

In the previous chapter we have seen that

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and} \\ f_n(x) \equiv 0 \pmod{p} \text{ has an integer solution} \end{cases}$$

The key ingredient are the polynomials  $f_n$  which we know are the minimal polynomials of the primitive elements of the ring class field of  $\mathbb{Z}[\sqrt{-n}]$ . But how can we find these primitive elements.

**DEFINITION** WE DEFINE A LATTICE TO BE AN ADDITIVE SUBGROUP  $\Lambda \subseteq \mathbb{C}$  GENERATED BY TWO COMPLEX NUMBERS  $w_1$  AND  $w_2$  LINEARLY INDEPENDENT OVER  $\mathbb{R}$

WE SAY THAT TWO LATTICES ARE HOMOTHEIC IF AND ONLY IF THERE EXISTS AN ELEMENT  $c \in \mathbb{C}^\times$  SUCH THAT  $\Lambda_1 = c\Lambda_2$ . WE WILL WORK OF  $\Lambda$  ONLY UP TO HOMOTHEITY. THUS, WE CAN NORMALIZE AND GET

$$\frac{1}{w_2} \Lambda = \frac{w_1}{w_2} \mathbb{Z} + \mathbb{Z}$$

USUALLY WE CHOOSE A POSITIVE ORIENTATION, I.E.,  $\text{Im}(w_1/w_2) > 0$  WHICH SUGGESTS LOOKING AT THE UPPER HALF PLANE  $\mathcal{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$

WE GET A SURJECTIVE MAP  $\mathcal{H} \xrightarrow{\quad} \mathbb{L}/\mathbb{C}^\times$ . HOWEVER THIS IS NOT INJECTIVE

**Lemma**  $\forall a, b, c, d \in \mathbb{R}, z \in \mathbb{C} \setminus \mathbb{R}$ , THEN  $\text{Im}\left(\frac{az+b}{cz+d}\right) = \frac{(ad-bc)}{|cz+d|^2} \text{Im}(z)$

**Proof**  $\frac{az+b}{cz+d} = \frac{(ac|z|^2 + (ad+bc)s + bd) + (ad-bc)t i}{|cz+d|^2}$   $z = s+it$

THE AMBIGUITY IN ASSOCIATING  $az$  TO A LATTICE LIES IN CHOOSING AN ORIENTED BASIS FOR  $\Lambda$ . SUPPOSE

$$\mathbb{Z}w_1 + \mathbb{Z}w_2 = \mathbb{Z}w'_1 + \mathbb{Z}w'_2$$

THEN  $\exists a, b, c, d, a', b', c', d' \in \mathbb{Z}$ :

$$\begin{cases} w'_1 = aw_1 + bw_2 \\ w'_2 = cw_1 + dw_2 \end{cases} \quad \begin{cases} w_1 = a'w'_1 + b'w'_2 \\ w_2 = c'w'_1 + d'w'_2 \end{cases}$$

AND CLEARLY  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . FURTHER,

$$0 < \text{Im}\left(\frac{w'_1}{w'_2}\right) = \text{Im}\left(\frac{aw_1 + bw_2}{cw_1 + dw_2}\right) \underset{z = \frac{w'_1}{w'_2}}{\uparrow} = \text{Im}\left(\frac{az+b}{cz+d}\right) = \frac{(ad-bc)}{|cz+d|^2} \text{Im}(z) \Rightarrow \text{Im}(z) > 0$$

IN OTHER WORDS,  $\Gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) = \{T \in M_2(\mathbb{Z}) \mid \det T = 1\}$

Lemma (Binet) (i) TWO ORIENTED BASIS FOR  $\Delta$  LATTICE  $\Lambda$  ARE RELATED BY A MATRIX IN  $SL_2(\mathbb{Z})$

(ii)  $\Lambda_{z_1}$  IS HOMOTHECTIC TO  $\Lambda_{z_2} \Leftrightarrow \exists T \in SL_2(\mathbb{Z})$  S.T. THAT  $z_2 = T \cdot z_1 = (az_1 + b) / (cz_1 + d)$

(iii)  $\forall \Lambda \in \mathcal{L} \exists z \in \mathcal{H} : \Lambda$  IS HOMOTHECTIC TO  $\Lambda_z$

we can therefore define an action of  $SL_2(\mathbb{Z})$  on  $\mathcal{H}$  and obtain a bijection

$$SL_2(\mathbb{Z}) \backslash \mathcal{H} \longleftrightarrow \mathcal{L} / \mathbb{C}^\times$$

Definition  $\Gamma(1) = SL_2(\mathbb{Z}) / \{\pm I\}$

Corollary  $\Gamma(1)$  ACTS FAITHFULLY ON  $\mathcal{H}$

we note that  $\Gamma(1)$  CAN BE GENERATED BY TWO IMPORTANT ELEMENTS

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \Gamma(1) = \langle S, T \mid S^2 = (ST)^3 = 1 \rangle$$

$$z \mapsto -1/z \quad z \mapsto z+1$$

Definition AN ELLIPTIC FUNCTION FOR  $\Lambda$  IS A FUNCTION  $f: \mathbb{C} \rightarrow \mathbb{C}$  S.T. THAT

1.  $f$  IS MEROMORPHIC ON  $\mathbb{C}$  (holomorphic on  $\mathbb{C} \setminus \{\text{discrete set of pts}\}$ )
2.  $f(z+w) = f(z) \quad \forall w \in \Lambda$

THUS, AN ELLIPTIC FUNCTION IS A DOUBLY PERIODIC MEROMORPHIC FUNCTION

there are two complex numbers  $w_1, w_2$  such that

$$f(z+w_1) = f(z+w_2) = f(z) \quad \forall z \in \mathbb{C}$$

WEIERSTRASS  $\wp$ -FUNCTION

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Lambda \setminus \{0\}} \left( \frac{1}{(z-w)^2} + \frac{1}{w^2} \right)$$

