Modular curves, forms, elliptic curves, and symbols

Lectured by John Cremona
Notes by Martin Dickson

Abstract. Lecture notes from the LMS-CMI Research School "Building Bridges" held at the University of Bristol in June/July 2014. Please email any comments or corrections to martin.dickson@bristol.ac.uk.

1 Outline

There are two different relationships between modular curves (e.g. $X_0(N)$) and elliptic curves. In the first lecture, we discuss how modular curves parameterise elliptic curves with level structure (over any field). In lecture 2, we discuss how modular curves are themselves a source of elliptic curves (over $\mathbb{Q}$).

References for lecture 1.

- Diamond–Shurman GTM 228, "A first course in modular forms" for background on modular curves and modular forms
- Shimura, "Introduction to the arithmetic theory of automorphic functions" (a classic, again for the background)
- Elkies, "Elliptic and modular curves over finite fields" in "Computational perspectives in number thery" 1995 Atkin conference, AMS (for the $X_0(11)$ example) .

References for lecture 2.

- Stein, "Modular forms: A computational approach"
- Cremona, "Algorithms for modular elliptic curves"

2 Lecture 1

Modular curves. The upper half plane $\mathfrak{H} = \{z = x + iy;\ y > 0\}$ comes with an action of $\mathrm{GL}_2^+(\mathbf{R})$ (the matrices in $\mathrm{GL}_2(\mathbf{R})$ with positive determinant); and hence also an action of the subgroups

$$\mathrm{GL}_2^+(\mathbf{R}) \supset \mathrm{SL}_2(\mathbf{R}) \supset \mathrm{SL}_2(\mathbf{Z}) \supset \Gamma,$$

where Γ denotes a subgroup of finite index in $\mathrm{SL}_2(\mathbf{Z})$. We are particularly interested in

$$\begin{aligned}
\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z});\ N \mid c \right\} \\
\Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N);\ d \equiv 1 \bmod N \right\} \\
&= \ker \left(\begin{array}{ll} \Gamma_0(N) & \to (\mathbf{Z}/N\mathbf{Z})^* \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto d \end{array} \right) \\
\Gamma(N) &= \ker(\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) \\
&= \ker \left(\begin{array}{ll} \Gamma_1(N) & \to (\mathbf{Z}/N\mathbf{Z}) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto b \end{array} \right)
\end{aligned}$$

Note that

$$\begin{aligned}
[\Gamma_0(N) : \Gamma_1(N)] &= \varphi(N) \\
[\Gamma_1(N) : \Gamma(N)] &= N
\end{aligned}$$

In the exercises we show that

$$[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(N)] = N \prod_{p \mid N} \left(1 + \frac{1}{p} \right).$$

Now let $\Gamma \leq \mathrm{SL}_2(\mathbf{Z})$ be a subgroup of index d; then

$$Y_\Gamma := \Gamma \backslash \mathfrak{H}$$

is a topological space, a real 2-manifold, and a Riemann surface of genus $g(\Gamma) := g(Y_\Gamma)$. This can be compactified by adding a finite number of cusps $\Gamma \backslash \mathbb{P}^1(\mathbf{Q})$ to get

$$X_\Gamma = Y_\Gamma \cup \{\text{cusps}\}.$$

We refer to such X_Γ as *modular curves*. We use the following notation:

Γ	X_Γ
$\Gamma_0(N)$	$X_0(N)$
$\Gamma_1(N)$	$X_1(N)$
$\Gamma(N)$	$X(N)$

The modular curve $X(1)$ is sometimes referred to as "the j-line". Points on the non-cuspidal part $Y(1)$ parameterise elliptic curves over $\mathbf{C}$ up to isomorphism. Indeed, any complex elliptic curve $E/\mathbf{C}$ tales the form $\mathbf{C}/\Lambda$ where Λ is a rank two $\mathbf{Z}$-lattice in $\mathbf{C}$. Two complex elliptic curves E_1 and E_2 are isomorphic if and only if the corresponding lattice Λ_1 and Λ_2 are *homothetic*, i.e. $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbf{C}^*$. In particular any complex elliptic curve $E/\mathbf{C}$ is isomorphic to some $\mathbf{C}/\Lambda_\tau$, where $\Lambda_\tau = \mathbf{Z} + \mathbf{Z}\tau$ with $\tau \in \mathfrak{H}$. Moreover, given $\tau_1, \tau_2 \in \mathfrak{H}$, the lattice Λ_{τ_1} and Λ_{τ_2} are homothetic if and only if τ_1 and τ_2 are in the same $\mathrm{SL}_2(\mathbf{Z})$-orbit.

