ASPECTS OF COMPLEX MULTIPLICATION

Contents

Date: August 29–October 14, 2000.

Notes by John Voight, jvoight@math.berkeley.edu, taken from a seminar taught by Don Zagier.

The following are notes taken from a seminar taught by Don Zagier at the University of California, Berkeley, in the Fall semester, 2000.

1. Preview

What follows is a preview of what these notes will cover; we defer proofs to the corresponding sections in the text.

Complex multiplication on elliptic curves over $\mathbb{C}$. Let

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots$$

be the modular j-function, where $\tau \in \mathfrak{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$ and $q = e^{2\pi i \tau}$. Then

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau) \text{ for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

If $\tau = u + iv$ and $u \in \mathbb{Q}$, $v^2 \in \mathbb{Q}$, then τ is an *CM point*. This is equivalent to the requirement that $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$. In fact, we will see that $j(\tau) \in \overline{\mathbb{Z}}$, i.e. $j(\tau)$ is an algebraic integer. For example, $j(i\sqrt{2}) = 8000$.

Associated to τ is a lattice $L_\tau = \mathbb{Z}\tau + \mathbb{Z}$, and hence an *elliptic curve* $E_\tau = \mathbb{C}/L_\tau$, and conversely. *$E$ has complex multiplication* iff $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$.

An *elliptic curve* E is a curve of genus $g = 1$ with a point $O \in E(\mathbb{C})$. The group law (with O as the identity) is unique, and conversely any curve with an abelian group law is elliptic. As a consequence of the Riemann-Roch theorem, such a curve can be given an affine model $y^2 = f(x)$, where $f(x) \in \mathbb{C}[x]$, $\deg f = 3$ with no double roots, together the point the infinity O. We can write $y^2 = x^3 - 3Ax + 2B$, where the double root condition is equivalent to $A^3 \neq B^2$. Then we have

$$j(E) = 1728\frac{A^3}{A^3 - B^2} \in \mathbb{C}.$$

If E, E' are elliptic curves, we can consider $\mathrm{Hom}_{\mathbb{C}}(E, E')$, and in particular $\mathrm{End}(E) = \mathrm{Hom}_{\mathbb{C}}(E, E)$. When E is defined over $\mathbb{C}$, either $\mathrm{End}(E) \simeq \mathbb{Z}$ or $\mathrm{End}(E) \simeq \mathscr{O}_D \subset \mathbb{C}$, an order in an imaginary quadratic field of discriminant D, namely $\mathbb{Z} + \mathbb{Z}((D + \sqrt{D})/2)$, for $D < 0$, $D \equiv 0, 1 \pmod 4$. The integers always occur because we have the multiplication by n map, $[n] : E \to E$.

Example. Let $E : y^2 = x^3 - x$. We can indeed "multiply" by complex numbers:

$$[i](x, y) = (-x, iy) = (x', y')$$

since if $(x, y) \in E$ then $(x', y') \in E$. By composition, we can multiply by any Gaussian integer $[a + bi]$. Here the lattice L_τ is given by $\tau = i$, and $j = 1728 \in \overline{\mathbb{Z}}$.

Example. Let $E : y^2 = x^3 - 35x + 98$. Then $\tau = (1 + \sqrt{-7})/2$, $j(\tau) = -3375 \in \overline{\mathbb{Z}}$. Here $\mathrm{End}(E) = \mathscr{O}_{-7} = \mathbb{Z} + \mathbb{Z}((1 + \sqrt{-7})/2)$. If we let

$$u = (1 + \sqrt{-7})/2, \quad \lambda = (7 + \sqrt{-7})/2, \quad B = (-7 + 21\sqrt{-7})/2,$$

then

$$[u](x, y) = \left(u^2\left(x + \frac{B}{x - \lambda}\right), v^3 y\left(1 - \frac{B}{(x - \lambda)^2}\right)\right) = (x', y')$$

has that $(x', y') \in E$ whenever $(x, y) \in E$.

In algebraic terms, the complex multiplication map can be very complicated; on the other hand, it is just the map $\mathbb{C}/\mathscr{O}_{-7} \xrightarrow{[(1+\sqrt{-7})/2]} \mathbb{C}/\mathscr{O}_{-7}$.

Traces of singular moduli. *Modular forms (of weight k)* are holomorphic functions on $\mathfrak{H}$ with

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \text{ for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

There exists a meromorphic modular form $g(\tau)$ of weight $3/2$ such that if $\tau \in \mathfrak{H}$ of discriminant D then $\mathrm{Tr}\, j(\tau)$ is the Dth Fourier coefficient of g.

Class field theory. If $K = \mathbb{Q}(\sqrt{D})$, let D be the actual discriminant, so $\mathscr{O}_D = \mathscr{O}$ is the maximal order. Then for $\tau \in \mathfrak{H}$, let $D(\tau) = D$ be the discriminant and $A\tau^2 + B\tau + C = 0$ for $A, B, C \in \mathbb{Z}$.

Then the maximal unramified extension of K, the *Hilbert class field* H, is generated by $j(\tau))$ over K. This is the only case where H is completely determined, and it has been a main problem of number theory to compute the Hilbert class field in a general situation.

The Kronecker limit formula and Kronecker's solution of Pell's equation. There exist solutions to Pell's equation $u^2 - Dv^2 = 1$ ($D > 0$, D not a square) constructed using elliptic functions, with applications to explicit class field theory and the class number formula. For $\tau \in \mathfrak{H}$ and $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$, we define the *(nonholomorphic) Eisenstein series of weight 0*

$$E(\tau, s) = \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{\operatorname{Im}(\tau)^s}{|mz+n|^{2s}}.$$

These are similar to the ordinary Eisenstein series

$$E_k(\tau) = \frac{1}{2} \sum_{m,n}{}' \frac{1}{(m\tau+n)^k} \in M_k$$

for $k = 4, 6, 8, \ldots$. We have that

$$E(\tau, s) = E\left(\frac{a\tau+b}{c\tau+d}, s\right).$$

If τ is a CM point, then

$$E(\tau, s) = \frac{1}{2}\left|\frac{D}{4}\right|^2 \sum_{m,n}{}' \frac{1}{(Am^2+Bmn+Cn^2)^s}.$$

If $h = 1$, this matches the *Epstein zeta function*

$$\zeta_Q(s) = \sum_{x \in \mathbb{Z}^2} \frac{1}{Q(x)^s}.$$

If A is an ideal class, $K = \mathbb{Q}(\sqrt{D})$, then we define the *partial zeta function*

$$\zeta_{K,A}(s) = \sum_{\mathfrak{a} \in A} \frac{1}{N(\mathfrak{a})^s}.$$

The *Kronecker limit formula* calculates $c'(\tau)$ where

$$E(\tau, s) = \frac{c}{s-1} + c'(\tau) + O(s-1).$$

This gives information about special partial zeta functions, Epstein zeta functions, and Eisenstein series, all at once.

There is also an application to the *Chowla-Selberg formula*: If τ is a CM-point, then $j(\tau) \in \overline{\mathbb{Q}}$. This is equivalent to proving $f(\tau) \in \overline{\mathbb{Q}}$ for all *modular functions* f over $\overline{\mathbb{Q}}$, meromorphic functions in $\mathfrak{H}$ invariant under $SL_2(\mathbb{Z})$ or a congruence subgroup. This follows from the fact that $f(\tau)$ is algebraic over $j(\tau)$. It is also equivalent to saying there exists $\Omega_\tau \in \mathbb{C}^\times$ such that $f(\tau)\Omega_\tau^{-k} \in \overline{\mathbb{Q}}$ for all modular forms of weight k and all k (to see this, set $f_1 \in M_1$, $f_1(\tau) = \Omega_\tau$, so that for $f \in M_k$, $f/f_1^k \in M_0$).

Application to Diophantine equations (Villegas). We have a functional equation

$$L(s, \psi^k) = cL(k-s, \psi^{k-1})$$

for some constant c; so if k is even, one may look at the central critical value $L(k/2, \psi^{k-1})$. We obtain a value for $L(1, s)$, which tells us on the BSD whether there is a point on the corresponding elliptic curve. This can be used to (conjecturally)

answer the question of Sylvester, asking for the primes which are sums of 2 (rational) cubes, e.g. $13 = (7/3)^3 + (2/3)^3$.

L-series and CM modular forms. To every elliptic curve $E/\mathbb{Q}$, we can associate an *L-series*

$$L(E/\mathbb{Q}, s) = \prod_p \left(1 - \frac{a_p}{p^s} + \frac{p}{p^{2s}}\right)^{-1}$$

for $a_p \in \mathbb{Z}$ where $|a_p| < 2\sqrt{p}$ (we must omit in finitely many cases the last term in the denominator). If $E : y^2 = f(x)$, then

$$a_p = p - \#\{(x, y) \in \mathbb{F}_p^2 : y^2 = f(x)\} = -\sum_{x \pmod p} \left(\frac{f(x)}{p}\right).$$

If E has CM, then there is a closed formula for a_p. In the first example,

$$\sum_{x \pmod p} \left(\frac{x^3 - x}{p}\right) = \begin{cases} 0, & p \equiv 3 \pmod 4 \\ \pm 2A, & p \equiv 1 \pmod 4,\ p = A^2 + 4B^2. \end{cases}$$

This is due to Gauss, with a formula to determine the appropriate sign. For the second,

$$\sum_{x \pmod p} \left(\frac{x^3 - 35x + 98}{p}\right) = \begin{cases} 0, & (p/7) = -1 \\ \pm 2A, & (p/7) = +1,\ p = A^2 + 7B^2. \end{cases}$$

Question. Is there an elementary proof of this?

When E has CM, its L-series $L(E, s)$ arises simultaneously as a theta series, an L-series of a Hecke character, and a Hasse-Weil zeta function. This shows that the three kinds of L-functions, those from algebraic geometry (like Dirichlet L-series), those from algebraic number theory (like the Riemann ζ function, $L(s, \chi)$, $\zeta_K(s)$, Artin $L(s, \pi)$, Hecke $L_K(s, \psi)$ for an adelic character ψ), and those arising from automorphic forms are linked in an important way (as contended by the Langlands program). In general, these three can be quite different.

If $Q(x_1, \ldots, x_{2h})$ is a positive definite quadratic form $\mathbb{Z}^{2h} \to \mathbb{Z}$, then

$$\sum_{x \in \mathbb{Z}^{2h}} q^{Q(x)} = \Theta_Q(\tau) \in M_h$$

is a modular form for some congruence subgroup. We may also insert a homogeneous polynomial $P(x_1, \ldots, x_{2h})$ of degree d that is *spherical*, and then

$$\sum_{x \in \mathbb{Z}^{2h}} P(x) q^{Q(x)} = \Theta_{Q,P}(\tau) \in M_{h+d}.$$

These Θ series in fact span the space of modular forms (there are also special types such as Eisenstein series).

If $h = 1$, Q is a binary quadratic form of discriminant $D < 0$ and hence arises from an order $\mathscr{O}_D$; we say $\theta_{Q,P} \in M_{d+1}$ is a *CM modular form*. Then $d = k - 1$, and ψ corresponds in some sense to the polynomial $P(x)$.

Other topics. There are also some other topics which arise in this context, including factorization of (norms of) (differences of) singular moduli (the values $j(2i) = 2^3 3^3 11^3$ and $j((1+\sqrt{-67})/2) = -2^{15}3^3 5^3 11^3$ demonstrate this compactness), Heegner points (in some cases, an elliptic curve can be shown by CM theory to have a nontrivial solution), special values of Green's functions, and a higher Kronecker limit formula. These topics are not covered here.

2. Complex Multiplication on Elliptic Curves over $\mathbb{C}$

Elliptic Curves over $\mathbb{C}$. We begin with a review of the theory of elliptic curves over $\mathbb{C}$. For more information about the material in this section, consult [7], [9], [18], and [4].

Theorem. *The following are equivalent definitions for an* elliptic curve *E over $\mathbb{C}$:*

(i) *A compact curve (Riemann surface) E of genus 1 (one topological hole), with a marked point $O \in E$;*
(ii) *A curve E which is also an (abelian) group;*
(iii) *$E = \{(x,y) \in \mathbb{C}^2 : y^2 = x^3 - 3Ax + 2B\} \cup \{\infty\}$;*
(iv) *$E = \mathbb{C}/L$ for a full lattice L.*

Proof. (iv) $\Rightarrow$ (i): Choose a fundamental domain for L, which will be the shape of a parallelogram. Identifying the edges, we get a torus.

(iv) $\Rightarrow$ (ii): $E = \mathbb{C}/L$ is the quotient of an abelian group by a subgroup.

(i) $\Rightarrow$ (iv) [18, Proposition VI.5.2]: If E is a curve of genus 1, let $\omega = dx/y$ be the invariant holomorphic differential on E. We then map $z \mapsto \int_O^z \omega \in \mathbb{C}$. In fact, since any two paths from O to x differ by something homologous to an element of $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ where γ_1, γ_2 generate the first homology of the torus and $\int_{\gamma_i} \omega = \omega_i$, we have a map $E \to \mathbb{C}/L$, and this is a complex analytic isomorphism of Lie groups. For a topological proof, we can take the universal cover, which is $\mathbb{C}$ modulo the fundamental group of E (a lattice).

(i) $\Rightarrow$ (ii) [18, Proposition III.3.4]: If $P_1, P_2 \in E$, we need to produce a $P_3 (= P_1 + P_2)$ and check that it satisfies the axioms of a group law. Let V be the set of meromorphic functions f on E with a pole of order ≤ 1 at P_1, P_2, and no other poles. By Riemann-Roch, $\dim V = 2$. So $V = \mathbb{C} \oplus \mathbb{C}f$ for some nonconstant f. Let $g(z) = f(z) - f(0)$. If g had no pole at P_1 or P_2, the dimension of V would drop to just a constant, so g must actually have only a simple pole at each of these points. Since principal divisors have degree zero, we have

$$(g) = (0) + (P_3) - (P_1) - (P_2)$$

for some P_3. This definition is compatible with the group law.

(i) $\Rightarrow$ (iii) [18, Proposition III.3.1]: By Riemann-Roch, we find that there are no functions with only a simple pole at O, but there is one with a double pole at O, which we call x. Continuing, we find a function y with a triple pole at O and further a relation between $1, x, y, x^2, xy, y^2, x^3$ in degree 6. We can reduce this to obtain a Weierstrass equation of the form above and check that this does indeed give an elliptic curve.

(ii) $\Rightarrow$ (i). Since the only surface with a group law must have topological Euler number zero, we find $\chi = 2 - 2g = 0$ so $g = 1$. $\square$

The group law on the elliptic curve can also be characterized by the following: if $P_1, P_2, P_3 \in E \cap \ell \subset \mathbb{P}^2_{\mathbb{C}}$ where ℓ is a projective line $ax + by + cz = 0$, then $P_1 + P_2 + P_3 = O$. The function defining ℓ has divisor $-3(O) + (P_1) + (P_2) + (P_3)$.

We let $\mathrm{Jac}(E)$ be the set of degree zero divisors $\mathrm{Div}^0(E)$ modulo principal divisors (f); then $\mathrm{Jac}(E) = E = \mathbb{C}/L$ [18, Proposition III.3.4]. Recall that if $D = \sum_i n_i(z_i)$ for $m_i \in \mathbb{Z}$, $z_i \in E$, then $D = (f)$ is principal iff $\sum_i n_i = 0$ and $\sum_i n_i z_i = 0$. If f is principal, look at $\int_{\partial L} f'(z)/f(z)\,dz$ and $\int_{\partial L} z\,(f'(z)/f(z))\,dz$ around the boundary of a fundamental domain. For the converse, we can use the group to replace $n_1(x_1) + n_2(x_2)$ with a term of the form $(x_1 + x_2)$, so we can reduce this to zero, which therefore must be constant so f is principal.

Elliptic functions. As a reference for elliptic functions, consult [11], [20], [3]. From now on, let $E = \mathbb{C}/L$, $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, where $\mathrm{Im}(\omega_1/\omega_2) > 0$.

We let $\mathbb{C}(E)$ be the set of meromorphic functions on E, which if we extend by periodicity is the same as the set of meromorphic functions f on $\mathbb{C}$ such that $f(z + \omega_1) = f(z) = f(z + \omega_2)$ for all $z \in \mathbb{C}$, which are *doubly periodic* and also called *elliptic functions*.

Proposition. *If $f \in \mathbb{C}(E)$ has zeros and poles $z_i \in \mathbb{C}/L$ with multiplicities m_i, we have $\sum_i m_i = 0$ and $\sum_i m_i z_i \in L$.*

The reverse implication, that given the z_i and m_i satisfying these conditions we can construct a (unique) elliptic function with the designated zeros and poles is due to Abel-Jacobi, as we will see below.

Proof. (See also [18, Proposition VI.2.2], [7, Proposition 9.2.5].) If near z_i we have $f(z) = c(z - z_i)^{m_i}(1 + \dots)$, so $f'(z)/f(z) = m_i/(z - z_i) + \dots$ has a simple pole with residue m_i. If we choose the fundamental domain such that no z_i is on the boundary of a fundamental domain (which we denote ∂L), we have by integrating along the edge that

$$\int_{\partial L} \frac{f'(z)}{f(z)}\,dz = \textstyle\sum_i m_i = 0;$$

by a direct calculation involving the periods of the lattice we find

$$\int_{\partial L} z\frac{f'(z)}{f(z)}\,dz = \textstyle\sum_i m_i z_i \in L.$$

□

Let $z \in \mathbb{C}/L$; the function

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) = \frac{1}{z^2} + {\sum_{\omega}}' \left(\frac{2z}{\omega^3} + \frac{3z^2}{\omega^4} + \dots \right) \\ &= \frac{1}{z^2} + \left(3{\sum_{\omega}}' \frac{1}{\omega^4} \right) z^2 + \left(5{\sum_{\omega}}' \frac{1}{\omega^6} \right) z^4 + \dots\end{aligned}$$

is even, doubly periodic, and has a unique double pole at zero [18, Proposition VI.3.1]. This function is called the *Weierstrass $\wp$-function*. Since

$$\wp'(z) = -\frac{2}{z^3} + 2cz + \dots$$

we have

$$\wp'^2(z) = \frac{4}{z^6} + \frac{8c}{z^2} + \dots = 4\wp(z)^3 - g_2\wp(z) - g_3;$$

g_3 is in fact a constant because the difference $\wp'^2(z) - 4\wp(z)^3 - g_2\wp(z)$ is elliptic but has no pole and thus must be constant [18, Proposition VI.2.1]. Thus $y^2 = 4x^3 - g_2x - g_3$ is an explicit way to get a Weierstrass equation for E.

If $\tau \in \mathfrak{H}$, $q = e^{2\pi i\tau}$, then we let $L_\tau = \mathbb{Z}\tau + \mathbb{Z}$ (substitute $\tau = \omega_1/\omega_2$ to get a new lattice and then rescale our functions). We then have

$$E = E_\tau = \mathbb{C}/L \simeq \{(x, y) : y^2 = x^3 - 3E_4(\tau)x + 2E_6(\tau)\},$$

where $E_4(\tau), E_6(\tau)$ are the Eisenstein series of weight four and six [16, §VII.4.2]:

$$E_4(\tau) = \frac{12}{(2\pi)^4}\sum_{\omega\in L}{}' \frac{1}{\omega^4} = 1 + 240(q + 9q^2 + 28q^3 + \cdots + \sigma_3(n)q^n + \dots)$$

$$E_6(\tau) = \frac{216}{(2\pi)^6}\sum_{\omega}{}' \frac{1}{\omega^6} = 1 - 504(q + 33q^2 + 244q^3 + \cdots + \sigma_5(n)q^n + \dots).$$

The way to remember these formulas is to let $\tau \to \infty$, so that the lattice becomes compressed and we approach a degenerate (singular) curve, $y^2 = (x-\alpha)^2(x-\beta) = x^3 + 0x^2 + \cdots = (x-\alpha)^2(x+2\alpha)$ which after scaling becomes $y^2 = (x-1)^2(x+2) = x^3 - 3x + 2$ which give the coefficients 3 and 2 on the standard model $y^2 = x^3 - 3Ax + 2B$.

Complex multiplication. We look at

$$\mathrm{Hom}_{\mathbb{C}}(E = \mathbb{C}/L, E' = \mathbb{C}/L') \simeq \{\alpha \in \mathbb{C} : \alpha L \subset L'\}$$

(see [18, Proposition IV.4.1]). Topologically, if we have a map $f : \mathbb{C}/L \to \mathbb{C}/L$ we can lift it to $\mathbb{C} \to \mathbb{C}$. f is a homomorphism of groups which is complex analytic, so locally near 0 it has power series $f(z) = \sum_{j=1}^{\infty} a_j z^j$ ($f(0) = 0$). Now $f(z_1)+f(z_2) = f(z_1 + z_2)$ for small z_1, z_2, so in particular $f(2z) = 2f(z)$ for small enough z and therefore

$$\sum_{j=1}^{\infty} a_j(2^j - 2)z = 0$$

which implies $a_j = 0$ for all $j \neq 1$. We extend this to all of $\mathbb{C}$ by $f(z) = nf(z/n)$ for appropriate n so that $f(z) = \alpha z$ for some $\alpha \in \mathbb{C}$. We have shown:

Proposition. *We have*

$$\mathrm{End}_{\mathbb{C}}(E) = \mathrm{Hom}_{\mathbb{C}}(E, E) = \{\alpha \in \mathbb{C} : \alpha L \subset L\}.$$

Therefore $\mathbb{Z} \subset \mathrm{End}_{\mathbb{C}}(E) = \mathscr{O}$, but it may be bigger. Since $\alpha \in \mathscr{O}$ iff $\alpha L \subset L$ iff $\alpha\omega_1 = a\omega_1 + b\omega_2$, $\alpha\omega_2 = c\omega_1 + d\omega_2$ for some integers a, b, c, d, we conclude

$$\frac{\omega_1}{\omega_2} = \tau = \frac{a\tau + b}{c\tau + d}$$

so $c\tau^2+(d-a)\tau-b = 0$. In other words, $\alpha = c\tau+d$, $\alpha\tau = a\tau+b$, so $\alpha \in \mathbb{Z}\tau+\mathbb{Z} = L_\tau$ so $\mathscr{O}_E \subset \mathbb{Z}\tau + \mathbb{Z}$. This quadratic equation must have discriminant < 0 (since it must have complex roots), so in this way we obtain an an order in an imaginary quadratic field [18, Proposition VI.5.5].

Theorem. *If $E = E_\tau$, then $\mathscr{O} = \mathrm{End}(E) = \mathbb{Z}$ if τ is not imaginary quadratic; otherwise, $\mathscr{O}$ is an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$, $D < 0$.*

Since $D<0$, we have $D\equiv 0,1 \pmod 4$ (if $A\tau^2+B\tau+C=0$, $D=B^2-4AC<0$ so $D\equiv 0,1 \pmod 4$, and conversely), and we write

$$\begin{aligned}\mathscr{O}_D &= \{(m+n\sqrt{D})/2 : m,n\in\mathbb{Z},\ m\equiv nD \pmod 2\}\\ &= \mathbb{Z}+\mathbb{Z}(D+\sqrt{D})/2\\ &= \begin{cases}\mathbb{Z}[\sqrt{-n}], & D\equiv 0 \pmod 4, D=-4n;\\ \mathbb{Z}[(1+\sqrt{D})/2], & D\equiv 1 \pmod 4.\end{cases}\end{aligned}$$

Let $E: y^2=x^3-3Ax+2B$ ($A^3\neq B^2$); we define

$$j(E)=(12A)^3/(A^3-B^2),$$

the *modulus* of E; since we can always map $(x,y)\mapsto(c^2x,c^3y)$ and $(A,B)\mapsto(c^4A,c^6B)$, the ratio A^3/B^2 and hence j is well-defined up to change of coordinates [18, §3.1].

Definition. We say E *has CM* if $\mathrm{End}(E)=\mathscr{O}_D$ for some D, i.e. there exists $\tau\in\mathfrak{H}$ with $[\mathbb{Q}(\tau):\mathbb{Q}]=2$ such that $E=E_\tau$. If E has CM, j is called *singular*.

So far, A,B may be in $\mathbb{C}$, but we will show that $j\in\overline{\mathbb{Q}}$.

j is Algebraic. The Eisenstein series E_4,E_6 are in fact modular (more on this below):

$$\begin{aligned}E_4(\tau)&=1+240q+\ldots, \text{ so } E_4^3(\tau)=1+720q+\cdots\in M_{12};\\ E_6(\tau)&=1-504q-\ldots, \text{ so } E_6^2(\tau)=1-1008q+\cdots\in M_{12}.\end{aligned}$$

Therefore $E_4^3-E_6^2=1728q+\cdots\in M_{12}$ so [16, §VII.4.4]

$$\begin{aligned}\Delta(\tau)&=\frac{E_4^3-E_6^2}{1728}=q-24q^2+252q^3-\cdots-6048q^6+\ldots\\ &=q\prod_{n=1}^{\infty}(1-q^n)^{24}\neq 0\in M_{12}.\end{aligned}$$

Remark. Note $-6048=-24\cdot 252$, and the multiplicativity of the coefficients of Δ was first proved by Mordell.

We let

$$j(E)=j(E_\tau)=j(\tau)=\frac{E_4(\tau)^3}{\Delta(\tau)}=\frac{1}{q}+744+196884q+21493760q^2+\ldots.$$

If $\tau\mapsto\dfrac{a\tau+b}{c\tau+d}$ for $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})=\Gamma_1=\Gamma$, we have

$$L_\tau=[\tau,1]=[a\tau+b,c\tau+d]=(c\tau+d)L_{(a\tau+b)/(c\tau+d)}$$

so $j(\tau)=j(\gamma(\tau))$ for all $\gamma\in\Gamma$.

Theorem. *If E has CM, then $j(E)=j(\tau)\in\overline{\mathbb{Q}}$.*

Proof. (See also [18, Appendix C, Corollary 11.1.1].) Let $\mathrm{End}(E)=\mathscr{O}_D$ and $\tau\in\mathfrak{H}$, and assume $A\tau^2+B\tau+C=0$, $A,B,C\in\mathbb{Z}$, $\gcd(A,B,C)=1$, $A>0$. Then $\tau=(-B+\sqrt{D})/2A$, $D=B^2-4AC<0$.

If $\alpha\in\mathrm{End}(E)$, $\alpha(\mathbb{Z}\tau+\mathbb{Z})\subset\mathbb{Z}\tau+\mathbb{Z}$, so $\alpha\tau=a\tau+b$, $\alpha=c\tau+d$; that is to say, there exists $M=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2(\mathbb{Z})$ with $\det M=ad-bc=n>0$. Then $c\tau^2+(d-a)\tau-b=0$, so there exists $u\in\mathbb{Z}$ such that $c=Au$, $d-a=Bu$,

$-b = Cu$ after matching coefficients, and certainly $t \in \mathbb{Z}$ such that $a + d = t$. We have therefore that

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} (t - Bu)/2 & -Cu \\ Au & (t + Bu)/2 \end{pmatrix} \in \mathscr{M}_n$$

where $\mathscr{M}_n \subset M_2(\mathbb{Z})$ denotes integer matrices with determinant n.

Therefore, there is a one-to-one correspondence between matrices $M \in \mathscr{M}_n$ subject to the above conditions and integer pairs $(t, u) \in \mathbb{Z}$; this is also in bijection with elements $\lambda = (t + u\sqrt{D})/2 \in \mathscr{O}_D$ with

$$N(\lambda) = \lambda\overline{\lambda} = n, \qquad \operatorname{tr} \lambda = \lambda + \overline{\lambda} = t$$

(note $\det M = n = (t^2 - B^2u^2)/4 + ACu^2 = (t^2 - Du^2)/4$ so that e.g. $D \equiv B \pmod 2$).

