Math 726: L-functions and modular forms Fall 2011

Lecture 16 : Algebraic Modular forms cont'd

Instructor: Henri Darmon *Notes written by: Maxime Turgeon*

In the last lecture, we gave two important examples of marked elliptic curves over a ring:

1. **The universal elliptic curve**

$$(\mathbb{C}/\langle 1,\tau\rangle)_{\mathcal{O}_{\mathcal{H}}} = (y^2 = 4x^3 - g_4(\tau)x - g_6(\tau), \frac{dx}{y})_{\mathcal{O}_{\mathcal{H}}};$$

2. **The Tate elliptic curve**

$$\left(\mathbb{C}^\times/\langle q\rangle, \frac{dt}{t}\right)_{\mathcal{O}_{D^\times}} = (y^2 = x^3 - a(q)x + b(q), \frac{dx}{y})_{\mathcal{O}_{D^\times}},$$

where $a(q) = \frac{1}{3}\left(1 + 240\sum_{n=1}^\infty \sigma_3(n)q^n\right)$ and $b(q) = \frac{2}{27}\left(1 - 504\sum_{n=1}^\infty \sigma_5(n)q^n\right)$.

Note that the Tate elliptic curve can be viewed as an elliptic curve over the ring $\mathbb{Z}[\frac{1}{6}]((q))$. But with more care (for example, by introducing new parameters), one can show that it can also be viewed as an elliptic curve over $\mathbb{Z}((q))$:

$$\left(E_{Tate}, \frac{dt}{t}\right)_{\mathbb{Z}((q))} = \left(\mathbb{G}_m/\langle q\rangle, \frac{dt}{t}\right)_{\mathbb{Z}((q))}.$$

We also defined a *weakly holomorphic algebraic modular form* of weight k and level 1 to be a rule

$$(E,\omega)_R \longrightarrow f(E,\omega)_R \in R,$$

subject to two conditions, namely, that it should be compatible with base change (see Lecture 15) and that it should satisfy the following homogeneity condition

$$f(E,\lambda\omega) = \lambda^{-k} f(E,\omega), \text{ for all } \lambda \in R^\times.$$

In particular, $f\left(\mathbb{C}/\langle 1,\tau\rangle, dz\right)_{\mathcal{O}_{\mathcal{H}}} \in \mathcal{O}_{\mathcal{H}}$ is the *classical* view of (weakly holomorphic) modular forms as holomorphic functions on $\mathcal{H}$. Also, note that $f\left(E_{Tate}, \frac{dt}{t}\right)_{\mathbb{Z}((q))} \in \mathbb{Z}((q))$ is the *q-expansion* of f.

Definition 1. An *algebraic modular form* over $\mathbb{Z}$ is a weakly holomorphic modular form over $\mathbb{Z}$ such that $f\left(E_{Tate}, \frac{dt}{t}\right)_{\mathbb{Z}((q))} \in \mathbb{Z}[[q]]$. Moreover, if $f\left(E_{Tate}, \frac{dt}{t}\right)_{\mathbb{Z}((q))} \in q\mathbb{Z}[[q]]$, we say that f is *cusp form.*

For an arbitrary ring S, f is a modular form if

$$f\left(E_{Tate}, \frac{dt}{t}\right)_{S[[q]]} \in S\left[[q]\right].$$

Thus, we say a modular form over S has Fourier coefficients in S (this is called the *q-expansion principle*).

Recall that we were able to give a good description of the ring of modular forms of level 1 in the classical setting, namely, we proved that the Eisenstein series E_4 and E_6 are generators. In a more general setting, we can give a good description of the **ring of algebraic modular forms over** $\mathbb{Z}[\frac{1}{6}]$.

