Review2 : Introduction to Elliptic Curves and Modular Forms

Lee Jinhyeong

Abstract

In this assignment, our purpose is to construct natural additional law in the elliptic curve by using Weierstrass $\mathfrak{P}$-function. Then by interpreting geometrically, we will show that the addition law is the same as the addition law which the instructor introduced before, which might be seem unnatural.

In last assignment, we have shown that the subfield $\mathcal{E}_L^+ \subset \mathcal{E}_L$ of even elliptic functions for L is generated by $\mathfrak{P}(z)$, i.e., $\mathcal{E}_L^+ = \mathbb{C}(\mathfrak{P})$. For its consequence corollary, we have the following result.

Corollary 1. *The function $\mathfrak{P}'(z)^2 \in \mathcal{E}_L^+$ is a cubic polynomial in $\mathfrak{P}(z)$.*

Since $\mathfrak{P}'(z)$ has single zeros at $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, and $\frac{\omega_1+\omega_2}{2}$ and has a triple pole at zero, $\{a_i\}$ of $\mathfrak{P}'(z)^2$ is $\{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$ and $\{b_i\}$ of $\mathfrak{P}'(z)^2$ is $\emptyset$. Thus, we have $g(z) = \prod_{i=1}^{3}(\mathfrak{P}(z) - \mathfrak{P}(a_i))$ and $\mathfrak{P}'(z) = cg(z)$. This concludes the proof of corollary.

By corollary, we have $\mathfrak{P}'(z)^2 = a\mathfrak{P}(z)^3 + b\mathfrak{P}(z)^2 + c\mathfrak{P}(z) + d$ for some constant $a, b, c, d \in \mathbb{C}$ and to compute the coefficients, we expand the power series.

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

We have $\frac{1}{(z-l)^2} - \frac{1}{l^2} = \frac{1}{l^2}\left((1-\frac{z}{l})^{-2} - 1\right) = \frac{1}{l^2}\sum_{k=1}^{\infty}(k+1)\left(\frac{z}{l}\right)^k$. Thus, for small enough z we have

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

By putting $G_k = \sum_{0 \neq l \in L} \frac{1}{l^k}$, for odd k we can easily check that $G_k = 0$ since $l \in L \Rightarrow -l \in L$. Thus we can conclude that

$$\mathfrak{P}(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \cdots .$$

By elementary computation, we can obtain that $\mathfrak{P}'(z)^2 = 4\mathfrak{P}(z)^3 - 60G_4\mathfrak{P}(z) - 140G_6$ and for simplicity, we write

$$\mathfrak{P}'(z)^2 = f(\mathfrak{P}(z)), \text{where } f(x) = 4x^3 - g_2 x - g_3 \in \mathbb{C}[x]$$

and $g_2 = 60G_4$, $g_3 = 140G_6$.

Our next goal is to identifying $\mathbb{C}/L$ and the elliptic curve $y = f(x)$.

Proposition 1. *The map T is an analytic one-to-one correspondence between $\mathbb{C}/L$ and the elliptic curve $y = f(x)$ in $\mathbb{P}^2_{\mathbb{C}}$ which is the projective plane of $\mathbb{C}^3$. The map T is given by*

$$z \mapsto [(\mathfrak{P}(z), \mathfrak{P}'(z), 1)] \text{ for } z \neq 0$$

$$0 \mapsto [(0, 1, 0)].$$

Here, $[v]$ implies the class of $v \in \mathbb{C}^3$ in $\mathbb{P}^2_{\mathbb{C}}$, i.e. $[v] = [cv]$.

If $f(x) \neq 0$, then $\mathfrak{P}(z) = x$ has two distinct roots. Thus, for x which is not a root of $f(x)$, the map T is one-to-one correspondence. For the case x is a root of the $f(x) = 0$, it implies that $\mathfrak{P}'(z) = 0$ and z are middle points of the lattice L and f has three roots, we can check that the map T is one-to-one correspondence. For analyticness, for the points in $\mathbb{C} \setminus L$, the map T itself is analytic. For the lattice points, the map $z \mapsto [(\frac{\mathfrak{P}(z)}{\mathfrak{P}'(z)}, 1, \frac{1}{\mathfrak{P}'(z)})]$ is the same map to T and is analytic.

For our goal, the addition law for points of the elliptic curve, now we can construct natural addition by computing $z_1 + z_2$ such that $(x_1, y_1) = (\mathfrak{P}(z_1), \mathfrak{P}'(z_1))$ and $(x_2, y_2) = (\mathfrak{P}(z_2), \mathfrak{P}'(z_2))$.

Definition 1. *For the elliptic curve $y^2 = f(x)$, let $P_z = [(\mathfrak{P}(z), \mathfrak{P}'(z), 1)]$ and $P_0 = [(0, 1, 0)]$ on the elliptic curve. We define $P_{z_1} + P_{z_2} = P_{z_1 + z_2}$.*

It is natural to check following property.

