Zeta Function over Elliptic Curves

<u>Dirichlet Series</u> : $\zeta(z) = \sum_{n \geq 1} \frac{1}{n^z}$.

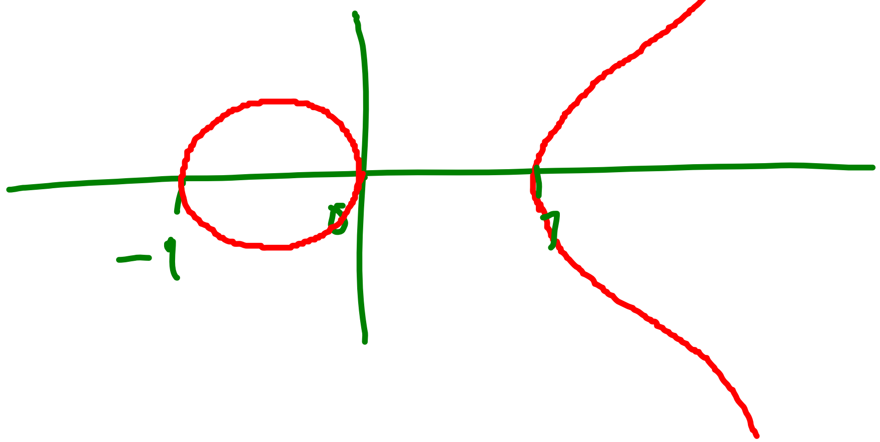
<u>Power Series</u> : $P(z) = \sum_{n \geq 1} z^n$

Elliptic Curves

$$y^2 = x^3 + Ax + B, \quad \underbrace{4A^3 - 27B^2 \neq 0}_{}$$

ensures that the curve in not degenerate

Examples: $y^2 = x(x-1)(x+1)$



Let $E(\mathbb{Q})$ = set of rational points on elliptic curve E

<u>Theorem</u>: $E(\mathbb{Q})$ or $E(\mathbb{R})$ or $E(\mathbb{C})$ alongwith ∞ are groups under $+$.

