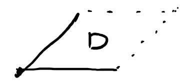
# 1/13

Monday, January 13, 2020 13:51

From last time: understand $(\wp(z) - \wp(z_0))$, $z_0 \in \mathbb{C}$.

- poles = lattice pts, double poles
- res. thm $\Rightarrow$ # poles = # zeroes in $D$




so $\wp(z) - \wp(z_0)$ has two zeroes. $z_0$ is one, $-z_0$ is another one.

two zeroes if $z_0 \neq -z_0 \bmod \Lambda$ (equiv. $2z_0 \notin \Lambda$).

if $z_0 \overset{\bmod \Lambda}{=} -z_0$ $z_0$ is a double zero, since $2z_0 \in \Lambda$.

$f$ even ell fn.

$$g(z) := \prod_{\substack{z_0 \in D' \\ \text{half-fd.}}} (\wp(z) - \wp(z_0))^{n_{z_0}} \qquad n_{z_0} = \begin{cases} \operatorname{ord}_{z_0}(f) & \text{if } 2z_0 \notin \Lambda, \\ \frac{1}{2}\operatorname{ord}_{z_0}(f) & \text{if } 2z_0 \in \Lambda. \end{cases}$$

$\frac{f(z)}{g(z)}$ holomorphic, no poles or zeroes, so $f(z) \in \mathbb{C}(\wp(z))$.

last time: $(\wp'(z))^2 = c\left(\wp(z) - \wp(\frac{w_1}{2})\right)\left(\wp(z) - \wp(\frac{w_2}{2})\right)\left(\wp(z) - \wp(\frac{w_1+w_2}{2})\right)$.

Lattices to elliptic curves.

$$\wp(z) := \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \Bigg( \underbrace{\frac{1}{(z-w)^2} - \frac{1}{w^2}}_{\frac{1}{w^2}\left[\frac{1}{(1-\frac{z}{w})^2} - 1\right]} \Bigg)$$

(do some computation & compare coefficients.)

$$= \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \sum_{m=1}^{\infty} (2m+1) \frac{z^{2m}}{w^{2m+2}}$$

by cancelling rel^ns from $w$ & $-w$ in $\Lambda$.

$$= \frac{1}{z^2} + \sum_{m=1}^{\infty} \underbrace{\Big( \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^{2m+2}} \Big)}_{G_{2m+2}(\Lambda)} (2m+1)\, z^{2m}$$

$G_{2m+2}(\Lambda)$ the eisenstein series of weight $2m+2$.

$$\Rightarrow \wp(z) = \frac{1}{z^2} + \sum_{m=1}^{\infty} (2m+1)\, G_{2m+2}(\Lambda)\, z^{2m}$$ Laurent series.

$\wp(z) = z^{-2} + 3G_4 z^2 + \cdots$

$\wp(z)^3 = \cdots$

... some other stuff...

$$\Rightarrow (\wp'(z))^2 - 4(\wp(z))^3 + 60G_4\, \wp(z) + 140G_6 = 0$$

so $C = 4$.

<u>Thm</u> $(\wp'(z))^2 = 4(\wp(z))^3 - \underbrace{60G_4}_{g_2} \wp(z) - \underbrace{140G_6}_{g_3}$

<u>Thm</u> $\exists$ isom (bij of pts)

$$\mathbb{C}/\Lambda \xrightarrow{\phi} E = \{ \underset{\mathbb{C}^2}{\overset{}{(x,y)}} : y^2 = 4x^3 - g_2 x - g_3 \}.$$

$$z \longmapsto (\wp(z), \wp'(z)).$$

(almost: for $z \in \Lambda$ ($z=0$), map is undefined).

<u>pf</u> let's just not consider $z=0$. $\phi$ is well-defined: $\phi(z) \in E$ by prev. thm.

- $\phi$ is surjective: take $(x,y) \in E$. Solve $\wp(z) = x$. $\exists\, a$ s.t. $\wp(a) - x = 0$ since $\wp(z) - x$ has two poles & so two zeroes.

<u>Q</u>: is $\wp'(a) = y$? We know $(\wp'(a))^2 = y^2$, so either

$\wp'(a) = y$ or $\wp'(a) = -y$, in which case $\wp'(-a) = y$ and $\wp(-a) = \wp(a)$ still. ✓

- $\phi$ is injective: suppose $\phi(z_1) = \phi(z_2)$. Consider $\wp(z) - \wp(z_1)$. This has two zeroes since it has two poles. $z_1$ is a solution, and so is $-z_1$. also, $z_2$ and $-z_2$ are solutions.

Consider two cases:

① $z_1 = -z_1 \mod \Lambda$. Then $z_1$ is a soln of order 2, so $z_1$ is only solution so $z_1 = z_2$.

② $z_1 \neq -z_1 \mod \Lambda$. Then either $z_2 = z_1$ or $z_2 = -z_1 \pmod \Lambda$. in the latter case, $\wp'(z_2) = -\wp'(z_1)$. This contradicts $\phi(z_1) = \phi(z_2)$, so $z_2 = z_1$, unless $\wp'(z_1) = 0 = \wp'(z_2)$. $\wp'(z)$ has 3 zeroes, $\frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1+w_2}{2}$. $z_1 \neq -z_1 \mod \Lambda \Rightarrow 2z_1 \notin \Lambda$, so this cannot happen.

$\square$

1. Why is it called an elliptic curve?

Ellipse: $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$

arc length $\int_0^t \sqrt{1+f'(t)^2}\, dt \qquad f(x) = y = \pm\sqrt{b^2\left(1-\frac{x^2}{a^2}\right)}$

$$\int_0^t \frac{\quad}{\sqrt{(1-x^2)(1-(1-b^2)x^2)}}\, dx$$ no closed form.

<u>Def</u> an elliptic integral is $\int \underset{\text{rat'l.}}{R}(x,y)\, dx$, where $y^2 =$ cubic or quartic in $x$.

$$I(t) = \int_t^\infty \frac{dx}{\sqrt{4x^3 - g_2 x - g_3}}$$

$\Rightarrow \; t = \wp(I(t))$ , $\wp$ is inverse function to $I$.

2. group structure on $E = \{ \underset{\in}{(x,y)}^{\mathbb{C}^2} : y^2 = 4x^3 - g_2 x - g_3 \}$.

given by group structure on $\mathbb{C}/\Lambda$ and bijection $\phi$.