moduli spaces of the stacks $\mathscr{Y}_0(N)$ and $\mathscr{Y}_1(N)$ here, and the modular curves $X_0(N)$ and $X_1(N)$ over k are compactifications of $Y_0(N)$ and $Y_1(N)$, respectively, where the cusps correspond to generalized elliptic curves with appropriate level structure.

Let $\mathscr{M}_{1,1}$ denote the moduli stack of elliptic curves over $\mathbb{Q}$ (or k). Here, because of the restriction on the characteristic of k, the forgetful maps $\mathscr{Y}_0(N) \to \mathscr{M}_{1,1}$ and $\mathscr{Y}_1(N) \to \mathscr{M}_{1,1}$ (just taking the elliptic curve E from the modular interpretation above) are étale, so the fibers are well understood. Because $\mathscr{M}_{1,1}$ is smooth and these maps are étale, the moduli stacks $\mathscr{Y}_i(N)$ here are smooth, as are the schemes $Y_i(N)$ for $i = 0$ or 1. (Note that the smoothness of the coarse space from the smoothness of the stack is only automatically true in dimension 1, e.g., with a curve over a field, and we will have to work harder in the sequel when considering the modular curve over, say, $\mathbb{Z}$.)

When the characteristic of the base field divides N, however, attempting to define the modular curves in the same way is problematic, as we will see below. Our goal for this lecture is to describe an appropriate regular model for $X_0(N)$ over $\mathbb{Z}$ (see the book of [Katz-Mazur] for proofs and details; other references include the earlier work of Deligne-Rapoport [Deligne-Rapoport] for the case N is squarefree and the ideas of Drinfeld [Drinfeld]).

2 p-torsion in characteristic p

Let k be a field not of characteristic p and E an elliptic curve over k. Then the p-torsion $E[p]$ of E over the algebraic closure $\overline{k}$ is well known to be isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ as a group (because multiplication by p has degree p^2).

On the other hand, now let k be a field of characteristic p and E an elliptic curve over k. Then E is either *ordinary* or *supersingular*. There are many equivalent definitions of these notions; today we will use the ones relevant to p-torsion. (However, it is not easy to show that all of these definitions are equivalent!) The elliptic curve E is *ordinary* if $E[p](\overline{k}) \cong \mathbb{Z}/p\mathbb{Z}$ and is *supersingular* if $E[p](\overline{k}) = 0$.

To show that these are the only two options for the p-torsion of E, we introduce the Frobenius map F and the Verschiebung map V. The naive definition of the Frobenius map for, say, a variety S over k in $\mathbb{A}^n$ is to send a point $x = (x_1, \ldots, x_n) \in S$ to $(x_1^p, \ldots, x_n^p) \in S^{(1)}$, which is a particular twist of S where the coefficients of the defining polynomials are raised to the pth power. It is not a priori clear, however, that this is a well defined map (e.g., it may depend on the embedding of S!). A perhaps better definition is more algebraic, as follows. If R is a k-algebra, let $\mathrm{Frob}_R : R \to R$ be defined by $\mathrm{Frob}_R(x) = x^p$. Then consider the diagram below:

$$\begin{tikzcd}
& & R \\
R \arrow[rru, bend left, "\mathrm{Frob}_R"] \arrow[r, "\mathrm{Frob}_k \otimes R"] & R^{(1)} := \mathrm{Frob}_k^* R \arrow[ur, dashed, "F"] & \\
k \arrow[u] \arrow[r, "\mathrm{Frob}_k"'] & k \arrow[u] \arrow[uur] &
\end{tikzcd}$$

Here, the map labeled $\mathrm{Frob}_k \otimes R$ is just acting as Frob_k on the "coefficients" in k. By the universal property of the tensor product, the dotted arrow exists and is unique, and that is the desired Frobenius map F. While the map Frob_R is not a k-linear map, the map F is k-linear. Note that if R is the base change to k of an $\mathbb{F}_p$-algebra, then $R^{(1)} \cong R$. By abuse of notation, we also call the geometric version of this Frobenius map F; we will consider $F : E \to E^{(1)}$ for our elliptic curve E.

The Verschiebung map V is the isogeny $V : E^{(1)} \to E$ dual to F. The compositions $V \circ F$ and $F \circ V$ are both the multiplication-by-p maps for E and $E^{(1)}$, respectively, because F has degree p. Thus, the p-torsion of $E^{(1)}$ is the preimage of the identity point O on $E^{(1)}$ under $F \circ V = p$. (Note that every elliptic curve arises as $E^{(1)}$ for some E by twisting by the inverse of Frobenius, which we can do over $\overline{k}$.)