Theorem I.  $\wp(z)$  IS AN ELLIPTIC FUNCTION FOR  $\Lambda$  WITH DOUBLE POLES ON  $\Lambda$

II.  $\wp(z)$  SATISFIES  $\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$   
 WHERE  $g_2(\Lambda) = 60 \sum_{w \in \Lambda \setminus \{0\}} \frac{1}{w^4}$   $g_3(\Lambda) = 140 \sum_{w \in \Lambda \setminus \{0\}} \frac{1}{w^6}$

III.  $\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4} \left( \frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2$   
 $\forall z, w \notin \Lambda$  S.T.  $z+w \notin \Lambda$

Lemma  $G_r(\Lambda) = \sum_{w \in \Lambda \setminus \{0\}} \frac{1}{|w|^r}$  CONVERGES ABSOLUTELY  $\forall r \geq 3$

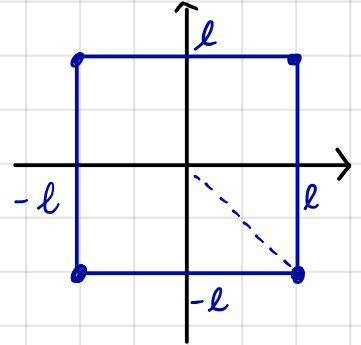
Proof LET  $w_1, w_2$  BE  $\Delta$  BASIS FOR  $\Lambda$ . FOR  $l \in \mathbb{Z}_{\geq 1}$   
 $P(l) = \{a_1 w_1 + a_2 w_2 \mid a_i \in \mathbb{Z}, \max_{i=1,2} |a_i| = l\}$

$$\#P(l) = 8l$$

$$\text{dist}(0, P(l)) \geq l \cdot \frac{\text{dist}(0, P(1))}{\delta}$$

$$\sum_{w \in P(l) \cap \Lambda} \frac{1}{|w|^r} \leq \frac{8l}{\delta^r l^r}$$

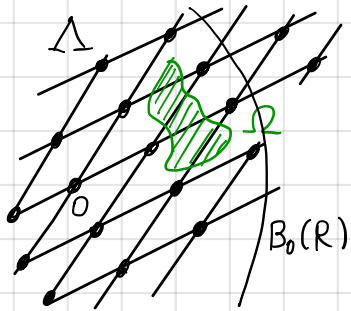
$$\sum_{w \in \Lambda \setminus \{0\}} \frac{1}{|w|^r} \leq \sum_{l=1}^{\infty} \frac{8l}{\delta^r l^r} = \frac{8}{\delta^r} \sum_{l=1}^{\infty} \frac{1}{l^{r-1}} < \infty$$



Remark Observe  $G_{2k+1}(\Lambda) = 0$

Proof of Theorem 1.  $\wp(z)$  IS HOLOMORPHIC OUTSIDE  $\Lambda$

We need to show that its series converges absolutely and uniformly in compact sets  $\Omega$



$$R \in \mathbb{R} : |z| \leq R \quad \forall z \in \Omega$$

$$z \in \Omega \quad w \in \Lambda \quad \text{we suppose } 2R \leq |w| \Rightarrow |z-w| \geq \frac{|w|}{2}$$

$$\left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| = \left| \frac{z(2w-z)}{w^2(z-w)^2} \right| \leq \frac{R(2|w| + \frac{1}{2}|w|)}{|w|^2 (\frac{1}{2}|w|^2)} = \frac{5R}{|w|^3}$$

$$\text{THUS } \sum_{w \in \Lambda \setminus \{0\}} \left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| \leq 5R \sum_{w \in \Lambda \setminus \{0\}} \frac{1}{|w|^3} < \infty$$

$\wp$  CONVERGES ABSOLUTELY AND UNIFORMLY.

$$\wp'(z) = -2 \sum_{w \in \Lambda} \frac{1}{(z-w)^3}$$

As above, this series converges and it is an elliptic function as well

SINCE  $\wp'$  IS PERIODIC,  
 $\wp(z)$  AND  $\wp(z+w)$  HAVE THE SAME DERIVATIVE AND SO

$$\wp(z+w) = \wp(z) + C$$

evaluating at  $-\frac{w}{2}$

$$\wp\left(\frac{w}{2}\right) = \wp\left(-\frac{w}{2}\right) + C, \quad \text{BUT } \wp \text{ IS EVEN } \Rightarrow C = 0$$

Lemma THE LAURENT SERIES FOR  $\wp(z)$  AROUND  $z=0$  IS

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

Proof For  $k > 1$   $|z| < |w|$

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \frac{1}{w^2} \left( \frac{1}{\left(1 - \frac{z}{w}\right)^2} - 1 \right) \stackrel{\Delta \text{ AROUND } 1}{=} \frac{1}{w^2} \sum_{n \geq 1} (n+1) \frac{z^n}{w^n}$$

$$\wp(z) = \frac{1}{z^2} + \sum_{n \geq 1} \sum_{w \in \Delta \setminus \{0\}} (n+1) \frac{z^n}{w^{2n+2}} = \frac{1}{z^2} + \sum_{n \geq 1} (n+1) G_{n+2} z^n$$

