AWS 2021: Modular Groups
Problem Set 3

Lecturer: Lori Watson

Written by: Tyler Genao, Hyun Jong Kim, Zonia Menendez and Sam Mundy (Assistants)

Last updated: February 6, 2021

1 Definitions and Notations

1. A *lattice* in $\mathbb{C}$ is a rank two $\mathbb{Z}$-submodule of $\mathbb{C}$ whose $\mathbb{R}$-span is $\mathbb{C}$. Less formally, it is a subgroup $\Lambda \subseteq (\mathbb{C}, +)$ generated by two $\mathbb{R}$-linearly independent complex numbers ω_1, ω_2. When we have a basis in mind, we usually write Λ as $[\omega_1, \omega_2] := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

2. One says that two lattices $\Lambda_1, \Lambda_2 \subseteq \mathbb{C}$ are *homothetic* if for some $\lambda \in \mathbb{C}^\times$ one has
$$\Lambda_2 = \lambda\Lambda_1.$$

3. Given two complex elliptic curves, i.e., two complex tori $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$, we say that a map
$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$
is *holomorphic* if there is a holomorphic map $f : \mathbb{C} \to \mathbb{C}$ and a commutative diagram
$$\begin{tikzcd} \mathbb{C} \arrow[r, "f"] \arrow[d] & \mathbb{C} \arrow[d] \\ \mathbb{C}/\Lambda_1 \arrow[r, "\phi"] & \mathbb{C}/\Lambda_2. \end{tikzcd}$$
Let us require that our lifts also satisfy $f(0) = 0$.

4. An *isogeny* between two complex elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ is a holomorphic map
$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$
such that $\phi(0) = 0$.

5. The *degree* of an isogeny $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is defined as the size of its kernel. If $\phi \neq 0$, then $\deg(\phi) > 0$; let us set $\deg(0) := 0$.

Alex Barrios's notes contain an introduction to holomorphic (also called analytic) functions. You can find a link to them on the AWS website.

2 Introductory Problems

Problem 1 (Lattices, I)**.** The following two exercises are meant to get you acquainted with the basics of lattices. As shown in the lectures, there are important connections between lattices and elliptic curves over $\mathbb{C}$: such an elliptic curve "is" a complex torus $\mathbb{C}/\Lambda$, and vice-versa.

a. (See Problem 6.1 on Problem Set 1) Show that for $z \in \mathbb{C}$ and $\gamma := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$, one has imaginary part

$$\mathrm{Im}(\gamma \cdot z) = \frac{\det(\gamma)\mathrm{Im}(z)}{|cz+d|^2}.$$

b. We say that a lattice $[\omega_1, \omega_2] \subseteq \mathbb{C}$ is *oriented* if $\omega_1/\omega_2 \in \mathbb{H}$. Using part a., show that two oriented lattices $[\omega_1, \omega_2]$ and $[\omega_1', \omega_2']$ are equal if and only if there exists a matrix $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that both

$$\omega_1' = a\omega_1 + b\omega_2$$

and

$$\omega_2' = c\omega_1 + d\omega_2.$$

Therefore, $\mathrm{SL}_2(\mathbb{Z})$ is the group of oriented basis changes of $[\omega_1, \omega_2]$.

Problem 2 (Lattices, II)**.**

a. Show that homothety of lattices is an equivalence relation.

b. Show that any lattice $\Lambda \subseteq \mathbb{C}$ is "orientable": Λ is homothetic to some lattice $[1, \tau]$ where $\tau \in \mathbb{H}$.

c. Given two lattices $\Lambda_1, \Lambda_2 \subseteq \mathbb{C}$ with $\lambda \in \mathbb{C}^\times$ such that

$$\lambda\Lambda_1 \subseteq \Lambda_2,$$

show that we have a group homomorphism of complex elliptic curves

$$\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

via multiplication by λ.

d. Show that two homothetic lattices $\Lambda_1, \Lambda_2 \subseteq \mathbb{C}$ induce canonically isomorphic complex elliptic curves,

$$(\mathbb{C}/\Lambda_1, +) \cong (\mathbb{C}/\Lambda_2, +).$$

Problem 3.

a. Given a lattice $\Lambda \subseteq \mathbb{C}$, what is the group structure of the N-torsion subgroup of $\mathbb{C}/\Lambda$? Recall that the N-torsion subgroup of an abelian group M is the subgroup $\{m \in M : Nm = 0\}$.

b. Note that each torus $\mathbb{C}/\Lambda$ has a multiplication-by-N isogeny $[N] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ (more specifically, $[N]$ is an endomorphism, see Problem 11). What is $\deg[N]$?

