Topics in Algebraic Geometry,
spring 2016

Elliptic curves over $\mathbb{C}$ with CM

Author:
J.E.F. Rood

February 24, 2016

The talk of today has two goals: Finding elliptic curves with CM by a certain ring R; Finding an example such that $H_1(E/\mathbb{C}, \mathbb{Z})$ is can not be algebraically defined.

1 Elliptic curves

Definition. An *elliptic curve* (E, O) is an projective smooth curve E of genus 1 with a distinguished point $O \in E$. We often denote an elliptic curve only by E. We say that E is an elliptic curve over a field K is it as a curve is defined over K and $O \in E(K)$.

For this talk we are only interested in elliptic curves E over $\mathbb{C}$ and so if not specified we assume it is. Then we define some quantities for $a_1, a_3, a_2, a_4, a_6 \in K$.

$$\begin{aligned}
b_2 &= a_1^2 + 4a_4, \\
b_4 &= 2a_4 + a_1 a_3, \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 a_4^2, \\
c_4 &= b_2^2 - 24 b_4, \\
c_6 &= -b_2^3 + 36 b_2 b_4 - 216 b_6, \\
\Delta &= -b_2^2 b_8 - 8b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6, \\
j &= \frac{c_4^3}{\Delta}
\end{aligned}$$

Definition. The quantity Δ we call as the *discriminant* and the quantity j we call the *j-invariant*.

If E is an elliptic curve over K, then by theorem 3.1 of [Sil86] there are $a_1, a_3, a_2, a_4, a_6 \in K$ with non-zero discriminant such that E is given by the equation:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

I.1 **Definition.** An *morphism* φ of two elliptic curves E_1, E_2 over K is an morphism of curves such that $\varphi(O_1) = O_2$. An *ismorphism* of curves is an isomorphism of curves such that $\varphi(O_1) = O_2$.

I.2 **Theorem.** *Let E_1, E_2 be two elliptic curves with respectively j-invariant j_1, j_2. Then we have that $E_1(\bar{K})$ and $E_2(\bar{K})$ are isomorphic if and only if $j_1 = j_2$. Furthermore if $j_0 \in \bar{K}$ the there is an elliptic curve E_0 defined over $K(j_0)$ with j-invariant j_0.*

Proof. Proposition III.1.4. of [Sil86]. □

Remark. An morphism $\varphi : E_1 \to E_2$ is either surjective ($\phi(E_1) = E_2$) and finite or constant ($\phi(E_1) = O_2$).

Definition. The degree of the constant morphism we set as 0. The degree of an non constant morphism $\varphi : E_1 \to E_2$ is the degree $[\bar{K}(E_1) : \varphi^*\bar{K}(E_2)]$ of the field extension of the function fields. Let respectively $\deg_s(\varphi)$, $\deg_i(\varphi)$ be the separable degree or the inseparable degree of this extension.

Remark.

- Let $\varphi_1 : E_1 \to E_2, \varphi_2 : E_2 \to E_3$ be morphisms, then:
$$\deg(\varphi_1) \cdot \deg(\varphi_2) = \deg(\varphi_1 \circ \varphi_2)$$
- Let $\varphi : E_1 \to E_2$ an morphism, then for all $Q \in E_2$ we have
$$\deg_s(\varphi) = \varphi^{-1}(Q).$$
Furthermore for all $P \in E_1$ holds
$$\deg_i(\varphi) = e_\varphi(P).$$
- **I.3** Let $\varphi, \psi : E_1 \to E_2$ morphisms, then $(\varphi + \psi)(Q) = \varphi(Q) + \psi(Q)$ for $Q \in E_1$ defines addition law on the set $\mathrm{Hom}(E_1, E_2)$ of morphisms. If we take $E_1 = E_2$ we can even define a mulitplication law $(\varphi\psi)(Q) = (\varphi(\psi(Q))$ on $\mathrm{Hom}(E, E) = \mathrm{End}(E)$. We set $Aut(E) = \{\sigma \in \mathrm{End}(E) | \deg \sigma = 1\}$.
- Let $n \in \mathbb{Z}$ then the multiplication-by-n map $[n] : E \to E$ is an morphism of degree n^2.

I.4 **Definition.** Let E be an elliptic curve over $\mathbb{C}$, then we say that E has *complex multiplication* iff there is an $\sigma \in \mathrm{End}(E)$ such that σ is not the multiplication-by-n morphism for all $n \in \mathbb{Z}$. In other words, $\mathrm{End}(E) \ncong \mathbb{Z}$.

