Elliptic Curves

JWR

Friday November 30, 2001,7:40 AM

This is an account of the talk of Cheol-Hyun Cho. The aim is to construct a "universal elliptic curve". Tong Hai Yang helped me with this - he told me about [1].

1 Discrete Groups

A good reference for the material in this section is [3].

1. Throughout $\mathbb{P} = \mathbb{C} \cup \{\infty\}$ denotes the Riemann sphere, $\mathbb{H}$ denotes the upper half plane, $\mathbb{C}^*$ denotes the multiplicative group of complex numbers, and $\mathbb{P}^n = (\mathbb{C}^{n+1} \setminus \{0\})/\mathbb{C}^*$ denotes n dimensional complex projective space. For $w \in \mathbb{C}^{n+1} \setminus \{0\}$ let $[w] := w\mathbb{C}^*$ denote the corresponding point of $\mathbb{P}^n$. For $A \in \mathrm{GL}_{n+1}(\mathbb{C})$ let M_A denote the corresponding automorphism of projective space so that

$$M_A([w]) = [Aw].$$

Identify $\mathbb{P}^1$ and $\mathbb{P}$ via $z = [z, 1]$ and $\infty = [1, 0]$ so that

$$M_A(z) = \frac{az+b}{cz+d}, \qquad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for $A \in \mathrm{GL}_2(\mathbb{C})$. A transformation of form M_A is called a **Möbius transformation**.

2. A matrix $A \in \mathrm{SL}_2(\mathbb{R}) \setminus \{\pm I_2\}$ is called **hyperbolic** iff its eigenvalues are real and distinct, **elliptic** iff its eigenvalues are distinct and not real (and therefore complex conjugate), and **parabolic** otherwise. It is easy to see that a nontrivial Möbius transformation has either exactly one or exactly two fixed points; Hence a matrix $A \in \mathrm{SL}_2(\mathbb{R}) \setminus \{\pm I_2\}$ is hyperbolic if and only if the corresponding automorphism M_A of $\mathbb{P}$ has two fixed points in $\mathbb{R}$, elliptic if and only if M_A has two fixed points one in $\mathbb{H}$ and the other in $-\mathbb{H}$, and parabolic if and only if it has exactly one fixed point. The fixed point of a parabolic element lies in $\mathbb{R} \cup \{\infty\}$.

3. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be a subgroup. A point $z \in \mathbb{H}$ is called a **regular point** of Γ iff the isotropy group Γ_z is essentially trivial, i.e. $\Gamma_z = \Gamma \cap \{\pm I_2\}$. A point $z \in \mathbb{H}$ is called an **elliptic point** of Γ iff it is a fixed point of M_A some elliptic element $A \in \Gamma$. A point $z \in \mathbb{R} \cup \{\infty\}$ is called an **cusp** of Γ iff it is a fixed point of M_A for some parabolic element $A \in \Gamma$. Denote by

$$X(\Gamma) := \{\Gamma(z) : z \in \mathbb{H} \cup \mathrm{Cusp}(\Gamma)\}, \qquad \Gamma(z) := \{M_A(z) : A \in \Gamma\}$$

the orbit space of Γ acting on the union of $\mathbb{H}$ with the set of cusps of Γ. For $z \in \mathbb{H} \cup \mathrm{Cusp}(\Gamma)$ let

$$\Gamma_z := \{A \in \Gamma : M_A(z) = z\}$$

denote the stabilizer group of z. Points on the same orbit have conjugate (in Γ) stabilizer groups so orbits of Γ in $\mathbb{H} \cup \mathrm{Cusp}(\Gamma)$ may be classified as regular, elliptic, or cusp. It is easy to see that the stabilizer group

$$\mathrm{SL}_2(\mathbb{R})_\infty := \{A \in \mathrm{SL}_2(\mathbb{R}) : M_A(\infty) = \infty\}$$

is the set of all real matrices A of form $A = \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ where $h \in \mathbb{R}$.

Lemma 4. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be a discrete group. Then*

(i) *Let $z_0 \in \mathbb{H}$ be an elliptic point of Γ. Then there is an element $C \in \mathrm{SL}_2(\mathbb{C})$ with $M_C(z_0) = 0$ and $M_C \circ \Gamma_z \circ M_C^{-1}$ a finite cyclic subgroup of the stabilizer subgroup $\mathbb{C}^* \cdot I_2$ of the origin in $\mathrm{GL}_2(\mathbb{C})$.*

(ii) *Let $x_0 \in \mathbb{R} \cup \{\infty\}$ is a cusp of Γ. Then is an element $C \in \mathrm{SL}_2(\mathbb{R})$ with $M_C(x_0) = \infty$ and $M_C \circ \Gamma_z \circ M_C^{-1}$ an infinite cyclic subgroup of $\mathrm{SL}_2(\mathbb{R})_\infty$.*

5. Introduce a topology in $\mathbb{H} \cup \mathrm{Cusp}(\Gamma)$ by taking as a basis for the open sets the open sets of $\mathbb{H}$ together with all sets $D \cup \{z_0\}$ where $z_0 \in \mathrm{Cusp}(\Gamma)$ and D is an open disk in $\mathbb{H}$ whose boundary is tangent to the $\mathbb{R} \cup \{\infty\}$ at z_0. (In case $z_0 = \infty$ this means a set of form $\Im(z) > c$.) Since Möbius transformations map circles to circles it follows that for every $A \in \Gamma$ the map $M_A : \mathbb{H} \cup \mathrm{Cusp}(\Gamma) \to \mathbb{H} \cup \mathrm{Cusp}(\Gamma)$ is a homeomorphism of in this topology.

