# MODULAR FORMS LECTURE 13: MODULAR FUNCTIONS AND ELLIPTIC CURVES

LARRY ROLEN, VANDERBILT UNIVERSITY, FALL 2020

> Everyone knows what a curve is, until he has studied enough mathematics to become confused through the countless number of possible exceptions.
>
> Felix Klein

We have characterized all holomorphic modular forms using the valence formula. What about other spaces of meromorphic modular forms? If we allow poles, we will get infinite dimensional spaces. This is still often manageable, though; for example, if we look at weakly holomorphic forms and bound the order of the pole at $\infty$, then we still obtain finite dimensional spaces. For example, we can multiply by powers of $\Delta$ to get to holomorphic modular form spaces and can go backwards because $\Delta$ has no poles on the upper half plane. Thus, $M_k^!$ is nearly as easy to specify as $M_k$.

There is a key case we want to look at now. We call any element of $M_0^{\text{mero}}$ a **modular function**. Let's try to construct an example of a modular function. If we take a quotient of two modular forms with the same weight, the result will be something of weight 0. If we use $M_{12}$, then we have a 2-dimensional space, and $\Delta$ has no zeros on $\mathbb{H}$. So we have

$$j(\tau) := \frac{E_4^3}{\Delta} = q^{-1} + 744 + 196884q + \ldots \in M_0^!.$$

This is called **Klein's $j$-invariant**.

**Theorem.** *The $j$-invariant is a bijection from $\mathcal{F}$ to $\mathbb{C}$. Further, it is a bijection between the compactified upper half plane $\overline{\mathbb{H}} = \mathbb{H} \cup \infty$ modulo $\Gamma$ to the Riemann sphere $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C} \cup \infty$.*

*Proof.* The function $j(\tau)$ has a simple pole at $\infty$ and no other poles. So it takes $\infty$ to $\infty$. Now we want to show that it is a bijection $\Gamma\backslash\mathbb{H} \to \mathbb{C}$. For any $c \in \mathbb{C}$, the modular form $E_4^3 - c\Delta \in M_{12}$ has by the Valence Formula exactly one zero (it can't be at $\infty$ as the Fourier expansion is $1 + O(q)$, and its a triple zero at $\omega$ if and only if $c = 0$) in $\mathbb{H}$. Dividing by $\Delta$, $j(\tau) - c = 0$ has a unique solution for each $c \in \mathbb{C}$. □

Modular functions are also easy to determine using $j$. This is a very special property of $\mathrm{SL}_2(\mathbb{Z})$; that its a **genus zero** group ($\Gamma\backslash\overline{\mathbb{H}}$ is a Riemann sphere) is why a function satisfying the next theorem exists. This makes $j(\tau)$ what we call a **Hauptmodul**.

**Theorem.** *We have $M_0^{\text{mero}} = \mathbb{C}(j)$, i.e., modular functions are rational functions in $j$.*

*Proof.* Its clear that $\mathbb{C}(j) \subseteq M_0^{\text{mero}}$. Conversely, if $f(\tau)$ is a modular function with poles at $\{\tau_j\}$ in $\mathcal{F}$, then

$$f(\tau) \cdot \prod_j (j(\tau) - j(\tau_j)) \in M_0^!$$

as this cancels out all poles on $\mathbb{H}$ and introduces no new ones there. So, WLOG, say $f \in M_0^!$. Then$f(\tau)\Delta(\tau)^j \in M_{12n}$ for sufficiently large $n$ to cancel the pole at $\infty$. Since holomorphic modular forms are linear combinations of powers of $E_4$ and $E_6$, we have that $f(\tau)$ is a linear combination of functions of the form $E_4^i E_6^j/\Delta^n$. Now $12|4i+6j$ so we have that $3|i$ and $2|j$. Write $i = 3i_0$, $j = 2j_0$. The original definition of $j(\tau)$, and our previous definition of $\Delta(\tau)$ show that $E_4^3/\Delta$ and $E_6^2/\Delta$ are rational functions in $j$ (the first *is* $j$ and for the second $E_6^2/\Delta \ddot{=} (E_4^3 + \Delta)/\Delta = j(\tau) + 1$, where $\ddot{=}$ means there are non-zero constants in front of each factor). Thus, $E_4^i E_6^j/\Delta^n = E_4^{3i_0} E_6^{j_0}/\Delta^n \in \mathbb{C}(j)$. □

Note that it is famously difficult to find this rational function in practice, but it exists!