We observe that  $G_{2n+1} = 0$ . then

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{+\infty} (2n+1) G_{2n+2} z^{2n} = \cancel{\frac{1}{z^2}} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \dots$$

$$\wp'(z) = -\frac{2}{z^3} + \sum_{n=1}^{+\infty} 2n(2n+1) G_{2n+2} z^{2n-1} = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + \dots$$

$$\wp(z)^3 = \cancel{\frac{1}{z^6}} + \cancel{9G_4} \cancel{\frac{1}{z^2}} + \cancel{15G_6} + 21G_8 z^2 + \dots$$

$$\wp'(z)^2 = \cancel{\frac{4}{z^6}} - \cancel{24G_4} \cancel{\frac{1}{z^2}} - \cancel{80G_6} - 168G_8 z^2 + \dots$$

$$\wp''(z) = \frac{6}{z^4} + \sum_{n=1}^{+\infty} (2n-1) 2n(2n+1) G_{2n+2} z^{2n-2} = \frac{6}{z^4} + 6G_4 + 60G_6 z^2 + 210G_8 z^4 + \dots$$

$$\wp'(z)^2 = \frac{1}{z^4} + 6G_4 + 10G_6 z^2 + (9G_4 + 14G_8) z^4 + \dots$$

And we may guess that

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

We define  $f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4 \wp(z) - 140G_6$

IT IS EASY TO SEE THAT  $f(0) = 0$  AND  $f(w) = 0 \forall w \in \Delta$  FOR THE PERIODICITY. SINCE  $f$  IS HOLOMORPHIC  $\Rightarrow f$  IS CONSTANT  $\Rightarrow f = 0$

Theorem THE FIELD OF DOUBLY PERIODIC MEROMORPHIC FUNCTIONS FOR  $\Delta$  IS  $\mathbb{C}(\wp, \wp')$  AND WE HAVE AN ISOMORPHISM

$$\frac{\mathbb{C}[x, y]}{(y^2 - 4x^3 + g_4 x + g_6)} \xrightarrow{\sim} \mathbb{C}[\wp, \wp']$$

example  $\wp''(z) = 6\wp'(z)^2 - 30G_4$



Lemma EACH  $G_{2n}$  IS A POLYNOMIAL IN  $G_4$  AND  $G_6$  WITH RATIONAL COEFFICIENTS

Proof BY INDUCTION

•  $G_8 = \frac{3}{7} G_4^2$  From  $\wp''(z) = 6\wp(z)^2 - 30G_4$

• SUPPOSE IT TRUE FOR  $G_{2h} \forall h \leq n$

Observe that the coefficient of  $z^{2n-2}$  in  $\wp''(z)$  is

$$(2h-1)2n(2h+1)G_{2n+2}$$

and in  $6\wp(z)^2$  is a rational polynomial in  $G_{2h} \quad h=2, \dots, n+1$

$$(2h+1)2n(2h-1)G_{2n+2} = 6P(G_4, \dots, G_{2n+2})$$

Notice that the coefficient of  $G_{2n+2}$  in the polynomial is

$$2(2n+1) - \text{DOUBLE PRODUCT BETWEEN } (2h+1)G_{2h+2} \text{ AND } \frac{1}{z^2}$$

$$\Rightarrow \underbrace{(2n+1)2n(2h-1) - 12(2n+1)}_{\neq 0 \forall n \geq 2} G_{2n+2} = 6P(G_4, \dots, G_{2n})$$

Theorem  $\Delta_t = \pi\mathbb{Z} + it\mathbb{Z}$  WHERE  $t \in \mathbb{R}$

$$\lim_{t \rightarrow +\infty} G_{2n}(\Delta_t) = 2 \frac{\zeta(2n)}{\pi^{2n}}$$

Proof  $G_{2n}(\Delta_t) = \sum_{w \in \Delta_t \setminus \{0\}} \frac{1}{w^{2n}} = \sum_{(z_1, z_2) \in \mathbb{Z}^2 \setminus \{0\}} \frac{1}{(z_1 + \pi + z_2 ti)^{2n}}$

$$= \sum_{z_1 \in \mathbb{Z} \setminus \{0\}} \frac{1}{(z_1, \pi)^{2n}} + \sum_{\substack{z_2 \in \mathbb{Z} \\ z_1 \in \mathbb{Z} \setminus \{0\}}} \frac{1}{(z_1 + \pi + z_2 ti)^{2n}} = 2 \sum_{z \geq 1} \frac{1}{(z, \pi)^{2n}} + \dots$$

$= 2 \frac{\zeta(2n)}{\pi^{2n}} + \dots$  and now taking the limit we cancel the second term. notice that we can switch the limit and the sum because the normal convergence of  $G_{2n}$ .

Corollary  $\zeta(2n)/\pi^{2n} \in \mathbb{Q} \quad \forall n \geq 1$

Proof WE PROVE FIRST THE CASE  $n=1, 2, 3$

It can be proved that  $\sin(\pi z) = \pi z \prod_{n=1}^{+\infty} \left(1 - \frac{z^2}{n^2}\right) = \pi z - \frac{\pi z^3}{3!} \zeta(2) + \dots$

on the other hand

$$\sin(\pi z) = \sum_{n=1}^{+\infty} \frac{(-1)^{n+1} (\pi z)^{2n-1}}{(2n-1)!} = \pi z - \frac{(\pi z)^3}{3!} + \dots$$

COMPARING COEFFICIENTS OF  $z^3$ :

$$\pi \zeta(2) = \frac{\pi^3}{6} \Rightarrow \zeta(2) = \frac{\pi^2}{6}$$

SOME THING FOR  $\zeta(4) = \frac{\pi^4}{90}$  AND  $\zeta(6) = \frac{\pi^6}{945}$

$$\begin{aligned} \text{NOW } \frac{2\zeta(2n)}{\pi^{2n}} &= \lim_{t \rightarrow +\infty} G_{2n}(\Lambda_t) = \lim_{t \rightarrow +\infty} P(G_2(\Lambda_t), G_4(\Lambda_t)) \\ &= P(\lim_{t \rightarrow +\infty} G_2(\Lambda_t), \lim_{t \rightarrow +\infty} G_4(\Lambda_t)) = P\left(\frac{2\zeta(4)}{\pi^4}, \frac{2\zeta(6)}{\pi^6}\right) \\ &= P\left(\frac{2}{90}, \frac{2}{945}\right) \in \mathbb{Q} \text{ SINCE } P \text{ IS RATIONAL.} \end{aligned}$$