Lemma 6. *For every point $z \in \mathbb{H} \cup \mathrm{Cusp}(\Gamma)$ there is an open neighborhood U of z such that for $A \in \Gamma$ we have*

$$A \in \Gamma_z \iff M_A(U) \cap U \neq \emptyset.$$

Such an open set U is called an **open slice** *centered at z.*

Lemma 7. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be a discrete group and $z_0 \in \mathbb{H} \cup \mathrm{Cusp}(\Gamma)$. Then there is a continuous function $\zeta : U \to \mathbb{C}$ defined in an open slice centered at z_0 which is holomorphic on $U \setminus \{z_0\}$ and such that for $z, z' \in U$ we have*

$$\zeta(z') = \zeta(z) \iff z' \in \Gamma(z).$$

(In case $z_0 \in \mathbb{H}$ the function ζ is holomorphic on U since the singularity is removable.)

8. A function ζ : U $\to \mathbb{C}$ as in Corollary 7 is called a **local holomorphic invariant** for Γ at z_0. The injective map from $U(\Gamma) := \{\Gamma(z) : z \in U\}$ to $\mathbb{C}$ induced by ζ is called a **holomorphic coordinate** for $X(\Gamma)$ at $\Gamma(z_0)$.

Theorem 9. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be a discrete group. Then the various holomorphic coordinates for $X(\Gamma)$ form an atlas. This atlas equips $X(\Gamma)$ with the structure of a (Hausdorff) orbifold Riemann surface.*

Example 10. By the Uniformization Theorem a compact Riemann surface of genus greater than one is isomorphic to some $X(\Gamma)$ where every element of Γ is hyperbolic.

Example 11. Let Γ be the cyclic subgroup of $\mathrm{SL}_2(\mathbb{R})$ generated by $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ where $h \neq 0$. Then every point of $\mathbb{H}$ is regular, $\mathrm{Cusp}(\Gamma) = \{\infty\}$, and $\zeta(z) = e^{2\pi i z/h}$ is a local holomorphic invariant for Γ. The holomorphic coordinate induced by ζ on $X(\Gamma)$ maps $X(\Gamma)$ isomorphically to the unit disk.

Remark 12. If Γ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ so is the group Γ' generated by Γ and $\pm I_2$. Since as $-I_2$ acts trivially, the group Γ' has the same orbits as Γ so $X(\Gamma') = X(\Gamma)$. In particular, any discrete subgroup of $\mathrm{SL}_2(\mathbb{R})_\infty$ has an orbit space identical to an $X(\Gamma)$ as in Example 11.

Example 13. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Then $\mathrm{Cusp}(\Gamma) = \Gamma(\infty) = \mathbb{Q} \cup \{\infty\}$. There are two elliptic orbits $\Gamma(i)$ and $\Gamma(e^{\pi i/3})$. The stabilizer subgroups at ∞, i, and $e^{\pi i/3}$ are generated by

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad AB = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

respectively. The element A has infinite order, the element B has order four, and the element AB has order six. The transformation M_A has infinite order, the transformation M_B has order two, and the transformation M_{AB} has order three. The function $z \mapsto e^{2\pi i z}$ is a local invariant at ∞, the function $z \mapsto ((z-i)/(z+i))^2$ is a local invariant at i, and the function $z \mapsto ((z - e^{\pi i/3})/(z - e^{-\pi i/3}))^3$ is a local invariant at $e^{\pi i/3}$. In Theorem 33 below construct an isomorphism from $X(\Gamma)$ to projective space $\mathbb{P}$; more precisely, to weighted projective space $\mathbb{P}(2, 4)$.

2 Lattices

14. A **lattice** is a subgroup of the additive group of $\mathbb{C}$ of form

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

where $\omega_1, \omega_2 \in \mathbb{C}$ are independent over $\mathbb{R}$, i.e. one of ω_1/ω_2 and ω_2/ω_1 lies in the upper half plane $\mathbb{H}$ and the other in the lower half plane. Choose the indexing so $\tau := \omega_1/\omega_2 \in \mathbb{H}$. Then the automorphism $z \mapsto z/omega_1$ of $\mathbb{C}$ carries the lattice Λ to a lattice

$$\Lambda_\tau := \mathbb{Z} + \mathbb{Z}\tau$$

where $\tau \in \mathbb{H}$.