Finally, we will fill in one detail that was promised in our earlier study of elliptic curves. For this, we first consider the meaning of $j(\tau)$ for elliptic curves.

**Definition.** The $j$-invariant of an elliptic curve $y^2 = x^3 + Ax + B$ is

$$-1728\frac{(4A)^3}{\Delta}.$$

The point is that it determines isomorphism classes of elliptic curves over $\mathbb{C}$.

**Definition.** We say that $E\colon y^2 = x^3 + Ax + B$ is isomorphic to $E'\colon y^2 = x^3 + A'x + B'$ over a field $K$ if there is a $\mu \in K^\times$ such that

$$A = \mu^4 A', \qquad B = \mu^6 B'.$$

**Remark.** *The point of this definition is that this is the only change of variables preserving the Weierstraß form of the elliptic curve equation. As an exercise, prove this.*

**Theorem.** *Two rational elliptic curves $E, E'$ over a field of characteristic not equal to 2 or 3 are isomorphic over $\mathbb{C}$ if and only if $j(E) = j(E')$.*

*Proof.* If $E \cong_{\mathbb{C}} E'$, then we have $A = \mu^4 A', B = \mu^6 B'$, so

$$j(E') = -1728\frac{(4A)'^3}{\Delta'} = -1728\frac{\mu^{12}(4A)^3}{-16(4A'^3 + 27B'^2)} = -1728\frac{(4A)^3}{-16(4A^3+27B^2)} = j(E).$$

Conversely, suppose $j(E) = j(E')$. Then

$$\frac{(4A)^3}{4A^3+27B^2} = \frac{(4A')^3}{4(A')^3+27(B')^2} \implies \frac{4A^3+27B^2}{(4A)^3} = \frac{4(A')^3+27(B')^2}{(4A')^3}$$

$$\implies A^3(B')^2 = (A')^3 B^2.$$

There are several cases.

**Case i).** $A = 0$**:** This is the case when $j = 0$. The discriminant can't be zero so $B \neq 0$, and we have $(A')^3B^2 = 0$, so we also have $A' = 0$. Then we satisfy the definition of isomorphism above with $\mu = (B/B')^{\frac{1}{6}}$.

**Case ii).** $B = 0$**:** This is the case when $j = 1728$. Again, we have $A \neq 0$, but $A^3(B')^2 = 0$, so $B' = 0$. Then we get our necessary change of variables $\mu = (A/A')^{\frac{1}{4}}$.

**Case ii).** $A, B \neq 0$**:** This is the case where $j \notin \{0, 1728\}$. We have that $A'B' \neq 0$, as if one of them was zero, then the relation above implies that both of them are, so we'd have that $\Delta' = 0$ and $E'$ wouldn't be an elliptic curve. Our rescaling is then given by $\mu = (A/A')^{\frac{1}{4}} = (B/B')^{\frac{1}{6}}$. □

**Remark.** *In particular, the above proof really shows that all we have to do is go to an algebraic closure of the field of definition of the curve, not necessarily all the way to* $\mathbb{C}$.

**Example 1.** Earlier we saw that the quadratic twists $E_n \colon y^2 = x^3 - n^2x$ are all isomorphic over $\mathbb{C}$, but not over $\mathbb{Q}$. We can see that they are isomorphic over $\mathbb{C}$ by checking the $j$-invariants. Indeed,

$$j(E_n) = -1728\frac{(-4n^2)^3}{-16 \cdot (-4n^6)} = 1728$$

is independent of $n$.

We now come to the promised result.

**Theorem.** *All rational elliptic curves are isomorphic to* $\mathbb{C}/\Lambda$ *for some lattice* $\Lambda$.

*Proof.* We saw earlier using $\wp, \wp'$ that there is an isomorphism from $\mathbb{C}/\Lambda$ to the elliptic curve $E_\Lambda \colon y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$. Let $j(\Lambda)$ be the $j$-invariant of this curve. Letting $\Lambda = \langle 1, \tau \rangle$, we see by tracing previous definitions that $j(\tau) = j(\Lambda)$. Then we need to show that there is a $\Lambda$ with $j(\Lambda) = j(E)$. In other words, we want to find a $\tau$ with $j(\tau) = j(E)$. But $j(E)$ is some fixed number, and we saw above that $j(\tau)$ takes every value in $\mathbb{C}$. □