Now we have an explicit description of the ring $\operatorname{End}(E) = \mathscr{O}_D$. $L_\tau = \mathbb{Z}\tau + \mathbb{Z} \subset K = \mathbb{Q}(\sqrt{D})$, with L_τ a proper $\mathscr{O}_D$-module. If $\mathfrak{a} \subset K$ is an $\mathscr{O}_D$-module with $\alpha\mathfrak{a} \subset \mathfrak{a}$, then $\alpha \sim c\alpha$ has the same multiplier, so we let $\operatorname{Cl}(D)$ be the set of proper $\mathscr{O}$-modules modulo $K^\times$, the *class group*, which is known to be finite. We let $\#\operatorname{Cl}(D) = h_D$, the *class number*.

So $\mathbb{C}/\mathfrak{a} = E_\mathfrak{a}$ has CM by $\mathscr{O}_D$. For fixed D, the set of elliptic curves with CM by $\mathscr{O}_D$ is in bijection with $\operatorname{Cl}(D)$, which is finite. On the other hand, if $y^2 = x^3 - 3Ax + 2B$, $A^3 \neq B^2$, and $\sigma \in \operatorname{Aut}(\mathbb{C}) = \operatorname{Gal}(\mathbb{C}/\mathbb{Q})$, then $A^{3\sigma} \neq B^{2\sigma}$, and have the curve $E^\sigma : y^2 = x^3 - 3A^\sigma x + 2B^\sigma$. But σ maps preserve addition, multiplication, so algebraic properties (including the endomorphism ring) are also preserved. Thus

$$\#\{j(E) : E \text{ has CM by } \mathscr{O}_D\} = h(D),$$

and there exists a subgroup $G \subset \operatorname{Gal}(\mathbb{C}/\mathbb{Q})$ of index $< \infty$ ($\leq h!$) such that $\sigma \in G$, $E \simeq E^\sigma$, which implies $j(E_1), \ldots, j(E_h) \in \mathbb{C}^G = H/\mathbb{Q}$ is finite. A complex number with only finitely many conjugates is algebraic, so $\prod_{i=1}^h (X - j(E_i)) \in \mathbb{Q}(x)$. □

We have actually proven:

Theorem. *For all $D < 0$, $D \equiv 0, 1 \pmod 4$, there exist exactly $h(D)$ nonisomorphic elliptic curves with $\operatorname{End}(E) = \mathscr{O}_D = \mathbb{Z} + \mathbb{Z}(D + \sqrt{D})/2$. Denoting these $E_1, \ldots, E_h$, we have $h_D(X) = \prod_{i=1}^h (X - j(E_i)) \in \mathbb{Q}[x]$.*

Example. If $D = -7$, $h(D) = 1$, so $\mathfrak{a} = \mathbb{Z} + \mathbb{Z}(1 + \sqrt{-7})/2$, $j = j((1 + \sqrt{-7})/2) = -3375$, $h_{-7}(x) = x + 3375$.

Example. If $D = -20$, $h(-20) = 2$, and $h_{-20}(x) = x^2 - 1264000x - 681472000$.

3. Complex Multiplication: A Modular Point of View

Theta series. We want to now utilize the correspondence between elliptic curves and modular forms. For more information on modular forms, consult [13], [21], and [18, Appendix C, §12].

If $E = \mathbb{C}/L$, $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\omega_2(\mathbb{Z}\tau + \mathbb{Z}) = \omega_2 L_\tau$, $\tau = \omega_1/\omega_2 \in \mathfrak{H}$, then $E \simeq \mathbb{C}/L_\tau = E_\tau$, so we can restrict our discussion to these curves. We have

$$L_{\gamma\tau} = L_{\frac{a\tau+b}{c\tau+d}} = \mathbb{Z}\left(\frac{a\tau + b}{c\tau + d}\right) + \mathbb{Z} = (c\tau + d)^{-1} L_\tau \text{ for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1 = SL_2(\mathbb{Z}),$$

so $\tau \sim \gamma(\tau)$. We defined the Weierstrass $\wp$-function

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

which we write now as

$$\wp(z,\tau) = \frac{1}{z^2} + \sum_{m,n \in \mathbb{Z}}{}' \left(\frac{1}{(z+m\tau+n)^2} - \frac{1}{(m\tau+n)^2} \right).$$

We have $\wp(z+m\tau+n,\tau) = \wp(z,\tau)$ and

$$\wp\left(\frac{z}{c\tau+d}, \frac{a\tau+b}{c\tau+d} \right) = (c\tau+d)^2 \wp(z,\tau).$$

This behaves like a modular form of weight 2.

The most famous of these series are theta functions [7, §10.2]:

$$\theta(z,\tau) = \theta_{00}(z,\tau) = \sum_{n=-\infty}^{\infty} \exp(\pi i n^2 \tau + 2\pi i n z).$$

We have $\theta(z+1,\tau) = \theta(z,\tau)$, $\theta(-z,\tau) = \theta(z,\tau)$, and

$$\begin{aligned} \theta(z+\tau,\tau) &= \sum_n \exp\left(\pi i (n^2+2n)\tau + 2\pi i n z\right) \\ &= \exp(-\pi i \tau - 2\pi i z) \sum_n \exp\left(\pi i (n+1)^2 \tau + 2\pi i (n+1) z\right) \\ &= \exp(-\pi i \tau - 2\pi i z)\theta(z,\tau). \end{aligned}$$

These series also carry the properties of a modular function, but they are not quite elliptic, since

$$\theta(z+m\tau+n,\tau) = \exp(-\pi i m^2 \tau - 2\pi i m z)\theta(z,\tau).$$

We define

$$\begin{aligned} \theta_{00}(z,\tau) &= \theta(z,\tau) \\ \theta_{0\frac{1}{2}}(z,\tau) &= \theta(z+1/2,\tau) \\ \theta_{\frac{1}{2}0}(z,\tau) &= \theta(z+\tau/2,\tau) \\ \theta_{\frac{1}{2}\frac{1}{2}}(z,\tau) &= \theta(z+(1+\tau)/2,\tau) \end{aligned}$$

by adding the 2-torsion points of $E = \mathbb{C}/L$. These satisfy similar formulas as the above. We map [7, §10.3]

$$\mathbb{C}/L \ni z \mapsto (\theta_{00} : \theta_{0\frac{1}{2}} : \theta_{\frac{1}{2}0} : \theta_{\frac{1}{2}\frac{1}{2}}) \in \mathbb{P}^3.$$

We have $\theta_{\frac{1}{2}\frac{1}{2}}(z,\tau) = 0$ iff $z \in L$, since the total number of zeros plus poles is zero, and by taking $\int_{\partial L} \theta'(z)/\theta(z)\,dz$, we see we have a unique zero, so it must be at the origin and the zero must be simple. (Alternatively, one can prove this fact using the Jacobi triple product [10, §3.2, Theorem 2].)

If $n_i \in \mathbb{Z}$, $z_i \in \mathbb{C}/L$, $\sum_i n_i = 0$, $\sum_i n_i z_i \in L$, then we let

$$f(z) = \prod_i \theta_{\frac{1}{2}\frac{1}{2}}(z - z_i, \tau)^{n_i}.$$

This is a doubly periodic function iff the above conditions are satisfied (just substitute $z \mapsto z + \tau$ in the above formulae). We now have constructed an explicit f with the desired zeros and poles which is elliptic.

Proposition. *A function f is elliptic iff it has zeros and poles at $z_i \in \mathbb{C}/L$ of multiplicity n_i with $\sum_i n_i = 0$ and $\sum_i n_i z_i = 0$, and conversely, there exists an elliptic function f with the prescribed multiplicities under this hypothesis.*

Modular forms. For $\Gamma = SL_2(\mathbb{Z})$, $M_k = M_k(\Gamma)$ is the space of modular forms of weight k on Γ, that is to say $f : \mathfrak{H} \to \mathbb{C}$ is holomorphic, f satisfies

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \text{ for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

and has less than exponential growth, i.e. $f(x + iy) = O(y^c) + O(y^{-c})$ for some c (which implies $f(x + iy) = O(1) + O(y^{-k})$) [16, §VII.2.1].

We know that $\dim M_k < \infty$ [16, §VII.3.2, Theorem 4], and in fact

k	$\dim M_k$	M_k
< 0	0	–
odd	0	–
0	1	$\mathbb{C}$
2	0	–
4	1	$\mathbb{C}E_4$
6	1	$\mathbb{C}E_6$
8	1	$\mathbb{C}E_8 = \mathbb{C}E_4^2$
10	1	$\mathbb{C}E_{10} = \mathbb{C}E_4E_6$
12	2	$\mathbb{C}E_{12} \oplus \mathbb{C}\Delta$

where the dimension cycles with period 12. The generating forms E_{2i} are Eisenstein series,

$$E_k(\tau) = \frac{1}{2} \sum_{\gcd(m,n)=1} \frac{1}{(m\tau + n)^k} = 1 + (-1)^k \frac{4k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ and B_k is the kth Bernoulli number.

So $M_* = \mathbb{C}(E_4, E_6)$, that is to say the modular forms are generated by E_4 and E_6. This is also true of $G_k \in \mathbb{C}(G_4, G_6)$. Recall

$$\wp(z) = \frac{1}{z^2} + 3G_4(\tau)z^2 + 5G_6(\tau)z^4 + \ldots, \quad z \to 0$$

hence

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

This gives a recursion for each G_k as a polynomial in the earlier G_k for $k > 6$.

We have found that there is a bijection

$$\begin{array}{ccccc} \{E/\mathbb{C} \text{ elliptic curve}\} & \longleftrightarrow & \{L \subset C \text{ lattice}\}/\mathbb{C}^\times & \longleftrightarrow & \mathfrak{H}/\Gamma \\ E & \longmapsto & \int_\gamma \omega & & \\ \mathbb{C}/L & \longmapsfrom & L & & \\ & & \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 & \longmapsto & \omega_1/\omega_2 \\ & & \mathbb{Z}\tau + \mathbb{Z} & \longmapsfrom & \tau \end{array}$$

There is a map $j : \mathfrak{H}/\Gamma \to \mathbb{C}$ by

$$\tau \mapsto j(\tau) = \frac{E_4(\tau)^3}{\Delta(\tau)} = \frac{1728E_4(\tau)^3}{E_4(\tau)^3 - E_6(\tau)^2},$$

and similarly one for the set of elliptic curves by $j(E_\tau) = j(\tau)$. Indeed, there exists a unique $\tau \in \mathfrak{H}$ such that $f(\tau) = E_4(\tau)^3 - \lambda\Delta(\tau) = 0$ for any $\lambda \in \mathbb{C}$ (the integral $\int_{\partial L} f'(z)/f(z)\,dz$ vanishes exactly once, so this zero must be λ) [16, §VII.3.3, Proposition 5].

We can modify the above bijection as follows:

$$\{E/\mathbb{C} \text{ CM elliptic curve}\} \longleftrightarrow \{\tau \in \mathfrak{H}/\Gamma : [\mathbb{Q}(\tau) : \mathbb{Q}] = 2\}$$

These sets are now countable, and if $D < 0$, $D \equiv 0, 1 \pmod 4$ is fixed, then the set with CM by $\mathscr{O}_D$ is in fact finite, as we shall see.

Quadratic forms. For more information, consult [5, §VII.2] and [11, §8.1].

Definition. Let $\mathscr{Q}_D$ be the set of positive definite quadratic forms of discriminant D, i.e.

$$\mathscr{Q}_D\{Q = [A, B, C] : Q(x, y) = Ax^2 + Bxy + Cy^2,\ A, B, C \in \mathbb{Z},\ D = B^2 - 4AC\}.$$

We denote by $\mathscr{Q}_D^0 \subset \mathscr{Q}_D$ be the subset of primitive quadratic forms, i.e. those with $\gcd(A, B, C) = 1$, $A > 0$.

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, we have $(Q \circ \gamma)(x, y) = Q(ax + by, cx + dy)$. We will show that $\mathbb{Q}/\Gamma < \infty$ (it is a class number).

Let $\mathscr{O}_D = \mathbb{Z} + \mathbb{Z}(D + \sqrt{D})/2 \subset K = \mathbb{Q}(\sqrt{D})$ be an order in an imaginary quadratic field. We define

$$\mathrm{Cl}(D) = \{\mathfrak{a} \subset K : (\mathbb{Z}\text{-rank } 2) \text{ proper } \mathscr{O}_D\text{-modules},\ \mathrm{mult}(\mathfrak{a}) = \mathscr{O}_D\}/K^\times$$

where $\mathrm{mult}(\mathfrak{a}) = \{\lambda \in K : \lambda\mathfrak{a} \subset \mathfrak{a}\}$. We let $h(D) = \#\,\mathrm{Cl}(D)$.

Since $\mathscr{Q}_D^0/\Gamma \simeq \mathrm{Cl}(D)$, we know

$$\mathscr{Q}_D = \bigsqcup_{n^2|D} n\mathscr{Q}_{D/n^2}^0$$

and thus $\#\mathscr{Q}_D = \sum_{n^2|D} h(D/n^2)$.

To each $Q = [A, B, C]$ we associate $\mathbb{Z}A + \mathbb{Z}(B + \sqrt{D})/2 = \mathfrak{a}$. We do this because the root $\tau = (-B + \sqrt{D})/2A$ of $A\tau^2 + B\tau + C = 0$ gives rise to the correct lattice $\mathbb{Z}\tau + \mathbb{Z}$. We have $\mathrm{mult}(\mathfrak{a}) = \mathscr{O}_D$, since $\lambda\mathfrak{a} \subset \mathfrak{a}$ iff $\lambda A, \lambda(B + \sqrt{D})/2 \subset \mathbb{Z}A + \mathbb{Z}(B + \sqrt{D})/2$, which can be written in matrix form

$$\lambda \begin{pmatrix} (B + \sqrt{D})/2 \\ A \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} (B + \sqrt{D})/2 \\ A \end{pmatrix}$$

for some $a, b, c, d \in \mathbb{Z}$. For a fixed choice of a basis, we have $\mathrm{mult}(\mathfrak{a}) \simeq \mathrm{End}(E) \hookrightarrow M_2(\mathbb{Z})$.

Relation to CM points. Recall that τ has CM iff there exists $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$, $\det(M) > 0$ with $\tau = M\tau$ for M not a scalar matrix (also see [2, I, §5]). We let $\operatorname{tr}(M) = t$ and $\det M = n = (t^2 - Du^2)/4$.

We are therefore interested in the set of matrices

$$M \in \mathscr{M}_n = \{M \in M_2(\mathbb{Z}) : \det M = n,\ \operatorname{tr} M = t\}.$$

We may assume that $t^2 - 4n = Du^2 \leq 0$ (so that M is an elliptic hyperbolic isometry and therefore has at least one fixed point). In order to study $M\tau = \tau$, we look at the map $\tau \mapsto M\tau = \tau'$ for fixed $\tau \in \mathfrak{H}$. We have an induced map $j(\tau) \to j(\tau')$, which runs over a finite set as follows: since $j(M\tau) = j(\gamma M\tau)$ for $\gamma \in \Gamma$, we have

$$\{j(\tau') : \tau' = M\tau,\ M \in \mathscr{M}_n\} = \{j(M\tau) : M \in \Gamma \setminus \mathscr{M}_n\}.$$

We relate two matrices if they differ by multiplication by an element of $SL_2(\mathbb{Z})$, therefore by the calculation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ a'c + c'd & b'c + dd' \end{pmatrix},$$

and the assumption $\gcd(c, d) = 1$, we may assume $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $ad = n$, $a, d > 0$. We then multiply

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b + rd \\ 0 & d \end{pmatrix}$$

to bring $0 \leq b < d$. We have shown [16, §VII.5.2, Lemma 2]:

Proposition.

$$\Gamma \setminus \mathscr{M}_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = n,\ 0 \leq b < d \right\},$$

so $\#(\Gamma \setminus \mathscr{M}_n) = \sum_{d|n} d = \sigma_1(n)$.

In particular,

$$\{j(M\tau) : M \in \mathscr{M}_n\} = \{j((a\tau + b)/d) : ad = n,\ 0 \leq b < d\}$$

and τ has CM iff $j(\tau)$ is in this set.

The modular polynomial Ψ. The next major result needed in this section regards the classical polynomial Ψ.

Theorem (Modular equation)**.** *For all $n \geq 1$, there exists a polynomial*

$$\Psi_n(X, Y) \in \mathbb{Z}[X, Y]$$

such that

$$\{j(M\tau) : M \in \Gamma \setminus \mathscr{M}_n\} = \{\textit{roots of } \Psi_n(X, j(\tau))\},$$

i.e.

$$\Psi_n(X, j(\tau)) = \prod_{M \in \Gamma \setminus \mathscr{M}_n} (X - j(M\tau)) = \prod_{\substack{ad=n \\ 0 \leq b < d}} (X - j((a\tau + b)/d))$$

with $\deg \Psi_n(X, j(\tau)) = \sigma(n)$.

Example. We have $\Psi_1(X, j(\tau)) = X - j(\tau)$,

$$\begin{aligned}\Psi_2(X,Y) &= Y^3 - (X^2 - 1488X + 162000)Y^2 \\ &\quad + (1488X^2 + 4077375X + 8748000000)Y \\ &\quad + (X^3 - 162000X^2 + 8748000000X - 157464000000000).\end{aligned}$$

and

$$\Psi_3(X, j(\tau)) = (X - j(3\tau))(X - j(\tau/3))(X - j((\tau+1)/3))(X - j((\tau+2)/3));$$

for $j(\tau) = q^{-1} + 744 + 196884q + \dots$ for $q = e^{2\pi i\tau}$, this gives

$$\begin{aligned}\Psi_3(X, j(\tau)) &= (X - q^{-3} - 744 - 196884q^3 + \dots) \\ &\quad \cdot (X - q^{-1/3} - 744 - 196884q^{1/3} + \dots) \\ &\quad \cdot (X - \zeta_3^{-2}q^{-1/3} - 744 - 196884\zeta_3^2 q^{1/3} + \dots) \\ &\quad \cdot (X - \zeta_3^{-1}q^{-1/3} - 744 - 196884\zeta_3 q^{1/3} + \dots) \in \mathbb{Z}[\zeta][X]((q^{1/3})).\end{aligned}$$

Proof of theorem. (See also [2, I, §4, Theorem 1].) $\Psi_n(X, j(\tau))$ is holomorphic in τ, Γ-invariant under $\tau \mapsto \gamma\tau$, $M\tau \mapsto M(\gamma\tau) = (M\gamma)(\tau)$ and is bounded at infinity (it has a finite pole of order n); any modular function satisfying these is a *polynomial* in $j(\tau)$ (see [17, §6, Proposition 12] or [11, §5.2, Theorem 2]).

A priori, $\Psi_n(X, j(\tau)) \in \mathbb{Z}[\zeta_n][X]((q^{1/n}))$ since $j((a\tau + b)/d) = \zeta_d^b q^{-a/d} + \dots$. The coefficients of fractional powers of q sum over a fixed power of a primitive nth root of unity, hence all powers are integral. Moreover, the Galois group acting on $j(M\tau)$ just permutes the factors, hence $\Psi_n(X, j(\tau)) \in \mathbb{Z}[X]((q))$. Inverting, $q = j(\tau)^{-1} - 744j(\tau)^{-2} - \dots \in \mathbb{Z}((1/j))$, so $\Psi_n(X, j(\tau)) \in \mathbb{Z}[X]((1/j))$, therefore by the above $\psi_n(X, j(\tau)) \in \mathbb{Z}[Y][j]$. □

We have shown [2, I, §5, Theorem 2]:

Corollary. $j(\tau) \in \overline{\mathbb{Z}}$.

If τ has CM, there exists $M \in \mathscr{M}_n$, M not a scalar matrix, such that $M\tau = \tau$. Then $\Psi_n(j(\tau), j(M\tau)) = 0$, and $j(\tau)$ is a root of $\Psi_n(X, X) \in \mathbb{Z}[X]$. To avoid trivialities, we must check that this polynomial is monic and not identically zero. To do this, we will prove the following below:

Claim. $\Psi_n(X, X) = \pm X^{\alpha(n)} + \dots$, where $\alpha(n) = \sum_{d|n} \max(d, n/d) > \sigma(n)$ when n is not a square.

A word on the polynomial Φ. In parallel to

$$\Psi_n(X, j(\tau)) = \prod_{M \in \Gamma\backslash\mathscr{M}_n} (X - j(M\tau)),$$

we let

$$\Phi_n(X, j(\tau)) = \prod_{M \in \Gamma\backslash\mathscr{M}_n^0} (X - j(M\tau))$$

where $\mathscr{M}_n^0$ runs over primitive matrices (i.e. $\gcd(a, d) = 1$). The same proof as above shows $\Phi_n(X, j(\tau)) \in \mathbb{Z}[X, j(\tau)]$. We have

$$\Psi_n(X, j(\tau)) = \prod_{\ell^2 | n} \Phi_{n/\ell^2}(X, j(\tau)).$$

Ψ_n has better analytic properties (because there is no primitivity condition), but Φ_n is better algebraically (it is irreducible).

Cyclic isogenies and the modular group. For the results of this section, consult [11, §5.3]. We are therefore interested in roots of $\Phi_n(X, j(\tau))$, i.e. $\tau, \tau' \in \mathfrak{H}/\Gamma$ such that $\Psi(j(\tau), j(\tau')) = 0$; this is the same as $\tau \sim \tau''$, $\tau' \sim n\tau''$, for some τ'', where $\sim$ denotes equivalence under Γ. But any $\gamma \in \Gamma$ can be written $\gamma_1 \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \gamma_2$, so after scaling we obtain

$$0 \to \mathbb{Z}/n\mathbb{Z} \to E' \to E \to 0,$$

a *cyclic isogeny*, corresponding to the inclusion of lattices $E = \mathbb{C}/L \hookleftarrow \mathbb{C}/L' = E'$, with $\deg(E' \to E) = n$. In other words, $\Psi_n(j(\tau), j(\tau')) = 0$ iff there exists a cyclic n-isogeny $E' \to E$.

To study these, we must define congruence subgroups. We have $SL_2(\mathbb{Z}) = \Gamma_1 = \Gamma_0(1) = \Gamma_1(1) = \Gamma(1)$, but we also have for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ the subsets

$$\begin{aligned} \Gamma_0(N) = \{\gamma : c \equiv 0 \pmod N\} \supset \Gamma_1(N) &= \{\gamma : a \equiv 1 \pmod N, c \equiv 0 \pmod N\} \\ &\supset \Gamma(N) = \{\gamma : a, d \equiv 1 \pmod N, b, c \equiv 0 \pmod N\} \end{aligned}$$

Since $\Gamma(N) \triangleleft \Gamma_1$, we have an exact sequence

$$1 \to \Gamma(N) \to \Gamma_1 \to SL_2(\mathbb{Z}/N\mathbb{Z}) \to 1.$$

These are the *modular groups*. Just as $\Gamma_1 \backslash \mathfrak{H}$ parameterizes elliptic curves, $\Gamma_0(N) \backslash \mathfrak{H}$ parameterizes triples (E, E', ϕ) with $\phi : E \to E'$ a cyclic N-isogeny. There are only finitely many sublattices of index N, so there are only finitely many E' for a fixed E. Equivalently, we can look at the kernel

$$1 \to \mathbb{Z}/N\mathbb{Z} \to E \to E' \to 1,$$

which corresponds to a subgroup of order N in E. In sum [18, Appendix C, §13], [7, §11.3],

$$\begin{aligned} \Gamma_1 \setminus \mathfrak{H} &\longleftrightarrow \{E\} \\ Y_0(N) = \Gamma_0(N) \setminus \mathfrak{H} &\longleftrightarrow \{(E, C) : E, C = \mathbb{Z}/N\mathbb{Z} \subset E\} \\ Y_1(N) = \Gamma_1(N) \setminus \mathfrak{H} &\longleftrightarrow \{(E, P) : E, P \in E \text{ of order } N\} \\ Y(N) = \Gamma(N) \setminus \mathfrak{H} &\longleftrightarrow \{(E, P_1, P_2) : P_1, P_2 \in E \text{ a basis for } N\text{-torsion}\} \end{aligned}$$

We can also take their compactifications $X_0(N)$, $X_1(N)$, and $X(N)$.

We have a map $j : \Gamma_0(N) \setminus \mathfrak{H} = X_0(N) \to \mathfrak{H} \simeq \mathbb{P}^1_{\mathbb{C}}$. Thus

$$\begin{aligned} \{(X, Y) \in \mathbb{C}^2 : \Phi_n(X, Y) = 0\} &= \{(j(E), j(E')) : E' \to E \ n\text{-cyclic}\} \\ &= \{([E], [E']) \subset X(1)^2 : E \to E' \ n\text{-cyclic}\}. \end{aligned}$$

So we have a map $j : X_0(N) \to X(1)^2 \to \mathbb{P}^1 \times \mathbb{P}^1$ by $(E, E') \mapsto ([E], [E'])$, and hence we obtain a model for this curve. This is generically one-to-one, but may be singular [18, Theorem 13.1].

A CM elliptic curve is cyclically isogeneous to itself, $E \xrightarrow{\phi} E' \simeq E$. If we look on the diagonal,

$$\Phi_n(X, X) = 0 = T_n \subset X_1 \times X_1.$$

If $\tau \in \mathfrak{H}$, $\tau = \tau_Q$ where $Q \in \mathscr{Q}_D^0$ (which is to say $B^2 - 4AC = D$, $A\tau^2 + B\tau + C = 0$, $A > 0$, $\gcd(A, B, C) = 1$). From before,

$$\begin{aligned}\operatorname{End}(E) &\simeq \{M \in M_2(\mathbb{Z}) : M\tau = \tau\} \cup \{0\} \\ &\longleftrightarrow \mathscr{O}_D = \{(t + u\sqrt{D})/2 : t, u \in \mathbb{Z},\ t \equiv Du \pmod 2\}\end{aligned}$$

where we associate to $\lambda = (t + u\sqrt{D})/2$ the matrix

$$M = \begin{pmatrix} (t - Bu)/2 & -Cu \\ Au & (t + Bu)/2 \end{pmatrix}.$$

We have $\operatorname{tr} M = \operatorname{Tr} \lambda = t$, $\det M = N\lambda = n = (t^2 - Du^2)/4$.

Therefore

$$\bigsqcup_D \mathscr{Q}_D^0 = \bigcup_n \{\text{fixed points of } M \in \mathscr{M}_n\}.$$

For fixed n, we have $t^2 - 4n = Du^2 \le 0$; hence $|t| < 2\sqrt{n}$, which allows only finitely many t, hence only finitely many u (if we assume n is not a square), and thus finitely many D.

Calculation for $n = 2$. We will now give an extended derivation of the fact that

$$\Phi_2(X, X) = (X - 8000)(X + 3375)^2(X - 1728).$$

The first term corresponds to $j = 20^3 = 8000$, $D = -8$; $j = -3375 = -15^3$ corresponds to $D = -7$, with the curve $y^2 = x^3 + 35x - 98$; and $j = 1728 = 12^3$, with the curve $y^2 = x^3 - x$. Since $|t| < 2\sqrt{2} < 3$, we have $t = 0, \pm 1, \pm 2$, which gives $d = -8$, -7 (twice), and -4 (twice, but we count it only have the time because of the extra involution of i in the fundamental domain—more on this below).