Lemma 15. *For $\tau, \tau' \in \mathbb{H}$ the following are equivalent:*

(i) *there exists $A \in \mathrm{SL}_2(\mathbb{Z})$ with $\tau' = M_A(\tau)$;*

(ii) *there is an automorphism $z \mapsto \alpha z + \beta$ of $\mathbb{C}$ with $\Lambda_\tau = \alpha\Lambda_{\tau'} + \beta$;*

Proof. Assume (i). Then

$$\mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) \subset \mathbb{Z} + \mathbb{Z}\tau = \Lambda_\tau.$$

The automorphism $z \mapsto z/(c\tau+d)$ sends this $a\tau+b$ to 1 and 1 to τ' and hence Λ_τ to $\Lambda_{\tau'}$. Since $ad-bc=1$ interchanging τ and τ' constructs the inverse homomorphism. Conversely assume (ii). Since $0 \in \Lambda_\tau$ we have $\beta \in \Lambda_{\tau'}$ so $\Lambda_\tau = \alpha\Lambda_{\tau'}$ so $\alpha\tau'$ and α generates Λ_τ. Hence there exist integers a, b, c, d with $ad - bc = \pm 1$, $\alpha\tau' = a\tau + b$, $\alpha = c\tau + d$ and hence $\tau' = (\alpha\tau')/\alpha = M_A(\tau')$. Since $\tau, \tau' \in \mathbb{H}$ we have $ad - bc = 1$ (and not -1). □

16. Warning: Lemma 15 says when the lattices are isomorphic, not when they are identical. The condition that $\tau' \in \Lambda_\tau$ implies that τ satisfies a quadratic equation with integer coefficients. There are only countably many such equations so for most τ we have $\Lambda_{\tau'} \neq \Lambda_\tau$ for *all* $A \in \mathrm{SL}_2(\mathbb{Z}) \setminus \{\pm I\}$. It is not hard to see when $\Lambda_{\tau'} = \Lambda_\tau$. Two lattices $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and $\Lambda' = \mathbb{Z}\omega'_1 + \mathbb{Z}\omega'_2$ are equal if and only if there are integers $a, b, c, d \in \mathbb{Z}$ with $ad - bc = \pm 1$ and $\omega'_1 = a\omega_1 + b\omega_2$, $\omega'_2 = c\omega_1 + d\omega_2$. Taking the cross product gives $\omega'_1 \times \omega'_2 = \pm\omega_1 \times \omega_2$, i.e. the vectors ω_1 and ω_2 determine a parallelogram with the same area as the one determined by ω'_1 and ω'_2. Hence $\Lambda_\tau = \Lambda_{\tau'}$ implies that $\Im(\tau) = \Im(\tau')$. Now $\Lambda_\tau = \Lambda_{\tau'} \implies \Lambda_{M_B(\tau)} = \Lambda_{M_{B(\tau')}}$ for $B \in \mathrm{SL}_2(\mathbb{Z})$ and $\Lambda_\tau = \Lambda_{t+1}$ so assume that τ lies in the fundamental region $-\frac{1}{2} < \Re(\tau) \leq \frac{1}{2}$ and $|\tau| \geq 1$ (see [3] page 16) and that $-\frac{1}{2} < \Re(\tau') \leq \frac{1}{2}$. Since $\Im(\tau) = \Im(\tau')$ it follows that $\tau = \tau'$ and hence that τ is an elliptic fixed point of A. The possibilities are $\tau = i$, $M_A =$ a power of $z \mapsto iz$ and $\tau = e^{\pi/6}$, $M_A =$ a power of $z \mapsto 1 - 1/z$. This discussion has the following

Corollary 17. *The lattice Λ_τ admits a nontrivial automorphism (i.e. one different from the two automorphisms $z \mapsto \pm z$) if and only if τ lies on one of the two elliptic orbits of* $\mathrm{SL}_2(\mathbb{Z})$.

3 Elliptic Curves

Theorem 18. *Let X be an* **elliptic curve**, *i.e. a compact Riemann surface of genus one. Then X is isomorphic to $\mathbb{C}/\Lambda_\tau$ for some $\tau \in \mathbb{H}$. For $\tau, \tau' \in \mathbb{H}$, the elliptic curves $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_{\tau'}$ are isomorphic if and only if τ and τ' lie in the same* $\mathrm{SL}_2(\mathbb{Z})$ *orbit.*