I.5 *Example.* Let $E/\mathbb{C}$ given by the relation
$$y^2 = x^3 - x.$$
Now the map $[i] : E \to E, (x : y : z) \mapsto (-x : iy : z)$ is well defined, rational in the coordinates and sends O to O, thus an morphism. Note that $[i] \circ [i] = [-1]$ and thus $[i] \neq [n]$ for $n \in \mathbb{Z}$. So we have that $\mathbb{Z}[i] \subset \mathrm{End}(E)$, but this turns out to be the complete endomorphism ring.

I.6 **Theorem.** *The endomorphism ring* $\mathrm{End}(E)$ *is either isomorphic to* $\mathbb{Z}$ *or is an order* R *in an imaginary quadratic extension of* $\mathbb{Q}$*. In the latter case we say that* E has CM by R.

Proof. See Theorem VI.5.5 of [Sil86]. □

2 Lattices

II.1 **Definition.** An subset Λ of $\mathbb{C}$ is a *lattice in* $\mathbb{C}$ if there are $w_1, w_2 \in \mathbb{C}^*$, such that $w_1/w_2 \notin \mathbb{R}$ and $\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$.

We look at two families of series given a lattice Λ, first the *weierstrass* $\wp$*-function* and it's derivative:

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{w\in\Lambda, w\neq 0} \frac{1}{(z-w)^2} - \frac{1}{w^2}$$
$$\wp'(z) = -2\sum_{w\in\Lambda} \frac{1}{(z-w)^3}.$$

and secondly the eisenstein series of weight $2n$:

$$G_{2n}(\Lambda) = \sum_{w\in\Lambda, w\neq 0} w^{-n}$$

These functions will help us demonstrate the correspondences between elliptic curves and lattices.

Theorem (Uniformization Theorem)**.** *Set* $g_2 = 60G_4(\Lambda)$ *and* $g_3 = 140G_6(\Lambda)$. *For* $z \in \mathbb{C}/\Lambda$ *the* weierstrass $\wp$-function *and it's derivative satisfy the relation*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

II.3 *and the discriminant* $\Delta(\Lambda) = g_2^3 - 27g_3^2$ *doesn't vanish. Now we can define* $E/\mathbb{C}$ *to be an elliptic curve with* j*-invariant* $1728\frac{g_2^3}{\Delta}$*, like the one given by the polynomial*

$$Y^2 = 4X^3 - g_2X - g_3.$$

Furthermore the map

$$G : \mathbb{C}/\Lambda \to E(\mathbb{C}), z \mapsto [\wp(z), \wp'(z), 1]$$

is an isomorphism of Riemann surfaces that is also a group homomorphism.

Proof. See Theorem 2.4 and 2.5 in [Ste91] or see Theorem 3.8 [Rho07]. □

II.3 **Theorem.** *Let* $E/\mathbb{C}$ *be an elliptic curve over* $\mathbb{C}$. *Then* $H_1(E,\mathbb{Z})$ *is isomorphic to a lattice* Λ *in* $\mathbb{C}$. *We have that there is an complex analytic map of lie groups, that is the inverse to the map given in 2 and is given by*

$$F : E(\mathbb{C}) \to \mathbb{C}/\Lambda, P \mapsto \int_O^P \frac{dx}{y} \pmod{\Lambda}$$

Proof. See Proposition VI.5.2 and VI.5.6 of [Sil86]. □

II.4 **Theorem.** *Let E_1, E_2 elliptic curves, with corresponding lattices Λ_1, Λ_2. There is an morphism $\phi : E_1 \to E_2$ if and only if there is an $\alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_1 \subset \Lambda_2$. Likewise, is there an isomorphism $\phi : E_1 \to E_2$ if and only if there is an $\alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_1 = \Lambda_2$.*

Proof. See Corollary VI.4.1.1 of [Sil86]. □

II.4 **Theorem.** *There is an equivalence of categories between elliptic curves with morphism and lattices in $\mathbb{C}$ with maps* $\mathrm{Hom}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$.

Proof. See Theorem VI.5.3 of [Sil86]. □

3 CM by ring of integers

Now we have more then enough theory to find an elliptic curve with CM.

Definition. The class group $Cl(R)$ of an ring of integers of an number field is defined as

$$\frac{\{\text{fractional ideal}\}}{\{\text{principal fractional ideals}\}}$$

and denote the number of class in $CL(R)$ as $h(R)$.

III.1 **Lemma.** *Let K be an imaginary quadratic extension of $\mathbb{Q}$ and $\mathcal{O}_K$ its ring of integers (i.e. maximal order). Then every ideal of $\mathcal{O}_K$ is a lattice in $\mathbb{C}$ and thus correspond to an elliptic curve. Moreover ideals corresponds to isomorphic elliptic curves if and only if the ideals are in same equivalence class in the class group.*

Exercise. Prove this lemma.