The modular curve $X(1)$ has genus 0, so $X(1)_{\mathbf{C}} \simeq \mathbf{P}^1(\mathbf{C})$. But $X(1)$ has the additional structure of an algebraic curve over $\mathbf{Q}$. The function field of $X(1)_{\mathbf{C}}$ is $\mathbf{C}(j)$; to get a $\mathbf{Q}$-structure we fix the subfield $\mathbf{Q}(j)$, which is the function field of $\mathbf{P}^1_{\mathbf{Q}}$. Thus a point on $X(1)$ is defined over $\mathbf{Q}$ if and only if the value of j at that point is in $\mathbf{Q} \cup \{\infty\}$.

We have many choices for a generator j for $\mathbf{C}(j)$, but we can fix one by specifying its value at three points. We take

$$\begin{aligned} j(\infty) &= \infty \\ j(i) &= 1728 \\ j(\rho) &= 0 \end{aligned}$$

where $\rho = (1+\sqrt{-3})/2$. Writing $q = e^{2\pi i \tau}$, it can be shown that the resulting j is given by

$$j = \frac{1}{q} + 744 + 196884q + ... \in \mathbf{Z}((q)).$$

So an isomorphism class of elliptic curves E over $\mathbf{C}$ is defined over $\mathbf{Q}$ if and only if $j(E) \in \mathbf{Q}$; i.e. E has a Weierstrass equation with coefficients in $\mathbf{Q}$.

Now let $\Gamma \leq \mathrm{SL}_2(\mathbf{Z})$ be an index d subgroup. We have a map $X_\Gamma \to X(1)$ (induced by the identity on $\mathfrak{H}$). This is a covering map of Riemann surfaces of degree d. It is unramified, except possibly above $j = \infty, 0, 1728$. Above $j = \infty$, the ramification degree is just the width of that cusp. Above $j = 0$, the ramification degree can be 1 or 3; above $j = 1728$ it can be 1 or 2. The Riemann–Hurwitz formula states

$$2g(\Gamma) - 2 = d(2 \times 0 - 1) + \sum_{P \in X_\Gamma} (e_P - 1)$$

(recall $X(1)$ has genus 0). Thus

$$g(\Gamma) = 1 - d + \frac{1}{2}\sum_P (e_P - 1).$$

For example, take $\Gamma = \Gamma_0(2)$. Then $d = 3$. Above ∞ we have two points: 0 with multiplicity 2, and ∞ with multiplicity 1. Above i we have two points: again one has multiplicity 2, and the other has multiplicity 1. Above ρ we have a single point with multiplicity 3. (These numbers can be verified by drawing the fundamental domain.) It follows that

$$\sum_P (e_P - 1) = 1 + 1 + 2 = 4,$$

and hence that $g(\Gamma_0(2)) = 0$.

For all $N \geq 1$, $X_0(N)$ and $X_1(N)$ have models over $\mathbf{Q}$, while $X(N)$ is only defined over $\mathbf{Q}(\zeta_N)$. $X_0(2)$ has function field $\mathbf{Q}(t)$. In particular, the covering $X_0(2) \to X(1)$ expresses $\mathbf{Q}(t)$ as an extension of $\mathbf{Q}(j)$. Thus $j = F(t)$, where F is a rational function of degree 3. We choose t so that above $j = \infty$ we have $t = 0, \infty, \infty$. This means that