Proof. We first show that the universal cover of X is $\mathbb{C}$ and not the upper half plane $\mathbb{H}$. The group of holomorphic automorphisms of $\mathbb{H}$ is the same as the group of isometries of $\mathbb{H}$ so if $\mathbb{H}$ were the universal cover the group of deck transformations would act by isometries and there would be a metric of negative curvature on X. By the Gauss Bonnett theorem, the Euler characteristic of X would be negative contradicting the hypothesis that X has genus one. Hence $X = \mathbb{C}/\Gamma$ where Γ is the group of deck transformations of the universal cover $\mathbb{C} \to X$. Every automorphism of $\mathbb{C}$ has the form $t \mapsto at+b$; every element of the subgroup Λ is fixed point free and so has the form $t \mapsto t+b$. Thus the orbit Λ of 0 under Γ is a subgroup of the additive group of $\mathbb{C}$ and so $X = \mathbb{C}/\Lambda$. We must show that Λ has the desired form. By composing with a rotation we may assume w.l.o.g. that $\Lambda \cap \mathbb{R} \neq \{0\}$. Since Λ is discrete, $\Lambda \cap \mathbb{R}$ must contain a smallest positive element so by rescaling we may assume w.l.o.g. that $\Lambda \cap \mathbb{R} = \mathbb{Z}$. We cannot have $\Lambda = \mathbb{Z}$, else $X = \mathbb{C}/\Lambda$ would be noncompact. Hence Λ contains elements of the upper half plane. As Λ is discrete, and as any element of $\Lambda \cap \mathbb{H}$ can be moved to the strip $\Im(\tau) > 0$, $-1/2 \leq \Re(\tau) < 1/2$ by translation by an element in $\mathbb{Z} \subset \Lambda$ there must be such a $\tau \in \Lambda \cap \mathbb{H}$ with $\Im(\tau)$ smallest. The parallelogram P with vertices $0, 1, \tau, 1+\tau$ is a fundamental domain for the lattice $\Lambda_\tau \subset \Lambda$, so for any $t \in \mathbb{C}$ there is an element $\omega \in \Lambda_\tau$ with $t + \omega \in P$. In particular this is so for $t \in \Lambda$. By construction $t + \omega$ cannot lie in the interior of P or in the interior of an edge of P. Hence $t+\omega$ is a vertex of P so $t \in \Lambda_\tau$. Thus $\Lambda = \Lambda_\tau$ as required.

Any isomorphism $\mathbb{C}/\Lambda_\tau \to \mathbb{C}/\Lambda_{\tau'}$ lifts to an automorphism of $\mathbb{C}$ which carries Λ_τ to $\Lambda_{\tau'}$. Hence, by Lemma 15, $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_{\tau'}$ are isomorphic if and only if there are integers a, b, c, d with $\tau' = (a\tau + b)/(c\tau + d)$ and $ad - bc = 1$. □

19. Define an action of $\mathbb{Z}^2$ on $\mathbb{H} \times \mathbb{C}$ by

$$T_{(m,n)}(\tau, t) = (\tau, t + m\tau + n)$$

for $(m, n) \in \mathbb{Z}^2$. This action maps each fiber of the projection $\mathbb{H} \times \mathbb{C} \to \mathbb{H}$ to itself. Introduce the space

$$W := (\mathbb{H} \times \mathbb{C})/\mathbb{Z}^2$$

and the projection $W \to \mathbb{H} : (\tau, t + \Lambda_\tau) \mapsto \tau$. The fiber over τ of this projection is the corresponding elliptic curve

$$W_\tau = \mathbb{C}/\Lambda_\tau.$$

20. Define an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H} \times \mathbb{C}$ by by

$$\Phi_A(\tau, t) = \left(\frac{a\tau + b}{c\tau + d}, \frac{t}{c\tau + d} \right), \qquad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Then the diagram

$$\begin{array}{ccc} \mathbb{H}\times\mathbb{C} & \xrightarrow{\Phi_A} & \mathbb{H}\times\mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{H} & \xrightarrow{M_A} & \mathbb{H} \end{array}$$

commutes (the vertical arrows are projection on the first factor). Note that the action $A \mapsto \Phi_A$ (unlike the action $A \mapsto M_A$) is effective:

$$\Phi_{-I}(\tau, t) = (\tau, -t).$$

Lemma 21. *For $A \in \mathrm{SL}_2(\mathbb{Z})$ and $(m,n) \in \mathbb{Z}^2$ we have*

$$\Phi_A \circ T_{(m,n)} = T_{\mu(m,n,A)} \circ \Phi_A$$

where $\mu(m,n,A) \in \mathbb{Z}^2$ is given by

$$\mu(m,n,A) = (m,n)A^{-1} = (dm - bn, -cm + an).$$

Corollary 22. *The action $A \mapsto \Phi_A$ of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}\times\mathbb{C}$ induces an action (denoted by the same symbol) of $\mathrm{SL}_2(\mathbb{Z})$ on W; the projection $W \to \mathbb{H}$ is equivariant. In other words, the diagram*

$$\begin{array}{ccc} \mathbb{H}\times\mathbb{C} & \xrightarrow{\Phi_A} & \mathbb{H}\times\mathbb{C} \\ \downarrow & & \downarrow \\ W & \xrightarrow{\Phi_A} & W \\ \downarrow & & \downarrow \\ \mathbb{H} & \xrightarrow{M_A} & \mathbb{H} \end{array}$$

commutes.

23. The stabilizer groups of the action on $\mathbb{H}$ are all finite: a point $\tau \in \mathbb{H}$ has nontrivial stabilizer if and only if it lies on one of the two orbits of elliptic fixed points.