Problem 4. As noted in the lectures, for a lattice $\Lambda \subseteq \mathbb{C}$ one can define an elliptic curve over $\mathbb{C}$ via the cubic equation

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

where $g_2(\Lambda) := 60G_4(\Lambda) \in \mathbb{C}$ and $g_3(\Lambda) := 140G_6(\Lambda) \in \mathbb{C}$.

a. If Λ is homothetic to the Gaussian integer ring $\mathbb{Z}[i] := [1, i]$, then after a coordinate change $(x, y) \mapsto (x, y/2)$ our equation becomes

$$y^2 = x^3 + Ax$$

for some $A \in \mathbb{C}^\times$.

b. If Λ is homothetic to the cyclotomic integer ring $\mathbb{Z}[\zeta_3] := [1, \zeta_3]$,[1] then after a coordinate change $(x, y) \mapsto (x, y/2)$ our equation becomes

$$y^2 = x^3 + B$$

for some $B \in \mathbb{C}^\times$.

(These are the "first" examples of elliptic curves which have *complex multiplication.*)

Problem 5. For this problem, read Problem 11 first.

There is an elliptic curve E over $\mathbb{C}$ given by the Weierstrass equation $y^2 = x^3 + x$. On E, there is an endomorphism $\phi : E \to E$ given by $(x, y) \mapsto (-x, iy)$. Can you tell what the composition $\phi \circ \phi$ is?

[1]Here, ζ_3 is a primitive cube root of unity, i.e., $\zeta_3^3 = 1$ and $\zeta_3 \neq 1$.

3 Intermediate Problems

Problem 6. Let $N \geq 1$ be an integer. How many points of exact order N are there on a complex elliptic curve?

By Problem 10, every isogeny $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is multiplication by a complex number $\alpha \in \mathbb{C}$ with $\alpha\Lambda_1 \subseteq \Lambda_2$. We assume this result in the following three problems.

Problem 7. Show that the kernel of any nonzero isogeny $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is finite and generated by two elements.

Problem 8 (The dual isogeny)**.** Show that for any isogeny $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$, there is another isogeny $\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_1$ such that $\phi \circ \hat{\phi} = [\deg \phi]$ and that $\hat{\phi} \circ \phi = [\deg \phi]$.

Problem 9.

a. Show that for any two isogenies $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ and $\varphi : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$, their composition $\varphi \circ \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_3$ is an isogeny, and satisfies $\deg(\varphi \circ \phi) = \deg(\varphi)\deg(\phi)$.

b. Using part a., show that the endomorphism ring $\mathrm{End}(\mathbb{C}/\Lambda)$ is an integral domain.

4 Advanced Problems

Problem 10 (Isogenies)**.** This exercise will classify all isogenies between two complex elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$.

a. Show that for a complex number $\alpha \in \mathbb{C}$, if $\alpha\Lambda_1 \subseteq \Lambda_2$ then multiplication by α induces a holomorphic group homomorphism

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

with $\phi_\alpha(0) = 0$. In particular, ϕ_α is an isogeny.

b. Show that two isogenies $\phi_\alpha, \phi_\beta : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ are equal iff $\alpha = \beta$.

c. Recall that an *elliptic function* (relative to a lattice Λ) is a meromorphic function

$$f : \mathbb{C} \to \mathbb{C}$$

which is "Λ-periodic", i.e.,

$$f(z + \omega) = f(z)$$

for all $\omega \in \Lambda$, $z \in \mathbb{C}$. Show that a holomorphic elliptic function is constant. (*Hint:* Liouville's Theorem.)

d. Show that an isogeny $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is equal to some isogeny ϕ_α for some $\alpha \in \mathbb{C}$ – i.e.,

$$\phi(z) = \alpha z$$

for all $z \in \mathbb{C}/\Lambda_1$. (*Hint:* apply part c. to f', where $f : \mathbb{C} \to \mathbb{C}$ is a holomorphic lift of ϕ.)

e. Conclude that there exists a bijection between the set of holomorphic maps

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

with $\phi(0) = 0$, and the set of complex numbers $\alpha \in \mathbb{C}$ with $\alpha\Lambda_1 \subseteq \Lambda_2$.