The preimage of O under F is the fat point at O of degree p; as a subscheme, it has coordinate ring $k[x]/(x^p)$ and we can think of it as a divisor $p \cdot O$. (Here, by abuse of notation, O refers to either the identity point of E or $E^{(1)}$ as appropriate.) Moreover, the map V is degree p, so it is either purely inseparable or separable. If the latter, it is étale (by, e.g., Riemann-Hurwitz). Thus, the preimage of O under V is either $p \cdot O$ or p distinct points over $\overline{k}$. Therefore, as a *set*, the preimage of O under the composition $F \circ V$ is either just the identity point O or p points; as a *group*, we see that $E[p](\overline{k})$ is either 0 or $\mathbb{Z}/p\mathbb{Z}$.

Note that $E[p]$ does have more interesting structure as a *group scheme*, however. In particular, if E is ordinary, then by the connected étale sequence, we have that $E[p]$ is the extension of an étale group scheme by a connected group scheme. Here, we have that the étale group scheme must be $\mathbb{Z}/p\mathbb{Z}$ (over $\overline{k}$) and thus by Cartier duality, the connected piece is $\mu_p \cong (\mathbb{Z}/p\mathbb{Z})^\vee$ (this is all of $E[p]$ because of degree considerations). We see that $E[p]$ as a group scheme over $\overline{k}$ is an extension of $\mathbb{Z}/p\mathbb{Z}$ by μ_p; over a perfect field L (like $\overline{k}$), we have $\mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z}, \mu_p) \cong H^1_{\text{flat}}(\mathrm{Spec}\ L, \mu_p) \cong L^\times/(L^\times)^p = 0$. Thus, over $\overline{k}$, we have that $E[p]$ is canonically isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mu_p$. If E is supersingular, note that $E[p]$ has no étale part from the description above, hence no μ_p piece either. Thus, $E[p]$ is an extension of α_p by α_p (here, α_p is the kernel of Frobenius on $\mathbb{G}_a$).

By purely formal arguments, the structure of $E[p]$ for ordinary elliptic curves shows that $E[p^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p \times \mu_{p^\infty}$ as a ind-(group scheme) (by p-divisibility and taking an inductive limit of $E[p^n]$).

By the above analysis of the p-torsion of elliptic curves in characteristic p, we see that the previous modular interpretations for the modular curves $Y_0(N)$ and $Y_1(N)$ would not be correct in characteristic p dividing N, or in particular, over $\mathbb{Z}$.

3 Drinfeld's level structure

To remedy the issue of p-torsion not behaving in a straightforward manner in characteristic p, we use Drinfeld's definitions of level structure (started in [Drinfeld] and expanded in a letter by Deligne).

Let E be an elliptic curve over a ring R. (In fact, we can take any curve over R that has a commutative group scheme structure for these definitions.)

Definition 1. For a positive integer N, we say that a point P on $E(R)$ has *exact order* N if the effective Cartier divisor

$$D := [P] + [2P] + \cdots + [NP]$$

is a **subgroup** of E over R.

In this definition, since D is a divisor, it is a closed subscheme of E, and if P is of exact order N, then D inherits the structure of an R-group scheme from E, i.e., for any R-algebra S, $D(S) \subset E(S)$ is a subgroup.

Lemma 3.1. *If $P \in E(R)$ has exact order N as above, then $NP = 0$ in $E(R)$.*

In fact, N kills the group scheme D (a result of Deligne found in [Oort-Tate]). If N is invertible in R, then any group scheme of order N is étale; using the lemma, one can show that P has exact order N as above if and only if the order of $P \in E(R)$ is N. Note that if $N = p^e$, then the points P of exact order N lie in the p-divisible group of E.

Example 3.2. If R is an $\mathbb{F}_p$-algebra, then the identity point O in E has exact order p^e for any positive integer e. For each p^e, the subgroup corresponding to D is the kernel of F^e.

Example 3.3. Let $E = \mathbb{G}_m$ over a field $R = k$ of characteristic p (possibly 0). If $p \nmid N$, then an element $\lambda \in \mathbb{G}_m(k) = k^\times$ has exact order N if and only if $D := [\lambda] + [\lambda^2] + \cdots + [\lambda^N]$ is a subgroup scheme of $\mathbb{G}_m$. The only subgroup schemes of $\mathbb{G}_m$ are μ_r's, so λ has exact order N if λ is a **primitive** Nth root of unity. (Note that if $\lambda = 1$, for example, and $N \neq 1$, then D is the N-fold infinitesimal neighborhood of 1, which is not a subgroup scheme of $\mathbb{G}_m$.)

For simplicity, assume $N = p^e$ for a positive integer e. Note that $\mathbb{G}_m[p](k) = \mu_p(k) = 0$ because a field of characteristic p has no nontrivial pth roots of unity. By the lemma, any λ of exact order $N = p^e$ must have order dividing p^e and thus must be 1, in which case the divisor D is μ_{p^e} as a subgroup scheme of $\mathbb{G}_m$.