We can find these roots from another point of view. We want all E such that there exists a 2-isogeny $E \to E$, $0 \to \langle T \rangle \to E \to E \to 0$ where $2T = O$ so T is a 2-torsion point, which is to say we want the set

$$\{(E, T) : T \in E,\ 2T = O,\ E/\langle T \rangle \subset E\}$$

for a fixed isogeny. In the Weierstrass model $y^2 = x^3 + Ax^2 + Bx$, $-(x, y) = (x, -y)$ so $2T = O$ iff $y = 0$; after translation we may assume that $T = (0, 0)$. (Note that this implies $X_0(2)$ is rational, as we can always rescale $A \mapsto \lambda A$, $B \mapsto \lambda^2 B$, so we have a unique choice $A^2/B \in \mathbb{C}$ determining the curve uniquely.)

To E and T we want to associate $E' = E/\langle T \rangle$, so to $P = (x, y) \in E$ we associate $P^* = P + T = (x^*, y^*) = (B/x, -By/x^2)$, and $(P^*)^* = P$. We have

$$\begin{aligned} xx^* &= B \\ x + x^* &= x + B/x = \xi \\ y + y^* &= y(1 - B/x^2) = \eta \\ yy^* &= -B(x + A + B/x) = -B(\xi + A) \end{aligned}$$

This implies $\eta^2 = (\xi^2 - 4B)(\xi + A)$, so we obtain the curve $E' : \eta^2 = \xi^3 + A\xi^2 - 4B\xi - 4AB$. According to our model, we take $\xi \mapsto \xi - A = \vartheta$ and have $\eta^2 = \left((\vartheta - A)^2 - 4B\right)\vartheta$.

So $E/\langle T \rangle = E'$, $E/\langle T' \rangle = E$, and $Y'^2 = X'^3 + A'X'^2 + B'X'$ for $T' = (0, 0)$, hence $A' = -2A$, $B' = A^2 - 4B$. $A'' = 4A$, $B'' = A'^2 - 4B'^2 = 16B$, so $E'' \simeq E$.

So we have a general description for 2-isogeny:

$$j(E) = 1728\frac{(B - A^2/3)^3}{B^2(B - A^2/4)} = 1728\frac{(1 - t^2/3)^3}{(1 - t^2/4)} = j$$

where we let $t = A^2/B$, and

$$j(E') = 1728\frac{(B + A^2/12)^3}{B(B - A^2/4)} = 1728\frac{(1 + t^2/12)^3}{(1 - t^2/4)} = j'.$$

We can now look for a relation between these two functions. Rewriting, we have

$$j = \frac{4^4(3 - t^2)^3}{4 - t^2} = X, \quad j' = \frac{4(1 + t^2)^3}{(4 - t^2)^2} = Y$$

and we get $\Phi_2(X, Y) = 0$. Setting them equal, we have $j = j'$ iff

$$(B - A^2/4)(B - A^2/3)^3 = B(B + A^2/12)^3.$$

If $A = 0$, $j = j' = 1728$, so this gives one solution. Since $A' = -2A$, $B' = 4B = A^2 - 4B$ so $A^2 - 8B = 0$ is another solution ($(1-2)(1-8/3)^3 = (1+2/3)^3$): $A^2 = 8B = 8000$. What is left is a quadratic equation: letting $\lambda = B/A^2$, $\lambda' = 1/4 - \lambda$, $B \mapsto \lambda$, $A \mapsto 1$, we obtain $(\lambda - 1/8)(\lambda^2 - 1/4\lambda + 4/81) = 0$. We find the final root in $\mathfrak{H}$

$$\lambda = \frac{1}{8} + \frac{5\sqrt{-7}}{72}, \quad j = -3375.$$

Therefore if $E \xrightarrow{2} E$, we have one of the following curves: If $D = -4$, we have $y^2 = x^3 + Bx$, and

$$(x, y) \mapsto \left(\frac{y^2}{2ix^2}, \frac{y(x^2 - B)}{2(1 - i)x^2}\right).$$

If $D = -8$, we have $y^2 = x^3 - 30c^2x + 56c^3$, and

$$(x, y) \mapsto \left(4c - \frac{y^2}{2(x - 4c)}, \frac{-y(x^2 - 8cx - 2c2)}{2\sqrt{-2}(x - 4c)^2}\right).$$

And if $D = -7$, we have $y^2 = x^3 - 35c^2x - 98c^3$, with a complicated rule.

4. A Class Number Relation and Traces of Singular Moduli

For the development of this section, see [22].

Hurwitz-Kronecker class number relation. For $K = \mathbb{Q}(\sqrt{D})$, we have the class group

$$\mathrm{Cl}(D) = \{\mathfrak{a} \subset K : \mathfrak{a}\ \mathbb{Z}\text{-rank } 2,\ \mathrm{mult}(\mathfrak{a}) \simeq \mathscr{O}_D\}/K^\times$$

We let $\#\,\mathrm{Cl}(D) = h(D)$. We define

$$h'(D) = \frac{h(D)}{(1/2)w(D)}$$

where $w(D)$ is the number of roots of unity in $\mathbb{Q}(\sqrt{D})$, thus

$$h'(D) = \begin{cases} 1/3, & D = -3 \\ 1/2, & D = -4 \\ h(D), & \text{otherwise.} \end{cases}$$

We have $\mathscr{Q}_D \supset \mathscr{Q}_D^0$ together with an action of Γ, and

$$\Gamma \setminus \mathscr{Q}_D^0 \simeq \mathrm{Cl}(D)$$
$$[A,B,C] \mapsto (x \mapsto N(x)/N(\mathfrak{a})),\ \mathfrak{a} = \mathbb{Z}A + \mathbb{Z}(B+\sqrt{D})/2.$$

where $Q \mapsto \tau_Q$, a root of $A\tau^2 + B\tau + C = 0$. Let

$$h(D) = \#(\Gamma \setminus \mathscr{Q}_D^0) = \sum_{Q \in \Gamma\setminus\mathscr{Q}_D^0} 1$$

and thus

$$h'(D) = \sum_{Q \in \Gamma\setminus\mathscr{Q}_D^0} \frac{1}{\#\Gamma_Q}$$

where $\#\Gamma_Q$ is the stabilizer of Q by $\Gamma = PSL_2(\mathbb{Z})$. We let $H(D)$ be the same expression dropping the primitivity condition (though we now may no longer have the full endomorphism ring), i.e.

$$H(D) = \sum_{Q \in \Gamma\setminus\mathscr{Q}_D} \frac{1}{\#\Gamma_Q}.$$

$H(D)$ is called the *Hurwitz class number*.

Example. The first nontrivial example is $d = -D = 15$, and we have the roots $\tau = (1+\sqrt{-15})/2$, $\tau^2 - \tau + 4 = 0$, and $\tau = (1+\sqrt{-15})/4$, $2\tau^2 - \tau + 2 = 0$. We find $h(15) = H(15) = 2$, and

$$j = \frac{-191025 \pm 85995\sqrt{5}}{2},$$

respectively.

Continuing in this way, we have

$\lvert D\rvert$	$h'(D)$	$H(D)$	$\lvert D\rvert$	$h'(D)$	$H(D)$
3	1/3	1/3	23	3	3
4	1/2	1/2	24	2	2
7	1	1	27	1	4/3
8	1	1	28	1	2
11	1	1	31	3	3
12	1	4/3	32	2	3
15	2	2	35	2	2
16	1	3/2	36	2	5/2
19	1	1	⋮	⋮	⋮
20	2	2			

Letting $H(D) = H(-D)$, we have

Theorem (Hurwitz-Kronecker)**.** *For all $n > 0$, n not a square, we have*

$$\sum_{|t|<2\sqrt{n}} H(4n - t^2) = \sum_{d|n} \max(d, n/d).$$

If we formally define $H(0) = -1/12$, then the formula is also true when n is a square.

Proof. We have the modular polynomial $\Psi_n(X, Y)$, where the degree of Ψ_n in both X and Y is $\sigma(n)$. For n not a square, we can write

$$\Psi_n(X, X) = \prod_{t^2<4n} \mathscr{H}_{4n-t^2}(X)$$

where

$$\mathscr{H}_D(X) = \prod_{Q\in\Gamma\backslash\mathscr{Q}_D} (X - j(\tau_Q))^{1/\Gamma_Q}.$$

Since $\deg \mathscr{H}_d(X) = H(D)$, $\deg \Psi_n(X, X) = \sum_{t^2<4n} H(4n - t^2)$. We have

$$\begin{aligned}\Psi_n(j(\tau), j(\tau)) = q^{-k} + \cdots &= \prod_{\substack{ad=n\\ 0\le b<d}} (j(\tau) - j((a\tau + b)/d)) \\ &= \prod_M (q^{-1} - \zeta_d^b q^{-a/d} + o(1)).\end{aligned}$$

Counting the order of the poles, we indeed have $k = \sum_{ad=n} \max(a, d)$. □

Traces of singular moduli: definitions. With $h(D) = h$, we showed that for the quadratic forms $\Gamma \setminus \mathscr{Q}_D^0 = \{Q_1, \ldots, Q_h\}$ the numbers $j(\tau_{Q_1}), \ldots, j(\tau_{Q_h})$ are conjugate algebraic numbers. Thus

$$\operatorname{Tr}(j((D + \sqrt{D})/2)) = \sum_{i=1}^{h(D)} j(\tau_{Q_i}).$$

This does not quite have the right analytic properties, so we replace $\mathscr{Q}_D^0$ with $\mathscr{Q}_D$, and count with multiplicities $1/\#\Gamma_Q$ as above.

Note that when we defined $j(\tau) = E_4(\tau)^3/\Delta(\tau) = q^{-1} + 744 + \ldots$, we could have replaced the constant with any other and still have a modular function; we may also choose to define $J(\tau) = j(\tau) - 744$ so that J has no constant term.

Definition. We let

$$t(d) = \sum_{Q\in\Gamma\mathscr{Q}_D} \frac{1}{\#\Gamma_Q} J(\tau_Q)$$

where $d = -D$.

Example. Following the computation above, we have the following values:

d	$H(d)$	$t(d)$
3	1/3	$-248 = (0 - 744)/3$
4	1/2	$492 = (1728 - 744)/2$
7	1	-4119
8	1	7256
11	1	-33512
12	4/3	53008
15	2	-192513
16	3/2	287244
19	1	-885480

In the following discussion, we need the following modular forms:

$$E_4(\tau) = 1 + 240(q + 9q^2 + \cdots + \sigma_3(n)q^n + \dots)$$
$$\Delta(\tau) = \frac{1}{1728}(E_4^3 - E_6^2) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$$
$$\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n) = q^{1/24} - q^{25/24} - \dots$$
$$\theta_1(\tau) = \sum_{n=-\infty}^{\infty}(-1)^n q^{n^2} = 1 - 2q + 2q^4 - 2q^9 + \dots$$

Definition. We define the weight 3/2 modular form

$$g(\tau) = \theta_1(\tau)\frac{E_4(4\tau)}{\eta(4\tau)^6} = (1 - 2q + 2q^4 + \dots)\frac{1 + 240q^4 + \dots}{q(1 - 6q^4 + \dots)}$$
$$= q^{-1} - 2 + 248q^3 - 492q^4 + 4199q^7 - \dots.$$

A quick check suggests:

Theorem. *Write $g(\tau) = \sum_{n=-1}^{\infty} B_n q^n$. Then $t(n) = -B_n$ for all $n > 0$.*

This theorem will follow from the following:

Theorem. *For all $n > 0$:*

(i) $$\sum_{r^2<4n} H(4n - r^2) = \sum_{d|n}\max(d, n/d) + \begin{cases} 1/6, & n \text{ a square;} \\ 0, & \text{else.} \end{cases}$$

(ii) $$\sum_{r^2<4n} (n - r^2)H(4n - r^2) = \sum_{d|n}\min(d, n/d)^3 - \begin{cases} n/2, & n \text{ a square;} \\ 0, & \text{else.} \end{cases}$$

(iii) $$\sum_{r^2<4n} t(4n - r^2) = \begin{cases} -4, & n \text{ a square;} \\ 2, & 4n+1 \text{ a square;} \\ 0, & \text{else.} \end{cases}$$

(iv) $$\sum_{1\le r<2\sqrt{n}} r^2 t(4n - r^2) = -240\sigma_3(n) + \begin{cases} -8n, & n \text{ a square;} \\ 4n+1, & 4n+1 \text{ a square;} \\ 0, & \text{else.} \end{cases}$$

If we take $H(0) = -1/12$, we can replace these with the simpler expressions:

(i) $$\sum_{r^2\le 4n} H(4n - r^2) = \sum_{d|n}\max(d, n/d).$$

(ii) $$\sum_{r^2\le 4n} (n - r^2)H(4n - r^2) = \sum_{d|n}\min(d, n/d)^3.$$

(iii) $$\sum_{r^2\le 4n+1} t(4n - r^2) = 0.$$

(iv) $$\sum_{1\le r\le\sqrt{4n+1}} r^2 t(4n - r^2) = -240\sigma_3(n).$$

In fact, these relations completely determine t and H successively, as we will see below.

Example. Let $n = 3$. We compute inductively in pairs. By (1) and (2),

$$H(12) + 2H(11) + 2 + 2(1/3) = 3 + 3 = 6$$
$$3H(12) + 4H(11) - 2 - 12(1/3) = 1 + 1 = 2$$

Solving these we find $H(11) = 1$, $H(12) = 4/3$. Similarly, once can compute $t(12)$ and $t(11)$.

Traces of singular moduli: proofs I. See [22, §2].

Proof (Equalities (iii)–(iv) imply the first theorem). We show that B_n satisfy the same equations (iii) and (iv) as $t(n)$. Since t is unique (as the above example suggests), this will imply the result.

We have

$$g(\tau) = q^{-1} - 2 + 248q^3 - \cdots = \sum_{n \equiv 0,3 \ (4)} B_n q^n \in M_{3/2}^+(\Gamma_0(4)).$$

But also we have

$$\theta(\tau) = \sum_{n \in \mathbb{Z}} q^{n^2} = 1 + 2q + 2q^4 + \cdots \in M_{1/2}^+(\Gamma_0(4))$$

with nonzero coefficients only when $n \equiv 0, 1 \pmod 4$. We multiply these:

$$g(\tau)\theta(\tau) = (q^{-1} - 2 + 248q^3 + \dots)(1 + 2q + 2q^4 + \dots) = q^{-1} + 0 + \cdots \in M_2(\Gamma_0(4))$$

which has every coefficient 2 (mod 4) equal to zero. Applying the U_2 operator which acts by $\sum_n a_n q^n \mapsto \sum_n a_{2n} q^n$, we obtain an element of $M_2(\Gamma_0(2))$ with only even coefficients, which then lives in $M_2(\Gamma(1))$; but this space is empty, therefore the form is constant and thus identically zero. In other words,

$$\begin{aligned}\left(\sum_d B_d q^d\right)\left(\sum_r q^{r^2}\right)\Big| U_4 &= \sum_n \left(\sum_r B_{n-r^2} q^n\right)\Big| U_4 \\ &= \sum_n \left(\sum_r B_{4n-r^2}\right) q^n = 0.\end{aligned}$$

For the other, use the Rankin-Cohen bracket; check that $g'(\tau)\theta(\tau) - 3g(\tau)\theta'(\tau) \in M_4(\Gamma_0(4))$ is modular with all coefficients with $n \equiv 2 \pmod 4$ equal to zero, so that we actually have an element of $M_4(SL_2(\mathbb{Z}))$, hence a constant multiple of E_4:

$$\begin{aligned}\left(g'\theta - 3g\theta'\right)|U_4 &= \left(\sum_d dB_d q^d\right)\left(\sum_r q^{r^2}\right) - 3\left(\sum_d B_d q^d\right)\left(\sum_r r^2 q^{r^2}\right)\Big| U_4 \\ &= \sum_r (4 - r^2 - 3r^2) B_d q^r.\end{aligned}$$

□

We now proceed to ([22, §3]):

Proof of (i) and (ii). For all $n \in \mathbb{N}$, we have $\Psi_n(X, Y) \in \mathbb{Z}[X, Y]$ with

$$\Psi_n(X, j(\tau)) = \prod_{M \in \Gamma \backslash \mathscr{M}_n} (X - j(M\tau)) = \prod_{\substack{ad=n \\ 0 \le b < d}} (X - j((a\tau + b)/d)$$

where $\mathscr{M}_n = \{M \in M_2(\mathbb{Z}) : \det M = n\}$. Then $\Psi_n(j(\tau), j(\tau)) = 0$ iff $\tau = M\tau$ for some $M \in \mathscr{M}_n$, which happens iff τ has CM by $\mathscr{O}_D$ where n is a norm in $\mathscr{O}_D$, $D = r^2 - 4n$. Thus for n not a square,

$$\Psi_n(X, X) = \prod_{r^2<4n} \mathscr{H}_{4n-r^2}(X),$$

where for all $d > 0$, $d \equiv 0, 3 \pmod 4$ we have

$$\mathscr{H}_d(X) = \prod_{\tau \in \Gamma\backslash \mathscr{Q}_d} (X - j(\tau_Q))^{1/\#\Gamma_Q}$$

($\mathscr{H}_d$ is a polynomial except for the cases $\mathscr{H}_3(X) = \sqrt[3]{X}$ and $\mathscr{H}_4(X) = \sqrt{X - 1728}$).

So $\mathscr{H}_d(X) = \prod_{i=1}^{H(d)} (X_j(\tau_i))$, and

$$\begin{aligned}\mathscr{H}_d(j(\tau)) &= \prod_{i=1}^{H(D)} (J(\tau) - J(\tau_i)) = \prod_{Q \in \Gamma\backslash \mathscr{Q}_D} (q^{-1} - J(\tau_Q) + O(q))^{1/\#\Gamma_Q} \\ &= q^{-H(d)}(1 - t(d)q + O(q^2)).\end{aligned}$$

and

$$\begin{aligned}\Psi_n(j(\tau), j(\tau)) &= \prod_{r^2<4n} \mathscr{H}_{4n-r^2}(j(\tau)) \\ &= q^{-\sum_r H(4n-r^2)}(1 - (\textstyle\sum_r t(4n - r^2))q + O(q^2)).\end{aligned}$$

Indeed,

$$\begin{aligned}\Psi_n(j(\tau), j(\tau)) &= \prod_{\substack{ad=n \\ 0\le b<d}} (q^{-1} - \zeta_d^b q^{-a/d} + 0 + O(q^{>0})) \\ &= \prod_{ad=n} (q^{-1} - \zeta_d^b q^{-a/d})(1 + O(q^{>1})) \\ &= \prod_{ad=n} (q^{-d} - q^{-a})(1 + O(q^2)) = \pm q^{-\sum_{ad=n} \max(a,d)} + \dots\end{aligned}$$

which proves (i). For (ii), we have the term $1 + \epsilon q + O(q^2)$ instead, where $\epsilon = -2$ if $n = \ell(\ell + 1)$, i.e. $4n + 1$ is a square.

If n is a square, $\Psi_n(X, X) = 0$; instead we use

$$\left.\frac{\Psi_n(X, Y)}{\Psi_1(X, Y)}\right|_{X=Y} = \frac{\prod_{r^2<4n} \mathscr{H}_{4n-r^2}(X)}{\mathscr{H}_4(X)\mathscr{H}_3(X)^2}$$

which implies the result up to a simple correction factor. □

Remark. In fact, the calculation $\#(C_1 \cap C_2) = [C_1] \cdot [C_2]$ is actually one of homology on $H(\mathbb{S}^2 \times \mathbb{S}^2) \simeq \mathbb{Z} \times \mathbb{Z}$. This looks locally like four branched lines, which correspond to four points in the projective line which will have a nontrivial invariant—therefore this is not just a homology intersection but sections are also involved, explaining the higher weight.

Traces of singular moduli: proofs II. Now consult [22, §4]. To prove (iii) and (iv), we need to set up some more machinery. We start with

$$\Psi_n(X,X) = \prod_{r^2<4n} \mathscr{H}_{4n-r^2}(X)$$

and take the logarithmic derivative of both sides to obtain

$$\sum_{M\in\Gamma\backslash\mathscr{M}_n} \frac{1}{(j(\tau)-j(M\tau))} = \sum_r \Lambda_{4n-r^2}(\tau)$$

where

$$\Lambda_d(\tau) = \frac{1}{2\pi\tau}\frac{d}{d\tau}\log \mathscr{H}_D(j(\tau)) = \frac{-1}{2\pi i} j'(\tau)\frac{\mathscr{H}_D'(j(\tau))}{\mathscr{H}_D(j(\tau))}$$

so since $j = E_4^3/\Delta$, $-1/(2\pi i)dj/d\tau = E_4^2E_6/\Delta$ by uniqueness.

Differentiating the relation in the preceding proof, we find

$$\Lambda_d(\tau) = H(d) + t(d)q + O(q^2).$$

Proposition. *We have*

$$\frac{E_4(\tau)E_6(\tau)}{\Delta(\tau)} \sum_{M\in\Gamma\backslash\mathscr{M}_n} \frac{(E_4|M)(\tau)}{j(\tau)-j(M\tau)} = \frac{1}{2}\sum_{r^2<4n}(n-r^2)\Lambda_{4n-r^2}(\tau)$$

where for $M = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathscr{M}_n$ *we let*

$$(E_4|M)(\tau) = \frac{n^3}{(c\tau+d)^4} E_4\left(\frac{a\tau+b}{c\tau+d}\right)$$

so $E_4|(\gamma M) = E_4|M$.

Proof. Both sides are meromorphic modular of weight 2, as $\tau\mapsto\gamma\tau$ just permutes M. Both are holomorphic at ∞ because each term is bounded. Both have only simple poles, since locally there are no multiple intersections. If the residues at the poles are the same, we are done.

Let $M\alpha = \alpha$, $M = \begin{pmatrix} a & b \\ c & d\end{pmatrix}$, $\lambda = c\alpha+d$, where α is a CM point. Then the residue of the left-hand side at $\tau=\alpha$ is

$$\begin{aligned}\frac{E_4(\alpha)E_6(\alpha)}{\Delta(\alpha)}\frac{(E_4|M)(\alpha)}{j'(\alpha)-(n/\lambda^2)j'(M\alpha)} &= \frac{E_4(\alpha)E_6(\alpha)}{\Delta(\alpha)}\frac{(n^3/\lambda^4)E_4(\alpha)}{(1-n/\lambda^2)j'(\alpha)} \\ &= \frac{-1}{2\pi i}\left(\frac{n^3/\lambda^4}{1-n/\lambda^2}\right) = \frac{-1}{2\pi i}\left(\frac{\overline{\lambda}^3}{\lambda-\overline{\lambda}}\right)\end{aligned}$$

since $n=\lambda\overline{\lambda}$, $M(\alpha,1)^t = \lambda(\alpha,1)^t$, $\lambda+\overline{\lambda}=r$. Therefore we obtain

$$\begin{aligned}\frac{-1}{2\pi i}\sum_{r^2<4n}\sum_{\alpha\in\mathscr{Q}_{r^2-4n}/\Gamma}\frac{-\overline{\lambda}^3}{\lambda-\overline{\lambda}} &= \frac{1}{4\pi i}\sum_r\sum_\alpha \frac{\lambda^3-\overline{\lambda}^3}{\lambda-\overline{\lambda}} \\ &= \frac{1}{4\pi i}\sum_{r^2<4n}\left(\lambda^2+\lambda\overline{\lambda}+\overline{\lambda}^2\right) = (\lambda+\overline{\lambda})^2-\lambda\overline{\lambda} = r^2-n\end{aligned}$$

If we total these, we will find simple poles, each with residue 1, added r^2-n times.

As $\tau \to \infty$, $q \to 0$, the right-hand side becomes

$$\frac{1}{2}\sum_{r^2<4n}(n-r^2)\left(H(4n-r^2)+t(4n-r^2)q+O(q^2)\right).$$

Expanding, we have on the left-hand side

$$\frac{(1+240q+\dots)(1-504q+\dots)}{q(1-24q+\dots)}\sum_{\substack{ad=n\\0\le b<d}}\left(\frac{a^3}{d}\right)\frac{E_4((a\tau+b)/d)}{j(\tau)-j((a\tau+b)/d)}$$

$$=q^{-1}(1-240q+\dots)\sum_{ad=n}\frac{a^3}{d}\sum_{b\pmod d}\frac{1+240\sum_{\ell=1}^{\infty}\sigma_3(\ell)\zeta_d^{b\ell}q^{a\ell/d}}{q^{-1}-\zeta_d^b q^{-a/d}+O(q^{>0})}$$

so if $a<d$, this becomes

$$\sum_{b\pmod d}240q\left(\sum_{\ell}\sigma_3(\ell)\zeta_d^{b\ell}q^{a\ell/d}\right)\left(\sum_{m=0}^{\infty}\zeta_d^{-bm}q^{(1-a/d)m}\right)$$

$$=240q\sum_{\ell,m}\sigma_3(\ell)q^{a\ell/d+m(1-a/d)}\begin{cases}d, & l\equiv m \pmod d\\ 0, & \text{else}\end{cases}$$

$$=qd(1+(240\sigma_3(\ell)\delta_{a,1}+\delta_{a,d-1})q+\dots).$$

We find that $\ell=m=1$ or $\ell=d, m=0$ $(a=1)$ or $\ell=0, m=d$ $(a=d-1)$. In total, we have

$$a^3(1+(240\sigma_3(d)\delta_{a,1}+\delta_{a,d-1}+\dots)q+O(q^2)$$

For $a>d$, there is no constant term, and we get $a^3(0+(-\delta_{a,d+1})q+O(q^2))$ so the sum is

$$\sum_{\substack{0<a<\sqrt{n}\\ a|n}}a^3+(240\sigma_3(d)+\epsilon)q+\dots$$

for a correction factor ϵ if $n=k(k+1)$. Altogether, this gives the result. □

Remark. This can be generalized as follows: we let

$$M_{3/2}^{+}=\sum_{\substack{d\gg-\infty\\ d\equiv 0,3\ (4)}}B_d q^d$$

where the + signifies allowing one pole. This space is generated by the forms

$$g_1=q^{-1}-2+248q^3-492q^4+\dots$$
$$g_4=q^{-4}-2-26752q^3-\dots$$
$$q_5=q^{-5}+85995q^3+\dots$$

Notice that

$$\frac{1}{\sqrt{5}}(j(\alpha_{-15})-j(\alpha'_{-15}))=(-191025-85995\sqrt{5})/2$$

so in some sense these represent twisted traces. We find the form

$$q^{-1}+10-64q^3+108q^4+\dots\in M_{-1/2}^{+},$$

where now the coefficients are the sum of $K(\alpha_Q)/\Gamma_Q$ for a different modular function K: letting $j(\tau) = E_4(\tau)^3/\Delta(\tau)$, the function

$$E_2^*(\tau) = E_2(\tau) - \frac{3}{\pi \operatorname{Im}(\tau)}$$

is modular of weight 2, and then

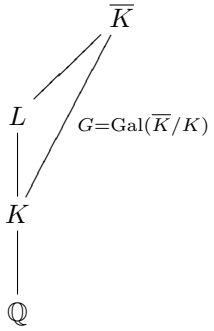
$$K(\tau) = \frac{E_2^* E_4 E_6 + 3E_4^3 + 2E_6^2}{6\Delta(\tau)}.$$

We have a similar theorem that if τ is CM then $K(\tau) \in \overline{\mathbb{Q}}$.

5. Constructing Class Fields

A review of class field theory. For the results of this section, see [8]. For a more general reference on class field theory, see [14, Chapter VI], [12, Part 2], or [1].

For K be a number field, one of the main motivating problems of algebraic number theory is to characterize finite extensions L/K.



