MA 598A LECTURE NOTES: FRIDAY, JANUARY 21

1. The Unit Circle

Last time, we defined a function $w : \mathbb{C} \to \mathbb{C}$ implicitly by the integral equation

$$z = \int_1^{w(z)} \frac{dx}{\sqrt{1-x^2}} \qquad \Longrightarrow \qquad w(z) = \cos z.$$

(The notation is modified just a little, but the same ideas apply.) We observed two facts:

(1) The point $(x, y) = (w(z),\, w'(z))$ is on the unit circle $S^1 : x^2 + y^2 = 1$.
(2) The function $w(z)$ is periodic with period

$$\omega_0 = 2 \int_{-1}^{1} \frac{dx}{\sqrt{1-x^2}} = 2\,\pi.$$

Recall that we proved these just by considering the implicit relation involving the integral.

Another way to state these facts is to say

$$\frac{\mathbb{C}}{2\pi\,\mathbb{Z}} \to S^1(\mathbb{C}), \qquad z \mapsto (\cos z,\, \sin z)$$

is a complex analytic isomorphism. For example, to see that this map has an inverse, we consider the map

$$S^1(\mathbb{C}) \to \frac{\mathbb{C}}{2\pi\,\mathbb{Z}}, \qquad P \mapsto \int_{(1,0)}^{P} \frac{dx}{y} \pmod{2\pi\,\mathbb{Z}}.$$

(This integral takes into account the cases where $y = \sqrt{1-x^2}$ is negative.)

We now generalize these ideas.

2. Elliptic Curves over $\mathbb{C}$

Fix complex numbers a and b such that $4\,a^3 + 27\,b^2 \neq 0$, and consider now the integral

$$\int_\infty^{\wp} \frac{dx}{\sqrt{x^3 + a\,x + b}}.$$

(Here, we take "∞" to mean the limit point of any sequence of complex numbers z_k such that $|z_k|$ increases without bound.) The integrand has poles at $x = e_1,\, e_2,\, e_3$ i.e. the three complex roots of $x^3 + a\,x + b$. Using a similar argument to above, we have two integrals to consider:

$$\omega_1 = 2 \int_{e_1}^{e_2} \frac{dx}{\sqrt{x^3 + a\,x + b}} \quad \text{and} \quad \omega_2 = 2 \int_{e_3}^{\infty} \frac{dx}{\sqrt{x^3 + a\,x + b}}.$$

Hence, we can define a function $\wp : \mathbb{C} \to \mathbb{C}$ implicitly by the relation

$$z = \int_\infty^{\wp(z)} \frac{dx}{\sqrt{x^3 + a\,x + b}}$$

We have two facts:

(1) The point $(x, y) = (\wp(z),\, \wp'(z))$ is on the curve $E : y^2 = x^3 + a\,x + b$.
(2) The function $\wp(z)$ is doubly-periodic i.e.

$$\wp(z + \omega_1) = \wp(z + \omega_2) = \wp(z).$$

Another way to say these facts is to say the map

$$\frac{\mathbb{C}}{\Lambda_E} \to E(\mathbb{C}), \qquad z \mapsto (\wp(z),\, \wp'(z))$$

is a complex analytic isomorphism, where we have denoted

$$\Lambda_E = \mathbb{Z}\langle \omega_1,\, \omega_2 \rangle = \{\omega = m\,\omega_1 + n\,\omega_2 \mid m,\, n \in \mathbb{Z}\} \subset \mathbb{C}$$

as a lattice in $\mathbb{C}$, and

$$E(\mathbb{C}) = \left\{ (x,\, y) \in \mathbb{C} \times \mathbb{C} \;\middle|\; y^2 = x^3 + A\,x + B \right\} \cup \{\mathcal{O}\}$$

as an elliptic curve considered over $\mathbb{C}$. Note that $\mathcal{O} \in E(\mathbb{C})$, the so-called "point at infinity,", is the image of the elements $\omega \in \Lambda_E$. We have an inverse map

$$E(\mathbb{C}) \to \frac{\mathbb{C}}{\Lambda_E}, \qquad P \mapsto \int_{\mathcal{O}}^{P} \frac{dx}{y} \pmod{\Lambda_E}.$$

We may think of the elliptic curve as being the complex plane modulo a lattice.