$$F(t) = \frac{\text{cubic in } t}{t}.$$

Above $j = 0$, $e = 3$, so we know that

$$F(t) = \frac{(t+a)^3}{t}.$$

Above $j = 1728$ we see

$$F(t) - 1728 = \frac{(t+b)^2(t+c)}{t}$$

where $a, b, c, 0, \infty$ are distinct. Thus

$$(t+a)^3 = 1728t + (t+b)^2(t+c).$$

This implies that $(a, b, c) = \pm(16, -8, 64)$. Thus

$$j = \frac{(t+16)^3}{t}$$

and

$$j - 1728 = \frac{(t-8)^2(t+64)}{t}.$$

For $\ell \geq 5$ prime,

$$g(X_0(\ell)) = \begin{cases} \frac{\ell-3}{12} & \ell \equiv 1 \bmod 12, \\ \frac{\ell-5}{12} & \ell \equiv 5 \bmod 12, \\ \frac{\ell-7}{12} & \ell \equiv 7 \bmod 12, \\ \frac{\ell+1}{12} & \ell \equiv 11 \bmod 12. \end{cases}$$

In particular, $g(X_0(\ell)) = 0$ if and only if $\ell = 2, 3, 5, 7, 13$. The parameters $t = t_\ell$ can be chosen to satisfy

$$\begin{aligned} j &= \frac{(t+27)(t+3)^2}{t} \text{ for } \ell = 3, \\ j &= \frac{(t^2+10t+5)^3}{t} \text{ for } \ell = 5, \\ j &= \frac{(t^2+13t+49)(t^2+5t+1)^3}{t} \text{ for } \ell = 7, \\ j &= \frac{(t^2+5t+13)(t^4+\dots)^3}{t} \text{ for } \ell = 13. \end{aligned}$$

The modular curve $X(N)$ has genus 0 for $N = 1, 2, 3, 4, 5$. Also, $g(X(6)) = 1$, and $g(X(7)) = 3$.

Level structure. For $X_0(N)$, the additional structure on the isomorphism classes of elliptic curves is a cyclic subgroup of order N. Thus we consider pairs (E, C) where E is an elliptic curve and C is a cyclic subgroup of E of order N. We say $(E_1, C_1) \sim (E_2, C_2)$ if and only if there is an isomorhism $\alpha : E_1 \to E_2$ such that $\alpha(C_1) = C_2$. One can easily show that, at least as sets, $Y_0(N) = \{(E, C) \text{ as above }\}/\sim$.

Indeed, take $E_i = \mathbf{C}/\Lambda_{\tau_i}$ with cyclic subgroup $C_i = \langle \frac{1}{N}\mathbf{Z} + \tau_i\mathbf{Z}\rangle$ for $i = 1, 2$. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ be such that

$$\tau_2 = \frac{a\tau_1 + b}{c\tau_1 + d}.$$

Then g maps C_1 to C_2 if and only if $g \in \Gamma_0(N)$.

One can also regard $Y_0(N)$ as parameterising isomorphism classes of pairs (E, E') with a cyclic isogeny $E \to E'$. Thus a rational point on $Y_0(N)$ gives an elliptic curve $E/\mathbf{Q}$ together with an N-isogeny defined over $\mathbf{Q}$.

For example, consider $X_0(2)$, so $j = (t+16)^3/t$. For fixed j, the three values of t correspond to the three possible 2-isogenies from E (with $j(E) = j$, $j \neq 0, 1728$). For example, consider the elliptic curves

$$y^2 = x(x-1)(x+2).$$

Then $j(E) = 2^6 7^3/3^2$. We get $t = 64/3, 8/3, -72$.

The Fricke involution and dual isogenies. Let $\varphi : E \to E'$ be a cyclic isogeny of degree N, and set $C = \ker(\varphi)$. The dual isogeny $\widehat{\varphi} : E' \to E$ is characterised by the condition $\widehat{\varphi} \circ \varphi = [N]_E$. The map

$$w_N : (E, C) \mapsto (E', \varphi(E[N])),$$

or equivalently

$$w_N : (E, E') \mapsto (E', E),$$

is called the *Fricke involution* on $X_0(N)$. For example, on $X_0(2)$ the Fricke involution is the map $t \mapsto 4096/t$. This fixes ± 64, which corresponds to $j = 8000$ and $j = 1728$. The former of these gives an isomorphism class of elliptic curves E which have complex multipliction by $\sqrt{-2}$; the latter gives an isomorphism class with complex multiplication by $\sqrt{-1}$.