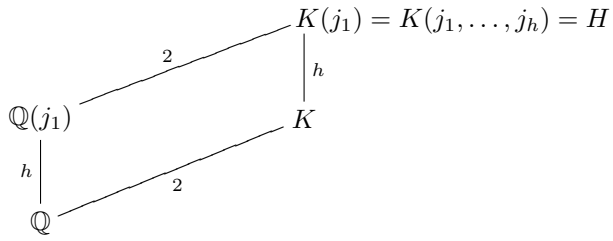
If L/K is Galois and abelian, then class field theory gives a one-to-one correspondence between such extensions and something explicit, namely, decompositions of ideals of K into classes.

We have the usual class group $\mathrm{Cl}(K)$ as the quotient of all fractional ideals by principal fractional ideals, with $\#\,\mathrm{Cl}(K) = h(K) < \infty$. In this case, the usual classes correspond to the Hilbert class field H of K which is the maximal abelian unramified extension of K (which class field theory says is of finite degree, indeed $[H : K] = h(K)$).

Theorem. *Let $K = \mathbb{Q}(\sqrt{D})$ for $D < 0$ squarefree, and*

$$h = h(K) = \#(\mathscr{Q}_D/\Gamma) = \#\{\tau \in \mathfrak{H}/\Gamma : \tau \text{ quadratic},\ D(\tau) = D\}.$$

Let $j_1 = j(\tau_1), \dots, j_h = j(\tau_h) \in \overline{\mathbb{Z}}$ be the corresponding conjugate algebraic integers. Then the Hilbert class field $H = K(j_1) = K(j_1, \dots, j_h)$.



Pick $\mathfrak{m} \subset \mathbb{Z}_K$ integral (this may involve some real place), and let $I_\mathfrak{m}$ be the set of fractional ideals prime to $\mathfrak{m}$ (in numerator and denominator); $I_\mathfrak{m}$ is a group under multiplication [14, §VI.1]. Let $P_\mathfrak{m} = \{\langle\xi\rangle : \xi \equiv 1 \pmod{m}\}$, which in the case $\mathfrak{p}_\infty \mid \mathfrak{m}$ corresponding to $\sigma : K \hookrightarrow \mathbb{R}$, we insist $\sigma(\xi) > 0$. If L/K is Galois, we let $N_\mathfrak{m}(L/K) = N_{L/K}(I_\mathfrak{m}(L))P_\mathfrak{m}(K)$.

Theorem (Second inequality of class field theory)**.**

$$h_\mathfrak{m}(L/K) = [I_\mathfrak{m} : N_\mathfrak{m}] \leq [L : K].$$

See e.g. [8, §4].

Definition. L/K is a *class field* if $h_\mathfrak{m}(L/K) = [L : K]$ for some $\mathfrak{m}$. The smallest such $\mathfrak{m}$ is called the *conductor*, $\mathfrak{f}$.

We have that

$$P_\mathfrak{m}(K) \subset N_\mathfrak{m}(L/K) \subset I_\mathfrak{m}(K).$$

The reason:

$$\{\mathfrak{p} : \mathfrak{p} \text{ a norm from } L\} \subset \{\mathfrak{p} : \mathfrak{p} \in N_\mathfrak{m}\} \subset \{\mathfrak{p} : \mathfrak{p} \in \mathbb{Z}_K\}.$$

The first has density $1/[L : K]$, the second has density $1/h_\mathfrak{m}(L/K)$.

Example. If $K = \mathbb{Q}$, $\mathfrak{m} = \langle p\rangle$, $p \equiv 1 \pmod 4$, $I_\mathfrak{m} = \langle\alpha\rangle$ prime to p, $P_\mathfrak{m} = \{\langle\xi\rangle : \xi \equiv 1 \pmod p\}$. $L = \mathbb{Q}(\sqrt{p})$ has $N = N_{L/K}(\mathfrak{a}) = ax^2 + bxy + cy^2$ where $b^2 - 4ac = p$, so $4aN = (2ax + by)^2 - py$, so $\left(\frac{N}{p}\right) = \left(\frac{a}{p}\right) = 1$.

Therefore $N_\mathfrak{m}(L/K)/P_\mathfrak{m} = ((\mathbb{Z}/p\mathbb{Z})^\times)^2$, and $\langle\alpha\rangle \sim \langle\beta\rangle$ if $\alpha \equiv \beta \pmod p$ and $\left(\frac{\alpha}{p}\right) = \left(\frac{\beta}{p}\right)$.

Theorem (Main theorem of class field theory)**.**

(i) *L/K is a class field iff L/K is abelian.*
(ii) *Given any $I_\mathfrak{m} \supset H \supset P_\mathfrak{m}$, there exists a unique class field L/K such that $H = N_\mathfrak{m}(L/K)$, so $[L : K] = (I_\mathfrak{m} : H)$.*
(iii) *$\mathfrak{p}$ is ramified in L/K iff $\mathfrak{p} \mid \mathfrak{f}(L/K)$.*
(iv) *(Artin reciprocity)* $\mathrm{Gal}(L/K) \simeq I_\mathfrak{m}/N_\mathfrak{m}(L/K)$.

See [8, §6]. For example, if we take $\mathscr{O}_K$, then $\mathrm{Gal}(H/K) \simeq \mathrm{Cl}(K)$.

The Artin map is defined as follows $I_\mathfrak{m}/H \to \mathrm{Gal}(L/K)$ by $[\mathfrak{a}] \mapsto \sigma_\mathfrak{a}$, defined multiplicatively where $[\mathfrak{p}] \mapsto \sigma_\mathfrak{p} = \mathrm{Frob}_\mathfrak{p}$, where $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$ for all $x \in \mathscr{O}_L$, so $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/K)$ is well-defined up to conjugation (for an abelian extension this condition is trivial).

To sum up, we have some partition of the (fractional) ideals of K, prime to some $\mathfrak{m}$, into finitely many classes $\mathscr{A}_1 = [\mathscr{O}], \ldots, \mathscr{A}_h$, such that if $\lambda \equiv 1 \pmod m$ for $\lambda \in K^\times$, then $\langle\lambda\rangle \in \mathscr{A}_1$.

Then the splitting of any prime ideal $\mathfrak{p}$ of K depends only on the class of $\mathfrak{p}$. We have $N_{L/K}(\mathfrak{P}_i) = \mathfrak{p}^f$, $fg = n$, f is the smallest number such that $\mathfrak{p}^f \in \mathscr{A}_1$. Every $N_{L/K}(\mathfrak{A}) = \mathfrak{a}$, implies $\mathfrak{a} \in \mathscr{A}_1$, so $N_\mathfrak{m}(L/K) \subset H \subset I_\mathfrak{m}(K)$, where the quotient $I_\mathfrak{m}(K)/N_\mathfrak{m}(L/K) \simeq \mathrm{Gal}(L/K)$.

Kronecker's congruence. If we take $K = \mathbb{Q}(\sqrt{D})$, we have $\tau_1, \ldots, \tau_h \in \mathfrak{H}/\Gamma$ where $h(K) = h = h(D)$, from $j(\tau_1), \ldots, j(\tau_h)$ by associating $\mathfrak{a}$ to $j(\mathfrak{a})$.

Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice; we define $\widetilde{f}(L) = \omega_2^{-k} f(\omega_1/\omega_2)$ implied by

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau).$$

so $\widetilde{f}(tL) = t^{-k}\widetilde{f}(L)$ for all $t \in \mathbb{C}^\times$. Thus modular forms of weight k correspond to functions of lattices which are homogeneous of degree k.

A modular function has $k = 0$, $\mathfrak{a} \mapsto j(\mathfrak{a}) = \mathbb{C}/\mathfrak{a} = j(\mathbb{Z}\tau + \mathbb{Z}) = j(\tau)$, and then we have $j(\lambda\mathfrak{a}) = j(\mathfrak{a})$, $\mathrm{Cl}(K) \to \overline{\mathbb{Q}}$.

Theorem. *If $\langle p\rangle = \mathfrak{p}\overline{\mathfrak{p}}$, $\mathfrak{p} \neq \overline{\mathfrak{p}}$, $\left(\frac{D}{p}\right) = 1$, and $\mathfrak{a}$ is a (fractional) ideal, then*

$$j(\mathfrak{a}\mathfrak{p}) \equiv j(\mathfrak{a})^p \pmod{\overline{\mathfrak{p}}}$$

(i.e. $j(\mathfrak{a}\mathfrak{p}) = \sigma_{\overline{\mathfrak{p}}}(j(\mathfrak{a}))$).

We will first prove that the congruence holds modulo $\mathfrak{p}$ or modulo $\overline{\mathfrak{p}}$, since then

$$j(\mathfrak{a}\mathfrak{p}\overline{\mathfrak{p}}) = j(\mathfrak{a}) \equiv j(\mathfrak{a}\overline{\mathfrak{p}})^p \pmod{\overline{\mathfrak{p}}}.$$

Claim (Kronecker's congruence). If $X = j(\alpha)$, $Y = j(\mathfrak{p}\mathfrak{a})$, then

$$(X - Y^p)(X^p - Y) \equiv 0 \pmod{p}.$$

Proof of claim. (See also [2, II, §5, Theorem 2], [11, §10.1, Theorem 1].) We have

$$\Phi_n(X, j(\tau)) = \prod_{M \in \Gamma\backslash\mathscr{M}_n^0} (X - j(M\tau)) \in \mathbb{Z}[X].$$

For $n = p$,

$$\Phi_p(X, j(\tau)) = (X - j(p\tau))(X - j(\tau/p)) \dots (X - j((\tau + p - 1)/p))$$

which is in $\mathbb{Z}[\zeta_p]((q^{1/p}))$. Let $\pi = 1 - \zeta_p$, so that $\pi \mid p$ and $\zeta_p \equiv 1 \pmod{\pi}$. We have $j(\tau) = q^{-1} + \dots$, hence $j(p\tau) = q^{-p} + \dots$, and $j(\tau/p) = q^{-1/p} + \dots$. Thus

$$\begin{aligned}\Phi_p(X, j(\tau)) &\equiv \left(X - \textstyle\sum_n c_n q^{np}\right)\left(X - \sum_n c_n q^{n/p}\right)^p \\ &\equiv \left(X - j(\tau)^p\right)\left(X^p - \textstyle\sum_n c_n^p q^n\right) \\ &\equiv (X - j(\tau)^p)(X^p - j(\tau)) \pmod{\pi}.\end{aligned}$$

Thus

$$\Phi(X, Y) \equiv (X - Y^p)(X^p - Y) \pmod{p}$$

in $\mathbb{Z}[X, Y]$. □

Letting $X = j(\mathfrak{a})$, $Y = j(\mathfrak{a}\mathfrak{p})$, we have the theorem. (Also see [8, §9].)

The function $\phi_M(\tau)$ and the polynomial $D_n(X, j(\tau))$. If $\mathfrak{a}$ as a lattice is spanned by ω_1, ω_2, then $\mathfrak{a}\mathfrak{p}$ is spanned by $a\omega_1 + b\omega_2, c\omega_1 + d\omega_2$, with $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\det P = p$. Similarly we have a matrix $\overline{P}$ that acts as multiplication by $\overline{\mathfrak{p}}$.

If $f \in M_k$, $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $f(L) = \overline{f}(L) = \omega_2^{-k} f(\omega_1/\omega_2)$. Then the correspondence $L \mapsto \Delta(L) \in \mathbb{C}$ has $\Delta(tL) = t^{-12}\Delta(L)$ for $t \in \mathbb{C}^\times$, where

$$\Delta(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \eta(C)^{24} \in M_{12}.$$

The function $F(\tau) = \sqrt{\operatorname{Im}\tau}|\eta(\tau)|^2$ has "weight zero" (it is not holomorphic, but $F : \mathfrak{H}/\Gamma \to \mathbb{R}_{>0}$ is well-defined). Since

$$\eta\left(\frac{a\tau + b}{c\tau + d}\right) = \zeta_{24}^n \left(\sqrt{c\tau + d}\right) \eta(\tau),$$

we have $|\eta(\gamma\tau)| = |c\tau + d|^{1/2}\eta(\tau)$ and $\operatorname{Im}(\gamma\tau) = 1/|c\tau + d|^2$.

If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathscr{M}_n$, we define

$$(\Delta|M)(\tau) = n^{12}(c\tau + d)^{-12}\Delta\left(\frac{a\tau + b}{c\tau + d}\right).$$

We have $(\Delta|M_1)|M_2 = \Delta|(M_1M_2)$, $\Delta|\gamma = \Delta$ for $\gamma \in \Gamma = SL_2(\mathbb{Z})$, so the definition depends only on $M \in \Gamma/\mathscr{M}_n$.

Let $\phi_M(\tau) = (\Delta|M)(\tau)/\Delta(\tau)$.

Proposition. *If $\tau \in \mathfrak{H}$ is a CM point, then $\phi_M(\tau) \in \overline{\mathbb{Q}}$.*

In fact, later we will show that $\phi_M(\tau)$ is a unit away from n.

Proof. (See also [2, II, §2].) The polynomial

$$D_n(X, j(\tau)) = \prod_{M \in \Gamma\backslash\mathscr{M}_n} (X - \phi_M(\tau))$$

is Γ-invariant, as

$$\phi_M(\gamma\tau) = \frac{(\Delta|M)(\gamma\tau)(c\tau + d)^{-12}}{(\Delta(\gamma\tau))(c\tau + d)^{-12}} = \phi_{M\gamma}(\tau).$$

Moreover, $D_n(X, Y) \in \mathbb{Z}[X, Y]$, since taking the usual cosets

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = n,\ 0 \le b < d \right\}$$

we have

$$D_n(X, j(\tau)) = \prod_{\substack{ad=n \\ 0<b\le d}} \left(X - \frac{a^{12}\Delta((a\tau + b)/d)}{\Delta(\tau)}\right) = \prod_{ad=n} \frac{a^{12}\zeta_\ell^b q^{a/d}(1 - 24\zeta_q^{a/d} + \dots)}{q(1 - 24q - \dots)}$$

so as with the proof for $\Psi_n(X, j(\tau))$ the polynomial must have integer coefficients. □

We actually have that:

Theorem. *If $n \in \mathbb{N}$, there exists a polynomial $D_n(X, Y) \in \mathbb{Z}[X, Y]$ such that*

$$\prod_{M \in \Gamma\backslash\mathscr{M}_n} (X - \phi_M(\tau)) = D_n(X, j(\tau)),$$

and $D_p(0, Y) = (-1)^{p-1}p^{12}$.

Proof. (See also [2, II, §2, Lemma 1].) The calculation of the constant coefficient in X is as follows:

$$\begin{aligned} -\phi_{\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)}(\tau) \prod_{b=0}^{p-1} (-\phi_{\left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right)}(\tau) &= p^{-12}\frac{\Delta(p\tau)}{\Delta(\tau)} \prod_{b=0}^{p-1} \frac{\Delta((\tau + b)/p)}{\Delta(\tau)} \\ &= p^{-12}\frac{q^p(1 + \dots)}{q(1 + \dots)} \prod_{b=0}^{p-1} \frac{\zeta_p^b q^{1/p} + \dots}{q(1 + \dots)} \\ &= p^{12}\zeta_p^{1+\dots+p(p-1)/2}(1 + O(q)) \end{aligned}$$

so the constant coefficient is $p^{12}(-1)^{p-1}$. □

Corollary. *If τ is a CM point, $M \in \mathscr{M}_n$, then $\phi_M(\tau) \in \overline{\mathbb{Z}}$.*

Proof. It is a root of a monic equation with coefficients in $\overline{\mathbb{Z}}$. □

We have $j(L) = j(\omega_1/\omega_2) = j(\mathbb{C}/L)$ (e.g. $\mathfrak{a} \subset \mathbb{C}$) if $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, and similarly $\Delta(L) = \omega_2^{-12}\Delta(\omega_1/\omega_2)$, which is independent of the choice of basis, and $\Delta(tL) = t^{-12}\Delta(L)$.

The proof of the congruence. We have shown $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \pmod p$, so

$$(j(\mathfrak{ap}) - j(\mathfrak{a})^p)(j(\mathfrak{ap})^p - j(\mathfrak{a})) \equiv 0 \pmod p.$$

Recall we have that $N_{L/K}(I_{\mathfrak{m}}(L)) \subset H \subset I_{\mathfrak{m}}(K)$ with

$$I_{\mathfrak{m}}(K)/H \simeq \mathrm{Gal}(L/K)$$
$$[\mathfrak{p}] \mapsto \mathrm{Frob}_{\mathfrak{p}}$$

Proof of the theorem. (See also [8, §8].) Let $j_1, \dots, j_h$ be conjugate over $\mathbb{Q}$, and let L be the Galois closure of $K(j_1, \dots, j_h)$. The prime ideals $\mathfrak{p}$ of K of degree 1, i.e. those with $N(\mathfrak{p}) = p$, $\langle p \rangle = \mathfrak{p}\overline{\mathfrak{p}}$, have density of order $1/h$. Let $\mathfrak{p}$ be unramified in L/K, with $\mathfrak{p} \nmid (j_i - \sigma(j_i))$ for $\sigma \in \mathrm{Gal}(L/K)$ and $i = 1, \dots, h$.

We know that

$$\mathrm{Frob}_{\mathfrak{p}}(j(\mathfrak{a})) \equiv j(\mathfrak{a})^p \equiv j(\mathfrak{a}\overline{\mathfrak{p}}) \pmod{\mathfrak{P}},$$

so that $\mathrm{Frob}_{\mathfrak{p}}(j(\mathfrak{a})) = j(\mathfrak{ap})$ for infinitely many $\mathfrak{p}$.

So for all $\sigma \in \mathrm{Gal}(L/K)$, the set contains infinitely many $\mathfrak{p}$ with $\mathrm{Frob}_{\mathfrak{p}} = \sigma$. Therefore $\sigma(j(\mathfrak{a}))$ is already contained in the conjugates above, so the original extension is Galois. Density $1/h$ primes have $\mathrm{Frob}_{\mathfrak{p}}(j(\mathfrak{a})) = j(\mathfrak{a}\overline{\mathfrak{p}})$, but class field theory says that this must be $\le 1/h$ with $= 1/h$ if it is the class field, so $\mathrm{Frob}_{\mathfrak{p}}(j(\mathfrak{a})) = j(\mathfrak{a}\overline{\mathfrak{p}})$. □

Explicit examples. As examples, we have

$$D_1(X,Y) = X - 1$$
$$D_2(X,Y) = (X + 2^4)^3 - XY$$
$$D_3(X,Y) = (X - 3^2)^3(X - 3^6) + 72X(X + 21)Y - XY^2$$
$$D_5(X,Y) = (X^2 - 8050X + 5^4)^3 + 800X(X + 25)(47X^2 + 269650X + 29375)Y$$
$$- 20X(207X^2 - 254750X + 129375)Y^2 + 120X(X + 25)Y^3 - XY^4$$

Example. For $D = -7$, $\tau_0 = (1 + \sqrt{-7})/4$, $j(\tau_0) = -3375 = -15^3$.

$$D_2(X, -3375) = (X + 16)^3 + 15^3X = (X + 1)(X^2 + 47X + 2^{12})$$

has roots $-1, \tau_0^{12}, \overline{\tau_0}^{12}$. Hence $\mathfrak{p}\overline{\mathfrak{p}} = 2$, but $\mathfrak{p} = \langle z_0 \rangle$.

$$\Gamma \setminus \mathscr{M}_2 = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, P = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \overline{P} = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \right\}$$

corresponding to

$$\tau_0 \mapsto 2\tau_0 = [1, 1 + \sqrt{-7}], \tau_0/2 = [2, (1 + \sqrt{-7})/2], (\tau_0 + 1)/2.$$

Note $j(2\tau_0) = 255^3$, $j(\tau_0/2) = -15^3$, $j((\tau_0 + 1)/2) = -15^3$, and we have:

M	$\phi_M(\tau_0)$
2τ	-1
$\tau/2$	$\overline{\tau_0}^{12}$
$(\tau + 1)/2$	τ_0^{12}

Example. For $D=-15$, $h(D)=2$, and $\tau_0=(1+\sqrt{-15})/2$, $\tau_1=\tau_0/2$. $j(\tau_0)=\lambda$, $j(\tau_1)=\lambda'=\overline{\lambda}$ where $\lambda=(-191025+85995\sqrt{5})/2$. Then

$$\begin{array}{c} H=K(\lambda)=\mathbb{Q}(\sqrt{5},\sqrt{-3}) \\ \Big| 2 \\ K=\mathbb{Q}(\sqrt{-15}) \\ \Big| 2 \\ \mathbb{Q} \end{array}$$

We have

M	$j(M\tau_0)$	$j(M\tau_1)$	$\phi_M(\tau_0)$	$\phi_M(\tau_1)$	$\langle\phi_M(\tau_0)\rangle$	$\langle\phi_M(\tau_1)\rangle$
$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	μ	λ	$-\epsilon^{-8}$	$\epsilon^{-4}\tau_0^6$	1	$\mathfrak{p}^{12}$
$\begin{pmatrix}1&0\\0&2\end{pmatrix}$	λ'	μ'	$\epsilon^4\overline{\tau_0}^6$	$\epsilon^{-4}\overline{\tau_0}^6$	$\overline{\mathfrak{p}}^{12}$	$\overline{\mathfrak{p}}^{12}$
$\begin{pmatrix}1&1\\0&2\end{pmatrix}$	λ'	λ	$\epsilon^4\tau_0^6$	$-\epsilon^{-8}$	$\mathfrak{p}^{12}$	1

where $\epsilon=(1+\sqrt{5})/2$ and $\mu=(37018076625+16554983445\sqrt{5})/2$.

The values $\phi_M(\tau)$. Motivated by the proceeding examples, we prove:

Theorem. *If $\mathfrak{p}$ is a prime of degree one, then*

$$\langle\phi_M(\tau)\rangle=\begin{cases}\mathfrak{p}^{12}, & M=\overline{P}\\ \overline{\mathfrak{p}}^{12}, & M=P\\ 1, & M\neq P,\overline{P}.\end{cases}$$

Proof. (See also [2, II, §3, Theorem 1].) Let $\mathfrak{p}^f=\langle\alpha\rangle$. Then

$$p^{12}\frac{\Delta(\mathfrak{a}\mathfrak{p})}{\Delta(\mathfrak{a})}=\phi_P(\tau)$$

with $P\in\mathscr{M}_p$. Then

$$\left(p^{12}\frac{\Delta(\mathfrak{a}\mathfrak{p})}{\Delta(\mathfrak{a})}\right)\left(p^{12}\frac{\Delta(\mathfrak{a}\mathfrak{p}^2)}{\Delta(\mathfrak{a})}\right)\cdots\left(p^{12}\frac{\Delta(\mathfrak{a}\mathfrak{p}^f)}{\Delta(\mathfrak{a})}\right)=p^{12f}\frac{\Delta(\alpha\mathfrak{a})}{\Delta(\mathfrak{a})}=p^{12f}\alpha^{-12}=\overline{\mathfrak{p}}^{12f}.$$

But $\phi_M(\tau)\in\overline{\mathbb{Z}}$, so $\phi_M(\tau)\mid p^{12}$, hence $\phi_P(\tau)\mid(p^{12}+\overline{\mathfrak{p}}^{12f})=\overline{\mathfrak{p}}^{12}$. We conclude that $\phi_{\overline{P}}(\tau)\mid\mathfrak{p}^{12}$, and therefore

$$\Big(\prod_{M\neq P,\overline{P}}\phi_M\Big)\phi_P\phi_{\overline{P}}=p^{12}=\mathfrak{p}^{12}\overline{\mathfrak{p}}^{12}$$

so $\left\langle\prod_{M\neq P,\overline{P}}\phi_M(\tau)\right\rangle=\langle 1\rangle$. □

The polynomial $G_p(X,Y,Z)$. We form

$$G_p(X,Y,j(\tau)) = \sum_{M\in\Gamma\backslash\mathscr{M}_p}(X-j(M\tau))\prod_{M'\neq M\in\Gamma\backslash\mathscr{M}_p}(Y-\phi_M(\tau)).$$

This function is invariant under Γ and has no poles. If we look at the q-expansions as we have done, we find $G_p(X,Y,Z)\in\mathbb{Z}[X,Y,Z]$ [2, II, §5].

We proved

$$\Phi_p(X,Y)\equiv(X^p-Y)(X-Y^p)\pmod p$$

by

$$\begin{aligned}\Phi_p(X,j(\tau)) &= (X-j(p\tau))\prod_{b\ (p)}(X-j((\tau+b)/p))\\ &\equiv (X-j(\tau)^p)(X-j(\tau/p))^p\\ &\equiv (X-j(\tau)^p)(X^p-j(\tau))\pmod p.\end{aligned}$$

Similarly, we have

$$\begin{aligned}G_p(X,Y,j(\tau)) = (X-j(p\tau))\prod_{b\ (d)}\Big(Y-\phi_{\left(\begin{smallmatrix}1&b\\0&p\end{smallmatrix}\right)}(\tau)\Big)\\ +\sum_{b\ (d)}(X-j((\tau+b)/p))\Big(Y-\phi_{\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)}\Big)\prod_{b'\neq b}\Big(Y-\phi_{\left(\begin{smallmatrix}1&b'\\0&p\end{smallmatrix}\right)}(\tau)\Big).\end{aligned}$$

Since

$$\phi_{\left(\begin{smallmatrix}1&b\\0&p\end{smallmatrix}\right)}(\tau)=\frac{\Delta((\tau+b)/p)}{\Delta(\tau)}=\frac{\zeta q^{1/p}+\dots}{q+\dots},$$

we have

$$G_p(X,Y,j(\tau))\equiv(X-j(\tau)^p)(Y^p-\Delta(\tau)/\Delta(p\tau))\pmod\pi.$$

Therefore

$$\frac{\Delta(\tau)}{\Delta(p\tau)}\equiv f(j(\tau))\pmod\pi,$$

where $f(X)\in\mathbb{Z}[X]$ is a certain polynomial of degree $p-1$, and in particular

$$G_p(X,Y,Z)\equiv(X-Z^p)(Y^p-f(Z))\pmod p$$

so in particular $G_p(Z^p,Y,Z)\equiv 0\pmod p$.

But then

$$G(j(\tau)^p,\phi_p(\tau),j(\tau))=(j(\tau)^p-j(P\tau))\prod_{M'\neq P}(\phi_P(\tau)-\phi_M(\tau))\equiv 0\pmod p$$

so $j(\tau)^p\equiv j(P\tau)\pmod{\overline{\mathfrak{p}}}$ since $\overline{\mathfrak{p}}^{12}\mid\phi_P(\tau)$ [2, II, §5].

We also define

$$H_n(X,Y,j(\tau))=\sum_{M\in\Gamma\backslash\mathscr{M}_n}(Y-\phi_M(\tau))\prod_{M'\neq M\in\Gamma\backslash\mathscr{M}_n}(Y-j(M'\tau)),$$

which is also a polynomial with integer coefficients.

