Elliptic Curves as Complex Tori

Theo Coyne

June 20, 2017

1 Misc. Prerequisites

For an elliptic curve E given by $Y^2Z = X^2 + aXZ^2 + bZ^3$, we define its j-invariant to be $j(E) = \frac{1728(4a)^3)}{4a^3+27b^2}$. Two elliptic curves over an algebraically closed field (in particular, over $\mathbb{C}$!) are isomorphic if and only if they have the same j-invariant. E is smooth (and hence actually an elliptic curve) if and only if $4a^3 + 27b^2 \neq 0$, so this is well-defined. See Milne's notes for proof.

In my lecture, I also included a review of basic complex analysis. Knowing the residue theorem and Liouville's theorem should be sufficient to continue.

2 Lattices in $\mathbb{C}$

A lattice Λ in $\mathbb{C}$ is a subgroup generated by elements ω_1, ω_2 that are $\mathbb{R}$-independent. That is, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. So, we can try to parameterize the space of lattices by M, the space of pairs of $\mathbb{R}$-independent complex numbers (ω_1, ω_2). We can specify a preferred order on the ω_i by requiring $\Im(\omega_1/\omega_2) > 0$. Also, (ω_1, ω_2) and (ω_1', ω_2') will define the same lattice if and only if they differ by $GL_2(\mathbb{Z})$ action, but to preserve positive imaginary part, we restrict ourselves to $SL_2(\mathbb{Z})$. Hence, we get a bijection from $M/SL_2(\mathbb{Z})$ to the set $\mathcal{L}$ of lattices.

A lattice Λ is determined up to scaling by the ratio $\omega_1/\omega_2 \in \mathbb{H}$. The above bijection then becomes one between $\mathcal{L}/\mathbb{C}^\times$ and $\mathbb{H}/SL_2(\mathbb{Z})$. It's easy to see that the induced $SL_2(\mathbb{Z})$ action on $\mathbb{H}$ is $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau+b}{c\tau+d}$.

We consider lattices because the quotients $\mathbb{C}/\Lambda$ are tori. We shall now completely characterize maps between these tori.

Proposition 1. *The only holomorphic maps $\mathbb{C}\Lambda \to \mathbb{C}/\Lambda'$ taking 0 to 0 are maps of the form $[z] \mapsto [\alpha z]$ for some $\alpha \in \mathbb{C}$ satisfying $\alpha\Lambda \subset \Lambda'$ (and of course all such α define holomorphic functions).*

Proof. It is clear that we need $\alpha\Lambda \subset \Lambda'$ for multiplication by α to be well-defined. Certainly such maps are all holomorphic. We must verify that every holomorphic map $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ (taking 0 to 0) is of this form.

By the theory of covering spaces, we may uniquely lift ϕ to a map $\tilde{\phi} : \mathbb{C} \to \mathbb{C}$ taking 0 to 0. Now, for any $\omega \in \Lambda$, the map $z \mapsto \tilde{\phi}(z+\omega) - \tilde{\phi}(z)$ is continuous and takes values in Λ, hence is constant. This implies $\tilde{\phi}'$ is doubly periodic and hence constant. Combining with the condition $\tilde{\phi}(0) = 0$, we get $\tilde{\phi}(z) = \alpha z$ for some fixed α by integration.

□

We may also define functions whose input is a lattice in $\mathbb{C}$. The most natural of these are the Eisenstein series. For Λ a lattice and $k > 1$, consider

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda}{}' \frac{1}{\omega^{2k}}.$$

The prime on the sum means to exclude $\omega = 0$. We only care about even exponents since the sum is zero if the exponent is odd.

By the correspondence described above, this gives rise to a function on the upper half plane, defined by $G_{2k}(\tau) = G_{2k}(\mathbb{Z}\tau + \mathbb{Z})$, also called an Eisenstein series. A recurring theme in this talk will be sweeping convergence questions under the rug. So: the sum G_{2k} converges and does so nicely enough to be a holomorphic function on $\mathbb{H}$.

3 Doubly Periodic Funcitons

We want to study functions on lattices $\mathbb{C}/\Lambda$. A map $\mathbb{C}/\Lambda \to \mathbb{C}$ is the same thing as a map $f : \mathbb{C} \to \mathbb{C}$ with $f(z+\omega_1) = f(z) = f(z+\omega_2)$ for all $z \in \mathbb{C}$. Such a map f is called "doubly period" for obvious reasons. A doubly periodic non-constant function cannot be holomorphic everywhere by Liouville's theorem. So, we will content ourselves with meromorphic doubly periodic functions. Two easy results:

Proposition 2. *Let f be doubly periodic, not identically zero, and let D be a fundamental domain for Λ with no zeroes or poles on $\partial\Lambda$. Then*

- $\sum_{P \in D} Res_P(f) = 0$
- $\sum_{P \in D} ord_P(f) = 0$,

where $ord_P(f)$ is the order of a zero, or the negative of the order of a pole.