The second goal was to find elliptic curves that demonstrate that $H_1(E, \mathbb{Z})$ can not be algebraically defined

III.2 **Corollary.** *The class number $h(\mathcal{O}_K)$ of $\mathcal{O}_K$ is also the number of isomorphism classed of elliptic curves with CM by $\mathcal{O}_K$.*

III.3 **Theorem.** *The If Λ is an fractional ideal in $\mathcal{O}_K$, then:*

1 $j(\Lambda) \in \bar{\mathbb{Q}}$ *and* $[\mathbb{Q}(j)(\Lambda) : \mathbb{Q}] = [K(j(\Lambda)) : K]$.

2 $K(j(\Lambda))$ *is the maximal unramified abelian extension of K.*

3 *If $[\Lambda_1], ..., [\Lambda_{h(\mathcal{O}_K)}]$ are the different classes of $Cl(\mathcal{O}_K)$ then $j(\Lambda_1), ..., j(\Lambda_{h(\mathcal{O}_K)})$ are the* $\mathrm{Gal}(\bar{K}/K)$ *conjugates of the class of* $[\Lambda]$.

Proof. See Theorem 11.2 in Appendix C of Silverman. □

III.4 So if we take $R = \mathbb{Z}[\sqrt{-5}]$, the ring of integers of $\mathbb{Q}(\sqrt{-5}]$ with $h(R) = 2$. Then (1) and $(2, \sqrt{-5}+1)$ are representatives of the two classes in the class group of R. We will work with the lattices $\Lambda_1 = \mathbb{Z} + \sqrt{-5}\mathbb{Z} = (1)$ and $\Lambda_2 = \mathbb{Z} + \frac{1+\sqrt{-5}}{2}\mathbb{Z} = \frac{1}{2}(2, \sqrt{-5}+1)$. To find the j-invariant we will use
II.2 q-expansion of the the eisenstein series for lattices of the form $\mathbb{Z} + \tau\mathbb{Z}$:

$$G_{2n}(\tau) = 2\zeta(2n) + 2\frac{(2\pi i)^{2n}}{(2n-1)!}\sum_{k=1}^{\infty}\frac{k^{2n-1}q^k}{1-q^k},$$

where $q = e^{2\pi i\tau}$ and ζ is the riemann zeta finction. I used Sage to find an approximation of the g_2 and g_3 for both lattices and the curve itself.

$$E_1 : y^2 = x^3 + ax + b$$
$$E_2 : y^2 = x^3 + \sigma(a)x + \sigma(b)$$

with $a = -1071214510080\sqrt{5} - 2395312128000$ and $b = -901828270977187840\sqrt{5} - 2016549312397312000$ and σ an automorphism of $\mathbb{C}$ such that $\sigma(\sqrt{5}) = -\sqrt{5}$ and $\sigma(\sqrt{-5}) = \sqrt{-5}$.

Now we can define an isomorphism $\bar{\sigma} : \mathbb{C}[x, y]/(-y^2 + x^3 + ax + b) \to \mathbb{C}[x, y]/(-y^2 + x^3 + \sigma(a)x + \sigma(b))$ where on $\mathbb{C}$ we apply the automorphism σ, $x \mapsto x$ and $y \mapsto y$.

VI.1 Now $H_1(E_1, \mathbb{Z})$ can't algebraically be defined, since then there would be an induced isomorphism of $H_1(E_1, \mathbb{Z})$ as module over $\mathrm{End}(E_1)$ to $H_1(E_2, \mathbb{Z})$ as module over $\mathrm{End}(E_2)$, but recall $\mathrm{End}(E_1) \cong \mathbb{Z}[\sqrt{-5}] \cong \mathrm{End}(E_2)$, that $\sigma_{|\,\mathrm{End}(E_1)} = \mathrm{Id}_{\mathbb{Z}[\sqrt{-5}]}$ and that $H_1(E_1, \mathbb{Z}) \cong \Lambda_1$ is free over $\mathbb{Z}[\sqrt{-5}]$ but $H_1(E_2, \mathbb{Z}) \cong \Lambda_1$ is not.

Exercise. Find an elliptic curve that doesn't have CM.

Exercise. Find the elliptic curve E with CM by a maximal order, such that $\#\,\mathrm{Aut}(E) = 6$, are there any such elliptic curves with $\#\,\mathrm{Aut}(E) > 6$

Exercise. There are 13 elliptic curves defined over $\mathbb{Q}$ with CM, find 9 of them.

References

[Rho07] R.C. Rhoades. Classifying elliptic curves. 2007.

[Sil86] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986.

[Ste91] P. Stevenhagen. *Elliptic Functions*. UvA, 1991.