We have shown that

$$\Psi_p(X,j(\tau))\equiv(X-j(\tau)^p)(X^p-j(\tau))\pmod p$$

and similarly

$$\begin{aligned} D_p(Y,j) &\equiv \left(Y - \frac{p^{12}\Delta(p\tau)}{\Delta(\tau)}\right) \prod_{b \ (d)} \left(Y - \frac{\Delta((\tau+b)/p)}{\Delta(\tau)}\right) \\ &\equiv Y\left(Y^p - \frac{\Delta(\tau/p)}{\Delta(\tau)}\right)^p \equiv Y\left(Y^p - \frac{\Delta(\tau)}{\Delta(\tau)^p}\right) \\ &\equiv Y(Y^p - f_p(j(\tau)) \pmod p. \end{aligned}$$

For this we need:

Proposition. *For all p, there exists a polynomial $f_p(X) \in \mathbb{Z}[X]$ such that*

$$\Delta(\tau)^{1-p} \equiv f_p(j(\tau)) \pmod p.$$

Proof. Since $\Delta(\tau)^p \equiv \Delta(p\tau)$, it suffices to note

$$\Delta(\tau)^{-n} = q^{-n} + \cdots = j^n + \cdots + O(q) = P_n(j) + O(q)$$

and then take $f_p = P_{p-1}$. □

Therefore

$$G_p(X, Y, j(\tau)) \equiv (X - j(\tau)^p)(Y^p - f_p(j(\tau))) \pmod p.$$

Similarly, one shows

$$H_p(X, Y, j(\tau)) \equiv Y(X^p - j(\tau)) \pmod p.$$

A congruence property of Δ. This section is developed in [11, §12.1].

Proposition. *$\phi_P(\tau)$, $\phi_{\overline{P}}(\tau)$ generate $\overline{\mathfrak{p}}^{12}$, $\mathfrak{p}^{12}$ in H.*

Proof. We have

$$\begin{aligned} H_n(j(P\tau), 0, j(\tau)) &= (0 - \phi_P(\tau)) \prod_{M \neq P} (j(P\tau) - j(M\tau)) \\ &= -\phi_P(\tau) \frac{\partial}{\partial X} \phi_P(j(P\tau), j(P\tau)) \in H. \end{aligned}$$

But $j(P\tau) \in H$, $j(M\tau) \notin H$ (it satisfies an equation of discriminant Dp^2). We showed $\phi_P(\tau) \in H$, so $\langle \phi_P(\tau) \rangle = \overline{\mathfrak{p}}^{12}$. □

Indeed,

$$\phi_P(\tau) = p^{12} \frac{\Delta(\mathfrak{a}\mathfrak{p})}{\Delta(\mathfrak{a})} = \frac{\Delta(\mathfrak{a}\overline{\mathfrak{p}}^{-1})}{\Delta(\mathfrak{a})} \in H.$$

But this only depends on ideal classes, as $\Delta(\mathfrak{a}\langle\lambda\rangle) = \lambda^{-12}\Delta(\mathfrak{a})$, for $\lambda \in K^\times$. So

$$\left\langle \frac{\Delta(\mathfrak{a}\mathfrak{b}^{-1})}{\Delta(\mathfrak{a})} \right\rangle = \mathfrak{b}^{12} \in H$$

and in particular

$$\left\langle \frac{\Delta(\mathscr{O})}{\Delta(\mathfrak{a})} \right\rangle = \mathfrak{a}^{12}.$$

In general, $\Delta(\mathfrak{a}) \notin \overline{\mathbb{Q}}$, but the ratio $\Delta(\mathfrak{a})/\Delta(\mathfrak{b}) \in H^\times$, and actually we have a well-defined map

$$\begin{aligned} \mathrm{Cl}(K) &\to H^\times/(K^\times)^{12} \\ [\mathfrak{a}] &\mapsto \lambda, \quad \langle\lambda\rangle = \mathfrak{a}^{12}. \end{aligned}$$

Theorem. *If $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals of K, then $\Delta(\mathfrak{a})/\Delta(\mathfrak{b}) \in H^\times$, and*

$$\left\langle \frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{b})} \right\rangle = (\mathfrak{b}\mathfrak{a}^{-1})^{12}.$$

Corollary. *If $\mathfrak{a} \subset K$ is any ideal, then $\mathfrak{a}^{12}$ is principal in H.*

Corollary. *If we let $F(\tau) = \mathrm{Im}(\tau)^{12}|\Delta(\tau)|^2$ (note $F(\tau) = F(\gamma\tau)$ for $\gamma \in \Gamma = SL_2(\mathbb{Z})$), then*

$$F(\tau_1)/F(\tau_2) \in \mathscr{O}_H^\times$$

for $\tau \in \mathscr{Q}_D$.

Proof. For $\mathscr{O} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, we have

$$\Delta(\mathfrak{a}) = (c\omega_1 + d\omega_2)^{-12}\Delta\left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}\right)$$

hence

$$\frac{\Delta(\mathfrak{a})}{\Delta(\mathscr{O})} = \frac{(c\tau + d)^{-12}\Delta(M\tau)}{\Delta(\tau)} = \frac{1}{n^{12}}\phi_M(\tau).$$

But

$$\langle \phi_M(\tau) \rangle = \overline{\mathfrak{a}}^{12} = \left\langle \frac{n^{12}(c\tau + d)^{-12}\Delta(M\tau)}{\Delta(\tau)} \right\rangle$$

and thus

$$\langle \phi_M(\tau)\overline{\phi_M(\tau)} \rangle = \mathfrak{a}^{12}\overline{\mathfrak{a}}^{12} = (N\mathfrak{a})^{12} = \langle n^{12} \rangle = \frac{n^{24}}{|c\tau + d|^{24}}\frac{|\Delta(M\tau)|^2}{|\Delta(\tau)|^2}.$$

Note that

$$\mathrm{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{n^{12}}{|c\tau + d|^{24}}\,\mathrm{Im}(\tau)^2,$$

so we have

$$n^{12}\frac{\mathrm{Im}(M\tau)^{12}}{\mathrm{Im}(\tau)^{24}} = n^{12}\frac{F(M\tau)}{F(\tau)}$$

and so

$$\left\langle \frac{F(M\tau)}{F(\tau)} \right\rangle = \langle 1 \rangle.$$

We have shown $F(\mathfrak{a})/F(\mathscr{O}) \in (\mathscr{O}_H^\times)^+$. □

Summary. In the past several sections, we have defined the four polynomials

$$\begin{aligned}
\Psi_n(X, j(\tau)) &= \prod_{M \in \Gamma\backslash\mathscr{M}_n} (X - j(M\tau)) \\
D_n(Y, j(\tau)) &= \prod_{M \in \Gamma\backslash\mathscr{M}_n} (Y - \phi_M(\tau)) \\
G_n(X, Y, j(\tau)) &= \sum_{M \in \Gamma\backslash\mathscr{M}_p} (X - j(M\tau)) \prod_{M' \neq M} (Y - \phi_{M'}(\tau)) \\
H_n(X, Y, j(\tau)) &= \sum_{M \in \Gamma\backslash\mathscr{M}_p} (Y - \phi_M(\tau)) \prod_{M' \neq M \in \Gamma\backslash\mathscr{M}_p} (X - j(M'\tau))
\end{aligned}$$

where

$$\phi_M(\tau) = n^{12}(c\tau + d)^{-12}\frac{\Delta(M\tau)}{\Delta(\tau)}.$$

All of these have integer coefficients, the first values being

$$\begin{aligned}
\Psi_1(X, j(\tau)) &= G_1(X, Y, j(\tau)) = X - j(\tau)\\
D_1(X, j(\tau)) &= H_1(X, Y, j(\tau)) = Y - 1,\\
\Psi_2(X, j(\tau)) &= j(\tau)^3 - (X^2 - 1488X + 162000)j(\tau)^2\\
&\quad + (1488X^2 + 40773375X + 8748000000)j(\tau)\\
&\quad + (X - 54000)^3,\\
D_2(Y, j(\tau)) &= -Yj(\tau) + (Y + 16)^3\\
D_3(Y, j(\tau)) &= -Yj(\tau)^2 + 72Y(Y + 21)j(\tau) + (Y - 9)^3(Y - 729)\\
G_2(X, Y, j(\tau)) &= j(\tau)^3 - (Y^2 + 48Y + 2256)j(\tau)^2\\
&\quad + (1488Y^2 + 67326Y + 1106688 - X)j(\tau)\\
&\quad + 3(Y + 16)^2(X - 54000)\\
H_2(X, Y, j(\tau)) &= 2j(\tau)^3 - (2(X - 744)Y + 48X - 425568))\, j(\tau)^2\\
&\quad + ((2976X + 40773375)Y + 67326X + 2234304000)j(\tau)\\
&\quad + 3(Y + 16)(X - 54000)^2.
\end{aligned}$$

For $n = p$ prime one has the congruences:

$$\begin{aligned}
\Psi_p(X, j(\tau)) &\equiv (X^p - j(\tau))(X - j(\tau)^p) \pmod{p}\\
D_p(Y, j(\tau)) &\equiv Y(Y^p - f_p(j(\tau))) \pmod{p}\\
G_p(X, Y, j(\tau)) &\equiv (X - j(\tau)^p)(Y^p - f_p(j(\tau))) \pmod{p}\\
H_p(X, Y, j(\tau)) &\equiv (X^p - j(\tau))Y \pmod{p}
\end{aligned}$$

where $f_p(j(\tau))$ is a polynomial of degree $p - 1$ such that $\Delta(\tau)^{1-p} \equiv f_p(j(\tau)) \pmod{p\mathbb{Z}((q))}$.

The above congruences for $\Psi_p(X, j(\tau))$ and $G_p(X, Y, j(\tau))$ modulo p imply that $j(\overline{P}\tau) \equiv j(\tau)^p \pmod{\mathfrak{p}}$ where $\overline{P} \in \mathscr{M}_p$ is the matrix acting on lattices that corresponds to multiplication by $\overline{\mathfrak{p}}$. Hence $j(\mathfrak{p}^{-1}\mathfrak{a}) = \sigma_{\mathfrak{p}}(j(\mathfrak{a}))$, where $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(H/K)$ is the Frobenius element attached to $\mathfrak{p}$, while the equation

$$\begin{aligned}
H_p(j(P\tau), 0, j(\tau)) &= -\phi_P(\tau) \prod_{M \neq \overline{P}} (j(P\tau) - j(M\tau))\\
&= -\phi_P(\tau) \frac{\partial \psi_p(X, j(\tau))}{\partial X}\bigg|_{X = j(P\tau)}
\end{aligned}$$

and the corresponding equation for $\overline{P}$ show that the numbers

$$\phi_P(\tau) = p^{12}\frac{\Delta(\mathfrak{p}\mathfrak{a})}{\Delta(\mathfrak{a})} = \frac{\Delta(\overline{p}^{-1}\mathfrak{a})}{\Delta(\mathfrak{a})} \text{ and } \phi_{\overline{P}}(\tau) = p^{12}\frac{\Delta(\overline{\mathfrak{p}}\mathfrak{a})}{\Delta(\mathfrak{a})} = \frac{\Delta(p^{-1}\mathfrak{a})}{\Delta(\mathfrak{a})}$$

belong to H. The equation $D_p(\phi_M(\tau), j(\tau)) = 0$ and the fact that $D_p(Y, j(\tau))$ is monic with constant term p^{12} imply that each $\phi_M(\tau)$ is an algebraic integer dividing p^{12}. Choosing $f > 0$ such that $\mathfrak{p}^f = \langle \alpha \rangle$ is principal, then $\phi_{\overline{P}}(\tau)$ also divides

$$\prod_{i=1}^{f} \frac{\Delta(\mathfrak{p}^{-i}\mathfrak{a})}{\Delta(\mathfrak{p}^{1-i}\mathfrak{a})} = \frac{\Delta(\alpha^{-1}\mathfrak{a})}{\Delta(\mathfrak{a})} = \alpha^{12}$$

and from this we deduce that the ideal it generates (in H) is exactly $\mathfrak{p}^{12}$. It then follows that $\Delta(\mathfrak{a})/\Delta(\mathfrak{ab})$ for any fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of K lies in H and generates the ideal $\mathfrak{b}^{12}$, which implies that the quotient $F(\mathfrak{a})/F(\mathfrak{ab})$ where $F(\tau) = \mathrm{Im}(\tau)^{12}|\Delta(\tau)|^2$ is a unit of H.

6. The Kronecker Limit Formula

For the results of this section, consult [11, §20]. Let K be a number field (not necessarily imaginary quadratic). Then we have the zeta function

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a}\subset\mathscr{O}_K \\ \text{integral}}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1-N(\mathfrak{p})^{-s}} = \frac{\kappa}{s-1} + O(1),$$

where $\kappa = (2^{r_1+r_2}\pi^{r_2})/\sqrt{|D_K|}h(K)R(K)$ where $h(K)$ is the class number and $R(K) = \det(\log|\epsilon_i^{(j)}|)$, a matrix of row and column size $r_1 + r_2 - 1$. So

$$\mathrm{Res}_{s=1}\,\zeta_H(s) \doteq h(H)R(H)$$

for H the Hilbert class field of K with Galois group $\mathrm{Gal}(H/K) = G \simeq \mathrm{Cl}(K)$. One can show

$$\zeta_H(s) = \prod_{\chi: G\to\mathbb{C}^\times} L_K(s,\chi) = \sum_{\mathfrak{a}\subset\mathscr{O}_K} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s},$$

since the product of $(1-N(\mathfrak{p})^{-s}\zeta_f)$ runs over the fth roots of unity, where $\mathfrak{p}$ splits into g primes with $fg = n = [H:K]$, so that $N(\mathfrak{P}) = \mathfrak{p}^f$, has $(1-N(\mathfrak{P})^{-s})^{-1} = g$.

Thus

$$L_K(s,\chi) = \sum_{\mathscr{A}\in\mathrm{Cl}(K)} \chi(\mathscr{A})\zeta_{\mathscr{A}}(s)$$

where

$$\zeta_{\mathscr{A}}(s) = \sum_{\mathfrak{a}\in\mathscr{A}} \frac{1}{N(\mathfrak{a})^s}$$

is the partial zeta function, and

$$\zeta_K(s) = \sum_{i=1}^{h(K)} \zeta_{\mathscr{A}_i}(s).$$

A lemma from group representation. Indeed, we have

$$\zeta_H(s) = \prod_{\chi\in\widehat{G}} \sum_{\mathscr{A}\in G} \chi(\mathscr{A})\zeta_{\mathscr{A}}(s) = \det \zeta_{\mathscr{A}\mathscr{B}^{-1}}(s).$$

If G is a finite abelian group, map $g \mapsto x_g \in \mathbb{C}$ compatibly. Then

Proposition. *We have*

$$\prod_{\chi\in\widehat{G}} \left(\sum_{g\in G} \chi(g)x_g \right) = \det(x_{gh^{-1}})_{\#G\times\#G}.$$

Example. For G cyclic of order 3, choosing x_0, x_1, x_2, we have

$$\begin{aligned}(x_0+x_1+x_2)&(x_0+\omega x_1+\overline{\omega}x_2)(x_0+\overline{\omega}x_1+\omega x_2)\\ &= (x_0+x_1+x_2)\left((x_0-(x_1+x_2)/2)^2+3(x_1-x_2)^2/2\right)\\ &= (x_0+x_1+x_2)(x_0^2-x_0x_1-x_0x_2+x_1^2+x_2^2-x_1x_2)\\ &= \begin{vmatrix} x_0 & x_1 & x_2\\ x_2 & x_0 & x_1\\ x_1 & x_2 & x_0\end{vmatrix}.\end{aligned}$$

Proof of proposition. (See also [11, §21.1, Theorem 5].) Let $\mathbb{C}^{\#G} = \{[g] = a_g \in \mathbb{C} : g \in G\} = V$, and

$$\begin{aligned}\lambda : V &\to V\\ [g_1] &\mapsto \sum x_g[gg_1]\end{aligned}$$

Choose for all $\chi \in \widehat{G}$ $v_\chi = \sum \chi(g)[g]$, so that

$$\lambda(v_\chi) = (\textstyle\sum_g \overline{\chi}(g)x_g)v_\chi \simeq \mathbb{C}^n.$$

These are the eigenvalues, which are distinct, so the determinant is their product. □

So

$$\prod_{\chi\in\widehat{G}} \sum_{\mathscr{A}\in G} \chi(\mathscr{A})\zeta_{\mathscr{A}}(s)),$$

where each individual term has a pole iff χ is trivial. We find

$$\prod_{\chi\neq 1}\sum_{g\in G}\chi(g)x_g = \det(x_{gh^{-1}} - x_g)_{(n-1)\times(n-1)}.$$

The statement. Write

$$\zeta_{K,\mathscr{A}}(s) = \sum_{\substack{\mathfrak{a}\subset\mathscr{O}_K\\ [\mathfrak{a}]=\mathscr{A}}} \frac{1}{N(\mathfrak{a})^s} = \frac{\kappa}{s-1} + c(\mathscr{A}) + O(s-1).$$

Definition. We let

$$c(\mathscr{A}) = \lim_{s\to 1}(\zeta_{K,\mathscr{A}}(s) - \kappa/(s-1)) \in \mathbb{C}.$$

We have

$$\left.\frac{\zeta_H(s)}{\zeta_K(s)}\right|_{s=1} = \prod_{\chi\neq 1}\sum_{\mathscr{A}\in\mathrm{Cl}(K)}\chi(\mathscr{A})(c(\mathscr{A})-c(\mathscr{O})) = \det(c(\mathscr{A}\mathscr{B})-c(\mathscr{B}))$$

for $\mathscr{A}, \mathscr{B} \neq 1 \in \mathrm{Cl}(K)$.

Now if K is an imaginary quadratic field, K has $(r_1, r_2, r) = (0, 1, 0)$ and H has $(0, h, h-1)$, so $R(H)$ is a determinant of an $(h-1)\times(h-1)$ matrix $\log|\epsilon_i^{(j)}|$, and this is exactly the size of the matrix of class groups above.

Since $h(H)$ is approximately the index in $\mathscr{O}_H^\times$ of $c(\mathscr{A})$, we have that $c(\mathscr{A}) - c(\mathscr{B})$ is approximately the log of a unit of H. Specifically [11, §20.4, First limit formula]:

Theorem (Kronecker limit formula)**.** *If $\mathscr{A} = [\mathfrak{a}] \in \mathrm{Cl}(K)$ for an imaginary quadratic field K, corresponding to $\tau \in \Gamma \setminus \mathscr{Q}_D$, then*

$$c(\mathscr{A}) = \frac{4\pi}{w\sqrt{|D|}}\left(\gamma - \frac{1}{2}\log 2 - \frac{1}{4}\log|D| - \frac{1}{24}\log F(\tau)\right).$$

We will find that

$$c(\mathscr{A}) - c(\mathscr{B}) = \frac{-\pi}{6w\sqrt{|D|}}\log\frac{F(\tau_{\mathscr{A}})}{F(\tau_{\mathscr{B}})} \in \mathscr{O}_H^\times,$$

and that $\langle F(\mathfrak{a})/F(\mathscr{O})\rangle \subset \mathscr{O}_H^\times$ occurs with index approximately $h(H)$.

Let

$$E(\tau, s) = \mathrm{Im}(\tau)^s \sum_{m,n\in\mathbb{Z}}{}' |m\tau + n|^{-2s}$$

for $\tau \in \mathfrak{H}$ and $\mathrm{Re}\, s > 1$. For example, $E(i,s) = \sum_{m,n}{}'(m^2+n^2)^s$, and more generally for $\tau \in \mathscr{Q}_D$,

$$E(\tau, s) = \left(\frac{|D|}{4}\right)^{s/2} \sum_{m,n}{}' Q(m,n)^s$$

where $Q(x,y)$ is a quadratic form with integer coefficients of discriminant D, $Q(m,n) = N(x)/N(\mathfrak{a})$, $x \in \mathfrak{a}$, i.e. if $\langle x\rangle = \mathfrak{a}\mathfrak{b}$ then $Q(m,n) = N(\mathfrak{b})$. Thus

$$E(\tau, s) = w(|D|/4)^{s/2}\zeta_{K,\mathscr{A}}(s),$$

where $\mathscr{A}$ corresponds to τ.

Generalized L-series. Before we get to the proof of this theorem, we set up some more general machinery. Consult [7, §16.4–16.5].

One can show that

$$\zeta_K(s) = \zeta(s)L(s,\epsilon)$$

where ζ is the ordinary Riemann zeta function and $\epsilon(n) = \left(\frac{D}{n}\right)$. Choose $\mathfrak{a}_0 \in \mathscr{A}^{-1}$ so that $\mathfrak{a}\mathfrak{a}_0 = \langle\lambda\rangle$; then $\lambda \in \mathfrak{a}_0$, and

$$\zeta(\mathscr{A}, s) = \sum_{\mathfrak{a}\in\mathscr{A}} N(\mathfrak{a})^{-s} = N(\mathfrak{a}_0)^s \sum_{\lambda\in(\mathfrak{a}_0\setminus\{0\})/\mathscr{O}_K^\times} |N(\lambda)|^s.$$

For an imaginary quadratic field, this is equal to

$$N(\mathfrak{a}_0)^s/w \sum_{\lambda\in\mathfrak{a}_0}{}' N(\lambda)^s$$

where $w = \#\mathscr{O}_K^\times$ is either 2, 4, or 6 is the number of roots of unity.

We let $\mathfrak{a}_0 = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$, $\lambda = m\omega_1 + n\omega_2$, so that $Q(m,n) = N(\lambda)/N(\mathfrak{a}_0) = am^2 + bmn + cn^2$, where $a = \omega_1\overline{\omega_1}/N(\mathfrak{a}_0)$, $b = (\omega_1\overline{\omega_2} + \overline{\omega_1}\omega_2)/N(\mathfrak{a}_0)$, and $c = \omega_2\overline{\omega_2}/N(\mathfrak{a}_0)$, all $a, b, c \in \mathbb{Z}$. Then

$$b^2 - 4ac = (\omega_1\overline{\omega_2} - \overline{\omega_1}\omega_2)^2/N(\mathfrak{a}_0) = D.$$

Thus

$$\zeta(\mathscr{A}, s) = \frac{1}{w}\sum_{m,n}{}' Q(m,n)^{-s}$$

where we associate as usual $\mathscr{A} \leftrightarrow [Q]$ for $Q \in \mathscr{Q}_D$. Sending $\tau = \omega_1/\omega_2 \in \mathfrak{H}$, we have $b^2 - 4ac = -4|\omega_2|^2 \operatorname{Im}(\tau)$, and

$$Q(m,n) = |D/4|^{1/2}|m\tau + n|^2/\operatorname{Im}(\tau)$$

so

$$\zeta(\mathscr{A}, S) = \frac{1}{w/2}|D/4|^{-s/2}E(\tau, s),$$

with

$$E(\tau, s) = \frac{1}{2}{\sum_{m,n}}' \frac{\operatorname{Im}(\tau)^s}{|m\tau + n|^{2s}}.$$

We may generalize this slightly: let

$$L_K(s, \chi) = \sum_{\mathfrak{a} \in \mathscr{O}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \sum_{i=1}^{h} \chi(\mathscr{A}_i)\zeta(\mathscr{A}_i, s)$$

for a character χ. We may also make the same definition for ψ where ψ is a Hecke character, i.e. a Grossencharacter, mapping fractional ideals to $\mathbb{C}^\times$ with the stipulation that $\psi(\langle\lambda\rangle) = \lambda^a$, for some $a \in \mathbb{Z}_{\geq 0}$. Then

$$\sum_{\mathfrak{a} \in \mathscr{A}} \frac{\psi(\mathfrak{a})}{N(\mathfrak{a})^s} = \frac{N(\mathfrak{a}_0)^s}{w}\psi(\mathfrak{a}_0)^{-1} \sum_{\lambda \neq 0 \in \mathfrak{a}} \frac{\lambda^a}{|\lambda|^{2s}}.$$

With $\mathfrak{a}\mathfrak{a}_0 = \langle\lambda\rangle$, $\psi(\mathfrak{a}\mathfrak{a}_0) = \psi(\langle\lambda\rangle) = \lambda^a$, we find this is

$$\frac{\operatorname{Im}(\tau)^s}{2}{\sum_{m,n}}' \frac{(m\tau + n)^a}{|m\tau + n|^{2s}} = E(\tau; a, s) = \frac{1}{w}|D/4|^{-s/2}\psi(\mathfrak{a}_0)E(\tau; a, s).$$

A triple coincidence. Let $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_k$ be a cusp form, to which we associate the Hecke L-series $\sum_{n=1}^{\infty} a(n)n^{-s}$, which has an Euler product and an analytic continuation $\int_0^\infty f(it)t^{s-1}\,dt$.

We have associated $[\mathfrak{a}] \leftrightarrow Q(m,n)$ for $Q \in \Gamma \setminus \mathscr{Q}_D$; we now define

$$\Theta_{\mathscr{A}}(z) = \sum_{m,n \in \mathbb{Z}} q^{Q(m,n)} \in M_1(\Gamma_0(D), \epsilon)$$

i.e. $\Theta_{\mathscr{A}}((az+b)/(cz+d)) = \epsilon(d)(cz+d)\Theta_{\mathscr{A}}(z)$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(D)$. For any $f \in M_k$, $\sum_{n=1}^{\infty} a(n)/n^s$ may have poles.

We have a triple coincidence: $L(\Theta_{\mathscr{A}}, s) = \sum_{m,n} Q(m,n)^{-s} = w\zeta(\mathscr{A}, s)$: The series

$$L_K(s, \psi) = \sum E(\tau_d; a, s) = L(s, f_\psi)$$

where f_ψ is a Hecke (CM) eigenform, a finite sum of Θ series

$$\Theta_{\mathscr{A}}(a)(z) = {\sum_{m,n}}' \operatorname{Re}((m\tau_{\mathscr{A}} + n)^a)q^{(m\tau+n)(m\overline{\tau}+n)/\operatorname{Im}\tau} \in M_{a+1}(\Gamma_0(D), \epsilon)$$

for a even.

Example. For $h = 1$, we have $\mathbb{Q}(i)$, $Q(m,n) = m^2 + n^2$, and

$$E(i, s) = {\sum_{m,n}}' (m^2 + n^2)^s = (1/4)\zeta_{\mathbb{Q}(i)}(s) = L(\theta, s)$$

where

$$\theta(z) = \sum_{m,n} q^{m^2+n^2} = \left(\sum_n q^{n^2}\right)^2 = (1+2q+\dots)^2.$$

For $a = 4$,

$$E(i,\psi,s) = 2\sum_{m,n}{}' \frac{(m+ni)^4}{(m^2+n^2)^s} = \sum_{m,n}{}' \frac{m^4-3m^2n^2}{(m^2+n^2)^s} = (1/4)L_{\mathbb{Q}(i)}(s,\psi) = L(\Theta^{(4)},s)$$

where $\psi(\langle a+bi\rangle) = (a+bi)^4$ and

$$\Theta^{(4)}(z) = \sum_{m,n}(m^4-3m^2n^2)q^{m^2+n^2} \in M_3(\Gamma_0(4), \left(\frac{-4}{-}\right)).$$

Corrolaries. Here is an equivalent statement of the formula:

Theorem (Kronecker Limit Formula)**.** *We have*

$$E(\tau,s) = \frac{\pi/2}{s-1} + \pi(\gamma - \log 2 - \log\sqrt{\mathrm{Im}(\tau)}|\eta(\tau)|)^2 + O(s-1)$$

where $\eta(\tau) = q^{1/24}\prod_n(1-q^n)$ *so that* $\sqrt{\mathrm{Im}\,\tau}\eta(\tau)^2 = F(\tau)^{1/24}$.

Corollary.

$$\zeta(\mathscr{A},s) = \frac{\kappa}{s-1} + c(\mathscr{A}) + O(s-1)$$

where

$$\kappa = \frac{\pi}{w/2\sqrt{|D|}} = \begin{cases} \pi/4, & D=-4 \\ \pi/3\sqrt{3}, & D=-3 \\ \pi/\sqrt{|D|}, & \textit{else.} \end{cases}$$

and $c(\mathscr{A}) = \kappa(\gamma - 2\log 2 - 1/2\log|D| - f(\tau_{\mathscr{A}}))$, $f(\tau) = 1/24\log F(\tau)$.