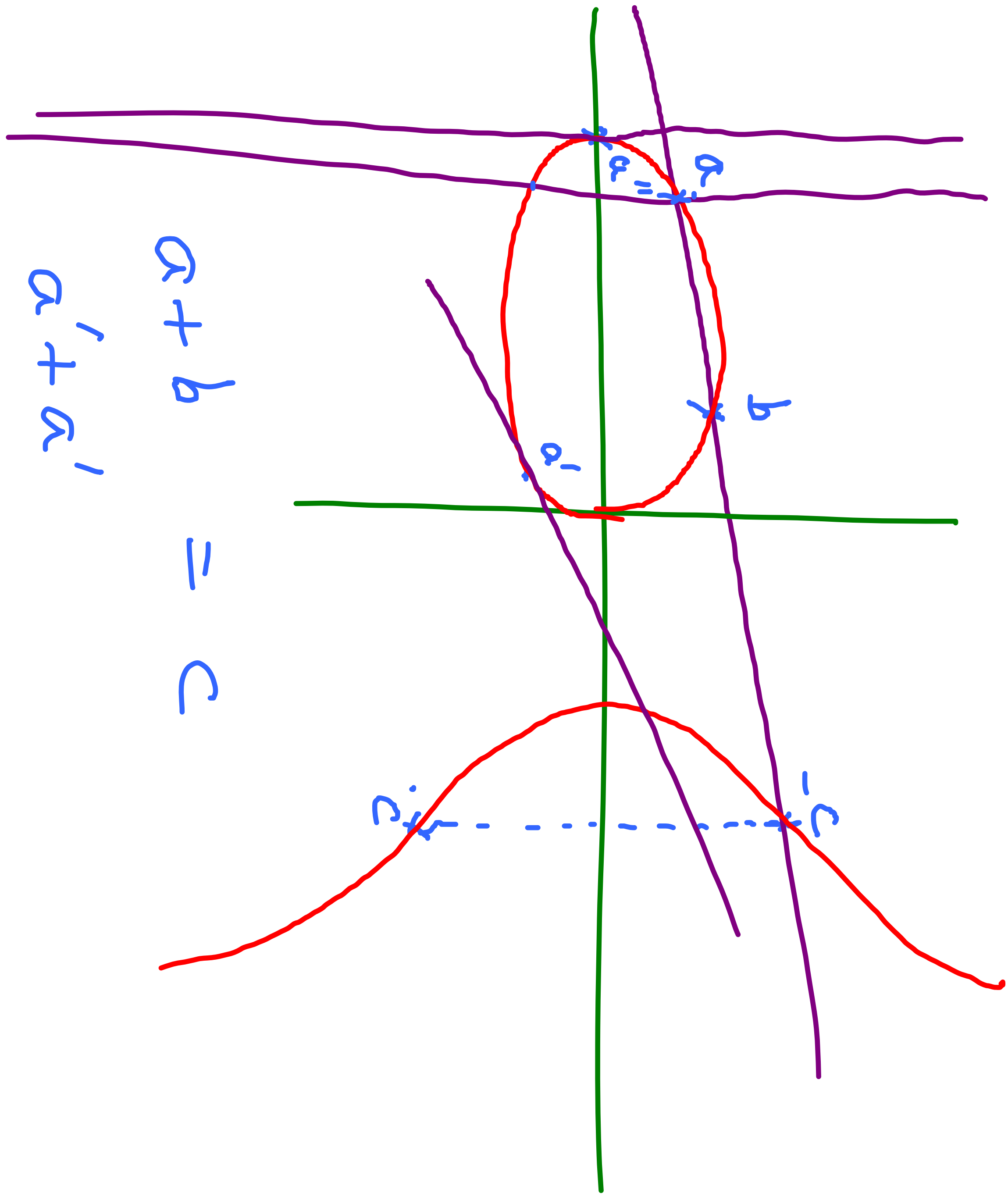
not usual addition

$a + b = c$

$a' + a'$

$a'' + a'' = \infty$

$a + \infty = a$



Elliptic Curves over finite fields

$y^2 = x^3 + Ax + B$, $4A^3 - 27B^2 \neq 0$

over field F_q of char $p \neq 2, 3$.

$E(F_q)$ = points on E in F_q

In general, $E(F_{q^k})$ = points on E in F_{q^k}.

Elliptic Curves over $\mathbb{Q}$

Let $E : y^2 = x^3 + Ax + B$,

$A, B \in \mathbb{Q}$

& $4A^3 + 27B^2 \neq 0$.

Prime p is good for E if

$p \nmid 4A^3 + 27B^2$.

Let $\zeta_E(z, \mathbb{Q}) = \prod_{\substack{p \\ p\,\text{good}}} \left(1 - a_p p^{-z} + p^{1-2z}\right) * (x)$

$$(x) = \prod_{\substack{p \\ p\,\text{bad}}} \left(1 - a_p p^{-z}\right), \quad a_p \in \{-1, 0, 1\}$$

Fermat's Last Theorem

There is no integral solution to equation $x^n + y^n = z^n$ for $n \geq 3$.

proof sketch: Assume that $a^n + b^n = c^n$ for $(a, b, c) = 1$ and $n \geq 6$.

Consider the following curve:

$$F: \quad y^2 = x(x-a^n)(x+b^n)$$

Discriminant of F:
$$\Delta_F = (-a^n)(b^n)(-a^n-b^n)$$
$$= a^n b^n (a^n+b^n)$$
$$= (abc)^n$$

<u>Theorem</u>: If Δ_F is l^{th} power of an integer, then it has a point of order l.

Theorem (Frey 80s): If F is modular, then it does not have a point of order ≥ 6.

Modular Curves

$$\zeta_E(z, \mathbb{Q}) = \sum_{n \geq 1} \frac{a_n}{n^z}, \text{ with } a_n \text{ "multiplicative"}$$

Let $$f_E(z, \mathbb{Q}) = \sum_{n \geq 1} a_n e^{2\pi i n z}$$

Observation:

$$f(z+1) = \sum_{n \geq 1} a_n e^{2\pi i n (z+1)}$$

$$= \sum_{n \geq 1} a_n e^{2\pi i n z} \cdot e^{2\pi i n}$$

$$= f(z).$$

Let $z = \alpha + i\beta$, $\beta > 0$.

Then $f(z) = \sum_{n} a_n e^{2\pi i n(\alpha + i\beta)}$

$$= \sum_{n} a_n e^{2\pi i n \alpha} \cdot e^{-2\pi n \beta}$$

$$\Rightarrow \quad |f(z)| \leq \sum_{n} |a_n| \, e^{-2\pi n \beta}$$

$$\leq \sum_{n \geq 1} \frac{O(n)}{\left(e^{2\pi\beta}\right)^n} < \infty$$

Möbius Transformation

$\tau : \mathbb{H}_+ \longrightarrow \mathbb{H}_+$, $\mathbb{H}_+$: upper half of $\mathbb{C}$

$\tau(z) = \dfrac{az+b}{cz+d}$, $a, b, c, d \in \mathbb{Z}$.