II APPROACH IT RELIES ON THE FOLLOWING FUNCTIONAL EQUATION FOR  $\zeta$

$$\begin{aligned} \zeta(z) &= 2(2\pi)^{z-1} \Gamma(1-z) \zeta(1-z) \sin \frac{\pi z}{2} \\ \zeta(1-z) &= 2(2\pi)^{-z} \Gamma(z) \zeta(z) \cos \frac{\pi z}{2} \end{aligned}$$

taking  $z = 2n$

$$\zeta(1-2n) = 2(2\pi)^{-2n} \Gamma(2n) \zeta(2n) \cos \frac{2\pi n}{2}$$

$$2^{2n} \zeta(1-2n) = \frac{2\zeta(2n)}{\pi^{2n}} \underbrace{\Gamma(2n)}_{\text{recall } \Gamma(n+1) = n! \forall n \in \mathbb{Z}_{>0}} \cos \pi n$$

$$\frac{\zeta(2n)}{\pi^{2n}} = \frac{2^{2n-1}}{(2n-1)! \cos(\pi n)} \zeta(1-2n)$$

Now we know that  $\zeta(-n) = -\frac{B_{n+1}}{n+1} \forall n \in \mathbb{Z}_{>0}$   
where  $B_n$  are Bernoulli's Numbers

$$B_n = \sum_{k=0}^n \binom{n}{k} B_k \quad B_0 = 1$$

$$\Rightarrow \zeta(1-2n) \in \mathbb{Q}$$

Remark

IT CAN BE PROVEN THAT

$$G_{2k}(z) = 2\zeta(2k) + \frac{2(2\pi i)^k}{(2k-1)!} \sum_{n=1}^{\infty} \frac{\sum_{d|n} d^{2k-1}}{b_{2k-1}(n)} q^n \quad q = e^{2\pi i z}$$

Weierstrass  $\zeta$ -function

As can be seen from the Laurent expansion of the Weierstrass  $\zeta$ -function, it has double poles with vanishing residues at the points of  $\Lambda \Rightarrow$  we can integrate

Theorem  $\zeta(z, \Lambda) = \frac{1}{z} + \sum_{w \in \Lambda \setminus \{0\}} \left( \frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} \right)$  IS AN

ABSOLUTELY AND UNIFORMLY CONVERGENT SERIES ON COMPACT SUBSETS OF  $\mathbb{C} \setminus \Lambda$  AND

I.  $\frac{d}{dz} \zeta(z) = -\wp(z)$

II.  $\zeta(z+w) = \zeta(z) + \eta(w)$  where  $\eta: \Lambda \rightarrow \mathbb{C}$  IS A HOMO MORPHISM

III.  $\zeta(\eta^{-1}(1)) = \zeta(z) + 2\pi i$

IV.  $\int \wp(z)^2 dz = \frac{1}{6} \wp'(z) + 5G_4 z + C$

$\int \wp(z)^3 dz = \frac{1}{120} \wp'''(z) - 9G_4 \zeta(z) + 14G_6 z + C$

WHERE  $\eta$  IS CALLED THE QUASI-PERIOD OF  $\zeta$  AND IT MEASURES THE FAILURE OF  $\zeta$  TO BE AN ELLIPTIC FUNCTION.

Notice that  $\eta$  encodes the periods of differentials of  $E_\Lambda$  when paired with a basis of the singular homology (later more details)

AROUND 0  $\zeta(z) = \frac{1}{z} - \sum_{n \geq 1} G_{2n+2} z^{2n+1}$

Weierstrass  $\sigma$ -function

$$\sigma(z) = z \prod_{w \in \Lambda \setminus \{0\}} \left( 1 - \frac{z}{w} \right) \exp \left( \frac{z}{w} + \frac{z^2}{2w^2} \right)$$

Theorem THIS INFINITE PRODUCT CONVERGES ABSOLUTELY TO A HOLONORPHIC FUNCTION ON  $\mathbb{C}$  WITH SIMPLE ZEROS ON  $\Lambda$  AND NO ZEROS ELSEWHERE

$$\sigma(z+w) = \sigma(z) \cdot \psi(w) \cdot \exp \left( \eta(w) \left( z + \frac{w}{2} \right) \right)$$

where 
$$\psi(w) = \begin{cases} 1 & w \in 2\Lambda \\ -1 & \text{otherwise} \end{cases}$$

Theorem  $d \log \sigma(z) = \zeta(z)$  logarithmic derivative

$$\wp(z_1) - \wp(z_2) = \frac{\sigma(z_1+z_2) \sigma(z_1-z_2)}{\sigma(z_1)^2 \sigma(z_2)^2}$$

# j-function

Remark If  $F$  is an elliptic function for  $\Lambda \Rightarrow F(\lambda^{-1}z)$  is an elliptic function for  $\lambda\Lambda$

$$\wp(\lambda z, \lambda\Lambda) = \frac{1}{\lambda^2 z^2} + \sum_{w \in \Lambda \setminus \{0\}} \left( \frac{1}{(\lambda z - \lambda w)^2} - \frac{1}{\lambda^2 w^2} \right) = \lambda^{-2} \wp(z, \Lambda)$$

Definition GIVEN  $\Lambda$ , WE WRITE  $\Delta(\Lambda) = g_2^3 - 27g_3^2$ . THIS IS CLOSELY RELATED TO THE DISCRIMINANT OF THE CUBIC POLYNOMIAL THAT APPEARS IN THE DIFFERENTIAL EQUATION FOR  $\wp$ .