3. Elliptic Integrals Revisited

It's natural to consider say the function $w(z)$ defined implicitly by the relation

$$z = \int_1^{w(z)} \frac{du}{\sqrt{(1 - u^2)\,(1 - k^2\,u^2)}}.$$

for a fixed complex number $k \neq -1,\, 0,\, 1$. Note that this integral is in the form

$$\begin{aligned} &\int_1^{w} \frac{du}{\sqrt{(1 - u^2)\,(1 - k^2\,u^2)}} \\ &\quad = \int_0^{w} \frac{du}{\sqrt{(1 - u^2)\,(1 - k^2\,u^2)}} - \int_0^{1} \frac{du}{\sqrt{(1 - u^2)\,(1 - k^2\,u^2)}} \\ &\quad = F(\arcsin w, k) - K(k) \end{aligned}$$

so $w = \sin\left(F^{-1}(z + K(k), k)\right)$. As before, we have two main properties:

(1) The point $(u, v) = (w(z), w'(z))$ is on the quartic curve

$$C : \qquad v^2 = \left(1 - u^2\right)\left(1 - k^2\,u^2\right).$$

(2) The function $w(z)$ is doubly-periodic with periods

$$\begin{aligned} \omega_1 &= 2 \int_{-1/k}^{1/k} \frac{du}{\sqrt{(1 - u^2)\,(1 - k^2\,u^2)}} = \frac{4}{k}\,K\left(\frac{1}{k}\right) \\ \omega_2 &= 2 \int_{-1}^{1} \frac{du}{\sqrt{(1 - u^2)\,(1 - k^2\,u^2)}} = 4\,K(k). \end{aligned}$$

Note that these periods can be expressed in terms of incomplete elliptic integrals of the first kind.

4. Weierstrass ℘-Function

Following the work of Karl Weierstrass, we construct elliptic curves without using integrals at all. Fix a lattice $\Lambda \subset \mathbb{C}$; a subset of $\mathbb{C}$ is called a lattice if $\Lambda = \mathbb{Z}[\omega_1, \omega_2]$ for two complex numbers such that $\tau = \omega_1/\omega_2$ is not a real number. Define the function

$$\wp(z;\Lambda) = 4\left(\frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

(This is not quite the usual Weierstrass ℘-function because there is a nonstandard factor of 4.) We also define the constants

$$a(\Lambda) = -4 \cdot 60 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^4} \quad \text{and} \quad b(\Lambda) = -4^2 \cdot 140 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^6}.$$

Weierstrass showed (by considering the Laurent expansions above) the relation

$$\wp'(z;\Lambda)^2 = \wp(z;\Lambda)^3 + a(\Lambda)\,\wp(z;\Lambda) + b(\Lambda).$$

The celebrated *Uniformization Theorem* states that given $a,\, b \in \mathbb{C}$ such that $4\,a^3 + 27\,b^2 \neq 0$, there exists a lattice $\Lambda \subset \mathbb{C}$ such that $a = a(\Lambda)$ and $b = b(\Lambda)$. Hence, any elliptic curve may truly be associated with a Weierstrass ℘-function relative to some lattice.

5. The Elliptic Curve as a Torus

We give a more topological interpretation of elliptic curves over the complex numbers. We know that $\mathbb{C}/\Lambda_E$ can be viewed as a torus, because the quotient looks like a parallelogram in the complex plane with the sides identified.

Conversely, say that we have a torus:

$$T: \quad \left(\sqrt{x^2+y^2} - a\right)^2 + z^2 = b^2, \qquad 0 < b < a.$$

(The torus is actually the collection of real points satisfying this relation: $T(\mathbb{R})$.) We explain how to construct an elliptic curve from this surface. We can integrate along a path from one point (x, y, z) to another, but we may loop around two specific closed paths:

$$\begin{aligned} \alpha: &\quad [0,1] \to T(\mathbb{R}), &\quad t \mapsto (a\,\cos 2\pi t,\, a\,\sin 2\pi t,\, b)\,; \\ \beta: &\quad [0,1] \to T(\mathbb{R}), &\quad t \mapsto (a + b\,\cos 2\pi t,\, 0,\, b\,\sin 2\pi t)\,. \end{aligned}$$

The integral homology group of the torus gives a very natural lattice:

$$H_1(T,\mathbb{Z}) = \left\{\gamma : [0,1] \to T(\mathbb{R}) \,\middle|\, \gamma = m\,\alpha + n\,\beta \text{ for } m, n \in \mathbb{Z}\right\} \simeq \mathbb{Z} \times \mathbb{Z}.$$

We may generate an elliptic curve using the ideas above from this lattice.