The modular curve $X_0(11)$. Note that $g(X_0(11)) = 1$. We would like (1) an equation for $X_0(11)$, (2) a formula for the map $X_0(11) \to X(1)$. Now the curve

$$X_0^+(11) = X_0(11)/\langle w_{11} \rangle$$

has genus 0, so we have a factorisation

$$X_0(11) \to X_0^+(11) \xrightarrow{\sim} \mathbb{P}^1.$$

(This also holds for 9 other prime values of N in place of 11.) Thus $X_0(11)$ is hyperelliptic, and the hyperelliptic involution is given by the Fricke involution.

We choose a modular function u with $u(\infty) = \infty$ which generates $\mathbf{Q}(X_0^+(11))$. Specifically

$$u = q^{-1} + 5 + 17q + 46q^2 + \dots$$

which is the quotient $u = \varepsilon/\omega$ of the weight 2 level 11 Eisenstein series

$$\varepsilon = 1 + 3q + 6q^2 + \dots$$

by the weight 2 level 11 normalised cusp form

$$\omega = q - 2q^2 - q^3 + \dots,$$

both of which are anti-invariant under w_{11}, so u is invariant. Take

$$v = \frac{1}{\omega}\frac{du}{q} = -q^{-2} - 2q^{-1} + 12 + 116q + \dots,$$

which is anti-invariant under w_{11}. Then comparing q-expansions gives

$$X_0(11) : v^2 = u^4 - 16u^3 + 2u^2 + 12u - 7.$$

(See the Sage worksheet for details.) Making the change of variables

$$u = \frac{6+x}{5-x}, \;\; v = \frac{-11(2y+1)}{(x-5)^2}$$

we get the expected Weierstrass equation

$$E : y^2 + y = x^3 - x^2 - 10x - 20.$$

We can compute the rational points

$$E(\mathbf{Q}) = \{\infty, (5,5), (5,-6), (16,6), (16,-61)\}.$$

Write $j = a(u) + vb(u)$ (map from the (u,v)-curve to the j-line). Then a and b are polynomials with $\deg(a) = 11$, $\deg(b) = 9$. Tabulating the j-invariants,

(x,y)	(u,v)	j
∞	$(-1,0)$	-2^{15}
$(5,5)$	∞^+	∞
$(5,-6)$	∞^-	∞
$(16,60)$	$(-2,-11)$	-11^2
$(16,-61)$	$(-2,11)$	-11×131^3

$j = -2^{15}$ is the j-invariant of an elliptic curve with complex multiplciation by $(1+\sqrt{-11})/2$. The j-invariants -11^2 and -11×131^3 come from the elliptic curves $121a1$ and $121a2$, and there is indeed a rational 11-isogeny between these non-isomorphic curves.

3 Lecture 2

Modular symbols provide a method to compute $\mathcal{S}_k(N)$, the space of cusp forms of weight k for $\Gamma_0(N)$. One is interested in knowing

- dimensions (there are formulas for this)
- explicit bases, in terms of q-expansions,
- the action of the Hecke algebra $\mathbb{T}$.

These are used in Sage. For example, at a Sage prompt, one can type `CuspForm(group=Gamma0(11), weight=2).basis()`, and Sage will return the basis

$$q - 2q^2 - q^3 + q^4 + q^5 + O(q^6)$$

or `CuspForms(group=Gamma0(11), weight=10, prec=10).basis()` and Sage will return the basis

$$\begin{aligned}
&[q - 9q^9 + O(q^{10}),\\
&\ q^2 - 8q^9 + O(q^{10}),\\
&\ q^3 + 10q^9 + O(q^{10}),\\
&\ ...,\\
&\ q^8 + 4q^9 + O(q^{10})]
\end{aligned}$$

In this lecture we will restrict to $\mathcal{S}_2(N)$.