Corollary. *Let* $\chi : \mathrm{Cl}(K) \to \mathbb{C}^\times$. *If* $\chi \neq 1$, *then*

$$L_K(1,\chi) = \sum_{\mathscr{A}} \chi(\mathscr{A})c(\mathscr{A}) = -\kappa/24\sum_{\mathscr{A}}\chi(\mathscr{A})\log F(\tau_{\mathscr{A}}).$$

Corollary.

$$\frac{\zeta_H(s)}{\zeta_K(s)} = \prod_{\chi\neq\chi_0} L(1,\chi)$$

and

$$\left.\frac{\zeta_H(s)}{\zeta_K(s)}\right|_{s=1} \doteq \frac{h(H)R(H)}{h(K)} = \prod_\chi L_K(1,\chi) = \prod_\chi\sum_{\mathscr{A}}\chi(\mathscr{A})c(\mathscr{A})$$
$$= \det(c(\mathscr{A}\mathscr{B}^{-1})) \doteq \det((\log\epsilon_{\mathscr{A}\mathscr{B}^{-1}})_{\mathscr{A},\mathscr{B}\neq 1\in\mathrm{Cl}(K)}$$

so $h(H)$ *is the index of* $\langle\epsilon_{\mathscr{A}}\rangle$ *in* $\mathscr{O}_H^\times$.

If $\chi : \mathrm{Cl}(K) \to \{\pm 1\}$, there exists a description of χ by genus theory. $D = D_1D_2$, chosen so that $D_1 > 0$, $D_2 < 0$. Then

$$\chi_{D_1D_2}(\mathfrak{p}) = \begin{cases} \left(\frac{D_1}{N(\mathfrak{p})}\right), & \gcd(N(\mathfrak{p}),D_1) = 1; \\ \left(\frac{D_2}{N(\mathfrak{p})}\right), & \gcd(N(\mathfrak{p}),D_2) = 1. \end{cases}$$

Since $N(\mathfrak{p})$ is equal to p, p^2, p as $(D/p) = 1, -1, 0$, this definition is compatible.

For $Q(m,n)$, $a = Q(1,0)$, $\gcd(a,D)=1$, and $\chi_{D_1D_2}([Q]) = \left(\frac{D}{a}\right)$. Thus

$$L_K(s,\chi_{D_1D_2}) = \prod_{\mathfrak{p}}(1-\chi(p)/p^s)^{-1} = \prod_{\mathfrak{p}}\left(1-\left(\tfrac{D_1}{p}\right)p^{-s}\right)^{-1}\left(1-\left(\tfrac{D_2}{p}\right)p^{-s}\right)$$
$$= L_{\mathbb{Q}}(s,\left(\tfrac{D_1}{-}\right))L_{\mathbb{Q}}(s,\left(\tfrac{D_2}{-}\right)).$$

Corollary (Kronecker's solution of Pell's equation)**.** *We have*

$$L(1,\left(\tfrac{D_1}{-}\right))L(1,\left(\tfrac{D_2}{-}\right)) = -\frac{\pi}{24\sqrt{|D|}}\sum_{\mathscr{A}}\chi(\mathscr{A})\log F(\mathscr{A})$$
$$= L(1,\left(\tfrac{D_1}{-}\right)) = \frac{2h(D_1)\log\epsilon(D_1)}{\sqrt{|D_1|}}\frac{\pi h(D_2)}{w_2/2\sqrt{|D_2|}}$$

hence $h_1h_2\log\epsilon_1 = (-1/12)\sum_{\mathscr{A}}\chi(\mathscr{A})\log\epsilon_{\mathscr{A}}$.

Therefore $\prod_{\mathscr{A}}F(\tau_{\mathscr{A}})^{\chi_{D_1D_2}(\mathscr{A})} = \epsilon_1^{-12h_1h_2}$.

Corollary. *If* $\chi = 1$, $\prod_{\mathscr{A}}F(\tau_{\mathscr{A}}) \doteq \prod_{0<n<|D|}\Gamma(n/|D|)$.

Proof of the formula. We are now ready to prove the formula. There are two proofs.

Proof of the Kronecker Limit Formula. THe series

$$E(\tau,s) = \mathrm{Im}(\tau)^s/2{\sum_{m,n}}' \frac{1}{|m\tau+n|^{2s}} = \frac{\pi/2}{s-1} + c + O(s-1)$$

has

$$E(\tau,s) = \mathrm{Im}(\tau)^s\zeta(s) + \mathrm{Im}(\tau)^s\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}|m\tau+n|^{-2s}.$$

Replace the sum with the integral:

$$\int_{-m}^{\infty}|m\tau+n|^{-2s}\,dn = \int_{\infty}^{\infty}\frac{dx}{((mx+n)^2+m^2y^2)^s}$$
$$= \int\frac{dt}{(t^2+m^2y^2)} = (my)^{1-2s}I(s)$$

where $I(s) = \int_{-\infty}^{\infty}dt/(t^2-1)^s$. Therefore this is equal to

$$\sum_{m=1}^{\infty}\left(\sum_{n=-\infty}^{\infty}\frac{1}{|m\tau+n|^{2s}} - \frac{I(s)}{(my)^{2s-1}}\right) + I(s)\zeta(2s-1)y^{1-2s}.$$

We have $\zeta(2s-1) = \pi/(2(s-1)) + c + \dots$ and $y^{1-2s} = y^{-1}(1-2(s-1)\log y + \dots)$, and

$$I(1) = \int_{-\infty}^{\infty}\frac{dt}{t^2+1} = \pi.$$

Therefore since $\zeta(s) = 1/(s-1)+\gamma+\dots$ and $\zeta(2s-1) = 1/2(s-1)+\gamma+\dots$, we have

$$c = \zeta(2)y + \sum_{m=1}^{\infty}\left(\sum_{n\in\mathbb{Z}}\frac{y}{|m\tau+n|^2} - \frac{\pi}{m}\right) + c - \pi\log y.$$

and

$$\sum_{n=-\infty}^{\infty} \frac{y}{|m\tau+n|^2} = \frac{1}{2im}\sum_{m,n}\left(\frac{1}{m\overline{\tau}+n} - \frac{1}{m\tau+n}\right)$$
$$= \frac{\pi}{2im}\left(\frac{1}{\tan(\pi m\overline{\tau})} - \frac{1}{\tan(\pi m\overline{\tau})}\right)$$

since $\sum_n 1/(x+n) = \pi/\tan \pi x$.

Now

$$\sum_{m,n} \frac{y}{|m\tau+n|^2} - \frac{\pi}{m} = \frac{\pi}{2im}(\cot(\pi m\overline{\tau}) - i) - \frac{\pi}{2im}(\cot(\pi m\tau) + i)$$
$$= \frac{\pi}{m}\left(\frac{1}{e^{2\pi i m\tau}-1} + \frac{1}{e^{-2\pi i m\tau}-1}\right)$$
$$= \frac{\pi}{m}\sum_{r=1}^{\infty}\left(e^{2\pi i m r\tau} + e^{-2\pi i m r\tau}\right)$$

thus

$$c = \zeta(2)y + \sum_{m=1}^{\infty}\left(\sum_{n=-\infty}^{\infty}\frac{2\pi}{m}\operatorname{Re}\left(\sum_{r=1}^{\infty} q^{mr}\right)\right)$$
$$= \frac{\pi^2}{6}y - 2\pi\operatorname{Re}\left(\sum_{r=1}^{\infty}\log(1-q^r)\right) + c - \frac{\pi}{2}\log y$$
$$= c - \pi\log\left(e^{-\pi y/6}y^{1/2}\prod_{r=1}^{\infty}|1-q^r|^2\right)$$

which checks because $\eta(\tau)^2 = e^{-\pi y/6}\prod(1-q^r)^2$. □

But we never used that η is modular, so:

Second proof. Let

$$E(\tau, s) = c - \pi\log\sqrt{y}|\eta(\tau)|^2 = (\pi/2)/(s-1) + c(\tau) + O(s-1)$$

with $c'(\tau) = c - \log(\sqrt{y}|\eta(\tau)|^2)$.

c and c' are Γ-invariant. Let $\nabla = y^2(\partial^2/\partial x^2 + \partial^2/\partial y^2)$, so that $\nabla(y^s) = s(s-1)y^2$. We have $\nabla(f(\gamma z)) = (\nabla f)(\gamma z)$ for $\gamma \in SL_2(\mathbb{R})$.

Note

$$\nabla(E(\tau, s)) = s(s-1)E(\tau, s)$$

and

$$\nabla(E(\tau, s) - (\pi/2)/(s-1)) \to \nabla(c(\tau)) = \pi/2.$$

Therefore $\nabla(c'(\tau)) = \pi(-1/2\log y) = \pi/2$ and $\nabla(c(\tau)) = \pi/2 = \nabla(c'(\tau))$, so $c(\tau) - c'(\tau)$ is harmonic on $\mathfrak{H}/\Gamma$, and therefore constant. □

Remark. A note about computing:

$$F(\tau) = F(x+iy) = y^{12}|\Delta(x+iy)|^2 = y^{12}e^{-4\pi y}\prod_{n=1}^{\infty}(1-2e^{-2\pi n y}\cos 2\pi n x + e^{-4\pi n y})^{24}$$

hence

$$f(\tau) = F(\tau)^{1/24} = \sqrt{y}e^{-\pi y/6}\prod_{n=1}^{\infty}(1 - 2e^{-2\pi ny}\cos 2\pi nx + e^{-4\pi ny});$$

the nth term in this expansion is $1 + O(e^{-2\pi ny})$ so choosing τ in the fundamental domain we have $|e^{-2\pi y}| \le e^{-\pi\sqrt{3}} = 0.0017$, so we have a very rapidly converging product.

Let $\epsilon(n) = (D/n)$; then

$$\begin{aligned} L(s,\epsilon) &= \sum_{n=1}^{\infty}\frac{\epsilon(n)}{n^s} = \sum_{0<n<|D|}\epsilon(n)\left(\frac{1}{n^s} + \frac{1}{(n+|D|)^s} + \dots\right) \\ &= \frac{1}{|D|^s}\sum_{n}\epsilon(n)\zeta(s, n/|D|) \end{aligned}$$

where $\zeta(s,x) = 1/x^s + 1/(x-1)^s + \cdots = 1/(s-1) + \dots$ is a shifted zeta function.
Example. For $D = -23$, $h = 3$,

$$f((1+\sqrt{-23})/2)f((1+\sqrt{-23})/4)^2 23^{3/2}2^6\pi/3 = 4972.31615... = \prod_{n=1}^{22}\Gamma(n/23)^{\left(\frac{n}{23}\right)}$$

so $(4\pi\sqrt{|D|})^h\prod_{\mathscr{A}} f(\tau_{\mathscr{A}}) = \prod_{0<n<|D|}\Gamma(n/|D|)^{\epsilon(n)}$.

If $\tau \in \mathfrak{H}$ is CM of discriminant D, then $f(\tau)$ is equal up to factors in $\mathbb{Q}^\times$

$$f(\tau) = 1/4\pi\sqrt{|D|}(\prod_{n}\Gamma(n/|D|)^{\epsilon(n)})^{1/h(D)} = \Omega(D),$$

so $f \in M_k^{\overline{\mathbb{Q}}}$ is equal to an algebraic number times $\Omega(D)^k$, the Chowla-Selberg formula.

7. CM Modular Forms

For more information on the many types of series covered in this section, consult [15], especially Chapter VI.

CM modular forms. The space of modular forms $M_k = \{f : f(\gamma\tau) = (c\tau + d)^k f(\tau)\}$ contains Eisenstein series, theta series, and CM forms.

Theorem. *If $Q : \mathbb{Z}^{2k} \to \mathbb{Z}$ is a positive definite quadratic form, then*

$$\Theta_Q(\tau) = \sum_{x\in\mathbb{Z}^{2k}} q^{Q(x)} = \sum_{n=0} r_Q(n)q^n \in M_k(\Gamma_0(N), \left(\frac{\Delta}{-}\right)),$$

where if $Qx = (1/2)x^tAx$, $A = A^t$ symmetric even, then $\Delta = \pm\det A$ and N is the smallest integer such that NA^{-1} is even.

To $f(\tau) = \sum_{n=0}^{\infty} a(n)q^n$, we associate the L-series $L(f,s) = \sum_{n=1}^{\infty} a(n)/n^s$. This series has a functional equation and various other properties. In this case, we have

$$L(\Theta_Q, s) = \sum_{n=1}^{\infty}\frac{r_Q(n)}{n^s} = \sum_{x}{}' \frac{1}{Q(x)^s} = Z_Q(s),$$

an *Epstein zeta function.*

Example. For $k=1$, $Q(x_1,x_2)=Ax_1+Bx_1x_2+Cx_2^2$, $B^2-4AC=D<0$, $Q\in\mathscr{Q}_D$, and $[Q]$ corresponds to an ideal class $\mathscr{A}$. Then

$$L(\Theta_Q,s)=\sum_{\mathfrak{a}}N(\mathfrak{a})^s=\zeta(\mathscr{A},s)=|D/4|^{-s/2}E(\tau_{\mathscr{A}},s).$$

Therefore we have the set of all generalized theta series contained in modular forms, containing usual theta series (when $P=1$, see below) and CM forms, and they intersect precisely in the binary quadratic forms.

Theorem. *If $Q:\mathbb{Z}^{2h}\to\mathbb{Z}$ is a positive definite quadratic form with associated N and $\left(\frac{\Delta}{-}\right)$, and $P:\mathbb{Z}^h\to\mathbb{C}$ is a spherical polynomial with respect to Q homogeneous of degree d (i.e. if $Q:V=\mathbb{R}^n\to\mathbb{R}$, P a polynomial on V, choose a basis of $V/\mathbb{R}$ so that $Q=x_1^2+\cdots+x_n^2$, then P is* spherical *iff*

$$\left(\frac{\partial^2}{\partial x_1^2}+\cdots+\frac{\partial^2}{\partial x_n^2}\right)P=0,$$

so if $Q=(1/2)x^tAx$, this holds iff

$$\sum_{i,j}(A^{-1})_{i,j}\frac{\partial^2P}{\partial x_i\partial x_j}=0.)$$

Then $\Theta_{Q,P}(\tau)=\sum_{x\in\mathbb{Z}^{2h}}P(x)q^{Q(x)}\in M_k\left(\Gamma_0(N),\left(\frac{\Delta}{-}\right)\right)$ where $k=h+d$.

Proposition.

(i) *Let $x_0\in V\otimes\mathbb{C}$, $Q(x_0)=0$. Then $P(x)=B(x,x_0)^d$ is spherical.*
(ii) *Any spherical P is a finite sum $\sum_i\lambda_iB(x,x_i)^d$.*
(iii) *Any polynomial is uniquely written as $F=H_0+QH_1+Q^2H_2+\dots$.*

If $h=1$, we have a lattice corresponding to an ideal $\mathfrak{a}$, and $Q(x)=N(x)/N(\mathfrak{a})$, where $N(x)=x\overline{x}$ for a basis. Then $P(x)=x^d$ or $P(x)=\overline{x}^d$, hence

$$\Theta_{Q,P}(\tau)=\sum_{x\in\mathfrak{a}}x^{k-1}q^{N(x)/N(\mathfrak{a})}\in M_k(\Gamma_0(D),\epsilon_D).$$

Example. For $Q=(x_1,x_2)=x_1^2+x_2^2$, $x=x_1+ix_2$. Then

$$\sum(x_1+ix_2)^{k-1}q^{x_1^2+x_2^2}\in M_k\left(\Gamma_0(4),\left(\frac{-4}{-}\right)\right)$$

where we take $k\equiv1\pmod 4$ to avoid cancellation.

Then

$$\Theta_{Q,P}(\tau)=\sum_{\lambda\in\mathfrak{a}}\lambda^dq^{N(\lambda)/N(\mathfrak{a})}=f(\tau)$$

a CM form with density zero nonzero terms.

$$L(f,s)=\sum_{\lambda}\frac{\lambda^d}{N(\lambda)^s}=L_K(s,\psi)$$

where ψ is a Grossencharacter. Then

$$\sum_{\mathfrak{a}}\frac{\psi(\mathfrak{a})}{N(\mathfrak{a})^s}=\sum_{m,n}{}'\frac{(m\tau+n)^a}{|m\tau+n|^{2s}}.$$

Example. For $a = 0$, we have $\sum_{d|n} \epsilon(d) = \sum_{\mathscr{A}} r_{\mathscr{A}}(n)$, and

$$\frac{h(D)}{w(D)} + \sum_{n=1}^{\infty} \left(\sum_{d|n} \epsilon(d) \right) q^n = \frac{1}{w(D)} \sum_{\mathscr{A}} \Theta_{\mathscr{A}}(\tau).$$

This is an Eisenstein series.

CM L-series and elliptic curves. For $a = 1$, $L_K(s, \psi) = L(\sum_{\mathscr{A}} \Theta_{Q,P}(\tau, s)) = L(s, f)$ for $f \in M_2(\Gamma_0(D), 1)$.

To each elliptic curve $E/\mathbb{Q}$ we associate a modular form $M_2(\Gamma_0(N))$ and an L-series $L(E, s) = L(f, s)$. Indeed, the CM forms correspond to elliptic curves with CM.

If $E/\mathbb{Q}$ has CM, then $j = 0, 1728, \ldots$, corresponding to discriminants $D = -3, -4, -7, -8, \ldots, -163$. Then $L(E, s) = L_K(s, \psi)$.

For $D = -4$, $y^2 = x^3 - x$, and

$$L(E, s) = \prod_{p \neq 2} \frac{1}{1 - a_p/p^s + p/p^{2s}}$$

where

$$a_p = p + 1 + \#E(\mathbb{F}_p) = p - \#\{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 - x\} = - \sum_{x \pmod p} \left(\frac{x^3 - x}{p} \right).$$

Theorem. *In this case,*

$$a_p = \begin{cases} 0, & p \equiv 3 \pmod 4 \\ \pm 2a, & p \equiv 1 \pmod 4 \end{cases}$$

where $p = a^2 + b^2$, a is odd and $(-1)^{n/2} a \equiv 1 \pmod 4$.

Therefore $\sum_n a_n/n^s$ has $\sum_n a_n q^n = \sum_{a,b} (a + ib) q^{a^2+b^2} = 1/2 \sum_{a,b} a q^{a^2+b^2}$ with a congruence mod 4. We have $h(D) = 1$, $p = (a^2 + Db^2)/4$.

We also have:

Theorem.

$$\sum_{x \pmod p} \left(\frac{x^3 - 1}{p} \right) = \begin{cases} 0, & p \equiv 2 \pmod 3; \\ \pm 2c, & p \equiv 1 \pmod 3 \end{cases}$$

where $p = c^2 + 3d^2$.

To prove these, we use:

Lemma. *If $\alpha, \beta \in \mathbb{Z}/\langle p \rangle$, then*

$$\sum_{n \pmod p} \left(\frac{(n - \alpha)(n - \beta)}{p} \right) = p\delta_{\alpha,\beta} - 1.$$

Proof. We may assume $\beta = 0$ by shifting, so we want to show

$$g(\alpha) = \sum_n \left(\frac{n(n - \alpha)}{p} \right) = p\delta_{\alpha,0} - 1.$$

Then

$$g(k\alpha) = \sum_n \left(\frac{kn(kn - k\alpha)}{p} \right) = \sum_n \left(\frac{n(n - \alpha)}{p} \right) = g(\alpha)$$

so that

$$g(\alpha) = \begin{cases} g(0), & \alpha = 0 \\ g(1), & \alpha \neq 0. \end{cases}$$

But then $\sum_\alpha g(\alpha) = p - 1 + (p-1)g(1) = 0$. □

Proof of theorem. Let

$$f(n) = \sum_{x \pmod p} \left(\frac{x^3 - nx}{p} \right).$$

Then for $k \not\equiv 0 \pmod p$, we let $k \mapsto kx$, $n \mapsto k^2 n$, so

$$f(k^2 n) = \sum_{x \pmod p} \left(\frac{k^3(x^3 - nx)}{p} \right) = \left(\frac{k}{p} \right) f(n).$$

Therefore $f(0) = 0$, $f(n) = 0$ for all n if $p \equiv 3 \pmod 4$, and if $p \equiv 1 \pmod 4$, then

$$f(n) = \begin{cases} 0, & n = 0; \\ A, & n = g^{4i}, \mathbb{F}_p^\times = \langle g \rangle; \\ -A, & n = g^{4i+2}; \\ B, & n = g^{4i+1}; \\ -B, & n = g^{4i+3}. \end{cases}$$

Now $f(n)$ is even because

$$f(n) \equiv \sum_{\substack{0 \neq x \pmod p \\ x^2 \not\equiv n \pmod p}} 1 \equiv 0 \pmod 2.$$

Hence

$$(1/2) f(n) \equiv \begin{cases} (p-1)/2 \equiv 0, & \left(\frac{n}{p}\right) = -1 \\ (p-3)/2 \equiv 1, & \left(\frac{n}{p}\right) = 1 \end{cases} \pmod 2.$$

So we replace A with $2A$, B with $2B$, where A is odd and B is (still) even. Then

$$\begin{aligned} \sum_{n \pmod p} f(n)^2 = \frac{4(p-1)}{2(A^2+B^2)} &= \sum_{n,x,y} \left(\frac{x^3 - nx}{p} \right) \left(\frac{y^3 - ny}{p} \right) \\ &= \sum_{x,y \neq 0} \left(\frac{xy}{p} \right) (p \delta_{x^2, y^2} - 1) = 2p \sum_{x \neq 0} 1 - \left(\sum_x \left(\frac{x}{p} \right) \right)^2 - 2p(p-1) \\ &= 2p(p-1) \end{aligned}$$

so $A^2 + B^2 = p$. □

Sketch of proof of second theorem. Let

$$f(n) = \sum_{x \pmod p} \left(\frac{x^3 - n}{p} \right).$$

Then $f(0) = 0$, and $f(k^3 n) = \left(\frac{k}{p}\right) f(n)$. We conclude that $f(n) = 0$ if $p \equiv 2 \pmod 3$, and if $p \equiv 1 \pmod 3$, then we have $f(n) = 0, A, B, C, -A, -B, -C$

according as the exponent of n in $\langle g\rangle = \mathbb{F}_p^\times$ is $6i, 6i+2, 6i+4, 6i+3, 6i+5, 6i+1$. One shows that $\sum_{x\ (p)} f(n)^2 = A^2 + B^2 + C^2$ by the lemma, and then

$$f(n^2) = \sum_{x,n} \left(\frac{x^3 - n^2}{p}\right) = \sum_{x,n} \left(\frac{nx^3 - 1}{p}\right) = 0.$$

□

Periods and L-series. We have seen that L-series of Grossencharacters are exactly Hecke L-series of CM modular forms as well as nonholomorphic derivatives of (nonholomorphic) Eisenstein series, i.e.

$$\sum_{m,n} \frac{y^s}{|mz+n|^{2s}} \frac{1}{(mz+n)^k}.$$

These functions also have special values.

Example. If $E/\mathbb{Q}$ is an elliptic curve with CM over K, then $L(E/\mathbb{Q}, s) = L_K(s, \psi)$; in the space of modular forms, we have the subset of forms coming from elliptic curves and those from CM modular forms intersecting exactly at forms coming from CM elliptic curves.

We are interested in special values of these functions, e.g. $L(E/\mathbb{Q}, 1)$, motivated by the Birch-Swinnerton-Dyer conjecture, which says that

$$L(E/\mathbb{Q}, 1) = \Omega_E S_e$$

where $\Omega_E \in \mathbb{R}_{>0}$ is a real period (up to a constant, it is $\int_\alpha^\infty dx/y$ for a loop α) and $S_E = 0$ if $\#E(\mathbb{Q}) = \infty$ and $\#Ш$ otherwise, where in the latter case this is a perfect square due to the existence of an anti-symmetric nondegenerate pairing to $\mathbb{Q}/\mathbb{Z}$.

Theorem (Villegas)**.** *If E has CM, then there is an explicit expression involving Θ-series for S_E which shows that S_E is a square. More generally, $L_K(s, \psi)$ is a product of a period and such an explicit expression for critical values $s = 1, \dots, k-1$.*

For this theorem and a development of the rest of this section, see [19].

Example (Gross-Zagier). Consider the elliptic curve $E : y^2 = x^3 - 35x - 98$ (which is also $X_0(49)$) with CM by $\mathbb{Q}(\sqrt{-7}) = K$. It has minimal model $y^2 + xy = x^3 - x^2 - 2x - 1$.

Then $L(E, s) = L_K(s, \psi)$, where $\psi(\mathfrak{a}) = \langle\alpha\rangle$, where $\alpha \equiv 1, \dots, 6$ modulo $\mathfrak{p}_7 = \langle\sqrt{-7}\rangle$, so we choose $\alpha \equiv 1, 2, 4 \pmod{\mathfrak{p}_7}$, and $\psi(\mathfrak{a}) = \left(\frac{n}{\mathfrak{p}_7}\right)\alpha$. Hence

$$L_K(s, \psi) = 1 + \frac{1}{2^s} + 0 + \frac{-1}{4^s} + 0 + \dots$$

where, for example, since $2 = ((1+\sqrt{-7})/2)((1-\sqrt{-7})/2) = \alpha\overline{\alpha}$, we have $\alpha \equiv 4 \equiv 1/2 \pmod{\mathfrak{p}_7}$, and so $\psi(\mathfrak{p}_2) = (1+\sqrt{-7})/2$.

One finds that $L(1, \psi) = (1/2)(2\pi/\sqrt{7})\Omega$ where

$$\Omega = \frac{\Gamma(1/7)\Gamma(2/7)\Gamma(4/7)}{4\pi^2}.$$

We have equalities $L_K(s, \psi) = L(E/\mathbb{Q}, s) = L(f_2, s)$ for $f_2 \in S_2(\Gamma_0(49))$, and more generally $L_K(s, \psi^{k-1}) = L(f_k, s)$, $f_k \in S_k(\Gamma_0(49), \left(\frac{-}{7}\right)^k)$. Since $s \mapsto k - s$ has a functional equation, we consider $L_k(k, \psi^{2k-1})$ with k odd, and we find

$$L(k, \psi^{2k-1}) = 2\left(\frac{2\pi}{\sqrt{7}}\right)^k \frac{\Omega^{2k-1}}{(k-1)!} A(k)$$

where $A(1) = 1/4$, $A(3) = 1$, $A(5) = 1$, $A(7) = 9$, $A(9) = 49$, and so on until $A(33) = 44762286327255^2$. All of these are squares!

Theorem. *Define a sequence of polynomials $\{a_{2n}(x)\}$ by*

$$a_{n+1}(x) = \sqrt{(1+x)(1-27x)}\left(x\frac{d}{dx} - \frac{2n+1}{3}\right)a_n(x) - \frac{n^2}{9}(1-5x)a_{n-2}(x)$$

with $a_0(x) = 1$. (E.g. $a_1(x) = (-1/3)\sqrt{(1+x)(1-27x)}$, but $a_2(x)$ is a polynomial.)

Then $A(2n+1) = (1/4)a_{2n}(-1)$, and $a_{2n}(x) \in \mathbb{Z}[1/6][x]$.

Theorem. *Define*

$$21b_{n+1}(x) = \left((32nx - 56n + 42) - (x-7)(64x-7)\frac{d}{dx}\right)b_n(x) - 2n(2n-1)(11x+7)b_{n-1}(x)$$

with $b_0(x) = 1/2$, $b_1(x) = 1$. Then $A(2n+1) = (b_n(0))^2$.

We will now set out to explain the derivation of these theorems.