IF  $e_1, e_2, e_3$  ARE ROOTS OF SUCH A POLYNOMIAL,

$$\Delta(\Lambda) = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2$$

$$\begin{aligned} \hookrightarrow e_1 &= \wp\left(\frac{\omega_1}{2}\right) & e_2 &= \wp\left(\frac{\omega_2}{2}\right) \\ e_3 &= \wp\left(\frac{\omega_1 + \omega_2}{2}\right) \end{aligned}$$

Proposition FOR A LATTICE  $\Lambda$ ,  $\Delta(\Lambda) \neq 0$ .

WE DEFINE THE j-INVARIANT OF A LATTICE IS

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}$$

Nice fact about j-invariant is that it characterizes lattices up to homothety:

Theorem IF  $\Lambda$  AND  $\Lambda'$  ARE TWO LATTICES IN  $\mathbb{C}$ , THEN  $j(\Lambda) = j(\Lambda') \Leftrightarrow \Lambda \sim \Lambda'$

Remark  $\Delta(\tau \cdot z) = (cz+d)^6 \Delta(z) \quad \forall$  any  $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$   
in fact  $g_2(\tau \cdot z) = (cz+d)^4 g_2(z)$   
 $g_3(\tau \cdot z) = (cz+d)^6 g_3(z)$

There is another definition for the j-invariant. We'll present it here since j-invariant plays a central role.

WE FIRST DEFINE THE DEDEKIND  $\eta$ -FUNCTION

$$\tau \in \mathcal{H} \quad \eta(\tau) = q^{\frac{1}{24}} \prod_{n \geq 1} (1 - q^n)$$

THIS FUNCTION SATISFIES  $\eta(\tau+1) = \zeta_{24} \eta(\tau) \quad \eta\left(-\frac{1}{\tau}\right) = \sqrt{-i\tau} \eta(\tau)$

where we choose the branch of the square root which is positive on the positive real axis.

THEN THE MODULAR DISCRIMINANT  $\Delta(z) = \eta(z)^{24}$  IS NOW CLEARLY A MODULAR FORM OF WEIGHT 12 ON  $SL_2(\mathbb{Z})$   
 WE DEFINE THE  $j$ -INVARIANT TO BE

$$j(z) = \frac{E_4^3(z)}{\Delta(z)}$$

$E_4(q) = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n$        $\sigma_3(n) = \sum_{d|n} d^3$   
 $\downarrow$   
 Normalized Eisenstein series. THE  $j$ -INVARIANT HAS FOURIER EXPANSION

$$j(q) = \frac{1}{q} \left( 1 + 240 \sum_{n \geq 1} n^3 \frac{q^n}{1 - q^n} \right) \prod_{n \geq 1} (1 - q^n)^{24} = \frac{1}{q} + \frac{744 + 196884q}{+ 21493760q^2}$$

Clearly  $j(z)$  is a holomorphic function on  $\mathcal{H}$  having meromorphic continuation to the cusps and it is  $SL_2(\mathbb{Z})$ -invariant. However,  $j$  is not an algebraic function in the sense that  $\exists \alpha \in \mathbb{C} \setminus \{0, 1\}, j(z)^\alpha \neq j(z^\alpha)$

## Weber Function

THE MODULAR DISCRIMINANT DOES NOT VANISH ON THE UPPER HALF PLANE, SO WE MAY CHOOSE A HOLOMORPHIC CUBIC ROOT WHICH IS REAL VALUED ALLOWING US TO DEFINE

$$\gamma_2(q) = \frac{E_4(q)}{\Delta(q)^{1/3}}$$

WHICH IS HOLOMORPHIC ON  $\mathcal{H}$  AND HAS TRANSFORMATION PROPERTIES

$$\begin{cases} \gamma_2(z+1) = \zeta_3^2 \gamma_2(z) \\ \gamma_2(-\frac{1}{z}) = \gamma_2(z) \end{cases}$$

BY INDUCTION  $\gamma_2\left(\frac{az+b}{cz+d}\right) = \zeta_3^{ac-bd+a^2cd-cd} \gamma_2(z)$

From this we see that  $\gamma_2$  is a modular function for the congruence subgroup:

$$\Gamma_0^1(3)^+ = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{array}{l} a \equiv d \equiv 0 \pmod{3} \text{ OR} \\ c \equiv b \equiv 0 \pmod{3} \end{array} \right\}$$



Now we can define Weber functions

$$f(z) = \zeta_{48}^{-1} \frac{\eta(\frac{z+1}{2})}{\eta(z)} = q^{-\frac{1}{48}} \prod_{n \geq 1} (1 + q^{n-\frac{1}{2}})$$

$$f_1(z) = \frac{\eta(\frac{z}{2})}{\eta(z)} = q^{-\frac{1}{48}} \prod_{n \geq 1} (1 - q^{n-\frac{1}{2}})$$

$$f_2(z) = \sqrt{2} \frac{\eta(2z)}{\eta(z)} = \sqrt{2} q^{\frac{1}{24}} \prod_{n \geq 1} (1 + q^n)$$

THESE FUNCTIONS SATISFY MANY INTERESTING IDENTITIES

$$f_1(2z) f_2(z) = f(z) f_1(z) f_2(z) = \sqrt{2}$$

The definition of Weber functions may seem quite unnatural at a first glance but these functions arise organically when studying the 2-torsion on the universal elliptic curve over  $\mathbb{C}$ .