4 Cubic Curves

24. For each lattice $\Lambda \subset \mathbb{C}$ define the **Weierstrass $\mathcal{P}$ function** by the

$$\mathcal{P}_\Lambda(t) = \frac{1}{t^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left\{ \frac{1}{(t+\omega)^2} - \frac{1}{\omega^2} \right\}.$$

In case $\Lambda = \Lambda_\tau$ we write $\mathcal{P}_\tau$ for $\mathcal{P}_\Lambda$. Define

$$\mathcal{P}_{\mathbb{Z}}(t) = \frac{1}{t^2} + \sum_{m \in \mathbb{Z}\setminus\{0\}} \left\{ \frac{1}{(t+m)^2} - \frac{1}{m^2} \right\}.$$

The following facts are not hard to prove:

(i) The series defining $\mathcal{P}_\Lambda$ and $\mathcal{P}_{\mathbb{Z}}$ converge uniformly on compact subsets to holomorphic maps $\mathbb{C} \to \mathbb{P}$.

(ii) Hence the derivatives are given by

$$\mathcal{P}'_\Lambda(t) = -\sum_{\omega \in \Lambda} \frac{2}{(t+\omega)^3}, \qquad \mathcal{P}'_{\mathbb{Z}}(t) = -\sum_{m \in \mathbb{Z}} \frac{2}{(t+m)^3}.$$

(iii) The limit

$$\lim_{\tau \to i\infty} \mathcal{P}_\tau(t) = \mathcal{P}_{\mathbb{Z}}(t)$$

holds uniformly on compact sets, i.e. for every neighborhood $\mathcal{U}$ of $\mathcal{P}_{\mathbb{Z}}$ in the compact open topology on $C^0(\mathbb{C}, \mathbb{P})$ and every $a > 0$ there exists $T > 0$ such that $\mathcal{P}_\tau \in \mathcal{U}$ for $\Im(\tau) > T$ and $-a \le \Re(\tau) \le a$.

(iv) The functions $\mathcal{P}_{\mathbb{Z}}$ and $\mathcal{P}_\Lambda$ are respectively periodic and doubly periodic in the sense that

$$\mathcal{P}_{\mathbb{Z}}(t+m) = \mathcal{P}_{\mathbb{Z}}(t), \qquad \mathcal{P}_\Lambda(t+\omega) = \mathcal{P}_\Lambda(t)$$

for $m \in \mathbb{Z}$ and $\omega \in \Lambda$. (It is obvious that the derivatives $\mathcal{P}'_Z$ and $\mathcal{P}'_\Lambda$ satisfy these relations.)

Lemma 25. *The functions $x = \mathcal{P}$ and $y = \mathcal{P}'$ satisfy a cubic equation*

$$y^2 = 4x^3 - g_2 x - g_3.$$

(Here $\mathcal{P}$ is either $\mathcal{P}_\Lambda$ or $\mathcal{P}_{\mathbb{Z}}$.)

Proof. By Laurent expansion

$$\begin{aligned}
\mathcal{P}(t) &= \frac{1}{t^2} + at^2 + bt^4 + O(t^6) \\
\mathcal{P}'(t) &= -\frac{2}{t^3} + 2at + 4bt^3 + O(t^5) \\
\mathcal{P}(t)^3 &= \frac{1}{t^6} + \frac{3a}{t^2} + 3b + O(t^2) \\
\mathcal{P}'(t)^2 &= \frac{4}{t^6} - \frac{8a}{t^2} - 16b + O(t)
\end{aligned}$$

so $\mathcal{P}'(t)^2 - 4\mathcal{P}(t)^3 + 20a\mathcal{P} + 28b = O(t)$. This function is doubly periodic, has no pole, and vanishes at the origin. Hence it vanishes identically. Take $g_2 = 20a$ and $g_3 = 28b$. □

26. To evaluate g_2 and g_3 calculate the Taylor expansion of $F(t) = \mathcal{P}(t) - t^{-2}$. Then $F''(0) = 6\sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-4}$ and $F^{(4)}(0) = 120\sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-6}$ so

$$g_2 = 60 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^4}, \qquad g_3 = 140 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^6}.$$

If Λ is replaced by $\mathbb{Z}$ this becomes $g_2 = 120\,\zeta(4)$ and $g_3 = 280\,\zeta(6)$ where $\zeta(s) := \sum_{n=1}^{\infty} n^{-s}$ is the Riemann zeta function. It is easy to see that functions

$$g_2(\tau) := g_2(\Lambda_\tau), \qquad g_3(\tau) := g_3(\Lambda_\tau)$$

are **modular forms** of weights four and six respectively, i.e.

