Arithmetic Moduli of Elliptic Curves, An Introduction

Chunlei Liu

July 20, 2005

Remark This note is based on a one-hour talk at a summer school on Shimura varieties in Hanzhou. It follows the book *p-adic automorphic forms on Shimura varieties* by Haruzo Hida.

1 Moduli of elliptic curves of level 1

Let R be a commutative ring with identity in which 2 and 3 are invertible. So R is a $\mathbb{Z}[\frac{1}{6}]$-algebra. We shall classify all pairs (E, ω), where E is elliptic curve over R and ω is a nowhere vanishing holomorphic form on E over R.

Definition 1.1 *A proper smooth curve over R whose geometric fibres are connected and of genus 1, together with an R-point O, is called an elliptic curve over R.*

Example 1.1 *Let $c_2, c_3 \in R$ such that $c_2^3 - 27c_3^2 \in R^\times$. Let*

$$E : Y^2Z = 4X^3 - c_2XZ^2 - c_3Z^3$$

be the gluing together of

$$E_0 : y^2 = 4x^3 - c_2x - c_3$$

and

$$E_1 : w = 4z^3 - c_2zw^2 - c_3w^3$$

along

$$E_0 \cap E_1 : \begin{cases} y^2 = 4x^3 - c_2x - c_3, \\ x = yz, \\ yw = 1. \end{cases}$$

Then E, together with the R-point O on E_1 defined by $z = w = 0$, is an elliptic curve over R. We call it a Weierstrass form over R. In particular,

$$\boldsymbol{E} : Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$$

is an elliptic curve over $\mathfrak{R} = \mathbb{Z}[\frac{1}{6}][g_2, g_3, \frac{1}{g_2^3 - 27g_3^2}]$, where g_2, g_3 are algebraically independent variables over $\mathbb{Z}[\frac{1}{6}]$.

The following lemma in some sense reduces the theory of elliptic curve to a theory of Weierstrass forms.

Lemma 1.2 *Every elliptic curve over R admitting a nowhere vanishing holomorphic form over R is isomorphic to a Weierstrass form over R.*

Remark In the CMS talk, the false statement that *every elliptic curve over R is isomorphic to a Weierstrass form over R* was made. Brian Conrad helps the author a lot in correcting that misunderstanding.

By that lemma,

$$\varphi \mapsto [(\mathbf{E} \otimes_{\mathfrak{R},\varphi} R, \frac{dx}{y})]$$

gives a one-to-one correspondence between $(\mathrm{Spec}\mathfrak{R})(R) := \mathrm{Hom}_{\mathbb{Z}[\frac{1}{6}]}(\mathfrak{R}, R)$ and the set $\{[(E,\omega)/R]\}$ of isomorphism classes of all pair (E,ω) over R. Moreover, if $\alpha \in \mathrm{Hom}_{\mathbb{Z}[\frac{1}{6}]}(R, R')$, then, the diagram

$$\begin{array}{ccc} (\mathrm{Spec}\mathfrak{R})(R) & \rightarrow & \{[(E,\omega)/R]\} \\ \downarrow & & \downarrow \\ (\mathrm{Spec}\mathfrak{R})(R') & \rightarrow & \{[(E,\omega)/R']\} \end{array}$$

commutes, where the vertical arrows are the morphisms induced by α. In that situation, we say that $\mathrm{Spec}\mathfrak{R}$ and the classifying functor $R \mapsto \{[(E,\omega)/R]\}$ are isomorphic over $\mathbb{Z}[\frac{1}{6}]$.

Proposition 1.3 *The functor $Spec\mathfrak{R}$ and the classifying functor of all pair (E,ω) are isomorphic over $\mathbb{Z}[\frac{1}{6}]$.*

2 Moduli of Elliptic curves of level $\Gamma_0(N)$

Let R be a commutative $\mathbb{Z}[\frac{1}{6}]$-algebra with identity, and (E, O) an elliptic curve over R.

Proposition 2.1 *There is a unique group scheme structure on E over R making E a group scheme over R with identity O.*

After classifying all triples $(E, \omega.P)$, we shall classify all pairs (E, P), where ω ia a nowhere vanishing holomorphic differential form on E over R, and P is an R-point on E of exact order N. We assume that $N > 3$.

Since closed immersions are stable under base change, $\mathbf{E}[N] := \ker\{N : \mathbf{E} \rightarrow \mathbf{E}\}$ is a closed sub-scheme of $\mathbf{E}$. It follows that

$$\mathfrak{M}_{\Gamma_1(N)} := \mathbf{E}[N] - \bigcup_{d|N, d<N} \mathbf{E}[d]$$

is a closed sub-scheme of $\mathbf{E}_0$. So we can write $\mathfrak{M}_{\Gamma_1(N)} = \mathrm{Spec}\mathfrak{R}_{\Gamma_1(N)}$.

Proposition 2.2 *The correspondence*

$$\varphi \mapsto [(\boldsymbol{E} \otimes_{\mathfrak{R},\phi} R, \frac{dx}{y}, \varphi \otimes id_R)],$$

where ϕ is the composition of φ and the structure morphism of $\boldsymbol{E}$ over $\mathfrak{R}$, gives an isomorphism over $\mathbb{Z}[\frac{1}{6}]$ between $\mathfrak{M}_{\Gamma_1(N)}$ and the classifying functor of all triples (E, ω, P).

