Review : Introduction to Elliptic Curves and Modular Forms

Lee Jinhyeong

Definition 1. *K be any field, and $f(x) \in K[x]$ be a cubic polynomial with coefficients in K which has distinct roots in K or extension of K. We assume K does not have characteristic 2. The solutions of the equation*

$$y^2 = f(x)$$

are called K'-points of the elliptic curve and the equation is called elliptic curve.

Let $F(x,y) = y^2 - f(x)$. For example $F(x,y) = y^2 - (x^3 - n^2x)$. To make this equation dimensional homogeneous, we take the total dimension k of $F(x,y)$ and let $\tilde{F}(x,y,z) = z^n F(\frac{x}{z}, \frac{y}{z})$. For example $\tilde{F}(x,y,z) = y^2z - (x^3 - n^2xz^2)$ in our example. Then we can easily check the fact that

$$\tilde{F}(x,y,z) = 0 \Leftrightarrow F(\frac{x}{z}, \frac{y}{z}) = 0 (z \neq 0)$$

Next we will define the fundamental parallelogram for ω_1, ω_2.

Definition 2. $\Pi = \{a\omega_1 + b\omega_2 | 0 \leq a \leq 1, 0 \leq b \leq 1\}$. *For* $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$

And the lattice $L = \{m\omega_1 + n\omega_2 | m, n \in \mathbb{Z}\}$

And we may assume the imaginary part of $\frac{\omega_1}{\omega_2}$ is positive.

Definition 3. *A lattice L is given, f is called elliptic function relative to L if it is meromorphic on $\mathbb{C}$ and $f(z+l) = f(z)$ for all $z \in \mathbb{C}, l \in L$.*

We will denote the set of elliptic functions relative to L by $\mathcal{E}_L$. Then $\mathcal{E}_L$ is a subfield of the all meromorphic functions and closed by sum, difference, product, quotient, and differentiation.

Proposition 1. *A function $f(z) \in \mathcal{E}_L$ has no pole in the fundamental parallelogram Π must be a constant.*

This is immediate result from Liouville's theorem.

Proposition 2. $\alpha + \Pi = \{\alpha + z | z \in \Pi\}$. *Suppose $f(z) \in \mathcal{E}_L$ has no poles on the boundary C of $\alpha + \Pi$. Then the sum of the residues of $f(z)$ in $\alpha + \Pi$ is zero.*

By residue theorem, the sum of the residues can be expressed as

$$\frac{1}{2\pi i} \int_C f(z) dz$$

and since $f(z)$ has the same value on the parallel sides with opposite orientation, the integral value is exactly zero. Also by this proposition, we can check that non constant $f(z) \in \mathcal{E}_L$ has at least two poles or has a multiple pole, since if it has only one simple pole, then the residue cannot be zero.

Proposition 3. *Suppose $f(z)$ has no zeros on the boundary of $\alpha + \Pi$. Then the sum of orders of zeros of $f(z)$ is equal to the sum of orders of poles of $f(z)$.*

Since $\mathcal{E}_L$ is closed under differentiation and quotients, and $f(z)$ has no zeros on the boundary of $\alpha + \Pi$, $\dfrac{f'(z)}{f(z)}$ is also an elliptic function and by proposition 2 and the fact that the sum of the residues of $\dfrac{f'(z)}{f(z)}$ is the difference between the sum of orders of zeros of $f(z)$ and the sum of orders of poles of $f(z)$.

Definition 4. *The Weierstrass $\mathfrak{P}$-function*

$$\mathfrak{P}(z) = \mathfrak{P}(z; L) = \frac{1}{z^2} + \sum_{0 \neq l \in L} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$

It is introduced as the key example of an elliptic function.