& $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$.

$$\tau(z) = \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}$$

$$= \frac{ac|z|^2 + bd + adz + bc\bar{z}}{|cz+d|^2}$$

$$\mathrm{Im}(\tau(z)) = \frac{(ad-bc)}{|cz+d|^2} \mathrm{Im}(z)$$

$$= \frac{\mathrm{Im}(z)}{|cz+d|^2}$$

Let $\Gamma(1) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \begin{array}{l} \det(\ ) = 1 \\ a, b, c, d \in \mathbb{Z} \end{array} \right\}$

Let $\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \begin{array}{l} (\ ) \in \Gamma(1) \\ \& \ c = 0 \ (\mathrm{mod}\ N) \end{array} \right\}$

<u>Def</u>: Function f is a <u>modular form of height 1 and level N</u> if

(1) $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$ for all $\gamma \in \Gamma(N)$

(2) $f\left(-\frac{1}{Nz}\right) = \pm N z^2 f(z)$

Observation : Let $W = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$, then

$$W \Gamma(N) W^{-1} = \Gamma(N).$$

Theorem : $f_E(z, Q)$ is a modular function of height 1 and level N iff

$$\left(\frac{\sqrt{N}}{2\pi}\right)^{z} \Gamma(z) \zeta_E(z, Q) = \mp \left(\frac{\sqrt{N}}{2\pi}\right)^{2-z} \Gamma(2-z) \zeta_E(2-z, Q).$$

__Defn__: Elliptic curve E is __modular__ if $f_E(z, Q)$ is a modular form of height 1 and level N for some $N > 0$.

__Theorem (Wiles, ...)__: All elliptic curves are modular.

proof of modular form & functional eqn equivalence

Suppose f_E is a modular form of level N.

Then $\left(\frac{\sqrt{N}}{2\pi}\right)^z \Gamma(z)\, \zeta_E(z) =$

$$\left(\frac{\sqrt{N}}{2\pi}\right)^z \left(\int_0^\infty t^{z-1} e^{-t}\, dt\right)\left(\sum_{n\geq 1} \frac{a_n}{n^z}\right)$$

$$= \sum_{n\geq 1} a_n \int_0^\infty \left(\frac{\sqrt{N}t}{2\pi n}\right)^z e^{-t}\, \frac{dt}{t}$$

Let $u = \frac{t}{2\pi n}$.

$$\text{LHS} = \sum_{n \geq 1} a_n \int_0^\infty (\sqrt{N} u)^z e^{-2\pi n u} \cdot \frac{du}{u}$$

$$= \int_0^\infty (\sqrt{N} u)^z \left(\sum_{n \geq 1} a_n e^{-2\pi n u} \right) \frac{du}{u}$$

$$= \int_0^\infty (\sqrt{N} u)^z f(iu) \frac{du}{u}$$

$$= \int_0^{1/\sqrt{N}} + \int_{1/\sqrt{N}}^\infty (\sqrt{N} u)^z f(iu) \frac{du}{u}$$

Let $I = \int_0^{1/\sqrt{N}} (\sqrt{N} u)^z f(iu) \frac{du}{u}$

Let $u = \frac{1}{Nv}$, Then $du = -\frac{1}{Nv^2}$

Then $I = \int_{1/\sqrt{N}}^{\infty} \left(\frac{1}{\sqrt{N} v} \right)^z f\left(\frac{i}{Nv} \right) \frac{dv}{v}$

$$f\left(\frac{i}{Nv}\right) = f\left(-\frac{1}{N(iv)}\right) = \pm N(iv)^2 f(iv)$$
$$= \mp N v^2 f(iv)$$

So,
$$I = \mp \int_{1/\sqrt{N}}^{\infty} \left(\frac{2}{\sqrt{N}v}\right)^{z} N v^{2} f(iv) \frac{dv}{v}$$
$$= \mp \int_{1/\sqrt{N}}^{\infty} 2^{z} \left(\sqrt{N} v\right)^{2-z} f(iv) \frac{dv}{v}$$

Functional equation for $\zeta_E(z)$ is symmetric around $\mathrm{Re}(z) = 1$.

<u>Question</u> : What is the behavior of $\zeta_E(1)$?

Answer is unknown!