Proof. Apply the residue theorem to f and f'/f respectively, noting that both are doubly periodic, and hence integrate to zero over ∂D. □

We also note that any non constant doubly periodic map f is surjective has a zero, as otherwise $1/f$ would be bounded. Replacing f by $f - a$ shows that non constant doubly periodic maps are surjective. This could also be seen by appealing to the second statement of the previous proposition.

Our job is now to search for doubly periodic maps. Consider

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda}{}' \frac{1}{(z-\omega)^2} - \frac{1}{\omega}.$$

It converges, and it converges nicely enough to practice term-wise differentiation. Believe me. So, its derivative is:

$\wp'(z) = \sum_{\omega \in \Lambda} \frac{-2}{(z-\omega)^3}$. Since $\wp'$ is clearly doubly periodic, so is $\wp$ (proof: $\wp(z + \omega_1) - \wp(z)$ must be constant, but $\wp$ is even).

Now comes a surprising fact, which will relate the $\wp$-function to elliptic curves.

Proposition 3. *For a lattice Λ, the associated function $\wp$ satisfies the differential equation*

$$\wp'(z)^2 = 4\wp(z)^3 - g_4\wp(z) - g_6,$$

where $g_4 = 60G_4(\Lambda)$ and $g_6 = 140G_6(\Lambda)$.

Proof. We have the identity $\frac{1}{(1-t)^2} = \sum_{n \geq 1} nt^{n-1} = \sum_{n \geq 0}(n+1)t^n$ for $|t| < 1$. Now, for $|z|$ smaller than all $\omega \neq 0$, we get:

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\omega \in \Lambda}{}' \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{z^2} + \sum_{\omega \in \Lambda}{}' \frac{1}{\omega^2}\left(\frac{1}{1-(z/\omega)^2} - 1\right) \\
&= \frac{1}{z^2} \sum_{n \geq 1} \sum_{\omega}{}' (n+1)\frac{z^n}{\omega^{n+2}} = \frac{1}{z^2} + \sum_{k \geq 1}(2k+1)G_{2k+2}(\Lambda)z^{2k} \\
&= \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \ldots
\end{aligned}$$

This gives $\wp'(z) = \frac{-2}{z^3} + 6G_4 z + 20G_6 z^3 + \ldots$.

Expanding out, we find that $\wp'(z)^2 - 4\wp(z)^3 + 60G_4(\Lambda)\wp(z) + 140G_6(\Lambda)$ has no negative powers z^n and its constant term is 0. So it is holomorphic at $z = 0$ (with value zero) and hence at all lattice points. So, by Liouville, this function of z is identically zero. □

With this differential equation in mind, it is natural to try to associate an elliptic curve $Y^2Z = 4X^3 - g_4XZ^2 - g_6Z^3$ to the lattice Λ. Of course, we need to verify that this curve is nonsingular. By Adam's talk last week, the following lemma is sufficient to guarantee this.

Lemma 1. *The polynomial $f(X) = 4X^3 - g_4(\Lambda) - g_6(\Lambda)$ has distinct roots, for any $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.*

Proof. Since $\wp'$ is odd and doubly periodic, we have $\wp'(\omega_1/2) = -\wp'(-\omega_1/2) = -\wp'(\omega_1/2)$ and hence the differential equation tells us that $\wp(\omega_1/2)$ is a zero of f. Similarly, the other zeroes are $\wp(\omega_2/2)$ and $\wp((\omega_1+\omega_2)/2)$. It remains to check that these are all distinct.

Consider the function $\wp(z) - \wp(\omega_1/2)$. It has a zero at $\omega_1/2$, which must be of order 2 since its derivative also vanishes there. Also, in a fundamental domain D containing 0, its pole of order 2 is its only pole in the fundamental domain. Hence, since $\sum_{p \in D} ord(p) = 0$, we find that there are no other zeroes of $\wp(z) - \wp(\omega_1/2)$. In particular, $\wp(\omega_2/2)$ and $\wp((\omega_1+\omega_2)/2)$ are not equal to $\wp(\omega_1/2)$. Repeating the argument for the other two points in question finishes the argument. □

Call this elliptic curve $E(\Lambda)(\mathbb{C})$. We have a map $\mathbb{C}/\Lambda \to E(\Lambda)(\mathbb{C})$ given by taking $z+\Lambda$ to $(\wp(z) : \wp'(z) : 1)$. We shall verify that this map is an isomorphism of Riemann surfaces and of groups (remember that $\mathbb{C}/\Lambda$ is a quotient group too!).