Cusp forms and homology. Given $f \in \mathcal{S}_k(N)$, we can form the holomorphic differential $\omega_f = 2\pi i f(z)dz$ on $X_0(N)$. (To be precise this is actually the pullback of such a differential to the upper half plane $\mathfrak{H}$). It follows that

$$\dim \mathcal{S}_2(N) = g(X_0(N)).$$

We use duality to switch from these cohomological objects to homology

$$H(N) := H_1(X_0(N), \mathbf{Z}) \simeq \mathbf{Z}^{2g}.$$

One can think of $H(N)$ as being the free abelian group on closed paths on $X_0(N)$, modulo homotopy. We also work with

$$H(N)^* := H_1(X_0(N), \mathbf{Z}; \text{cusps}),$$

the homology relative to the cusps. One can think of $H(N)^*$ as being generated by paths which start and end at cusps (but are not necessarily closed in $X_0(N)$).

If $\gamma \in H(N)$ then γ defines a $\mathbf{C}$-linear map

$$\mathcal{S}_2(N) \to \mathbf{C}$$

by the rule

$$f \mapsto \int_\gamma \omega_f =: \langle \gamma, f \rangle.$$

We can therefore identify $H(N)$ with a lattice of rank $2g$ in the dual space of $\mathcal{S}_2(N)$, which has complex dimension g and real dimension $2g$.

The Hecke alegbra acts on $H(N)$ and $\mathcal{S}_2(N)$ in a compatible way:

$$\langle \gamma | T, f \rangle = \langle \gamma, f | T \rangle$$

for all $T \in \mathbb{T}$. Our strategy is to compute $H(N)$ explicitly, and to compute the action of each $T \in \mathbb{T}$ on $H(N)$ as a $2g \times 2g$ integer matrix. This will give us the structure of $\mathcal{S}_2(N)$ as a Hecke module, from which (by linear algebra) we can find out what we want, for example eigenforms.

Modular symbols. Let $\alpha, \beta \in \mathbb{P}^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$. We write $\{\alpha, \beta\}$ for the geodesic path in $\mathfrak{H}^*$ from α to β. We use the same symbol to denote its image in $X_0(N)$, and the same symbol again to denote the image of that in $H(N)^*$. As a path on the upper half plane, $\{\alpha, \beta\}$ is either a vertical line or a semicircle in $\mathfrak{H}$ meeting the real axis at rational points. We have the relations

$$\begin{aligned} \{\alpha, \alpha\} &= 0, \\ \{\alpha, \beta\} + \{\beta, \alpha\} &= 0, \\ \{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} &= 0. \end{aligned}$$

Also, for $g \in \Gamma_0(N)$, we have

$$\{g(\alpha), g(\beta)\} = \{\alpha, \beta\},$$

and one can use these to show that the class

$$\{\alpha, g(\alpha)\} \in H(N)$$

is independent of the choice of α. Furthermore, the map

$$g \mapsto \{\alpha, g(\alpha)\}$$

defines a group homomorphism

$$\Gamma_0(N) \to H(N)$$

(for any choice of α).

Let $\alpha = b/d$, $\beta = a/c$ be points of $\mathbb{P}^1(\mathbf{Q})$. Define the matrix $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbf{Z})$. Then

$$\{\alpha, \beta\} = \{g(0), g(\infty)\} = g\{0, \infty\}.$$

Using continued fractions, one can show that every $\{\alpha, \beta\}$ is a finite sum of paths of the form $g\{0, \infty\}$ where $g \in \mathrm{SL}_2(\mathbf{Z})$. We write

$$(g) = \{g(0), g(\infty)\}$$

for such paths, where $g \in \mathrm{SL}_2(\mathbf{Z})$.