Birch-Swinnerton-Dyer Conjecture

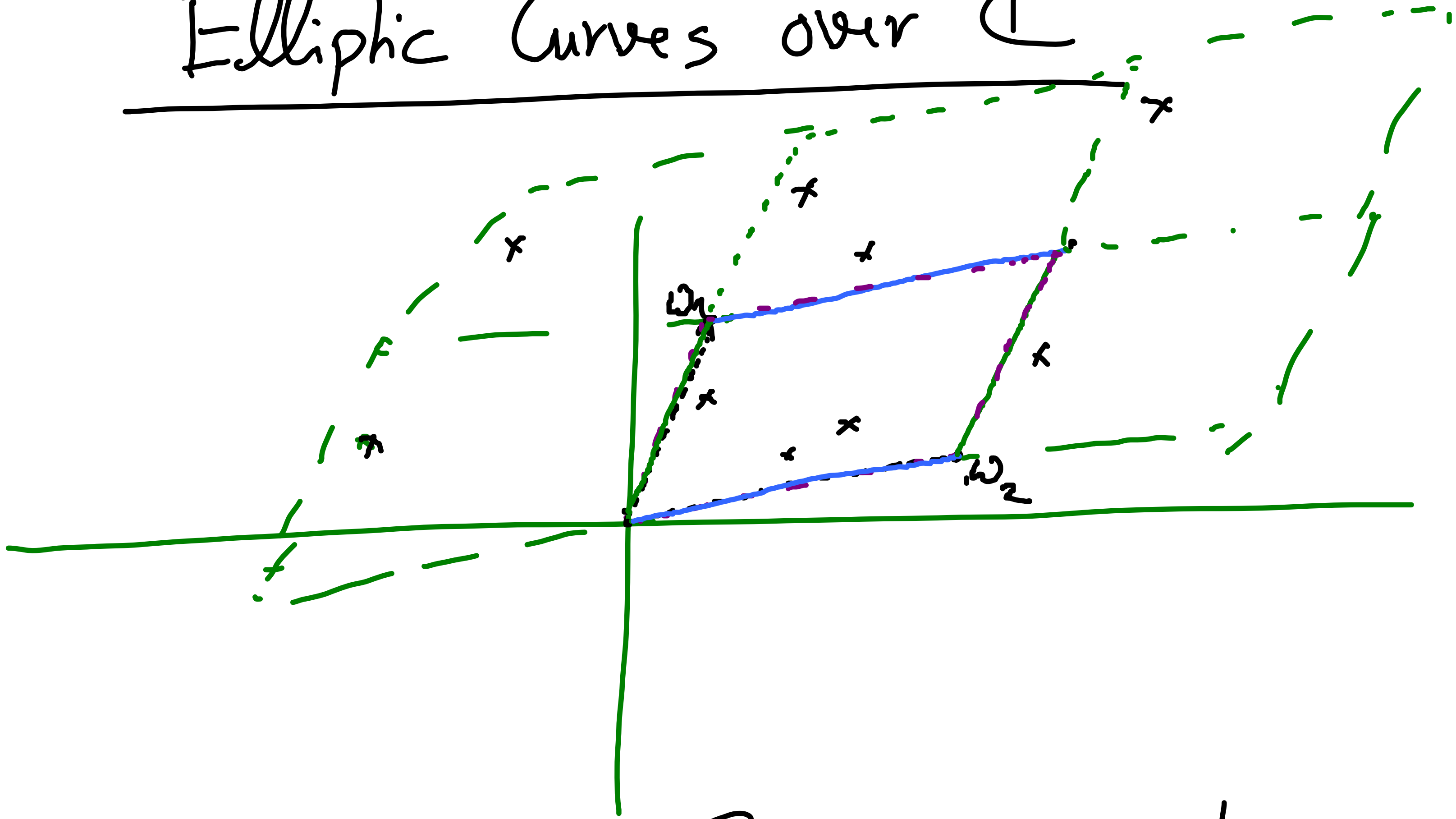
Let E be an elliptic curve.

Fact: $E(\mathbb{Q}) \cong \text{torsion} \oplus \mathbb{Z}^r$, $r \geq 0$.

$$\zeta_E(z) = \sum_{n \geq 1} \frac{a_n}{n^z}$$

Conjecture: $$\zeta_E(z) = (z-1)^r \cdot \frac{|\omega_2|}{|\text{torsion}|} \cdot \text{const} + (z-1)^{r+1} \cdot \text{const} + \cdots$$

Elliptic Curves over $\mathbb{C}$



Let $L = \left\{ m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z} \right\}$

We can view a torus as $\mathbb{C}/L$.