Proposition 4. *The above map is an isomorphism of Riemann surfaces.*

Proof. Surjective: The map $\wp : \mathbb{C}/\Lambda \to \hat{\mathbb{C}} = \mathbb{P}^1(\mathbb{C})$ is surjective, as any non-constant doubly periodic map must be. As $\wp$ is even, the values $[z]$ and $[-z]$ map to the same value. Choose the one of the two that gives the correct y coordinate.

Injective: Suppose $(\wp(z_1), \wp'(z_1)) = (\wp(z_2), \wp'(z_2))$. First suppose $2z_1 \notin \Lambda$. Then $\wp(z) - \wp(z_1)$ is elliptic of order 2 and vanishes at $z_1, -z_2, z_2$, so two of these must be congruent modulo Λ (since $2z_1 \notin \Lambda$). Hence $z_2 \equiv \pm z_1 \mod \Lambda$. Comparing the values of $\wp'$ at these points gives $z_1 \equiv z_2 \mod \Lambda$.

On the other hand, suppose $2z_1 \in \Lambda$. Then $\wp(z) - \wp(z_1)$ has a double zero at z_1 (since $\wp'(z_1) = 0$) and vanishes at z_2. The same result follows.

The map is clearly holomorphic. That its inverse is holomorphic too may be proven by showing that the derivative never vanishes and appealing to the inverse function theorem. We shall not do this here. □

Proposition 5. *The map is also a group homomorphism.*

Proof. We verify the following addition formula:

$$\wp(z+z') = \frac{1}{4}\left(\frac{\wp'(z) - \wp'(z')}{\wp(z) - \wp(z')}\right) - \wp(z) - \wp(z').$$

Let $f(z)$ be the difference between the left and right hand sides. Its only possible poles are at $0, \pm z'$ and by calculating Laurent series, only $-z'$ is a possible pole, and at worst simple. But since $\wp(z+z')$ is doubly periodic this means it must be constant, and thus identically zero since $f(0) = 0$.

This agrees with the elliptic curve group law by the following calculation: let $P = (x, y)$ and $P' = (x', y')$ be points on the elliptic curve $Y^2 = 4X^3 - g_4X - g_6$

and let $Y = mX+b$ be the line passing through them. Then, x, x', and $x(P+P')$ are the roots of the cubic equation $(mX + c)^2 - 4X^3 + g_4X + g_6$ and so we get $x(P + P') + x + x' = m^2/4 = \frac{1}{4}\left(\frac{y-y'}{x-x'}\right)^2$. □

It turns out that every isomorphism class of elliptic curve comes from some torus. We won't prove this, but, following Milne, we will rephrase the question in terms of the j function. The j invariant of the curve $E(\Lambda)$ is

$$j(\Lambda) = \frac{1728 g_4(\Lambda)^3}{g_4(\Lambda)^3 - 27 g_6(\Lambda)^2}.$$

For $\tau \in \mathbb{H}$, we can define $j(\tau) = j(\mathbb{Z}\tau + \mathbb{Z})$. Since the j invariant of Λ depends only on Λ up to scaling, we see that the isomorphism class of $E(\Lambda)$ depends only on the isomorphism class of Λ.

We can rephrase the claim that every isomorphism class of elliptic curve arises from a lattice as the statement that this j function is surjective.

4 Some remarks about complex multiplication

Let's say something about the endomorphism ring $End(\mathbb{C}/\Lambda)$. We always have $\mathbb{Z} \subset End(\mathbb{C}/\Lambda)$, but if $\tau = \omega_1/\omega_2$ satisfies $[\mathbb{Q}(\tau) : \tau] = 2$, then $End(\mathbb{C}/\Lambda)$ is a rank 2 subring of $\mathbb{Q}(\tau)$.

For example, $\mathbb{C}/\mathbb{Z}[i]$ has multiplication by i as an element.

For some concrete examples in elliptic curves, we see that $y^2 = x^3 + ax$ admits the automorphism $(x : y : z) \mapsto (-x : iy : z)$ of order 4.

Also, $y^2 = x^3 + b$ has the automorphism $(x : y : z) \mapsto (e^{2\pi i/3} : y : z)$.

Elliptic curves with endomorphisms other than multiplication by $n \in \mathbb{Z}$ are said to have complex multiplication, called such because the corresponding endomorphism of a torus is multiplication by a non-real complex number.