Example 3.4. If E is an ordinary elliptic curve over an algebraically closed field $\overline{k}$ of characteristic p, then recall that the p-divisible group $E[p^\infty]$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p \times \mu_{p^\infty}$. So the set of points $P \in E(\overline{k})$ of exact order p are those corresponding to $(a, 1) \in \mathbb{Q}_p/\mathbb{Z}_p \times \mu_{p^\infty}$, where a is an element of the natural subgroup $\mathbb{Z}/p\mathbb{Z}$ of $\mathbb{Q}_p/\mathbb{Z}_p$. More generally, the points of exact order p^e correspond to $(a, 1)$ where a is an element of the natural subgroup $\mathbb{Z}/p^e\mathbb{Z}$. Observe that the identity point has exact order p^e for any positive integer e, as seen in Example 3.2.

4 Regular models for $X_0(p)$ and $X_1(p)$

We now specialize to the case $N = p$ to describe a regular model for the modular curves $X_0(p)$ and $X_1(p)$ over $\mathbb{Z}$.

For $X_1(p)$, we consider the moduli stack $\mathcal{Y}_1(p)$ of elliptic curves E equipped with a point P of exact order p (from Definition 1), or equivalently, p-isogenies $\varphi : E \to E'$ of elliptic curves together with a generator P in the kernel of φ. Note that the divisor D associated to a point P of exact order p gives an isogeny $E \to E/D$. Then we have:

Theorem 4.1 ([Katz-Mazur, Chapter 5]). *The stack $\mathcal{Y}_1(p)$ over $\mathbb{Z}$ is finite and flat over $\mathscr{M}_{1,1}$ and regular.*

Idea of proof: The finiteness is clear, and the flatness follows from showing that $\mathcal{Y}_1(p)$ is regular (via the "miracle flatness" theorem). To show that this stack is regular, because the regular locus is open and regularity only depends on the p-divisible group of the corresponding elliptic curves, it is enough to show regularity at a single point corresponding to a supersingular elliptic curve E_0 over $\mathbb{F}_{p^e}$. Let $E/W(\mathbb{F}_{p^e})[\![t]\!]$ be the universal deformation of E_0. Then $W(\mathbb{F}_{p^e})[\![t]\!]$ is the complete local ring of $\mathscr{M}_{1,1}$ at E_0. Its preimage in $\mathcal{Y}_1(p)$ is of the form $\mathrm{Spec}(A)$ for some finite $W(\mathbb{F}_{p^e})[\![t]\!]$-algebra A, and the pullback $E_A \to \mathrm{Spec}\,(A)$ is equipped with a point $P \in E_A(A)$ of exact order p by definition of the moduli problem $\mathcal{Y}_1(p)$. One then shows that T and $x(P)$ generate the maximal ideal A, proving regularity.

We now consider the moduli stack $\mathcal{Y}_0(p)$ of p-isogenies of elliptic curves $\varphi : E \to E'$ where $\ker\varphi$ has a generator P of exact order p étale (= fppf here) locally. In fact, this stack $\mathcal{Y}_0(p)$ is isomorphic to $[\mathcal{Y}_1(p)/(\mathbb{Z}/p\mathbb{Z})^\times]$, where $(\mathbb{Z}/p\mathbb{Z})^\times$ acts on the point P of exact order p in $\ker\varphi$. Because $\mathcal{Y}_1(p)$ is finite and flat over $\mathscr{M}_{1,1}$ and regular, so is $\mathcal{Y}_0(p)$. We can also compactify this stack to $\mathcal{X}_0(p)$ in a natural way (by including generalized elliptic curves and appropriate conditions on $\ker\varphi$. It is clear that $\mathcal{Y}_0(p)$ and $\mathcal{X}_0(p)$ are well behaved in characteristics other than p.

To describe the geometry of $\mathcal{Y}_0(p)$ in characteristic p (i.e., tensor everything in the next two paragraphs with $\mathbb{Z}/p\mathbb{Z}$), we construct two distinct maps $a, c : \mathscr{M}_{1,1} \to \mathcal{Y}_0(p)$. In particular, we have $a(E) = (F : E \to E^{(1)})$ and $c(E) = (V : E^{(1)} \to E)$. Note that composing a and c with the forgetful map $\mathcal{Y}_0(p) \to \mathscr{M}_{1,1}$ (sending $\varphi : E \to E'$ to E) gives the identity map and Frobenius, respectively. Each of these maps is a closed immersion, so we obtain two irreducible components of $\mathcal{Y}_0(p)$. Because $\mathcal{Y}_0(p) \to \mathscr{M}_{1,1}$ has degree $p+1$ (by calculating in characteristic 0, using flatness), these two components are the only components.