Problem 11 (Complex Multiplication)**.** This problem assumes some basic algebraic number theory.

By Problem 10, for a lattice $\Lambda \subseteq \mathbb{C}$ we can define the set of isogenies from $\mathbb{C}/\Lambda$ to itself, the *ring of endomorphisms*

$$\mathrm{End}(\mathbb{C}/\Lambda) := \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}.$$

a. Problem 9 shows that $\mathrm{End}(\mathbb{C}/\Lambda)$ is an integral domain. Using that Λ is homothetic to $[1, \tau]$ for some $\tau \in \mathbb{H}$, show that $\mathrm{End}(\mathbb{C}/\Lambda)$ is either $\mathbb{Z}$ or an order in an imaginary quadratic field.[2]

b. We say that a complex elliptic curve $\mathbb{C}/\Lambda$ has *complex multiplication*, or CM, if $\mathrm{End}(\mathbb{C}/\Lambda) \neq \mathbb{Z}$. By part a., a CM complex elliptic curve $\mathbb{C}/\Lambda$ has not just "integer multiplications", but also "complex multiplications".

   i. Show that for any imaginary number $\tau \in \mathbb{C}$ with $\tau[1, \tau] \subseteq [1, \tau]$, one has

$$\mathrm{End}(\mathbb{C}/[1, \tau]) = [1, \tau].$$

   ii. More generally, show that for any imaginary $\tau \in \mathbb{C}$ the complex elliptic curve $\mathbb{C}/[1, \tau]$ has CM iff τ is a quadratic algebraic number.

c. Let $I \neq 0$ be an ideal in the ring of integers $\mathcal{O}_K$ of an imaginary quadratic number field K. Show that $I \subseteq \mathbb{C}$ is a lattice, and that the complex elliptic curve $\mathbb{C}/I$ has complex multiplication by $\mathcal{O}_K$.

d. For an imaginary quadratic number field K, show there exists a bijection between the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ of K and the set of homothety classes of lattices $\Lambda \subseteq \mathbb{C}$ for which $\mathrm{End}(\mathbb{C}/\Lambda) = \mathcal{O}_K$.

e. Up to isomorphism, how many complex elliptic curves $\mathbb{C}/\Lambda$ are there with $\mathrm{End}(\mathbb{C}/\Lambda) = \mathbb{Z}[i]$?

f. Give two non-isomorphic complex elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ with CM by $\mathbb{Z}[\sqrt{-5}]$.

Problem 12. This problem assumes some topology.

Let $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ be a map between two complex tori. Show that ϕ is holomorphic, in the sense given in the section in this problem set on definitions, if and only if the following condition holds: First, let π_1 and π_2 be the natural projection maps $\mathbb{C} \to \mathbb{C}/\Lambda_1$ and $\mathbb{C} \to \mathbb{C}/\Lambda_2$, respectively. Then for any open subsets $U_1 \subset \mathbb{C}$ and $U_2 \subset \mathbb{C}$ such that $\pi_i(U_i)$ is in bijection with its image in $\mathbb{C}/\Lambda_i$ for $i = 1, 2$, and such that $\phi(\pi_1(U_1)) \subset \pi_2(U_2)$, the function $(\pi_2|_{U_2})^{-1} \circ \phi \circ \pi_1 : U_1 \to U_2$ is holomorphic. [*Hint:* What are the universal covers of these complex tori?]

[2] An *order* $\mathcal{O}$ in a number field K is a subring of $\mathcal{O}_K$, and a $\mathbb{Z}$-submodule of rank $[K : \mathbb{Q}]$. The rank condition implies the index $[\mathcal{O}_K : \mathcal{O}] < \infty$.