$$g_2(M_A(\tau)) = (c\tau + d)^4 g_2(\tau), \qquad g_3(M_A(\tau)) = (c\tau + d)^6 g_3(\tau)$$

for $\tau \in \mathbb{H}$ and $A \in \mathrm{SL}_2(\mathbb{Z})$ as in paragraph 1. We extend g_2 and g_3 to $\mathbb{H} \cup \{\infty\}$ via

$$g_2(\infty) := g_2(\mathbb{Z}), \qquad g_3(\infty) := g_3(\mathbb{Z}).$$

27. An explicit formula for the map $\mathcal{P}_{\mathbb{Z}}$ is

$$\mathcal{P}_{\mathbb{Z}}(t) = \pi^2 \csc^2(\pi t) - \frac{\pi^2}{3}.$$

This follows from termwise differentiation of the series

$$\pi \cot(\pi t) = S(t) := \frac{1}{t} + \sum_{n\in\mathbb{Z}\setminus\{0\}} \left(\frac{1}{t+m} - \frac{1}{m} \right)$$

together with Euler's formula

$$\sum_{m=1}^{\infty} \frac{1}{m^2} = \frac{\pi^2}{6}.$$

To prove that $\pi \cot(\pi t) = S(t)$ note that both have the same poles with the same residues and that both are odd and have period one. This means that the difference $\pi \cot(\pi t) - S(t)$ is bounded in a strip about the real axis and, as $\cot(w) = i(e^{iw}+e^{-iw})/(e^{iw}-e^{-iw})$, both are bounded on the complement of this strip. Thus the difference $\pi\cot(\pi t) - S(t) = c$ a constant. To see that $c = 0$ is zero evaluate at $t = 1/2$: We get $S(1/2) = S(1/2-1) = S(-1/2) = -S(1/2)$ by periodicity and oddness so $S(1/2) = 0 = \cot(\pi/2)$ so $c = 0$. To prove Euler's formula calculate the Fourier series $\theta = \sum_n c_n e^{in\theta}$ and use Parseval's equality.

28. Since $\mathcal{P}_\Lambda$ has a pole of order two at the origin, the map $\mathbb{C}/\Lambda \to \mathbb{P}$ induced by $\mathcal{P}_\Lambda$ has degree two and the origin is a critical point. The other critical points are the zeros of the map $\mathbb{C}/\Lambda \to \mathbb{P}$ induced by $\mathcal{P}'_\Lambda$. This map has degree three (because it has a unique pole of order three) so $\mathcal{P}'_\Lambda$ has at most three zeros modulo Λ. Let ω_1 and ω_2 be generators of Λ. The half periods $\omega_1/2$, $\omega_2/2$ and $(\omega_1+\omega_2)/2$ satisfy $t = -t \mod \Lambda$ and hence are zeros of the odd doubly periodic function $\mathcal{P}'_\Lambda$.

29. Similarly the map $\mathbb{C}/\mathbb{Z} \to \mathbb{P}$ induced by $\mathcal{P}_\mathbb{Z}$ has degree two. To prove this use the identities $\csc^2(\pi t) = \cot^2(\pi t) + 1$ and

$$\cot(\pi t) = -i\frac{e^{\pi i t}+e^{-\pi i t}}{e^{\pi i t}-e^{-\pi i t}} = -i\frac{q+1}{q-1}$$

where $q = e^{2\pi i t}$. By paragraph 27 we have

$$\mathcal{P}_\mathbb{Z}(t) = -\pi^2\left(\frac{q+1}{q-1}\right)^2 + \frac{2\pi^2}{3}, \qquad \mathcal{P}'_\mathbb{Z}(t) = 2i\pi^3\left(\frac{q+1}{q-1}\right)^2\frac{q+1}{q-1}$$

where we have used $\mathcal{P}'_\mathbb{Z}(t) = -2\pi^3\csc^2(\pi t)\cot(\pi t)$ in the second formula. The formula for $\mathcal{P}'_\mathbb{Z}(t)$ shows that t is a critical point of $\mathcal{P}_\mathbb{Z}$ if and only if $t = n + \frac{1}{2}$ where $n \in \mathbb{Z}$.

30. For $\tau \in \mathbb{H} \cup \{\infty\}$ denote by $X_\tau \subset \mathbb{P}^2$ the cubic curve

$$X_\tau := \{[x,y,z] \in \mathbb{P}^2 : y^2z = 4x^3 - g_2(\tau)xz^2 - g_3(\tau)z^3\}.$$

Define projections $Q_\tau : \mathbb{C} \to \mathbb{C}/\Lambda_\tau$ and $Q_\infty : \mathbb{C} \to \mathbb{P} \setminus \{0,\infty\}$ by

$$Q_\tau(t) = t + \Lambda_\tau, \qquad Q_\infty(t) = e^{2\pi i t}.$$

For $\tau \neq \infty$ define $F_\tau : \mathbb{C}/\Lambda_\tau \to \mathbb{P}^2$ by

$$F_\tau(Q_\tau(t)) = [\mathcal{P}_\tau(t), \mathcal{P}'_\tau(t), 1]$$

for $t \neq 0$ with $F_\tau(0) = [0, 1, 0]$. Define $F_\infty : \mathbb{P} \to \mathbb{P}^2$ by

$$F_\infty(Q_\infty(t)) = [\mathcal{P}_\mathbb{Z}(t), \mathcal{P}'_\mathbb{Z}(t), 1]$$

with $F_\infty(0) = F_\infty(\infty) = [0, 1, 0]$.