These two components intersect exactly at the set of points in $\mathcal{Y}_0(p)$ corresponding to isogenies of supersingular elliptic curves. If $E \in \mathscr{M}_{1,1}$ is an ordinary elliptic curve, then $a(E)$ and $c(E)$ are different points in $\mathcal{Y}_0(p)$ because $\ker F$ is a connected group scheme and $\ker V$ is an étale group scheme. On the other hand, if E is a supersingular elliptic curve, then so is $E^{(1)}$; it thus has only one cyclic p-isogeny, so $a(F(E)) = c(E)$.

5 Regular models for $X_0(N)$

In this section, we simply summarize the results from [Gross-Zagier, §III.1] for more general N.

We consider the moduli stack $\mathcal{X}_0(N)$ (or $\mathscr{M}_{\Gamma_0(N)}$) of isogenies $\varphi : E \to E'$ of degree N between generalized elliptic curves E and E' such that the group scheme $\ker\varphi$ meets every irreducible component of every geometric fiber and $\ker\varphi$ has a point of exact order N étale locally. Let $\underline{X} = \underline{X_0(N)}$ denote the coarse moduli scheme of $\mathcal{X}_0(N)$. Then $\underline{X} \otimes \mathbb{Z}[1/N]$ is smooth and proper over $\overline{\mathbb{Z}[1/N]}$, but $\underline{X} \otimes \mathbb{Z}/p\mathbb{Z}$ is singular and reducible for any prime p dividing N.

Let $N = p^n M$ with $p \nmid M$. Then $\underline{X} \otimes \mathbb{Z}/p\mathbb{Z}$ has $n+1$ irreducible components, denoted $\mathcal{F}_{a,n-a}$, where a is an integer between 0 and n; the stratification into these components is based on the group scheme $\ker\varphi$ for the points of $\underline{X}$ corresponding to ordinary elliptic curves. In particular, at the ordinary points of the component $\mathcal{F}_{a,n-a}$, the group scheme $\ker\varphi$ is isomorphic to $\mu_{p^a} \times \mathbb{Z}/p^{n-a}\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$. Each component is isomorphic to $X_0(M) \otimes \mathbb{Z}/p\mathbb{Z}$ and has multiplicity $\phi(p^{\min(a,n-a)})$ in $\underline{X} \otimes \mathbb{Z}/p\mathbb{Z}$, where ϕ denotes the Euler ϕ function. Analogous to the case of $X_0(p)$, the components $\mathcal{F}_{a,n-a}$ intersect at each of the points of $\underline{X}$ corresponding to $\varphi : E \to E'$ where both E and E' are supersingular elliptic curves.

The argument for $\mathcal{X}_0(p)$ can be generalized to show that the moduli stack $\mathcal{X}_0(N)$ is regular over $\mathbb{Z}$. Analyzing the automorphism groups (with some work) gives that the coarse moduli scheme $\underline{X}$ over $\mathbb{Z}$ is regular except at the supersingular points in characteristics dividing N (unless the automorphism group of the corresponding isogeny is just $\{\pm 1\}$).

The cusps of $\underline{X}$ can also be analyzed combinatorially. For each positive divisor d of N, there is one irreducible component isomorphic to Spec $\mathbb{Z}[\mu_{\gcd(d,N/d)}]$, with $\phi(\gcd(d,N/d))$ geometric points, each corresponding to isogenies of Néron polygons with $\ker\varphi \cong \mu_d \times d\mathbb{Z}/N\mathbb{Z}$. In characteristic p, this cusp component lies on the component $\mathcal{F}_{a,n-a}$ of $\underline{X}$ where $a = \mathrm{ord}_p(d)$.

References

[Deligne-Rapoport] Pierre Deligne and Michael Rapoport. **Les schémas de modules de courbes elliptiques.** *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pp. 143Ð316. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

[Drinfeld] V. G. Drinfeld. **Elliptic modules.** *Mat. Sb. (N.S.)* **94 (136)** (1974), 594–627, 656.

[Gross-Zagier] Benedict H. Gross and Don B. Zagier. **Heegner points and derivatives of L-series.** *Invent. math.* **84**, 225-320 (1986).

[Katz-Mazur] Nicholas Katz and Barry Mazur. **Arithmetic moduli of elliptic curves.** Annals of Mathematics Studies, 108, *Princeton University Press*, Princeton, 1985.

[Oort-Tate] Frans Oort and John Tate. **Group schemes of prime order.** *Ann. Scient. Ecole Norm. Sup.*, 4e série, t.3, 1970, 1-21.