For $\mathscr{O} = \mathbb{Z}[(1+\sqrt{-7})/2]$, we let

$$\begin{aligned} f(\tau) = L(s,\psi^{2k-1}) &= \sum_{\substack{\alpha\in\mathscr{O}\\ \alpha\equiv 1,2,4 \ (\mathfrak{p}_7)}} \alpha^{2k-1}q^{N(\alpha)} \\ &= \frac{1}{2}\sum_{m,n}\left(\frac{m+n\sqrt{-7}}{2}\right)^{2k-1} q^{(m^2+7n^2)/4}\left(\frac{m}{7}\right) \\ &= L(s,f) = \frac{1}{2}\sum_{m\equiv n \ (2)}{}' \frac{\left(\frac{m}{7}\right)((m+n\sqrt{-7})/2)^{2k-1}}{((m^2+7n^2)/4)^s}. \end{aligned}$$

This is essentially

$$\sum_{m,n}(m+n)/2\frac{(m\tau+n)^{2k-1}}{|m\tau+n|^2}\Big|_{\tau=(1+\sqrt{-7})/2=\tau_0}.$$

A quasi-recursion. Since $f(\tau) \in M_k$, $f'(\tau) \notin M_{k+2}$, but this almost holds: if we replace the derivative with

$$\partial = \left(\frac{1}{2\pi i}\frac{d}{d\tau} - \frac{k}{4\pi y}\right),$$

then $\partial f \in M^*_{k+2}$ where the * signifies nonholomorphic. So we have a map $M^*_k \xrightarrow{\partial^h} M^*_{k+2h}$, which takes

$$\partial^h\left(\frac{1}{(m\tau+n)^k}\right) = \frac{\Gamma(h+k)}{\Gamma(k)}\left(\frac{-1}{4\pi y}\frac{m\overline{\tau}+n}{m\tau+n}\right)^h\frac{1}{(m\tau+n)^k}.$$

We have nonholomorphic Eisenstein series

$$E_{k,s} = \sum \frac{y^s}{|m\tau+n|^{2s}}\frac{1}{(m\tau+n)^s}$$

given by some derivative of a (holomorphic) Eisenstein series. Explicitly,

$$\partial_k^n = \sum_{j=0}^n \binom{n}{j}\frac{\Gamma(n+k)}{\Gamma(j+k)}\left(\frac{-1}{4\pi y}\right)^{n-j}\left(\frac{1}{2\pi i}\frac{d}{dz}\right)^j.$$

Therefore $L(s,\psi) = (\partial^* E)(\tau_0)$, so

$$L(\psi^{2k-1}, k+r) = \partial^{k-r-1} E_{2r+1,\epsilon}(\tau_0).$$

So the central value where $r=0$ has $\partial^{k-1} E_{1,\epsilon}(\tau_0)$, here

$$E_{1,\epsilon} = \frac{1}{2} + \sum_{n=1}^{\infty}\left(\sum_{d|n}\left(\frac{d}{7}\right)\right)q^n = \frac{1}{2} + q + 2q^2 + 3q^4 + \cdots \in M_1\left(\Gamma_0(7), \left(\tfrac{=}{7}\right)\right).$$

Since $\psi_1(\langle\alpha\rangle) = \left(\frac{\alpha}{2}\right)\alpha$, we have

$$L(\psi^{2k-1}, k) = \frac{(2\pi\sqrt{7})^k}{(k-1)!}\partial^{k-1} E_{1,\epsilon}((7+\sqrt{-7})/14).$$

Proposition. *If f is a modular form, $\tau_0 \in \mathfrak{H}$, then $\{\partial^n f(\tau_0)\}_n$ satisfies a quasi-recursion (which is always effectively computable).*

For example, $M_*(SL_2(\mathbb{Z})) = \mathbb{C}(E_4, E_6)$,

$$E_2 = 1 - 24\sum_n \sigma_1(n)q^n \notin M_2, \quad E_2^*(\tau)E_2(\tau) - \frac{3}{\pi y} \in M_2^*$$

and

$$\bigoplus_k M_k^* = \mathbb{C}[E_2^*, E_4, E_6]$$

with $\partial E_4 = (1/3)(E_2^* E_4 - E_6)$, $\partial E_6 = (1/2)(E_2^* E_6 - E_4^2)$, and $\partial E_2^* = (1/12)((E_2^*)^2 - E_4)$, and

$$E_{1,\epsilon} = \frac{h(D)}{2} + \sum_{n=1}^{\infty}\left(\sum_{d|n}\left(\frac{D}{d}\right)\right)q^n = \frac{1}{2}\sum_{Q\in\mathscr{Q}_D/\Gamma}\Theta_Q(\tau).$$

In other words, suppose that f is a Hecke eigenform, then

$$f(\tau) = \sum_{\mathfrak{a}\subset\mathscr{O}_K}\psi(\mathfrak{a})q^{N(\mathfrak{a})}$$

where ψ is a Grossencharacter; the corresponding L series

$$L(f,s) = L_K(s,\psi) = \sum_{\mathfrak{a}}\frac{\psi(\mathfrak{a})}{N(\mathfrak{a})^s}.$$

Then $L(k+r,\psi)$ for $0 \le r < k$ is a finite linear combination of $(\partial^{k-r-1}E_{2r+1,\epsilon})(\tau_{\mathscr{A}})$.

We are interested in a quasi-recursion because one may want examples of Shimura curves, for which there may not be a Fourier expansion at ∞: one can either take a Fourier series along closed geodesics, an expansion at ∞^2 on $(\mathfrak{H}\times\mathfrak{H})/SL_2(\mathscr{O}_K)$, or what we will do here: expand about $z_0 \in \mathfrak{H}/\Gamma$.

We now introduce the operators:

$$D = \frac{1}{2\pi i}\frac{\partial}{\partial z}, \quad \partial = D - \frac{k}{4\pi y}$$

and

$$\mathscr{D} = D - \frac{k}{12}E_2(z) = \partial - \frac{k}{12}E_2^*$$

where E_2 is the usual Eisenstein series of weight 2, with $E_2^* = E_2 - 3/\pi y \in M_2^*$. Note that $\mathscr{D}$ preserves modularity: $\mathscr{D} : M_k \to M_{k+2}$.

For $f \in M_k$, we form the power series

$$f_D(z,X) = \sum_{n=0}^{\infty} \frac{D^n f(z)}{k(k+1)\dots(k+n-1)} \frac{X^n}{n!} \in \mathscr{C}(\mathfrak{H})[[X]].$$

We define $f_\partial(z,X)$ analogously, and note that

$$f_D\left(\frac{a\tau+b}{c\tau+b}, \frac{X}{(c\tau+d)^2}\right) = (c\tau+d)^k \exp(cX/2\pi i(c\tau+d)) f_D(\tau,X).$$

Therefore

$$f_\partial(z,X) = \exp(-X/4\pi y) f_D(z,X)$$

and we define

$$f_{\mathscr{D}}(z,X) = \exp(-X/12E_2) f_D = \exp(-X/12E_2^*) f_\partial(z,X).$$

Proposition. *We have*

$$f_{\mathscr{D}}(z,X) = \sum_{n=0}^{\infty} \frac{F_n(X)}{k(k+1)\dots(k+n-1)} \frac{X^n}{n!}$$

where $F_0 = f$, $F_1 = \mathscr{D}f$, *and*

$$F_{n+1} = \mathscr{D}F_n - \frac{n(n+k-1)}{144} E_4 F_{n-1}$$

with $\mathscr{D}(E_2) = (E_2^2 - E_4)/12$.

Example. We have $E_2^*(i) = 0$, and so $f_\partial(i,X) = f_{\mathscr{D}}(i,X)$, $\partial^n f(i) = F_n(i) = i$, e.g. for $f = E_4$, $F_0 = E_4$, $F_1 = -1/3E_6$, $F_2 = 5/36E_4^2$, and similarly since $\mathscr{D}(E_4) = -(1/3)E_6$ and $\mathscr{D}(E_6) = -(1/2)E_4^2$, and then we continue using $\mathscr{D}(ab) = \mathscr{D}(a)b + a\mathscr{D}(b)$, therefore F_n in general is a polynomial in E_4 and E_6 and therefore after factoring out $E_4^{n/2+1}$ it becomes a polynomial f_n of degree n in $E_6/E_4^{3/2}$. In particular, $f_0(t) = 1$, $f_1(t) = -1/3t$, and $f_{n+1} = (t^-1)/2f_n' - (n+2)/6tf_n - n(n+3)/144f_{n-1}$.

Now we have the factorization formula

$$L(\psi_1^{2k-1}, k) \doteq \partial^{k-1}\Theta \doteq |\partial^{(k-1)/2}\Theta|^2$$

as a formal consequence of Poisson summation.

Application to Diophantine equations. Sylvester asked which primes p are sums of $x^3 + y^3 = p$, $x, y \in \mathbb{Q}$. This equation gives the elliptic curve $E : y^2 = x^3 - 432p^2$ after a change of coordinates. To solve this, we form

$$L(E_p, s) = L_{\mathbb{Q}(\sqrt{-3})}(\psi\chi_p, s)$$

where ψ is the Grossencharacter of weight 1 and χ_p is the cubic character modulo p.

Then by the preceding discussion, we find

$$L(E_p, 1) = \frac{\sqrt{3}\Gamma(1/3)^3}{2\pi^3\sqrt{p}} S_p$$

for an integer $S_p \in \mathbb{Z}$. According to the BSD, $S_p = 0$ if p is a sum of cubes and is the order of $Ш_E$ otherwise. Under this hypothesis (the work of Coates-Wiles allows us only to say that $S_p \neq 0$ implies $p \neq x^3 + y^3$), and assuming $p \not\equiv 4, 7, 8 \pmod 9$ because the sign of the functional equation is negative in this case, and

$p \equiv 2, 5 \pmod 9$ implies that $S_p \equiv 1 \not\equiv 0 \pmod 3$, so we must only consider $p \equiv 1 \pmod 9$.

Theorem.

(a) *Let* $p = 9k + 1$. *Then*

$$S_p = \operatorname{Tr}(\alpha_p)$$

where

$$\alpha_p = \frac{\sqrt[3]{p}}{54} \frac{\Theta(p\delta)}{\Theta(\delta)}$$

so that $\deg \alpha_p = 18k$ *and*

$$\Theta(q) = \frac{1}{2} \sum_{m,n} q^{m^2+mn+n^2} = \frac{3}{2} + 3 \sum_n \left(\sum_{d|n} \left(\frac{d}{3} \right) \right) q^n$$

and $\delta = -1/2 + 2/6\sqrt{3} \in \mathfrak{H}$ *with*

$$\Theta(\delta) = \frac{-3\Gamma(1/3)^3}{(2\pi)^2}.$$

(b) *Moreover,*

$$S_p = (\operatorname{Tr} \beta_{\mathfrak{p}})^2$$

where if $p = \mathfrak{p}\overline{\mathfrak{p}}$, $\mathfrak{p} = \langle p, -r + \sqrt{-3}/2 \rangle$ *so that* $r^2 \equiv -3 \pmod{4p}$, *then*

$$\beta_{\mathfrak{p}} = -\beta_{\overline{\mathfrak{p}}} = \frac{6\sqrt{p}}{\sqrt{\pm 12}} \frac{\eta(pz_0)}{\eta(z_0/p)}$$

so that $\deg \beta_p = 6k$.

(c) *If we define* $f_0(t) = 1$, $f_1(t) = t^2$,

$$f_{n+1} = (1 - t^3) f_n' + (2n + 1) t^2 f_n - n^2 t f_{n-1},$$

and $A_k = f_{3k}(0)$, *then*

$$S_p \equiv (-3)^{(p-10)/3} (3k!)^2 A_{2k} \pmod p$$

with $|S_p| < p/2$.

S_p *can also be given as an explicit formula in* B_k^2 *with* $A_{2k} = B_k^2$.

Link to hypergeometric functions. Let

$$h = F(1/3, 1/3; 2/3; x) = \sum_{k=0}^{\infty} \frac{A_k}{(3k)!} T^k,$$

with

$$T = x \frac{F(2/3, 2/3; 4/3; x)^3}{F(1/3, 1/3; 2/3; x)^3} = x + \dots;$$

then

$$(1 - x)^{1/24} \sqrt{h} = \sum_{k=0}^{\infty} \frac{B_k}{(3k)!} (-T/2)^k.$$

Then

$$\begin{aligned} \frac{1}{\sqrt{1-u}} \eta \left(\frac{\omega - \overline{\omega} u}{1 - u} \right) &= \eta(\omega) + (\eta'(\omega) = \eta(\omega)) u + \dots \\ &= c_1 \sum_{n=0}^{\infty} \frac{B_n}{(3n)!} (-c_2 u)^{3n} \end{aligned}$$

where $c_1 = \eta(\omega) = e^{\pi i/24}(3^{1/4}\Omega/2\pi)^{1/2}$ and $c_2 = -3\sqrt{3}/4\pi\Omega^2$. This gives us an explicit formula for calculating the above values.

Other special values. Therefore from the Kronecker limit formula we obtain special values $\zeta(\mathscr{A},1)$. One can also ask for the values $\zeta(\mathscr{A},m)$ for $m>1$ and to what they correspond (for example, $\prod_{\chi\neq 1} L_K(1,\chi) \doteq (h(H)/h(K))R(K)$). Classically, $\zeta_F(1)$ for a number field F corresponds to units and the class number; Borel discovered that $\zeta_F(m)$ corresponds to the K group $K_{2m-1}(F)$.

What we will need from K-theory is as follows: $K_1(R) = R^\times$ for any ring R, so $K_1(\mathscr{O}_F) \doteq \mathbb{Z}^{r_1+r_2-1}$ ignoring torsion, and $K_1(F) = \bigoplus_\pi \mathbb{Z}$ generated by chosen prime elements π of F (ignoring units). We have

$$\operatorname{rk} K_{2m-1}(F) = \begin{cases} 0, & n \text{ even;} \\ r_2, & n = 2m-1,\ m \text{ even;} \\ r_1+r_2, & n = 2m-1,\ m \text{ odd.} \end{cases}$$

and for higher n, $K_n(\mathscr{O}_F) \doteq K_n(F)$, again up to torsion (or tensoring with $\mathbb{Q}$).

Recall we have $F \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, where the latter can be broken up into real and imaginary pieces, hence we obtain two disjoint $\mathbb{R}$-vector spaces of dimension r_1+r_2. We will now show that the image of $K_{2m-1}(F)$ embeds as a lattice in such a vector space, and the covolume of this lattice gives us $\zeta_F(m)$.

We have the dilogarithm $\operatorname{Li}_m(X) = \sum_{n=1}^\infty X^n/n^m$, e.g.

$$\operatorname{Li}_2(X) = \int_0^x \frac{1}{t}\log\frac{1}{1-t}\,dt.$$

The function

$$D_2(x)\operatorname{Im}(\operatorname{Li}_2(X) - \log|x|\operatorname{Li}_1(x))$$

is single-valued, like $\operatorname{Re}(\log x) = \log|x|$.

Conjecture. *$K_{2m-1}(F) \doteq B_m(F)$, where $B_m(F)$ is the Bloch group, which for now is just certain $\mathbb{Z}$-combinations of elements of F modulo a certain subgroup.*

We will define the regulator map from K_{2m-1} to $\mathbb{R}^{r_1+r_2}$ or $\mathbb{R}^{r_2}$ using the dilogarithm $D_m : \mathbb{C} \to \mathbb{R}$; since $D_m(\overline{x}) = (-1)^{m-1}D_m(x)$, this number is determined by the character of the embeddings of F.

Conjecture. *If K is an imaginary quadratic field and $m \geq 2$, then there exists an $\eta_m \in B_m(H) \hookrightarrow B_m(\mathbb{C})^n \xrightarrow{D_m} \mathbb{R}^n$ such that*

$$\zeta(\mathscr{A},m) = \frac{2^{(-1)^{(m-1)/2}}(2\pi)^m}{(m-1)!}|D|^{1/2-m}D_m(\sigma_{\mathscr{A}}|\eta_m)).$$

For $m=2$, this is a theorem, as we will see.

Example. Take $K = \mathbb{Q}(\sqrt{-23})$, $h=3$, then $\mathscr{A}_0 \leftrightarrow [1,1,6]$, $\mathscr{A}_1 \leftrightarrow [2,1,3]$, and $\mathscr{A}_2 = \mathscr{A}_1^{-1}$. Then

$$\zeta_0(s) + 2\zeta_1(s) = \zeta_K(s) = \zeta(s)L(s,\left(\tfrac{-}{23}\right))$$

since $\zeta_1 = \zeta_2$, and hence we also have

$$\zeta_0(s) + \zeta_1(s) = \zeta_0(s) + \omega\zeta_1(s) + \overline{\omega}\zeta_2(s) = L_K(s,\chi)$$

where χ is a cubic character. We compute:

$$\zeta_0(2) = 1.219266\ldots, \quad \zeta_1(2) = 0.54446\ldots$$

and

$$\zeta_0(2) - 2\zeta_1(2) = \zeta_K(2) = \frac{4\pi^2}{2(23)^{3/2}} D(\xi_K)$$

$$\zeta_0(2) - \zeta_1(2) = L(2,\chi) = \frac{16\pi^2}{23^{3/2}} D(\theta)$$

where

$$\xi_K = 21[(1+\sqrt{-23})/2]+7[2+\sqrt{-23}]+[(3+\sqrt{-23})/2]-3[(5+\sqrt{-23})/2]+[3+\sqrt{-23}].$$

and $\theta^3 + \theta + 1 = 0$ is contained in the real subfield of H.

Case $m = 2$**.** We investigate the Bloch group $B_2(F) = B(F)$ (see [6]). In this case,

$$B(F) = \{\textstyle\sum_i n_i[x_i] : \sum_i n_i[x_i] \wedge [1-x_i] = 0\} / H$$

where

$$H = \{[a] + [b] + [(1-a)/(1-ab)] + [1-ab] + [(1-b)/(1-ab)]\}.$$

We want $\ker\left(\mathbb{Z}[F] \xrightarrow{\delta} \bigwedge^2(F^\times)\right)$ by $[x] \mapsto [x] \wedge [1-x]$. Note that $B_2(F)$ is torsion if F is totally real, e.g. $F = \mathbb{Q}$. The relation corresponds to the relation of the dilogarithm $D(a) + D(b) + \cdots + D((1-b)/(1-ab)) = 0$.

Example. For $F = \mathbb{Q}$, the elements $x = 1/2, 1/3, 3/4, 8/9, \ldots$, all defined multiplicatively using the primes $2, 3$, have $1 - x = 1/2, 2/3, 1/4, 1/9, \ldots$ with the same property. For example $\delta([1/2]) = [1/2] \wedge [1/2] = 0$, and

$$[1/3] \mapsto [1/3] \wedge [2/3] = -[3] \wedge ([2] - [3]) = [2] \wedge [3]$$

and similarly

$$[3/4] \mapsto [3/4] \wedge [1/4] = 2([2] \wedge [3]),$$

so already we have the Bloch group elements $[1/2]$ and $[3/4] - 2[1/3]$.

Proposition (A. Levin)**.** *For* $\mathfrak{a} \subset K$*,* $\lambda \in \mathscr{O}_K$*,* $\mu = 1 - \lambda$*, and* $\mathscr{A} = [\mathfrak{a}]$*, we define*

$$\xi_{\mathscr{A},\lambda} = 4N(\lambda)N(\mu)[\lambda] + {\sum_{\substack{\alpha \in \lambda^{-1}\mathfrak{a}/\mathfrak{a} \\ \beta \in \mu^{-1}\mathfrak{a}/\mathfrak{a}}}}' \sum_{\ell \ (N(\lambda))} [\gamma_{\alpha,\beta,\ell+m\beta}].$$

where

$$\gamma_{a,b,c} = \frac{\wp(a) - \wp(c)}{\wp(a) - \wp(b)} = \frac{\sigma(a-c)\sigma(a+c)\sigma(b)^2}{\sigma(a-b)\sigma(a+b)\sigma(c)^2} \in H' \supset H,$$

where σ *is the Weierstrass* σ*-function.*

Then $\xi_{\mathscr{A},\lambda} \in H'$*.*

One checks that $\delta(\xi) = [\xi] \wedge [1-\xi] = 0$.

Theorem (A. Levin)**.** *We have*

$$D(\xi_{\mathscr{A},\lambda}) = (N(\lambda)+1)(N(\mu)+1)\zeta_K(\mathscr{A}, 2).$$

8. Bowen Lectures: Periods and Special Values of L-functions

The contents of these lectures will appear as an article in the upcoming Springer volume covering mathematics of the twenty-first century.

Periods. We have the hierarchy of numbers $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \overline{\mathbb{Q}}$ (countable, constructible, accessible) but also $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ with $\overline{\mathbb{Q}} \subset \mathbb{C}$ (uncountable, unconstructible, inaccessible). There is an intermediate class $\overline{\mathbb{Q}} \subset \mathscr{P} \subset \mathbb{C}$ (constructible, but only partially accessible).

Definition. A *period* is a complex number whose real and imaginary parts can be given as an absolutely convergent integrals of rational functions with rational coefficients over domains in $\mathbb{R}^n$ given by polynomial inequalities with rational coefficients.

$$\Omega = \int_{\substack{f_1(x_1,\dots,x_n)\geq 0 \\ f_m(x_1,\dots,x_n)\geq 0}} (R_1(x_1,\dots,x_n) + iR_2(x_1,\dots,x_n))\, dx_1 \dots dx_n$$

Example. $\sqrt{2} = \int_{2x^2\leq 1} dx$.

Example.

$$\begin{aligned}\pi &= \iint_{x^2+y^2\leq 1} dx\, dy = \int_{-\infty}^{\infty} \frac{dx}{1+x^2} \\ &= 2\int_{-1}^{1} \sqrt{1-x^2}\, dx = \int_{-1}^{1} \frac{dx}{\sqrt{1-x^2}} \\ &= \frac{1}{2i} \oint_{|z|=1} \frac{dz}{z}.\end{aligned}$$

Example. $\log 2 = \int_1^2 dx\, x$, but is also

$$\int_0^1 \frac{x\, dx}{\log\left(1/(1-x)\right)}.$$

Alternative definitions:

- Allow algebraic functions and algebraic coefficients.
- Integrate only 1, so $\Omega = A_1 - A_2 + iA_3 - iA_4$ with A_j a volume of a domain in $\mathbb{R}^n$ defined by polynomial inequalities.
- If X is a smooth quasiprojective variety, $Y \subset X$ subvariety, defined over $\overline{\mathbb{Q}}$, ω a closed algebraic n-form on X such that $\omega|_Y = 0$, C a singular n-chain in $X(\mathbb{C})$ with $\partial C \subset Y(\mathbb{C})$, then we let $\int_C \omega \in \mathscr{P}$.

Example. If $a, b \in \mathbb{Q}_{\geq 0}$, $a \neq b$,

$$E(a,b) = 2\int_{-b}^{b} \sqrt{\frac{1+a^2x^2}{b^4-b^2x^2}}\, dx$$

is not in $\overline{\mathbb{Q}}\pi$.

Example. We have

$$\zeta(n) = 1 + 1/2^n + 1/3^n + \dots$$

for $n \geq 2$, e.g.

$$\zeta(3) = \iiint_{0<x<y<z<1} \frac{dx\, dy\, dz}{(1-x)yz}.$$

Example. For μ the Mahler measure, and P a polynomial in $x_1^{\pm 1}$, …, $x_n^{\pm 1}$ with coefficients in $\mathbb{Q}$, we have

$$\mu(P) = \int \dots \int_{|x_1|=\dots=|x_n|=1} \log|P(x_1,\dots,x_n)| \frac{dx_1}{x_1} \dots \frac{dx_n}{x_n} \in \mathscr{P}.$$

Example. $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}\, dt$, has $\Gamma(p/q)^q \in \mathscr{P}$.

e and γ are presumably not periods, but we do not know this.

Properties of periods.
Question. $\pi\sqrt{163}/3 = 13.36972333037750$ equal to the real number $\log(640320) = 13.36972333037750$?
Question. What about $\pi/6\sqrt{3502}$ and

$$\log\left(2\prod_{j=1}^{4}(x_j+\sqrt{x_j^2-1})\right)$$

where $x_1 = 1071/2 + 92\sqrt{34}$, $x_2 = 627/2 + 221\sqrt{2}$, $x_3 = 1553/2 + 133\sqrt{34}$, $x_4 = 429 + 304\sqrt{2}$. They agree to 80 decimal places.

The answer to both of these questions is no, as one can check by taking a longer approximation to each.
Question. Finally, what about

$$\sqrt{11+2\sqrt{29}} = \sqrt{16-2\sqrt{29}+2\sqrt{55-10\sqrt{29}}}$$
$$= 7.381175940895657970 9872 = \sqrt{5}+\sqrt{22+2\sqrt{5}}?$$

This time the numbers are algebraic. Are they equal? We can tell by determining their minimal polynomial. For two algebraic numbers of bounded degree there is an explicit bound on the number of digits we must write down to tell if they are equal. There is nothing true for periods. Similarly, given a real number one can construct a minimal polynomial which by LLL can construct it; nothing such is true for periods.

Rules of calculus. We have the following rules from calculus which allow us to operate on periods:

(i) Additivity:

$$\int_a^b (f(x)+g(x))\,dx = \int_a^b f(x)\,dx + \int_a^b g(x)\,dx$$

and

$$\int_a^b f(x)\,dx = \int_a^c f(x)\,dx + \int_c^b f(x)\,dx.$$

(ii) Change of variables:

$$\int_{f(a)}^{f(b)} F(y)\,dy = \int_a^b F(f(x))f'(x)\,dx.$$

(iii) Newton-Leibniz formula:

$$\int_a^b f'(x)\,dx = f(b)-f(a).$$

For higher dimensional integrals, there are also corresponding formulas.

Conjecture. *Any two representations of the same number as a period can be obtained from one another using only the preceding rules, with all functions and domains of integration algebraic with coefficients in* $\mathbb{Q}$.

There is also a fourth rule: $\pi A = \pi B$ implies $A = B$ for any period π.

Principles:

(1) If an interesting number arises, try to exhibit it as a period!
(2) If an equality of two numbers is conjectured, try to write them both as periods and prove their equality using the "Rules of calculus".

Example. $\mu(P)$ the Maahler measure; show by the "rules of calculus" that

$$6\mu(x+y+16+x^{-2}+y^{-2}) = 11\mu(x+y+5+x^{-1}+y^{-1}).$$

Open problems:

(1) Find an algorithm to determine whether two given numbers in $\mathscr{P}$ are equal.
(2) Find an algorithm to determine whether a numerically given element of $\mathbb{C}$ is equal (to given precision) to a simple element of $\mathscr{P}$.
(3) Explicit examples of numbers *not* belonging to $\mathscr{P}$.

Periods and differential equations. Start with $\mathbb{Z} \subset \mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathscr{P}$. We have the analogy $\mathbb{Z}[T] \subset \mathbb{Q}(T) \subset \overline{\mathbb{Q}(T)}$ and the analogy of $\mathscr{P}$ are solutions of (special) differential equations with algebraic coefficients coming from integrals with a free parameter.

Example. Elliptic curves $E_t : y^2 = x(x-1)(x-t)$. Have

$$\Omega_1(t) = \int_t^1 \frac{dx}{\sqrt{x(x-1)(x-t)}} = \int_t^1 \frac{dx}{y}$$

and similarly $\Omega_2(t) = \int_1^\infty dx/y$.