THEOREM 2. *Let $(E,\omega)_k$ be a marked elliptic curve over a field k of characteristic different from 2 and 3. Then, there exist* uniquely defined *elements $x, y \in H_0(E\backslash\{O\}, \mathcal{O}_E)$ (that is, functions regular outside the origin) satisfying*

- *The function x has a double pole at the origin, whereas the function y has a triple pole at the origin;*
- *x, y satisfy a cubic equation of the form $y^2 = x^3 + ax + b$;*
- *$\frac{dx}{y} = \omega$.*

Sketch of proof. First, we define two families of k-vector spaces:

$$\begin{aligned} \mathcal{L}_r &= \{f \in H_0(E\backslash\{O\}, \mathcal{O}_E) \mid ord_O(f) < -r\}, \\ \mathcal{L}_r^* &= \{\omega \in H_0(E, \Omega^1) \mid ord_O(\omega) > r\}, \end{aligned}$$

where $r \geq 0$ is an integer. The Riemann-Roch theorem gives the following relation between the respective dimensions of these two vector spaces:

$$\dim_k \mathcal{L}_r - \dim_k \mathcal{L}_r^* = r + (1-g),$$

where g is the genus; in our case $g = 1$. Using this relation, we can build the following table:

r	$dim\mathcal{L}_r$	$dim\mathcal{L}_r^*$	basis for $\mathcal{L}_r$
0	1	1	$\{1\}$
1	1	0	$\{1\}$
2	2	0	$\{1, x\}$
3	3	0	$\{1, x, y\}$
4	4	0	$\{1, x, y, x^2\}$
5	5	0	$\{1, x, y, x^2, xy\}$
6	6	0	$\{1, x, y, x^2, xy, \frac{x^3}{y^2}\}$

Table 1: Dimensions of the vector spaces

After eventualy rescaling x and y, we can assume $x^3 - y^2 \in \mathcal{L}_5$, which gives us a dependence relation:

$$y^2 = x^3 + axy + bx^2 + cy + dx + e, \text{ where } a, b, c, d, e \in k.$$

When choosing the vector x, we could have chosen any vector of the form $x + \mu$, with $\mu \in k$. Similarly for y, we could have chosen any vector of the form $y + \mu' x + \rho'$, where $\mu', \rho' \in k$. Hence, by replacing y by $y + \mu' x + \rho'$ (with appropriate μ', ρ'), we can eliminate the xy and y terms, which gives a relation of the form

$$y^2 = x^3 + b' x^2 + c' x + d'.$$

Note that at this stage, we have to assume that char $k \neq 2$: in order to eliminate the xy term, we need $\mu' = \frac{a}{2}$, and to eliminate the y term, we need $\rho' = \frac{c}{2}$, which only makes sense if 2 is invertible. Furthermore, by replacing x by $x + \mu$ (with appropriate μ), we can eliminate the x^2 term, and this gives a relation of the form

$$y^2 = x^3 + a'' x + b''.$$

At this stage, we have to assume that char $k \neq 3$: to eliminate the x^2 term, we need $\mu = \frac{-b'}{3}$, which can only be done if 3 is invertible. With these choices, x and y are completely determined, up to the following change of variables:

$$(x, y) \longmapsto (\lambda^2 x, \lambda^3 y),$$

for a nonzero $\lambda \in k$. The effect of this change of variables on the differential is $\frac{dx}{y} \mapsto \frac{1}{\lambda} \frac{dx}{y}$. Thus, the condition $\omega = \frac{dx}{y}$ specifies the pair (x, y) *uniquely.* $\square$

The equation $y^2 = x^3 + ax + b$ is called the *canonical equation* associated to the pair (E, ω). We thus get the following bijection:

$$\left\{ \begin{array}{c} \text{Marked elliptic} \\ \text{curves } (E, \omega)_k \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} (a, b) \in k^2 \text{ satisfying} \\ \Delta(a, b) \neq 0 \end{array} \right\}.$$

Note that we have two distinguished algebraic modular forms over $\mathbb{Z}[\frac{1}{6}]$:

1. $\mathbf{a}(E, \omega) = a$, where a is the coefficient of x in the canonical equation of (E, ω). This $\mathbf{a}$ is a suitable multiple of the Eisenstein series of weight 4.

2. $\mathbf{b}(E, \omega) = b$, where b is the constant coefficient in the canonical equation of (E, ω). Note that $\mathbf{b}$ is a suitable multiple of the Eisenstein series of weight 6.

From the above discussion, we conclude that the ring of algebraic modular forms over $\mathbb{Z}[[\frac{1}{6}]]$ is generated by the modular forms $\mathbf{a}$ and $\mathbf{b}$.