Hellegouarch 5.8-6.1 Notes

We first finish up with chapter five, defining L-functions of modular forms and discover that we can associate elliptic curves to a corresponding modular form with the same L-function

Definition Let $f(\tau) = \sum_{m=0}^{\infty} a(m)\, q^m \in M_k$ be a modular form for $SL_2(\mathbb{Z})$. The L-function of f is:

$$L(f,s) = \sum_{m=1}^{\infty} \frac{a(m)}{m^s}$$

The numerator $a(m)$ is limited by the limiting function $O(m^{k-1})$, so $L(f,s)$ converges in the right half plane $Re(s) > k$

From a previous lecture, we proved that if f is a Hecke form, $a(n)$ will be multiplicative. (Recall that a Hecke form is an eigenfunction of the Hecke operators)
In particular, $a(mn) = a(m)a(n)$ when n,m are coprime.

In this case, we can construct $L(f,s)$ by the Euler product:

$$L(f,s) = \prod_p \left(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots\right)$$

Using the relation $a(p^{r+1}) = a(p)a(p^r) - p^{k-1}a(p^{r-1})$, we can simplify the sum in each factor of this product and find that (through some algebraic manipulation)

Thm

$$L(f,s) = \prod_p \frac{1}{1 - a(p)p^{-s} + p^{k-1-2s}}$$

In order to eliminate the infinite sum in each factor.

As a sidenote, if f is modular only for $\Gamma_0(N)$, (i.e. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $c \equiv 0 \bmod N$), we must define our L-functions differently, as:

$$L(f,s) = \prod_{p \mid N} \frac{1}{1-a(p)p^{-s}} \prod_{p \nmid N} \frac{1}{1-a(p)p^{-s}+p^{k-1-2s}}$$

Functional Equation for $L(f,s)$

If we want to continued $L(f,s)$ to the entire complex plane, it is necessary to define the Mellin transform and use a related theorem

Let $\varphi : \mathbb{R}_+^* \to \mathbb{C}$ s.t. $\varphi(t) = O(t^{-A})$ as $t \to \infty$ $\forall A \in \mathbb{R}$, and $\varphi(t) = O(t^{-C})$ when $t \to 0$ for a constant C.
Then $M_\varphi(s) = \int_0^\infty \varphi(t) t^{s-1} dt$ converges abs. and uniformly in $\mathrm{Re}(s) \geq c + \varepsilon$ $\forall \varepsilon > 0$.
Call this integral the Mellin transform of φ

$$\left[\begin{array}{l} \Gamma(s) = M_{\varphi(s)} \\ \varphi(t) = e^{-t} \end{array}\right]$$

Thm

Using the Mellin transform, we introduce this theorem (which we won't prove)

If φ satisfies $\varphi\left(\frac{1}{t}\right) = \sum_{j=1}^{\ell} A_j t^{\lambda_j} + \varepsilon t^h \varphi(t)$ for $t > 0$,

where, $h, A_j, \lambda_j \in \mathbb{C}$, $\varepsilon \in \{-1, 1\}$, then M_φ can be meromorphically continued to all of $\mathbb{C}$, holomorphic everywhere but at $s = \lambda_j$, where it has simple pole residue A_j.

Moreover, we have functional equation:

$$M_\varphi(h-s) = \varepsilon M_\varphi(s)$$

Relating this to the L-function, we can deduce a functional equation for $L(f,s)$:

$$(2\pi)^{-s}\Gamma(s)L(f,s) = (-1)^{k/2}(2\pi)^{s-k}\Gamma(k-s)L(f,k-s)$$

With this continuation holomorphic if f vanishes at the cusps (Zach's talk).
(pf taking $\varphi(t) = F(it) - a(0)$, and applying its Mellin transform)

Wiles Thm

Again, we want to associate modular forms to elliptic curves through their L-functions, so we need to find an elliptic curve which has the same L-function as a modular form.

Weil Curves

Let E be an elliptic curve defined over $\mathbb{Q}$, and

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be a minimal Weierstrass model for E over $\mathbb{Z}$.
If E has a good reduction at p, set

$$a_p = p + 1 - N_p$$

(N_p denotes # of points of the curve reduced mod p in the projective plane of the Galois field of order p)

If E has a bad reduction, set

$$a_p = \begin{cases} 1 & \text{if } E \text{ admits 2 tangents at double rational point on } \mathbb{F}_p \\ -1 & \text{if } E \text{ admits an isolated double point} \\ 0 & \text{if } E \text{ has an additive reduction} \end{cases}$$

If E is semistable, Π bad primes $= N_E$, conductor of E.
Recall in ch 4 we defined L-function of E as

$$L_E(s) = \prod_{\text{bad } p} \frac{1}{1 - a(p)p^{-s}} \prod_{\text{good } p} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

Hasse's conjecture states that the L-function of E can be continued to all of $\mathbb{C}$ and that if we set

$$\Lambda_E(s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s)$$

we have the functional equation

$$\Lambda_E(2-s) = \pm\Lambda_E(s)$$

Theory by Eichler-Shimura allows us to associate elliptic curves to Hecke forms

Thm

Let $N \in \mathbb{Z}, N \geq 1$ $f \in S_2(\Gamma_0(N))$ be a Hecke form. Then $\exists$ elliptic curve E s.t. Mellin transform of f is

$$(2\pi)^{-s}\Gamma(s)L_E(s) = N^{-s/2}\Lambda_E(s)$$

Call this curve a Weil curve (or modular curve)