Theorem LET  $e_1 = \wp_z(\frac{z}{2})$ ,  $e_2 = \wp_z(\frac{1}{2})$ ,  $e_3 = \wp_z(\frac{1+z}{2})$ , THEN

$$\begin{cases} e_2 - e_1 = \pi^2 \eta(z)^4 f(z)^8 \\ e_2 - e_3 = \pi^2 \eta(z)^4 f_1(z)^8 \\ e_3 - e_1 = \pi^2 \eta(z)^4 f_2(z)^8 \end{cases}$$

Corollary 
$$\chi_2(z) = \frac{f(z)^{24} - 16}{f(z)^8} = \frac{f_1(z)^{24} + 16}{f_1(z)^8} = \frac{f_2(z)^{24} + 16}{f_1(z)^8}$$

Corollary 
$$\begin{aligned} f(z+1) &= \zeta_{48}^{-1} f(z) & f(-1/2) &= f(z) \\ f_1(z+1) &= \zeta_{48}^{-1} f_1(z) & f_1(-1/2) &= f_2(z) \\ f_2(z+1) &= \zeta_{24} f_2(z) & f_2(-1/2) &= f_1(z) \end{aligned}$$

It follows that  $f^6$  is a modular function for the congruence sub.

$$\Gamma_0^0(8) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid b \equiv c \equiv 0 \pmod{8} \right\}$$

whereas  $f_2$  is a modular function for  $\Gamma(24)$

### Geometric Interpretation

We saw before that there exists an isomorphism

$$\begin{array}{ccc} \mathbb{C}/\Delta_z & \xrightarrow{\quad} & E_z \\ z & \xrightarrow{\quad} & (\wp : \wp' : 1) \end{array}$$

This map describes how the algebraic description, as a curve with Weierstrass equation connects to the complex analytic description

$$E_L = \mathbb{C}/\Lambda_L$$

THIS ALSO SHOWS THAT THE STANDARD BASIS  $H_{\text{DR}}^1(E_L/\mathbb{C}) = \langle \frac{dx}{y}, x \frac{dx}{y} \rangle$  ADMITS A SIMPLE DESCRIPTION ON THE ANALYTIC SIDE AS  $dz, \wp dz$ .

Given an element  $w \in \Lambda_L$  we obtain a corresponding element in the singular homology by considering the image of a path from 0 to  $w$  in  $\mathbb{C}$

$$\begin{array}{ccc} \Lambda_L & \xrightarrow{\quad} & H_1(E|\mathbb{C}) \\ w & \xrightarrow{\quad} & [\gamma_w^0] \end{array}$$

The Seinfeld duality pairing may now be computed by calculating the line integrals

$$\int_0^1 dz = 1 \quad \int_0^L dz = L \quad \text{and} \quad \int_0^1 \wp(z) dz \quad \int_0^L \wp(z) dz$$

The Weierstrass  $\zeta$ -function provides us with a primitive for  $\wp(z) dz$  as  $\zeta'(z) = -\wp(z)$ , so we see that the periods are described precisely by the failure of  $\zeta$  to be elliptic and are encoded in the quasi-period map.

Similarly, the Weierstrass  $\sigma$ -function is related to differentials of the III kind.

## COMPLEX MULTIPLICATION

WE RECALL THAT ORDERS IN QUADRATIC FIELDS GIVE RISE TO CLASS OF LATTICES

$\Omega =$  proper fractional  $\mathcal{O}$ -ideal.

$$\Omega = [\alpha, \beta] \text{ SOME } \alpha, \beta \in K$$

NOW WE REGARD  $K$  AS A SUBSET OF  $\mathbb{C}$ :  $K \hookrightarrow \mathbb{C} \Rightarrow [\alpha, \beta]$  GIVES RISE TO  $\Lambda = \alpha\mathbb{Z} + \beta\mathbb{Z}$  SINCE  $\alpha$  AND  $\beta$  ARE INDEPENDENT OVER  $\mathbb{R}$ .

THEN WE DEFINE THE  $j$ -INVARIANT

$$j(\Omega) = j(\Lambda_\Omega)$$

Recall  $\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4} \left( \frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2$

IF  $z = w$   $\wp(2z) = -2\wp(z) + \frac{1}{4} \left( \frac{\wp''(z)}{\wp'(z)} \right)^2$

Recall  $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$   
 $\wp''(z) = 6\wp(z)^2 - \frac{g_2}{2}$

$$\text{THUS } \wp(2z) = -2\wp(z) + \frac{(12\wp(z)^2 - g_2)^2}{16(4\wp(z)^3 - g_2\wp(z) - g_3)}$$

BY INDUCTION  $\wp(nz)$  IS A RATIONAL FUNCTION IN  $\wp(z)$  FOR ALL  $n$

Theorem LET  $\Lambda$  BE A LATTICE. THEN FOR ALL  $\alpha \in \mathbb{C} \setminus \mathbb{Z}$  THE FOLLOWING STATEMENTS ARE EQUIVALENT

- I.  $\wp(\alpha z)$  IS A RATIONAL FUNCTION IN  $\wp(z)$
- II.  $\alpha\Lambda \subset \Lambda$
- III.  $\exists \mathcal{O} \subseteq K$  IMAGINARY QUADRATIC FIELD SUCH THAT  $\alpha \in \mathcal{O}$  AND  $\Lambda$  IS HOMOTHETIC TO A PROPER FRACTIONAL  $\mathcal{O}$ -IDEAL.

FURTHER, IF THESE CONDITIONS ARE SATISFIED THEN

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))} \quad \text{WITH } A(x) \text{ AND } B(x)$$

RELATIVELY PRIME POLYNOMIALS SUCH THAT  
 $\deg A = \deg B + 1 = [\Lambda : \alpha\Lambda] = N(\alpha)$

This theorem shows that if an elliptic function has multiplication by some  $\alpha \in \mathbb{C}$ , then it has multiplication by an entire order  $\mathcal{O} \subset K$ .