Proposition 2. *The additional identity is $[(0, 1, 0)]$ and the additive inverse of $[(x, y, 1)]$ is $[(x, -y, 1)]$.*

It is clear that the additional identity is $P_0 = [(0, 1, 0)]$. For the additive inverse, let $P_z = [(x, y, 1)]$, then we have $\mathfrak{P}(-z) = \mathfrak{P}(z)$ and $\mathfrak{P}'(-z) = -\mathfrak{P}(z)$. Thus, the additive inverse $P_{-z} = [(x, -y, 1)]$.

For geometric interpretation of the addition law, we need to show a lemma first.

Lemma 1. *For a lattice L and the fundamental parallelogram Π for $f(z) \in \mathcal{E}_L$, if there is no zeros or poles of $f(z)$ on the boundary of $\alpha + \Pi$ for a complex number α, and let $\{a_i\}$, $\{b_j\}$ be the zeros and poles in $\alpha + \Pi$ of $f(z)$ with multiplicity, respectively. Then $\sum a_i - \sum b_j \in L$.*

For the proof, we might consider the function $\frac{zf'(z)}{f(z)}$. If f has a zero at a of order m, then $\frac{f'(z)}{f(z)}$ has its expansion at a as $\frac{m}{z-a} + \cdots$. For a pole b of order m, $\frac{f'(z)}{f(z)}$ has its expansion at b as $-\frac{m}{z-a} + \cdots$. Thus by multiplicating $a + (z - a)$, $\frac{zf'(z)}{f(z)}$ has its expansion at a as $\frac{am}{z-a} + \cdots$ and at b, $-\frac{am}{z-a} + \cdots$.

Thus, (the residue of $\frac{zf'(z)}{f(z)}$) $= \sum a_i - \sum b_j$. By the residue theorem, we have $\sum a_i - \sum b_j = \frac{1}{2\pi i} \int_C \frac{zf'(z)}{f(z)} dz$ where C is the boundary of $\alpha + \Pi$. Since f is doubly periodic, we have

$$\frac{1}{2\pi i} \left(\int_{\alpha}^{\alpha+\omega_1} \frac{zf'(z)}{f(z)} dz - \int_{\alpha+\omega_2}^{\alpha+\omega_1+\omega_2} \frac{zf'(z)}{f(z)} dz \right) = \frac{1}{2\pi i} \int_{\alpha}^{\alpha+\omega_1} (-\omega_2) \frac{f'(z)}{f(z)} dz$$

$$= (-\omega_2) \frac{1}{2\pi i} \int_{\tilde{C}} \frac{du}{u}$$

and since $f(\alpha) = f(\alpha + \omega_1)$, $\tilde{C}$ is closed curve. Thus $\frac{1}{2\pi i}\int_{\tilde{C}} \frac{du}{u}$ is winding number of $\tilde{C}$ which implies it is integer. Similarly, we can conclude that $\frac{1}{2\pi i}\int_{C} \frac{zf'(z)}{f(z)}dz = a\omega_1 + b\omega_2$ for some integers a, b. Thus this implies the lemma holds.

And there is well-known theorem.

Theorem 1. (**Bezout's**) *$\tilde{F}(x,y,z), \tilde{G}(x,y,z)$ are homogeneous polynomials of degree m, n, respectively and there is no common polynomial factor. Then the curves in $\mathbb{P}^2_K$ defined by $\tilde{F}, \tilde{G}$ have mn common points with multiplicity.*

Our preparation is done. There is the main theorem.

Theorem 2. *If $P_1 + P_2 = P_3$, then $-P_3$ is the third intersection point of $\overline{P_1P_2}$ with the elliptic curve.*

Let $\overline{P_1P_2}$ be $\mathfrak{P}'(z) - m\mathfrak{P}(z) - b = 0$. We will check the zeros and poles of $\mathfrak{P}'(z) - m\mathfrak{P}(z) - b = 0$. Since $\mathfrak{P}'(z)$ has triple pole at zero and $\mathfrak{P}(z)$ has double pole at zero and nowhere else, $\mathfrak{P}'(z) - m\mathfrak{P}(z) - b = 0$ has triple pole at zero and nowhere else. Thus by proposition in the first assignment, $\mathfrak{P}'(z) - m\mathfrak{P}(z) - b = 0$ has three zeros. By Bezout's theorem, for $\tilde{F}(x,y,z) = y^z - 4x^3 + g_2xz^2 + g_3z^3$, $\tilde{G}(x,y,z) = y - mx - bz$, they has three intersections in $\mathbb{P}^2_{\mathbb{C}}$. Since z_1, z_2 are zeros of $\mathfrak{P}'(z) - m\mathfrak{P}(z) - b = 0$, by lemma above, the last zero is $-z_1 - z_2$ modulo the lattice. Thus, $-P_3 = P_{z_1+z_2} = P_{z_1} + P_{z_2}$. This concludes the proof.