We define $f : \mathbb{C} \longrightarrow \mathbb{C}$ such that ~~if~~ it is also a map from $\mathbb{C}/L$ to $E(\mathbb{C})$.

We must have $f(z) = f(z+\omega_1)$

& $f(z) = f(z+\omega_2)$.

Such functions are called <u>doubly periodic</u>.

Let f be a meromorphic & doubly periodic function.

<u>Theorem</u>: Let F be the fundamental parellelopiped of the lattice L. Then:

(1) $\displaystyle\sum_{z \in F} \operatorname{res}_z(f) = 0$

(2) $\displaystyle\sum_{z \in F} \operatorname{ord}_z(f) = 0$

(3) For any $w \in \mathbb{C}$, $f(z) = w$ for ℓ

values of z (counting multiplicity) in F,

where $\ell = -\sum_{\substack{z \in F \\ z \text{ is a pole}}} \operatorname{ord}_z(f)$ & f is not constant.

proof:

$$2\pi i \sum_{z \in F} \operatorname{res}_z(f) = \int_{\delta F} f(w)\,dw$$

$$= \int_0^{\omega_1} + \int_{\omega_1}^{\omega_1+\omega_2} + \int_{\omega_1+\omega_2}^{\omega_2} + \int_{\omega_2}^{0} f(w)\,dw$$

$=$

$$= \int_0^{\omega_1} + \int_0^{\omega_2} + \int_{\omega_1}^0 + \int_{\omega_2}^0 f(\omega)\,d\omega = 0.$$

(2) $$2\pi i \sum_{z \in F} \operatorname{ord}_z(f) = \int_{\delta F} \frac{f'(\omega)}{f(\omega)}\,d\omega$$
$$= 0$$

(3) Consider $f(z) - \omega$. If f has no poles, then it is constant. Using (2), we get the result. $\boxtimes$

Weierstrass $\wp$-function

Let L be a lattice. Define.

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Theorem: (1) $\wp(z)$ converges uniformly at all $z \notin L$.

(2) $\wp(z) = \wp(-z)$ & $\wp(z+\omega) = \wp(z)$. $\omega \in L$.

(3) Any doubly periodic function for L

So,

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}}$$

is in $\mathbb{C}(\wp, \wp')$.

(4) $\wp$ has a pole of order 2 at $\omega \in L$.

<u>proof sketch</u>: Considering z, $|z| < |\omega|$ for all $\omega \in L$, $\omega \neq 0$.

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left[\frac{1}{(1-z/\omega)^2} - 1\right]$$

$$= \frac{1}{\omega^2}\left[\sum_{n \geq 0} (n+1)\frac{z^n}{\omega^n} - 1\right]$$

$$= \frac{1}{\omega^2} \sum_{n \geq 1} (n+1)\frac{z^n}{\omega^n}$$

So,

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \sum_{n \geq 1} (n+1) \frac{z^n}{\omega^{n+2}}$$

$$= \frac{1}{z^2} + \sum_{n \geq 1} (n+1) z^n \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^{n+2}}$$

$$= \frac{1}{z^2} + \sum_{n \geq 1} (n+1) z^n G_{n+2}$$

Eisenstein series

$$= \frac{1}{z^2} + 3 G_4 z^2 + 5 G_6 z^4 + \cdots$$

So, $\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20 G_6 z^3 + \cdots$

$$\Rightarrow \quad \wp^3(z) = \frac{1}{z^6} + 9G_4 \frac{1}{z^2} + 15 G_6 + \cdots$$

$$\wp'^2(z) = \frac{4}{z^6} - 24 G_4 \frac{1}{z^2} - 80 G_6 + \cdots$$

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

$$= c_1 z + c_2 z^2 + \cdots$$

LHS is a doubly periodic function with lattice L and has no poles inside F.

Also, LHS does not have a pole at $z=0$.

$\Rightarrow$ LHS has no poles.

$\Rightarrow$ LHS = const

$\Rightarrow$ LHS $= 0$

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

Let $\Phi(z) = (\wp(z), \wp'(z))$.

Then Φ maps the torus $\mathbb{C}/L$ to

Elliptic curve $y^2 = 4x^3 - 60\,G_4 x - 140\,G_6$.

It can be shown that Φ is a group

isomorphism too.

<u>Theorem</u>: For any elliptic curve E over $\mathbb{C}$,

there is a lattice L such that

$\Phi : \mathbb{C}/L \to E(\mathbb{C})$ is a group isomorphism.