Theorem 31. *(i) For $\tau \neq \infty$ the map $F_\tau : \mathbb{C}/\Lambda_\tau \to \mathbb{P}^2$ is a holomorphic embedding with image X_τ. (ii) The map $F_\infty : \mathbb{P} \to \mathbb{P}^2$ is a holomorphic immersion, injective except for a single double point, with image X_∞.*

Proof. Lemma 25 says that the image of F_τ is a subset of X_τ. If F_τ is not an immersion at some point $q = Q_\tau(t_0)$ where $t_0 \in \mathbb{C} \setminus \Lambda_\tau$, then $\mathcal{P}'(t_0) = \mathcal{P}''(t_0) = 0$ so $\mathcal{P} - \mathcal{P}(t_0)$ has a zero of order three at t_0 contradicting the fact that the map induced by $\mathcal{P}$ has degree two. Near 0 the map $F_\tau \circ Q_\tau$ has the form $F_\tau \circ Q_\tau(t) = [t + O(t^2), -2 + O(t), t^3]$ which shows that F_τ is an automorphism at the points $q \in Q_\tau(\Lambda_\tau)$ as well. The only case not covered by these arguments is the case $\tau = \infty$ and $q = \infty$. That F_∞ is an immersion at this point follows from the symmetry $F_\infty(q^{-1}) = T \circ F_\infty(q)$ where $T([x, y, z]) = [x, -y, z]$.

The map $\mathbb{C}/\Lambda_\tau \to \mathbb{P}$ induced by $\mathcal{P}$ has degree two and its branch points are the (projections of the) half periods of Λ_τ which are not periods (see paragraphs 28 and 29). In particular, $\mathcal{P}(t_1) = \mathcal{P}(t_2)$ implies that $t_1 = \pm t_2$ modulo Λ_τ. Since the map $\mathbb{C}/\Lambda_\tau \to \mathbb{P}$ is surjective and $\mathcal{P}'$ is odd it follows from Lemma 25 that the image of F_τ is X_τ. For the injectivity properties of F_τ note first that the preimage of $[0, 1, 0]$ consists of one point if $\tau \in \mathbb{H}$ and exactly two points if $\tau = \infty$ and that moreover $[0, 1, 0]$ is the only point at which the image of F_τ intersects the line at infinity. Hence it suffices to prove that the restriction of F_τ to $\mathbb{C}/\Lambda_\tau \setminus \{0\}$ is injective. Hence we assume that $\mathcal{P}(t_1) = \mathcal{P}(t_2)$, $\mathcal{P}'(t_1) = \mathcal{P}'(t_2)$, $t_1, t_2 \in \mathbb{C} \setminus \Lambda_\tau$ and prove that $t_1 = t_2$ modulo Λ_τ. If not, then $t_1 = -t_2$ modulo Λ_τ so, as $\mathcal{P}'$ is odd, $\mathcal{P}'(t_1) = \mathcal{P}'(t_2) = 0$. Hence t_1 and t_2 are branch points of $\mathcal{P}$. But the branch points of $\mathcal{P}$ are half periods of Λ_τ and two half periods t_1 and t_2 which are distinct modulo Λ_τ cannot be negatives of one another modulo Λ_τ. $\square$

Corollary 32. *For $\tau \in \mathbb{H} \cup \{\infty\}$ the discriminant $g_2(\tau) - 27g_3(\tau)$ vanishes if and only if $\tau = \infty$.*

Proof. The discriminant vanishes precisely when the polynomial $4x^3 - g_2x - g_3$ has a double root and this occurs precisely when X_τ is not a submanifold. $\square$

5 A Projective Embedding

Theorem 33. *For* $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ *the Riemann surface* $X(\Gamma)$ *defined in Theorem 9 is isomorphic to the Riemann sphere* $\mathbb{P}$*.*

Lemma 34. *There is a holomorphic map* $J : \mathbb{H} \to \mathbb{P}$ *such that for* $\tau, \tau' \in \mathbb{H}$ *we have* $J(\tau) = J(\tau')$ *if and only if* τ *and* τ' *lie in the same* $\mathrm{SL}_2(\mathbb{Z})$ *orbit. Thus* J *induces a bijection* $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C} = \mathbb{P} \setminus \{\infty\}$*.*

Proof. The **cross ratio** (e_1, e_2, e_3, e_4) of four distinct points e_1, e_2, e_3, e_4 of $\mathbb{C}$ is defined by

$$(e_1, e_2, e_3, e_4) = \frac{e_1 - e_2}{e_1 - e_3} \cdot \frac{e_4 - e_2}{e_4 - e_3};$$

the definition extends to four distinct points of $\mathbb{P} = \mathbb{C} \cup \{\infty\}$ by continuity. The symmetric group Σ_4 permutes the four numbers e_i and permutes their cross ratios accordingly:

$$\Sigma_4(\lambda) = \{\lambda, 1/\lambda, 1 - \lambda, 1/(1 - \lambda), \lambda/(\lambda - 1), (\lambda - 1)/\lambda\}.$$

It is easy to check that the polynomial

$$S(\lambda) = \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (1 - \lambda)^2}$$

has the property that $S(\lambda) = S(\lambda')$ if and only if $\lambda' \in \Sigma_4(\lambda)$.