Manin showed that these (g) generate $H(N)^*$, subject to the relations

$$\begin{aligned} (g_0 g) &= (g) \text{ for } g \in \mathrm{SL}_2(\mathbf{Z}), g_0 \in \Gamma_0(N), \\ (g) + (gS) &= 0, \\ (g) + (gTS) + (g(TS)^2) &= 0. \end{aligned}$$

In the second and third relations,

$$\begin{aligned} S &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ T &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \\ TS &= \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}. \end{aligned}$$

To explain the second and third relations, one can check that S interchanges 0 and ∞, whereas TS cycles the three points $0, \infty, 1$.

To recover $H(N)$ from $H(N)^*$, we take the kernel of the boundary map

$$\delta : H(N)^* \to \bigoplus_{[\alpha] \in \Gamma_0(N) \backslash \mathbb{P}^1(\mathbf{Q})} \mathbf{Z}[\alpha]$$

given by

$$\delta(\{\alpha, \beta\}) = [\beta] - [\alpha],$$

where $[\alpha]$ denotes the equivalance class of α in $\Gamma_0(N) \backslash \mathbb{P}^1(\mathbf{Q})$.

Now the cosets of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbf{Z})$ are in bijection with elements of $\mathbb{P}^1(\mathbf{Z}/N\mathbf{Z})$, via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (c : d).$$

Indeed, note that

$$\Gamma_0(N) \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \Gamma_0(N) \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

if and only if

$$c_1 d_2 \equiv c_2 d_1 \bmod N,$$

if and only if

$$(c_1 : d_1) = (c_2 : d_2).$$

We will think of the symbols $(c : d)$ as representing an element of $H(N)^*$, via

$$(c : d) \leftrightarrow g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftrightarrow \{g(0), g(\infty)\} = \left\{ \frac{b}{d}, \frac{a}{c} \right\}.$$

Here a, b are any integers such that $ad-bc=1$ (we can choose such integers as $\gcd(c,d)=1$, and a different choices of a, b leads to a matrix in the same $\Gamma_0(N)$-coset). We refer to the symbols $(c:d)$ viewed as elements of $H(N)^*$ as *M-symbols* (after Manin).

Thus $H(N)^*$ is generated by M-symbols $(c:d)$ subject to the relations

$$\begin{aligned}(c:d)+(d:-c)&=0\\(c:d)+(c+d:-c)+(-d:c+d)&=0\end{aligned}$$

The map δ is given in terms of M-symbols by

$$\delta((c:d))=\left[\frac{a}{c}\right]-\left[\frac{b}{d}\right],$$

and as above $\ker\delta=H(N)$.

Now complex conjugation acts on $H(N)^*$ by

$$(c:d)\mapsto(-c:d),$$

and we can factor out by this relation to form

$$H^+(N)=H(N)/\langle(c:d)=(-c:d)\rangle.$$

Then $\dim H^+(N)=g$ (wheras $\dim H(N)=2g$). This is useful for speeding up implementations.

Example: $N=2$**.** We have

$$\mathbb{P}^1(\mathbf{Z}/2\mathbf{Z})=\{(1:0),(0:1),(1:1)\}.$$

These satisfy the relations

$$\begin{aligned}(0:1)+(1:0)&=0,\\(1:1)+(1:1)&=0,\\(1:0)+(0:1)+(1:1)&=0.\end{aligned}$$

Thus

$$H(2)^*=\langle(0:1)\rangle.$$

But $(0:1)$ represents the path $\{0,\infty\}$. Since $[\infty]\neq[0]$, this is not in $\ker\delta$, so we deduce that

$$H(2)=0.$$

Example: $N=11$**.** We have

$\mathbb{P}^1(\mathbf{Z}/11\mathbf{Z})=\{(1:0),(0:0),(1:1),(2:1),(3:1),(4:1),(5:1),(-1:1),(-2:1),(-3:1),(-4:1),(-5:1).\}$

These satisfy the relations

$$\begin{aligned}(0:0)+(1:0)&=0\\(1:1)+(-1:1)&=0\\(2:1)+(5:1)&=0\\(-2:1)+(-5:1)&=0\\(3:1)+(-4:1)&=0\\(-3:1)+(4:1)&=0\\(0:0)+(1:0)+(-1:0)&=0\\(1:1)+(-2:1)+(5:1)&=0\\(2:1)+(4:1)+(-4:1)&=0\\(-5:1)+(-3:1)+(3:1)&=0\end{aligned}$$