Finally, the Shimura-Taniyama-Weil conjecture asked if:

E an elliptic curve over $\mathbb{Q}$ with L-series $\sum_{n=1}^{\infty} a(n)n^{-s}$ $f_E(\tau) = \sum_{n=1}^{\infty} a(n)q^n$ the inverse Mellin transform of:

$$(2\pi)^{-s}\Gamma(s)L_E(s)$$

Then F is in $S_2(\Gamma_0(N))$, f in Hecke Form (N conductor of E)

This, if proven, this conjecture would allow us to produce an elliptic curve with the same L-function as a given cusp form of weight 2.

(i.e. every rational elliptic curve is modular)

Wiles proved this for semi-stable elliptic curves.

Thm

For E defined as above, with $a(p)$ given by

$$\begin{cases} 1+a(p) = \#\{\text{solutions of } x^2+a_1x-a_2 \equiv 0 \bmod p\} & \text{if } p \mid N \\ p+1-a(p) = \#E(\mathbb{F}_p) & \text{otherwise} \end{cases}$$

Then if $f(\tau) = \sum a(n) e^{2\pi i n \tau}$ for $\operatorname{Im}(\tau) > 0$, we have

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 f(\tau)$$

for each $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$

and for each $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$,

$$\tau \mapsto (c\tau+d)^{-2} f\left(\frac{a\tau+b}{c\tau+d}\right)$$

admits an expansion as an integral series in the powers of $q^{1/N} = e^{2\pi i \tau/N}$

Thus we can find a common L-function for elliptic curves and modular forms of weight 2.

Example

$y^2 - y = x^3 - x^2$ has conductor $N_E = 11$

If we consider $f = q\prod_{n=1}(1-q^n)(1-q^{11n})^2$

$$= q - 2q^2 - 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + \cdots$$

$$= \sum a(n) q^n$$

with the series a_q satisfying above relations when p is prime.

Additionally, recall dimension of $S_2(\Gamma_0(N))$ is given by

$$g = 1 + \frac{N}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

where these terms were defined in 5.4 (Zach L's lecture)

We generate the table

Conductor N	1	2	...	10
Dim g	0	0		0

Which indicates that there are no cusp forms of weight 2 and level $N<11$.

Chapter 6

We have previously considered reduction of elliptic curves mod p. It is necessary sometimes however to work mod a higher power of p, and indeed eventually "mod p^∞".
To understand what this means, we need a new conception of the p-adics, we give a new construction of $\mathbb{Z}_p$ for fixed p-prime.

For $n \geq 1$ integer, let A_n denote the ring $\mathbb{Z}/p^n\mathbb{Z}$

Since congruence mod p^n implies congruence mod p^{n-1}, we have homomorphisms φ_n

$$\cdots \to A_n \xrightarrow{\varphi_n} A_{n-1} \cdots \xrightarrow{\varphi_1} A_1 = \mathbb{Z}/p\mathbb{Z}$$

The object we are constructing is at infinity on the left, so a ring equipped with homomorphisms

$$\cdots \circ \varphi_{n+2} \circ \varphi_{n+1} = \pi_n : X \to A_n$$

We define

$$X = \left\{ x \in \prod_{n \geq 1} A_n : \forall n \geq 1, \varphi_n \circ \varepsilon_n(x) = \varepsilon_{n-1}(x) \right\}$$

Where ε_n denotes the projection of $\prod A_n$ onto the nth-coordinates.

X is a subring of $\prod A_n$, and compact, and $\varepsilon_1(X) = \mathbb{Z}/p\mathbb{Z}$ is a field, so $\ker(\varepsilon_1) = pX$ is a maximal ideal (for X).

If $\exists$ greatest integer $n \geq 1$ s.t. $\varepsilon_n(x) = 0$, let p-adic valuation of x be

$$v_p(x) = n$$

$v = \qquad \neq$ and $v = +\infty$ when all $x =$

& we have:

Thm

(1) X is a ring

(2) $x \in X$ is invertible iff it is not divisible by p

(3) $x \in X$, $x \neq 0$ can be written in a unique way in form $p^n u$, with $n \in \mathbb{N}$ and u invertible. $v_p(x) = n$

(4) p-adic v_p has

$$v_p(xy) = v_p(x) + v_p(y)$$
$$v_p(x+y) \geq v_p(x) + v_p(y)$$

We can also have a notion of p-adic distance

$$d_p(x,y) = p^{-v_p(x-y)}$$

We consider the fraction field K of X,*
where every non-zero $x \in K$ is uniquely written:

$$x = p^n u \quad n \in \mathbb{Z},\ u \in X \text{ invertible.}$$

We are able to define p-adic absolute value on K.

$$v_p(x) := n, \quad v_p(0) = +\infty$$
$$|x|_p = p^{-v_p(x)}$$
$$d_p(x,y) = |x-y|_p$$

* Smallest field containing the integral domain X

So we have defined a field K, with a p-adic distance
Leo will continue with work on this field.

QED