For $\tau \in \mathbb{H}$ the four branch points of the map $\mathbb{C}/\Lambda_\tau \to \mathbb{P}$ induced by $\mathcal{P}_\tau$ are $e_4 = \infty$ and

$$e_1 = \mathcal{P}_\tau(1/2), \qquad e_2 = \mathcal{P}_\tau(\tau/2), \qquad e_3 = \mathcal{P}_\tau((1 + \tau)/2)$$

(see paragraph 28). Let λ be the cross ratio of the four branch points so $\lambda = (e_1 - e_2)/(e_1 - e_3)$ and then define $J(\tau) = 4S(\lambda)/27$. (The factor of 4/27 is traditional.) □

Remark 35. Since e_1, e_2, e_3 are the zeros of the polynomial $4x^3 - g_2 x - g_3$ we have

$$e_1 + e_2 + e_3 = 0, \qquad e_1 e_2 + e_2 e_3 + e_3 e_1 = -\frac{g_2}{4}, \qquad e_1 e_2 e_3 = \frac{g_3}{4}.$$

It follows easily that

$$J(\tau) = \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}.$$

36. Recall the cubic curve X_τ defined in paragraph 30 for $\tau \in \mathbb{H} \cup \{\infty\}$. Define

$$V := \{([x, y, z], \tau) \in \mathbb{P}^2 \times \mathbb{H} \cup \{\infty\} : [x, y, z] \in X_\tau\}$$

and subsets

$$V_1 := \{([x, y, z], \tau) \in V : \tau \in \mathbb{H}\}, \qquad V_2 := \{([x, y, z], \tau) \in V : \tau \in U \cup \{\infty\}\}$$

where U is as in Lemma **??**.

Lemma 37. *For $A \in \mathrm{SL}_2(\mathbb{Z})$ and $([x, y, z], \tau) \in V_1$ the point*

$$R_A([x, y, z], \tau) := ([(c\tau + d)^2 x, (c\tau + d)^3 y, z], M_A(\tau))$$

(see paragraph 26) also lies in V_1. For $A \in \mathrm{SL}_2(\mathbb{Z})_\infty$ and $([x, y, z], \tau) \in V_2$ the point

$$R_A([x, y, z], \tau) := ([x, ay, z], \tau + n)$$

*also lies in V_2. (See Lemma **??**.)*

Proof. □

6 A Projective Model

Lemma 38. *Let $B = \mathbb{C}^2 \setminus \{0\}$ and W be the set of all pairs $([x, y, z], a, b)$ in $\mathbb{P}^2 \times B$ such that*

$$y^2 z = 4x^3 - axz^2 - bz^3.$$

Then

(i) *The set W is a complex submanifold of $\mathbb{P}^2 \times B$.*

(ii) *The set of critical values of the projection $W \to B$ onto the second factor is the zero set of the discriminant $a^3 - 27b^2$ of the polynomial $4x^3 - ax - b$.*

(iii) *Over each critical value (a, b) there is a unique critical point namely the point $[x_0, 0, 1]$ where x_0 is the double root of the polynomial $4x^3 - ax - b$.*

39. Define actions of the complex multiplicative group $\mathbb{C}^*$ on B and W, by

$$\lambda_B(a,b) = (\lambda^4 a, \lambda^6 b), \qquad \lambda_W([x,y,z],(a,b)) = ([\lambda^2 x, \lambda^3 y, z], \lambda_B(a,b)).$$

so the projection $W \to B$ is equivariant. It is easy to see that the set of critical values of the projection $W \to B$ form a single orbit of the action of $\mathbb{C}^*$ on B. Define $\Phi : V \to W$ by

$$\Phi([x,y,z],\tau) = ([x,y,z],(g_2(\tau), g_3(\tau))).$$

Lemma 40. *The map $\Phi|V_1$ induces a bijection from the $\mathrm{SL}_2(\mathbb{Z})$ orbits of V_1 onto the $\mathbb{C}^*$ orbits of the set of regular points of the projection $W \to B$. The map $\Phi|V_2$ induces a bijection from the $\mathbb{Z}$ orbits of V_2 onto the $\mathbb{C}^*$ orbits of a neighborhood of the set of critical points of the projection $W \to B$.*

References

[1] D. Mumford: *Tata lectures on theta*, Progress in mathematics **28, 43, 97** Birkhuser, 1983-1991.

[2] E. Reyssat: *Quelques Aspects des Surface de Riemann*, Progress in mathematics **77**, Birkhäuser, 1989.

[3] G. Shimura: *Introduction to the Theory of Automorphic Functions*, Princeton University Press, 1971.