Remark WE CAN RELATE HOMOTHETY CLASSES OF LATTICES WITH IDEAL CLASSES  
 Fix  $\mathcal{O}$  and choose  $\Lambda \in \mathbb{C}$  such that  $\mathcal{O} = \text{pulling of complex multiplication of } \Lambda$   
 $\Lambda$  IS A PROPER FRACTIONAL  $\mathcal{O}$ -IDEAL AND CONVERSELY, ANY PROPER FRACTIONAL  $\mathcal{O}$ -IDEAL IS A LATTICE WITH CM BY  $\mathcal{O}$

TWO PROPER FRACTIONAL  $\mathcal{O}$ -IDEALS ARE HOMOTHETIC AS LATTICES IF AND ONLY IF THEY ARE IN THE SAME EQUIVALENCE CLASS IN  $\mathcal{C}(\mathcal{O})$

Corollary THERE IS A BIJECTION

$$\mathcal{C}(\mathcal{O}) \longleftrightarrow \left\{ \begin{array}{l} \text{homothety classes} \\ \text{of lattices with cm by } \mathcal{O} \end{array} \right\}$$

example SUPPOSE  $\Lambda$  HAS COMPLEX MULTIPLICATION BY  $\sqrt{-3}$   
 $\Rightarrow \mathcal{O} \subset K$  CONTAINS  $\sqrt{-3} \Rightarrow \mathcal{O}$  IS EITHER  $\mathbb{Z}[\sqrt{-3}]$  OR  $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$   
 AND THEY BOTH HAVE CLASS NUMBER 1.

THEN THE ONLY LATTICES (UP TO HOMOTHETY) WITH COMPLEX MULTIPLICATION ON BY  $\sqrt{-3}$  ARE  $[1, \sqrt{-3}]$  AND  $[1, \frac{1+\sqrt{-3}}{2}]$

Question How does complex multiplication affect the  $j$ -invariant.

$$j(i) = j([1, i]) \quad \Delta = [1, i]$$

↳ only lattice, up to homothety with complex multiplication

$$g_3(i\Delta) = g_3(\Delta) = i^6 g_3(\Delta) = -g_3(\Delta) \Rightarrow g_3(\Delta) = 0$$

THEN  $j(i) = 1728$

SUPPOSE NOW  $\omega = \frac{1+\sqrt{-3}}{2}$ , THEN  $\bar{\omega} = \omega^2 = -1 - \omega$

$$G_{2k}(\Delta) = \sum_{\substack{h, m \in \mathbb{Z} \\ (h, m) \neq (0, 0)}} \frac{1}{(h + m\bar{\omega})^{2k}} \stackrel{\downarrow}{=} \sum_{\substack{h, m \in \mathbb{Z} \\ (h, m) \neq (0, 0)}} \frac{1}{(n - (1+\omega)m)^{2k}}$$

$$= \sum_{\substack{h, m \in \mathbb{Z} \\ (h, m) \neq (0, 0)}} \frac{1}{((n-m) - \omega m)^{2k}} \quad \uparrow \text{ } m, n \text{ runs over all } \mathbb{Z}$$

THUS  $G_{2k}(\Delta) \in \mathbb{R} \Rightarrow G_4 \in \mathbb{R}$ . NOW

$$\omega G_4 = \sum_{\substack{h, m \in \mathbb{Z} \\ (h, m) \neq (0, 0)}} \frac{\omega}{(h + m\omega)^4} = \sum_{\substack{h, m \in \mathbb{Z} \\ (h, m) \neq (0, 0)}} \left( \frac{\omega}{h + \omega m} \right)^4 = \sum_{\substack{h, m \in \mathbb{Z} \\ (h, m) \neq (0, 0)}} \left( \frac{1}{\frac{n}{\omega} + m} \right)^4$$

$$= \sum_{\substack{h, m \in \mathbb{Z} \\ (h, m) \neq (0, 0)}} \frac{1}{(\bar{\omega}n + m)^4} = \bar{G}_4 = G_4 \Rightarrow (\omega - 1)G_4 = 0 \Rightarrow G_4 = 0$$

$$\Rightarrow g_4 = 0$$

THUS  $j(\omega) = 0$

Theorem ORDER IN QUADRATIC IMAGINARY FIELD

$\mathfrak{a}$  = PROPER FRACTIONAL  $\mathfrak{O}$ -IDEAL  $\Rightarrow j(\mathfrak{a})$  IS AN ALGEBRAIC NUMBER OF DEGREE AT MOST  $h(\mathfrak{O})$

Proof  $\wp(z, g_2, g_3) = \frac{1}{z^2} + \sum_{n \geq 1} a_n(g_2, g_3) z^{2n}$

By assumption  $\forall \alpha \in \mathfrak{O}, \wp(\alpha z, g_2, g_3) = \frac{\Delta(\wp(z, g_2, g_3))}{B(\wp(z, g_2, g_3))} \in \mathbb{C}((z))$

IN  $\mathbb{C}((z))$  elements are  $\sum_{n=-M}^{+\infty} b_n z^n$

ON THE OTHER HAND  $\wp(\alpha z, g_2, g_3) = \frac{1}{\alpha^2 z^2} + \sum_{n \geq 1} a_n(\alpha, g_2, g_3) \alpha^{2n} z^{2n}$

NOW FOR  $\sigma \in \text{Aut}(\mathbb{C})$

$$(*) \quad \wp(\sigma(\alpha)z, \sigma(g_2), \sigma(g_3)) = \frac{\Delta^\sigma(\wp(z), \sigma(g_2), \sigma(g_3))}{B^\sigma(\wp(z), \sigma(g_2), \sigma(g_3))}$$

SINCE  $g_2^3 - 27g_3^2 \neq 0 \Rightarrow \sigma(g_2)^3 - 27\sigma(g_3)^2 \neq 0$

We'll prove in the next talk that this condition guarantees the existence of a lattice  $\Lambda'$  such that

$$\begin{aligned} g_2(\Lambda') &= g_2' = \sigma(g_2) \\ g_3(\Lambda') &= g_3' = \sigma(g_3) \end{aligned}$$