Proposition 4. *The Weierstrass $\mathfrak{P}$-function converges absolutely and uniformly on any compact set in $\mathbb{C} \setminus L$*

For a compact set in $\mathbb{C} \setminus L$,

$$\sum_{0 \neq l \in L} \frac{1}{(z-l)^2}, \sum_{0 \neq l \in L} \frac{1}{l^2}$$

both converges absolutely and uniformly since L is a lattice.
Also the differentiation of the Weierstrass $\mathfrak{P}$-function is

$$\mathfrak{P}'(z) = -2 \sum_{l \in L} \frac{1}{(z-l)^3}$$

Next theorem is the main result in this report. An arbitrary elliptic function can be rationally expressed in $\mathfrak{P}(z)$, $\mathfrak{P}'(z)$. It is why the Weierstrass $\mathfrak{P}$ function was introduced as the key example of the elliptic functions.

Theorem 1. *Any elliptic function for L is a rational expression in $\mathfrak{P}(z)$, $\mathfrak{P}'(z)$. $\forall f(z) \in \mathcal{E}_L$, there exist two rational functions $g(X)$, $h(X)$ such that*

$$f(z) = g(\mathfrak{P}(z)) + \mathfrak{P}'(z) h(\mathfrak{P}(z))$$

For the proof, we will use a lemma.

Lemma 1. *The subfield $\mathcal{E}_L^+ \subset \mathcal{E}_L$ of even elliptic functions for L is generated by $\mathfrak{P}(z)$, i.e., $\mathcal{E}_L^+ = \mathbb{C}(\mathfrak{P})$*

(pf) We will construct a function which has the same poles and zeros as $f(z)$ using $\mathfrak{P}(z)$.
First let $\Pi' = \{a\omega_1 + b\omega_2\}$ and for $a \in \Pi' (a \neq 0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1 + \omega_2}{2})$, let

$$a^* = \begin{cases} \omega_1 + \omega_2 - a & \text{for} \quad a \in \dot{\Pi}' \\ \omega_1 - a & \text{for} \quad a = k\omega_1 \\ \omega_2 - a & \text{for} \quad a = k\omega_2 \end{cases}$$

then $a \neq a^*$ and the multiplicity of a is equal to the multiplicity of a^*. This is because the double periodicity, we have $f(a^* - z) = f(-a - z) = f(a + z)$ since f is even. Thus, $f(a + z)$ and $f(a^* + z)$ have the same degree of Laurent series.
Also in the case of $a = \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1 + \omega_2}{2}$, we can check that a has the even multiplicity of zero or pole since $f(\frac{\omega_1}{2} + z) = f(-\frac{\omega_1}{2} + z) = f(\frac{\omega_1}{2} - z)$ and this implies that the highest degree m must be even so that $a_m z^m = a_m (-z)^m$.

By this fact we can list zeros and poles as multi set $\{a_i\}$,$\{b_i\}$ respectively. We only list one of a, a^* for the multi set and we list them by their multiplicity. In the case of $a = \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1 + \omega_2}{2}$, we list them half of the multiplicity times. Thus the cardinality of the multi set is half of the cardinality of zeros of $f(z)$.

Since a_i's and b_i's are nonzero, the elliptic function

$$g(z) = \frac{\prod(\mathfrak{P}(z) - \mathfrak{P}(a_i))}{\prod(\mathfrak{P}(z) - \mathfrak{P}(b_i))}$$

is well defined. Our claim is that $g(z)$ has the exactly same zeros and poles as $f(z)$.

Since $\mathfrak{P}(z) - \mathfrak{P}(a_i)$ has a double zero if a_i is half lattice point and $\mathfrak{P}(z) - \mathfrak{P}(a_i)$ has a pair of zero at a_i and a_i^* otherwise, we can check that g, f has the same poles and zeros except at $z = 0$. In addition by Proposition 3 above, they also has the same multiplicity at $z = 0$ and by Proposition 1, we can have $f(z) = cg(z)$.

For the proof of the theorem, since

$$f(z) = \left(\frac{f(z) + f(-z)}{2}\right) + \mathfrak{P}'(z)\left(\frac{f(z) - f(-z)}{2\mathfrak{P}'(z)}\right)$$

and both of them are even elliptic functions, by Lemma, we have $f(z) = g(\mathfrak{P}(z)) + \mathfrak{P}'(z)h(\mathfrak{P}(z))$.