Elliptic functions are doubly periodic. If $t \in \overline{\mathbb{Q}}$, $\Omega_1(t), \Omega_2(t) \in \mathscr{P}$; and $\Omega_1(t)$ and $\Omega_2(t)$ satisfy the differential equation

$$t(t-1)\Omega''(t) + (2t-1)\Omega'(t) + 1/4\Omega(t) = 0.$$

Example. Hypergeometric functions

$$F(a,b;c;x) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n n!} x^n$$

where $(a)_n = a(a+1)\dots(a+n-1)$. If $a, b, c \in \mathbb{Q}$, then $x \in \overline{\mathbb{Q}}$ implies $F(a,b;c;x) \in (1/\pi)\mathscr{P}$.

There are relations among these examples:

$$\begin{aligned}\Omega_2(t) &= \int_1^\infty \frac{dx}{\sqrt{x(x-1)(x-t)}} = 2\int_0^{\pi/2} \frac{d\theta}{\sqrt{1-t\sin^2\theta}} \\ &= 2\sum_{n=0}^{\infty} \binom{2n}{n} (t/4)^n \int_0^{\pi/2} \sin^{2n}\theta \, d\theta \\ &= \pi \sum_{n=0}^{\infty} \binom{2n}{n}^2 t^n/16^n = \pi F(1/2, 1/2; 1; t).\end{aligned}$$

Example. Modular forms: $z \in \mathfrak{H}$, $f(z)$ holomorphic, not too big,

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $z \in \mathfrak{H}$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ is a modular form of weight k. For example,

$$\Delta(z) = e^{2\pi iz} \prod_{n=1}^{\infty} (1 - e^{2\pi inz})^{24}$$

($k = 12$) and

$$j(z) = \frac{1}{\Delta(z)} \left(1 + \sum_{n=1}^{\infty} \frac{240n^3}{e^{-2\pi inz} - 1} \right)^3$$

($k = 0$) are modular.

$j(z) \in \overline{\mathbb{Q}}$ and $\Delta(z) \in \mathscr{P}[1/\pi]$. Moreover, $\Delta(z) = F(j(z))$, implies $F(t)$ satisfies a linear differential equation of order 13.

$$\sqrt[4]{1 + \sum_{n=1}^{\infty} \frac{240n^3}{e^{-2\pi inz} - 1}} = F(1/12, 5/12; 1; 1728/j(z)).$$

E.g. $j(i) = 1728$, $\Delta(i) = \Gamma(1/4)^{24}/2^{24}\pi^{28}$.

An overview of L-functions. Let X be an arithmetical object (a number field, character, Galois representation, arithmetic algebraic variety, modular form, etc.). Then we associate to it $L(X, s)$, the Dirichlet series encoding certain characteristics of X:

$$L(s) = L(X, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Assume the a_n have polynomial growth so that the series converges; then it does so for $\mathrm{Re}(s) \gg 0$.

There are five typical properties:

(1) Euler product: $L(s) = \prod_p P_p(p^{-1})^{-1}$ where $P_p(T)$ is a polynomial with integral coefficients of degree $\leq n$ with $= n$ when $p \nmid \Delta$.

n is called the level, Δ is called the conductor. This directly measures the p-adic properties of X (the number of points on a variety, eigenvalues of a Hecke operator, how a prime splits, etc.).

(2) Meromorphic continuation and functional equation:

$$L^*(s) = \gamma(s)L(s) = \pm L^*(k - s)$$

where

$$\gamma(s) = \Delta^{s/2}\pi^{-ns/2} \prod_{j=1}^{n} \Gamma((s + \alpha_j)/2)$$

for $k \in \mathbb{N}$.

(3) Local Riemann hypothesis: $P_p(p^{-s}) = 0$ implies $\mathrm{Re}(s) = (k - 1)/2$.

(4) Global Riemann hypothesis: $L(s) = 0$ implies $\mathrm{Re}(s) = k/2$ or $s \in \mathbb{Z}$.

(5) Special values: For certain $s \in \mathbb{Z}$ such that $\gamma(s) \neq \infty$, $\gamma(k - s) \neq \infty$, then $L(s) \in \mathscr{P}[1/\pi]$.

Example. $L(s) = \zeta(s) = \sum_n 1/n^s = \prod(1 - p^{-1})^{-1}$, so $P_p(X) = 1 - X$, $n = 1$, $\Delta = 1$ (Euler). $\zeta^*(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) = \zeta^*(1 - s)$, so $k = 1$ (Euler, Riemann). $1 - p^{-s} = 0$ implies $\mathrm{Re}(s) = 0$, and the global Riemann hypothesis $\zeta(s) = 0$ implies $s \in -2\mathbb{N}$ or $\mathrm{Re}(s) = 1/2$ (this has been checked for the first 2 billion zeros, but still not known).

We have $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$, ... and $\zeta(-1) = -1/12$, $\zeta(-3) = 1/120$, ... (again due to Euler), with a simple relationship between certain pairs.

There are examples that come from number theory:

Example (Dirichlet). We have $L(s, \chi)$ for χ a Dirichlet character. $P_p(x) = 1 - \chi(p)$, $n = 1$, Δ is the conductor of χ, $k = 1$.

Example (Dedekind). We have $\zeta_F(s)$ for F a number field. $n = [F : \mathbb{Q}]$, δ is the discriminant of F, and $k = 1$. If $F = \mathbb{Q}(\alpha)$, and $f(\alpha) = 0$ is minimal, then $P_p(T) = \prod_{1-X^{\deg f_i}}$ if $f = \prod_i f_i \pmod p$ for $p \nmid \Delta$.

Example (Artin). We have $L(s, \rho)$, where ρ a Galois representation. Here $n = \dim \rho$, Δ is the conductor of ρ, $k = 1$, and the P_p is obtained from eigenvalues of Frobenius.

There are also examples that come from algebraic geometry:

Example (Hasse-Weil). For $L(C/\mathbb{Q}, s)$, C a curve, $n = 2g$, $k = 2$, we have $P_p(T) = 1 - a_p T + \cdots + p^g T^{2g}$ for $p \nmid \Delta$, where e.g. a_p counts the the number of points in $\mathbb{Z}/\langle p \rangle$, etc. We conjecture with $\gamma(s) = N^{3/2}(2\pi)^{2g}\Gamma(s)^g$ that

$$L^*(s) = \pm L * (k - s);$$

this is known for genus 1 curves (Wiles) and modular curves.

Example (Weil, Grothendieck, Dwork, Deligne). More generally, for any algebraic geometry X, we have

$$\zeta_X(s) = \exp\left(\sum_p \sum_{r=1}^{\infty} \#X(\mathbb{F}_{p^r}) \frac{p^{-rs}}{r}\right) = \frac{L_0(s)L_2(s)\dots L_{2d}(s)}{L_1(s)\dots L_{2d-1}(s)}$$

where $d = \dim X$, and for $L_i(T)$, $n = \dim H_i(X)$, $k = i + 1$.

Finally, there are examples coming from modular (automorphic) forms:

Example. Let f be a modular form of weight k, e.g.

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} n^3/(q^{-n} - 1)$$

for $q = e^{2\pi i \tau}$ and

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

Then we obtain $1/240 L(E_4, s) = \zeta(s)\zeta(s - 3)$, and (Ramanujan)

$$L(\Delta, s) = 1 - \frac{24}{2^s} + \frac{252}{3^s} + \cdots = \prod_p P_p(p^{-s})^{-1}$$

with $P_p(T) = 1 - \pi(p)T + p^{11}T^2$, $n = z$ have local Riemann hypothesis, $|\tau(p)| \leq 2p^{11/2}$. Then we associate $L(f, s)$, $n = 2$, k the weight, and Δ the level of f, and

$$L^*(f, s) = (2\pi)^{-s}\Gamma(s)L(f, s) = \pm L^*(f, k - s)$$

where the γ term is in fact $(1/2\sqrt{\pi})\pi^{-1}\Gamma(s/2)\Gamma((s + 1)/2)$.

We can also take $L(\mathrm{Sym}^2 f, s)$ the symmetric square (Rankin-Selberg), $n = 3$, k twice the weight minus 1 and many others (L-series of Siegel and Hilbert modular forms, L-series of automorphic representations) (Langlands).

Langlands tells us that there is only *one* kind of L-series: already, the case of algebraic number theory is just algebraic geometry in dimension zero.

Special values. Recall the special values of the ζ function: $\zeta(1) = \infty$, $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$, ..., and $\zeta(0) = -1/2$, and $\zeta(-1) = -1/12$, ... There is no such result for $\zeta(3)$, since $\zeta^*(s) = \gamma(s)\zeta(s) = \zeta^*(1-s)$; since $\Gamma(s) \neq 0$, but $\Gamma(s) = \infty$ if $s = 0, -1, -2, \ldots$, so $\gamma(s) = \infty$ iff $s = 0, -2, -4, \ldots$, and $\Gamma(1-s) = \infty$ as well for $s = 1, 3, \ldots$.

Definition (Deligne 1979). Let $L(\chi, s)$ be an L-series as above. s is called *critical* for X if $s \in \mathbb{Z}$, $\gamma(s) \neq \infty$, and $\gamma(k-s) \neq \infty$.

Conjecture (Deligne's conjecture)**.** *If s is critical, then $L_X(s) \in \widehat{\mathscr{P}} = \mathscr{P}[1/\pi]$.*

This conjecture is absolutely explicit; up to a rational number, there is a specific matrix with the period equal to a determinant.

This was generalized by Beilinson (and Scholl):

Conjecture. *For $s \in \mathbb{Z}$ critical, let m the order of vanishing at s of L. Then $L^{(m)}(s) \in \widehat{\mathscr{P}}$.*

Example. The Dedekind zeta-function. The critical values: if F is totally real, then already $\zeta_F(2), \zeta_F(4), \cdots \in \overline{\mathbb{Q}}[\pi]$, $\zeta_F(-1), \zeta_F(-3), \cdots \in \mathbb{Q}$ (Klingen-Siegel). (If the field is not totally value, all are noncritical, since $\gamma(s)$ has the factors $\Gamma(s/2)^{r_1+r_2}\Gamma((s+1)/2)^{r_2}$.)

For noncritical values, $s = 1$ implies $\zeta_F(s)/\zeta(s)\big|_{s=1} \in \overline{Q}[\pi, \log|\epsilon|]$, ϵ units of F (Dirichlet). If $s = m > 1$, $\zeta_F(m)$ the regulator for $K_{2m-1}(F)$, so is in $\mathscr{P}$ (Borel).

Conjecture (Zagier)**.** $\zeta_F(m) \in \overline{\mathbb{Q}}[\pi, \mathrm{Li}_m|\alpha|]$, *where*

$$\mathrm{Li}_m(T) = \sum_{n=1}^{\infty} \frac{T^n}{n^m}.$$

For $m = 2$, $F = \mathbb{Q}(\sqrt{-d}) \supset \mathscr{O}$ the ring of integers, we have

$$\zeta_F(2) = \frac{4\pi^2}{d^{3/2}} \mathrm{vol}(\mathfrak{H}^3/SL_2(\mathscr{O}))$$

(Humbert). More generally, $\zeta_F(2)$ for any number field is the volume of some hyperbolic ($r_2 = 1$) or multihyperbolic ($r_2 > 1$) manifold.

If Δ is a hyperbolic 3-simplex (a tetrahedron), then $\mathrm{vol}(\Delta)$ is a combination of values of $D(x)$ (Lobachevski), where

$$D(x) = \mathrm{Im}(\mathrm{Li}_2(x) + \log|x| \log(1-x)$$

is a uniquely defined function.

Example. For $F = \mathbb{Q}(\sqrt{-7})$,

$$\zeta_F(2) = \frac{4\pi^2}{21\sqrt{7}}(2D\left(D((1+\sqrt{-7})/2) + D((1+\sqrt{-7})/4)\right).$$

Also there are many examples for $m > 2$, e.g.

$$\zeta(3) = D_3(1) = 8/7 D_3(1/2) = 6/13(2D_3(3) - D_3(-3)$$

and so forth. This is proved for $m = 2, 3$ (Goncharov). Generalization to Artin L-functions specializes to:

Conjecture (Zagier)**.** *Let $Q(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$ be a positive definite binary quadratic form, then*

$$\zeta_Q(s) = \sum_{x,y \in \mathbb{Z}}{}' \frac{1}{Q(x,y)^s}$$

is an Epstein zeta function. For $m > 1$,

$$\zeta_{\mathbb{Q}}(m) = \frac{\pi^m}{\sqrt{|D|}} \sum_j \alpha_j D_m(x_j)$$

for $\alpha_j \in \mathbb{Q}$, $x_j \in \overline{\mathbb{Q}}$.

The conjecture has been proved for $m = 2$ (Levin). Explicit computation has been done for $Q(x, y) = 2x^2 + xy + 3y^2$.

Example (Mahler measures). (Deninger, Boyd, Villegas) For example, for $k > 0$, $k \neq 4$, let

$$P_k(x, y) = (x + y)(xy + 1) - kxy$$

The eqatuion $P_k(x, y) = 0$ defines an elliptic curve E_k and one expects

$$|L'(E_k, 0)| = N/4\pi^2 L(E_k, 0) = B_k \mu(P_k)$$

where μ is the Mahler measure with $B_k \in \mathbb{Q}$. For example, $k = 1, 2, 3, \ldots$ give $B_k = 1, 1, 1/2, 1/6, 2, 2, 1/4, \ldots$.

Modular forms. For f a modular form, the only special values are $s = 1, \ldots, k-1$, and we need only to know half by the functional equation.

The theory of "period polynomials" or the Rankin-Selberg method imply that there exist two periods $\Omega_\pm \in \mathscr{P}$ such that for $0 < s < k$,

$$L^*(f, s) \in \begin{cases} \overline{\mathbb{Q}}\Omega_+, & s \text{ even;} \\ \overline{\mathbb{Q}}\Omega_-, & s \text{ odd.} \end{cases}$$

Example. For $\Delta(z)$, $L(\Delta, s) = 1 - 24/2^s + 252/3^s - \ldots$:

s	$L^*(\Delta, s)$
6	$1/30\ \Omega_+$
7	$1/28\ \Omega_-$
8	$1/24\ \Omega_+$
9	$1/18\ \Omega_-$
10	$2/25\ \Omega_+$
11	$90/691\ \Omega_-$

According to Deligne, $L(\Delta, s)$ is a motivic L-function, corresponding to a piece of $H^{11}(K)$ for a certain 11-dimensional variety K (Kuga variety, 11th symmetric power of the universal elliptic curve). Hence $L^*(s, \Delta)$, $s = 1, \ldots, 11$, should be given by integrals of 11-forms over 11-cycles. Can we make this explicit? Yes!

Step 1:

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t}\, dt$$

so

$$(2\pi)^{-s}\Gamma(s) n^{-s} = \int_0^\infty t^{s-1} e^{-2\pi n t}\, dt$$

and

$$(2\pi)^{-s}\Gamma(s) L(\Delta, s) = \int_0^\infty t^{s-1} \Delta(it)\, dt.$$

Step 2: Recall the Legendre family of elliptic curves

$$E_t : y^2 = x(x-1)(x-t)$$

for $t \in \mathbb{C}$ with periods

$$\Omega_1(t) = \int_t^1 \frac{dx}{y}, \quad \Omega_2(t) = \int_1^\infty \frac{dx}{y}.$$

If we substitute

$$t = \lambda(z) = 16\frac{\Delta(z/2)^{1/3}\Delta(2z)^{2/3}}{\Delta(z)} = 16q^{1/2} - 128q + 704q^{3/2} - \dots$$

for $z \in \mathfrak{H}$, $q = e^{2\pi i z}$. Then

$$\Omega_2(t) = \pi F(1/2, 1/2; 1; t) = \pi\theta(z)^2$$

and

$$\Omega_1(t) = \pi z\theta(z)^2$$

where $\theta(z) = \sum_n e^{\pi i n^2 z} = 1 + \dots$.

Step 3: Thus $\Omega_2(t)$ for $t = \Lambda(z)$ is a modular of weight 1, $\Omega(z)$ is a modular form of weight 12. Therefore $\frac{\Delta(z)}{\Omega_2(t)^{12}}$ is a modular function, and hence an algebraic function of $t = \lambda(z)$, and in fact a short calculation gives this as $t^2(t-1)^2$. Since $dt = \lambda'(z)\,dz$, $\lambda'(z) = \Omega_2(t)^2/t(1-t)$ is a modular form of weight 2, and $\Omega_1(t) = z\Omega_2(t)$. Hence for $s = 1, \dots, 11$,

$$\begin{aligned} L^*(\Delta, s) &= \int_0^\infty t^{s-1}\Delta(it)\,dt \\ &= i^{s-1}\pi^{-11}\int_0^1 \Omega_1(t)^{s-1}\Omega_2(t)^{11-s}t(1-t)\,dt. \end{aligned}$$

Noncritical values.

Theorem (Beilinson, Deninger-Scholl)**.** *For f a modular form, weight k, $m \geq k \geq 2$. Then $L(f, m) \in \widehat{\mathscr{P}} = \mathscr{P}[1/\pi]$.*

Beilinson's proof gives $L(f, 2)$ as the sum of integrals of the form

$$\int_a^b \log|A(x)|B(x)\,dx$$

with $a, b \in \overline{\mathbb{Q}}$, $A, B \in \overline{\mathbb{Q}(x)}$, equal to the Mahler measure in some cases.

For $k = 1$, the corresponding statement would follow from Stark's ($m = 1$) and Zagier's ($m > 1$) conjectures in general and is true for "CM forms".

Corollary. *If n is even, $Q(x_1, \dots, x_n)$ a positive definite quadratic form with integral coefficients. Let*

$$\zeta_Q(s) = {\sum_{x_1,\dots,x_n \in \mathbb{Z}}}' \frac{1}{Q(x_1, \dots, x_n)^s}$$

(Epstein zeta function, converges for $\mathrm{Re}(s) > n/2$). Then $s \in \mathbb{Z}$ implies $\zeta_Q(s) \in \widehat{\mathscr{P}}$.

Question (Open). Is this true also for n odd? In particular, is "Glaischer's constant"

$${\sum_{x,y,z \in \mathbb{Z}}}' \frac{1}{(x^2+y^2+z^2)^2} = 16.53231595\dots$$

a period?

Central values. If k is even, then the central value $s = k/2$ is critical, but $L(f, k/2)$ often vanishes (e.g. if the functional equation $L^*(f,s) = \pm L^*(f, k-s)$ has a minus sign). In this case, the Beilinson-School conjecture still predicts that the first nonzero derivative of $L(f,s)$ at $s = k/2$ is a period.

Theorem. *If f is a Hecke eigenform of weight k, $L^*(f,s) = -L^*(f,k-s)$ implies $L'(f,k/2) \in \widehat{\mathscr{P}}$.*

Idea of proof. The central derivative $L'(f,k/2)$ can be expressed as a finite rational linear combination of logarithms of integers and special values of *higher weight Green's functions* $G_{k/2}(z,z')$ with $z, z' \in \overline{\mathbb{Q}}$ (Gross-Zagier). These special values are sometimes conjectured to be logarithms of algebraic numbers, e.g.

$$\frac{-1}{\sqrt{2}G_2(i, i\sqrt{2})} = \log \frac{27+19\sqrt{2}}{27-19\sqrt{2}}$$

but can be *proved* to be periods by a calculation like the one for critical values of $L(\Delta, s)$. There are formulas:

$$\frac{-1}{\sqrt{2}} G_2(i, i\sqrt{2}) = \frac{20}{\pi} G + 1728 \int_{\sqrt{2}} \frac{E_4(iy)\Delta(iy)}{E_6(iy)^2}(y^2-2)\, dy \ldots$$

which can be expressed explicitly. □

Conjecture of Birch and Swinnerton-Dyer. For $E/\mathbb{Q}$ an elliptic curve over $\mathbb{Q}$, so that (Mordell)

$$E(\mathbb{Q}) \simeq \mathbb{Z}P_1 \oplus \cdots \oplus \mathbb{Z}P_r \oplus \mathbb{Z}_{\text{tors}}.$$

By Wiles, $L(E,s) = L(f,s)$ for f a modular form of weight 2. Then the Birch and Swinnerton-Dyer conjecture says that $\operatorname{ord}_{s=1} L(E,s) = r$ and

$$L^{(r)}(E,1) = c\Omega R$$

where $c \in \mathbb{Q}$, $c \neq 0$ (there explicit formulas for it), Ω a real period of E, equal to $\int_{E(\mathbb{R})} dx/y$, and R is the regulator of E, the determinant of the $r \times r$ matrix $(\langle P_i, P_j \rangle)_{i,j}$ where $\langle , \rangle$ is the bilinear height pairing on $E(\mathbb{Q})$ defined by $\langle P, P \rangle = h(P)$, the canonical height, defined as follows: $h_0(P)$ is the naive height

$$\log \max(|x_1|, |x_2|, |y_1|, |y_2|)$$

where $P = (x_1/x_2, y_1/y_2)$, then $h(P) = \lim_{n\to\infty} h_0(nP)/n^2$.

Example. The simplest example $E : y^2 = 4x^3 - 4x + 1$ of conductor 37. $E(\mathbb{Q}) = \mathbb{Z}P$, $P = (0,1)$, and

n	nP
2	$(1,1)$
3	$(-1,-1)$
4	$(2,-5)$
5	$(1/4, -3/4)$
6	$(6,29)$

Then $\Omega = 5.98691729\ldots$, $R = h(P) = 0.0511114082\ldots$, and $L'(E,1) = \Omega R = 0.305999773\ldots$.

Theorem. *The quantity ΩR appearing in the BSD conjecture is always a period, more specifically, it is the determinant of an $(r+1)\times(r+1)$ matrix whose entries are $\mathbb{Q}$-linear combinations of integrals $\int_a^b \omega$, $a, b \in E(\overline{\mathbb{Q}})$, ω an algebraic 1-form.*

Example. E, P as above $y = \sqrt{4x^3 - 4x + 1}$ implies

$$\Omega R = \begin{vmatrix} \int_{-1}^{0} \frac{dx}{y} & \int_{-1}^{0} \left(1 - \frac{1}{y}\right) \frac{dx}{2x} \\ \int_{1}^{2} \frac{dx}{y} & \int_{-1}^{0} \left(1 - \frac{1}{y}\right) \frac{dx}{2x} \end{vmatrix}$$

Question. Show that f a modular form of even weight k, $r = \operatorname{ord}_{s=k/2} L(f, s)$, implies $L^{(r)}(f, k/2) \in \widehat{\mathscr{P}}$.

This is a previously stated theorem if $r = 0$, $r = 1$. There are not even examples known for elliptic curves of higher rank.

Sketch of proof. For $\langle P, Q \rangle = \sum_v \langle P, Q \rangle_v$, a sum over the places v of $\mathbb{Q}$ of local heights. Then

$$\langle P, Q \rangle = \sum_p (P \cdot Q) \log p + G(P, Q)$$

where the finite primes runs over only finitely many primes, and G is a Green's function. $G(P, z)$ is harmonic in z except for logarithmic singularity at P, namely $G(P, z) = \operatorname{Re} \int_{z_0}^{z} \omega_P$ where ω_P is a 1-form over $\mathbb{R}$ with a simple pole at P with residue 1 and $\operatorname{Re}\left(\int_{E(\mathbb{R})} \omega_P\right) = 0$.

Choose ω_P^* a 1-form defined over $\mathbb{Q}$, with a pole at P, so that $\omega_P^* = \omega_P + \lambda\omega_0$, $\omega_0 = dx/y$ the holomorphic 1-form. Then

$$0 = \operatorname{Re}\left(\int_{E(\mathbb{R})} \omega_P\right) = \operatorname{Re}\left(\int_{E(\mathbb{R})} \omega_P^*\right) - \lambda\Omega$$

so $\lambda = (1/\Omega) \operatorname{Re}\left(\int_{E(\mathbb{R})} \omega_P^*\right)$. Thus

$$G(P, Q) = \operatorname{Re}\left(\int_{z_0}^{Q} \omega_P\right) = \operatorname{Re}\left(\int_{z_0}^{Q} (\omega_P^* - \lambda\omega_0)\right) = \frac{1}{\Omega} \begin{vmatrix} \operatorname{Re}(\int_{E(\mathbb{R})} \omega_0) & \operatorname{Re}(\int_{z_0}^{Q} \omega_0) \\ \operatorname{Re}(\int_{E(\mathbb{R})} \omega_P^*) & \operatorname{Re}(\int_{z_0}^{Q} \omega_P^*) \end{vmatrix}$$

and is therefore a matrix of periods. □

References

[1] Emil Artin and John Tate, *Class field theory*, W.A. Benjamin, Inc.: New York-Amsterdam, 1968.

[2] A. Borel, *Class invariants I–II*, Seminar on complex multiplication, Lecture notes in mathematics, no. 21, Springer-Verlag: Berlin-New York, 1966, III-1–IV-10.

[3] Ph. Cassou-Noguès and M.J. Taylor, *Elliptic functions and rings of integers*, Progress in mathematics, vol. 66, Birkhäuser: Boston, 1987.

[4] Henri Cohen, *Elliptic curves*, From number theory to physics (Les Houches, 1989), Springer: Berlin, 1992, 212–237.

[5] A. Fröhlich and M.J. Taylor, *Algebraic number theory*, Cambridge University Press: Cambridge, 1991.

[6] A.B. Goncharov and A.M. Levin, *Zagier's conjecture on $L(E, 2)$*, Invent. Math. 132 (1998), no. 2, 393–432.

[7] Dale Husemöller, *Elliptic curves*, Graduate texts in mathematics, vol. 111, Springer-Verlag: New York-Berlin, 1987.

[8] K. Iwasawa, *Class fields*, Seminar on complex multiplication, Lecture notes in mathematics, no. 21, Springer-Verlag: Berlin-New York, 1966, V-1–V-13.

[9] Anthony W. Knapp, *Elliptic curves*, Mathematical notes, vol. 40, Princeton University Press: Princeton, 1992.

[10] Marvin I. Knopp, *Modular functions in analytic number theory*, Markham: Chicago, 1970.

[11] Serge Lang, *Elliptic functions*, 2nd ed., Graduate texts in mathematics, vol. 112, Springer-Verlag: New York-Berlin, 1987.
[12] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate texts in mathematics, vol. 110, Springer-Verlag: New York, 1994.
[13] Serge Lang, *Introduction to modular forms*, corrected ed., Grundlehren der Mathematischen Wissenschaften, vol. 222, Springer-Verlag: Berlin, 1995.
[14] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag: Berlin, 1999.
[15] Andrew Ogg, *Modular forms and Dirichlet series*, W.A. Benjamin: New York, 1969.
[16] Jean-Pierre Serre, *A course in arithmetic*, Graduate texts in mathematics, vol. 7, Springer-Verlag: New York, 1973.
[17] J.-P. Serre, *Modular forms*, Seminar on complex multiplication, Lecture notes in mathematics, no. 21, Springer-Verlag: Berlin-New York, 1966, II-1–II-16.
[18] J.H. Silverman, *The arithmetic of elliptic curves*, Berlin: Springer, 1994.
[19] Fernando Rodriguez Villegas and Don Zagier, *Square roots of central values of Hecke L-series*, Advances in number theory (Kingston, ON, 1991), Oxford Univ. Press: New York, 1993, 81–99.
[20] André Weil, *Elliptic functions according to Eisenstein and Kronecker*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 88, Springer-Verlag: Berlin-New York, 1976.
[21] Don Zagier, *Introduction to modular forms*, From number theory to physics (Les Houches, 1989), Springer: Berlin, 1992, 238–291.
[22] Don Zagier, *Traces of singular moduli*, Preprint of the Max Planck Institut für Mathematik, 2000, available at `http://www.mpim-bonn.mpg.de/cgi-bin/preprint/preprint_search.pl`.