NOW  $(*)$  IMPLIES THAT  $\Lambda'$  HAS CM BY  $\sigma(\alpha)$ . THEN  $\mathcal{O} = \sigma(\mathcal{O}) = \mathcal{O}'$

REPLACING  $\sigma$  WITH  $\sigma^{-1}$   $\mathcal{O} \subset \mathcal{O}' \subset \mathcal{O} \Rightarrow \mathcal{O} = \mathcal{O}'$ . LOOKING AT EQUATIONS FOR  $g_2, g_3$ , WE CONCLUDE  $j(\Lambda') = \sigma(j(\Lambda))$

SINCE  $\Lambda'$  HAS CM BY  $\mathcal{O}$  WE KNOW THAT THERE ARE ONLY  $h(\mathcal{O})$  POSSIBILITIES FOR  $j(\Lambda')$   $\Rightarrow$  ONLY  $h(\mathcal{O})$  POSSIBILITIES FOR  $\sigma(j(\Lambda))$

SINCE THIS IS TRUE FOR ALL  $\sigma \in \text{Aut}(\mathbb{C}) \Rightarrow j$  IS AN ALGEBRAIC NUMBER WITH DEGREE  $\leq h(\mathcal{O})$ .

exercise I WE KNOW  $j(\Lambda_1) = j(\Lambda_2) \Leftrightarrow \exists \alpha \in \mathbb{C}^\times: \alpha \Lambda_1 = \Lambda_2$   
SHOW THAT FOR AN ELLIPTIC CURVE  $E$  WITH LATTICE  $\Lambda$ ,  $E$  CAN BE DEFINED OVER  $\mathbb{R} \Leftrightarrow \exists \alpha \in \mathbb{C}^\times: \alpha \Lambda = \overline{\alpha \Lambda}$

exercise II LET  $E$  BE AN ELLIPTIC CURVE WITH CORRESPONDING LATTICE  $\Lambda = \overline{\Lambda}$   
SHOW THAT THERE IS A BASIS SUCH THAT  $\Lambda = \omega \mathbb{Z} + \tau \mathbb{Z}$   
WITH  $\omega \in \mathbb{R}$   $\text{Re}(\tau) = \frac{\omega}{2}$  OR  $\text{Re}(\tau) = 0$

BESIDES, SHOW THAT  $\text{Re}(\tau) = 0 \Leftrightarrow$  THE CUBIC POLYNOMIAL HAS THREE REAL ROOTS (THUS  $E[2] \subset \mathbb{R}$ )





OBSERVE THAT  $q_{\frac{1}{2}} = e^{2\pi i \frac{1}{2}} = e^{\pi i} = -1$ ,  $q_{\frac{1}{2}} = e^{\pi i z} = q_z^{\frac{1}{2}}$ ,  $q_{\frac{1}{2}} = -q_z^{\frac{1}{2}}$ , THUS

$$\text{den} = [(2\pi i)^{-3} e^{\frac{1}{4} \eta(1)[z^2+z+1] - \pi i - \pi i z} \cdot 2 \cdot (1 - q_z^{\frac{1}{2}})(1 + q_z^{\frac{1}{2}}) \cdot \prod_{n \geq 1} \frac{(1 + q_z^n)(1 + q_z^n)(1 - q_z^{n+\frac{1}{2}})(1 - q_z^{n-\frac{1}{2}})(1 + q_z^{n+\frac{1}{2}})(1 + q_z^{n-\frac{1}{2}})]^4 (1 - q_z^n)^6]$$

$$\Delta(q) = \cancel{16} (2\pi i)^{12} \frac{e^{\cancel{\eta(1)[z^2+z+1] - 4\pi i - 4\pi i z} - 2\pi i - 2\pi i z} \prod_{n \geq 1} (1 - q_z^n)^{24}}{\cancel{16} e^{\eta(1)[z^2+z+1] - 4\pi i - 4\pi i z} (1 - q_z)^4 \prod_{n \geq 1} (1 + q_z^n)^8 (1 - q_z^{2n+1})^4 (1 - q_z^{2n-1})^4}$$

$$= (2\pi i)^{12} \underbrace{e^{2\pi i z}}_{q_z} \frac{\prod_{n \geq 1} (1 - q_z^n)^{24}}{(1 - q_z)^4 \prod_{n \geq 1} (1 + q_z^n)^4 (1 - q_z^{2n+1})^4 (1 + q_z^n)^4 (1 - q_z^{2n-1})^4}$$

NOW

$$\prod_{n \geq 1} (1 - q_z^n)^2 \cdot \prod_{n \geq 1} (1 + q_z^n)^2 (1 - q_z^{2n+1}) (1 - q_z^{2n-1}) =$$

$$= \prod_{n \geq 1} (1 - q_z^{2n})^2 (1 - q_z^{2n+1}) (1 - q_z^{2n-1}) = (1 - q_z) (1 - q_z^2)^2 (1 - q_z^3) (1 - q_z^3)$$

$$(1 - q_z^4)^2 (1 - q_z^5) (1 - q_z^5) (1 - q_z^6) (1 - q_z^7) \dots$$

$$= \frac{\prod_{n \geq 1} (1 - q_z^n)^2}{(1 - q_z)} \quad \text{since odd exponents appear twice (except 1) and so do even exponents}$$

$$\Rightarrow \prod_{n \geq 1} (1 + q_z^n)^2 (1 - q_z^{2n+1}) (1 - q_z^{2n-1}) = \frac{1}{(1 - q_z)}$$

HENCE

$$\Delta(q) = (2\pi i)^{12} q_z \frac{\prod_{n \geq 1} (1 - q_z^n)^{24}}{(1 - q_z)^4 \left[ \frac{1}{(1 - q_z)} \right]^4} = (2\pi i)^{12} q_z \prod_{n \geq 1} (1 - q_z)^{24}$$