In fact, suppose that we are given an elliptic curve E over R, an R-point P of exact order N, and a nowhere-vanishing holomorphic differential form ω over R. We can assume that E is a Weierstrass form $Y^2Z = 4X^3 - c_2XZ^2 - c_3Z^3$ and $\omega = \frac{dx}{y}$. Then $E = \mathbf{E} \otimes_{\mathfrak{R},\phi} R$, and P lies in $\mathfrak{M}_{\Gamma_1(N)} \otimes_{\mathfrak{R},\phi} R$, where ϕ is the R-point of Spec$\mathfrak{R}$ sending g_2 to c_2 and g_3 to c_3. Let φ be the composition of P and the projection of $\mathfrak{M}_{\Gamma_1(N)} \otimes_{\mathfrak{R},\phi} R$ to $\mathfrak{M}_{\Gamma_1(N)}$. Then $P = \varphi \otimes \mathrm{id}_R$, and ϕ is the composition of φ and the structure morphism of $\mathbf{E}$ over $\mathfrak{R}$.

The group $\mathbb{G}_m(R) := R^\times$ acts on the set of isomorphism classes of all triples (E, ω, P) over R as follows:

$$\lambda \circ [(E, \omega, p)] = [(E, \lambda\omega, p)].$$

That action gives rise to an action of $\mathbb{G}_m(R)$ on $\mathfrak{M}_{\Gamma_1(N)}(R)$. Moreover, if $\alpha \in \mathrm{Hom}_{\mathbb{Z}[\frac{1}{6}]}(R, R')$, then, for every $\lambda \in \mathbb{G}_m(R)$, the diagram

$$\begin{array}{ccc} \mathfrak{M}_{\Gamma_1(N)}(R) & \stackrel{\lambda}{\to} & \mathfrak{M}_{\Gamma_1(N)}(R) \\ \downarrow & & \downarrow \\ \mathfrak{M}_{\Gamma_1(N)}(R') & \stackrel{\alpha(\lambda)}{\to} & \mathfrak{M}_{\Gamma_1(N)}(R') \end{array}$$

commutes, where the vertical arrows are the morphism induced by α. In that situation, we say that $\mathbb{G}_m$ acts on $\mathfrak{M}_{\Gamma_1(N)}$ over $\mathbb{Z}[\frac{1}{6}]$.

Lemma 2.3 *Let M be an A-algebra, and $\mathbb{G}_m$ acts on Spec$M$ over A. Then M is a graded A-algebra.*

In fact, since the $M \otimes_A A[t, t^{-1}]$-points of $\mathbb{G}_m$ acts on the $M \otimes_A A[t, t^{-1}]$-points of Spec$M$, there are endomorphisms $p_k \in \mathrm{End}_A(M)$, $k \in \mathbb{Z}$, such that

$$t \circ (\mu \mapsto \mu \otimes_A 1) = (\mu \mapsto \sum_{k \in \mathbb{Z}} p_k(\mu) \otimes_A t^k).$$

Moreover, for each A-algebra B, $\mathbb{G}_m(B)$ acts on $(\mathrm{Spec}M)(B)$ as follows:

$$\lambda \circ \varphi = (\mu \mapsto \sum_{k \in \mathbb{Z}} \varphi(p_k(\mu))\lambda^k).$$

Set $B = M \otimes_A A[t, t^{-1}] \otimes_A A[t, t^{-1}]$. On one hand, we have

$$(t \otimes_A t) \circ (\mu \mapsto \mu \otimes_A 1 \otimes_A 1) = (t \otimes_A 1) \circ (\mu \mapsto \sum_{k \in \mathbb{Z}} p_k(\mu) \otimes_A (1 \otimes_A t)^k)$$

$$= (\mu \mapsto \sum_{k,l \in \mathbb{Z}} p_l(p_k(\mu)) \otimes_A t^l \otimes_A t^k).$$

On the other hand, we have

$$(t \otimes_A t) \circ (\mu \mapsto \mu \otimes_A 1 \otimes_A 1) = (\mu \mapsto \sum_{k \in \mathbb{Z}} p_k(\mu) \otimes_A (t \otimes_A t)^k).$$

It follows that $p_l \circ p_k = \delta_{lk} p_k$, where δ_{lk} is Kronecker's δ function. Hence $M = \oplus_{k \in \mathbb{Z}} p_k(M)$ is a graded A-algebra.

By that lemma, $\mathfrak{R}_{\Gamma_1(N)} = \oplus_{k \in \mathbb{Z}} \mathfrak{R}_{\Gamma_1(N),k}$ is a graded $\mathbb{Z}[\frac{1}{6}]$-algebra. Write $Y_1(N) := \mathrm{Spec}\mathfrak{R}_{\Gamma_1(N),0}$.

Proposition 2.4 *For $N \geq 4$, $Y_1(N)$ and the classifying functor of all pairs (E, P) are isomorphic over $\mathbb{Z}[\frac{1}{6}]$.*