Thus

$$H(11)^* = \langle A, B, C \rangle$$

where $A = (2:1)$, $B = (3:1)$, $C = (0:1)$. Complex conjugation maps $A \mapsto A$, $B \mapsto A - B$, $C \mapsto C$. One can check that $\delta(A) = \delta(B) = 0$. Thus

$$H^+(11) = \langle A \rangle.$$

The Hecke operator T_2 acting on A is defined by the formal sum

$$T_2(A) = \left(\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \right) \left\{ 0, \frac{1}{2} \right\}.$$

Carrying this out, we obtain

$$\begin{aligned} T_2(A) &= \{0, 1\} + \left\{ 0, \frac{1}{4} \right\} + \left\{ \frac{1}{2}, \frac{3}{4} \right\} \\ &= (1:1) + (4:1) + \left\{ \frac{1}{2}, 1 \right\} + \left\{ 1, \frac{3}{4} \right\} \\ &= (1:1) + (4:1) + (-5:1) + (-4:1) \\ &= 0 + (B - A) + (-A) + (-B) \\ &= -2A, \end{aligned}$$

using the relations. Thus the Hecke eigenvalue is $a_2 = -2$. Similarly, we can compute

p	2	3	5	7	11	13
a_p	-2	-1	1	-2	1	13

The value of a_{11} comes from looking at the Fricke involution

$$w_{11} : z \mapsto \frac{-1}{11z}.$$

This sends $\left\{0, \frac{1}{2}\right\}$ to $\left\{\infty, \frac{-2}{11}\right\}$, so $w_{11}(A) = -A$ and so the eigenvalue is in fact -1; the value of a_{11} is minus this. This gives us the first few Fourier coefficients of the q-expansion of the weigth 2 cusp form on $\Gamma_0(11)$. We can also compute numerical values for the periods

$$\begin{aligned} \langle A, f \rangle &= \omega_1, \\ \langle B, f \rangle &= \omega_2. \end{aligned}$$

We have also obtain the sign in the functional equation of $L(f, s)$. Recall that if

$$f = \sum_{n \geq 1} a_n q^n$$

is a cusp form then the L-function is given by

$$L(f, s) = \sum_{n \geq 1} a_n n^{-s}.$$

This is also given as a Mellin transform

$$L(f, s) = (2\pi)^s \Gamma(s)^{-1} \int_0^{i\infty} (-i\tau) f(\tau) \frac{d\tau}{\tau}.$$

It follows that $\langle \{0, \infty\}, f \rangle = -L(f, 1)$.

Observe the following pattern:

p	2	3	5	7	11	13
$1+p-a_p$	5	5	5	10		10

This can be explained as follows. Note that

$$\begin{aligned} T_2\{0,\infty\} &= \{0,\infty\} + \{0,\infty\} + \left\{\frac{1}{2},\infty\right\} \\ &= 3\{0,\infty\} - \left\{0,\frac{1}{2}\right\}, \end{aligned}$$

thus

$$(T_2 - 3)\{0,\infty\} = -A.$$

This implies that

$$(2+3)\langle\{0,\infty\}, f\rangle = \langle A, f\rangle = \omega_1,$$

hence,

$$L(f,1) = \frac{1}{5}\omega_1,$$

or

$$\frac{L(f,1)}{\omega_1} = \frac{1}{5}.$$

In general $(1+p-T_p)\{0,\infty\} \in H^+(11)$. Hence

$$\frac{L(f,1)}{\omega_1} = \frac{n_p}{1+p-a_p}$$

where $n_p \in \mathbf{Z}$, holds for all $p \neq 11$. Thus

$$\frac{n_p}{1+p-a_p} = \frac{1}{5}$$

with $n_p \in \mathbf{Z}$, for all $p \neq 11$, so $1+p-a_p \equiv 0 \pmod 5$, as we had observed.

Next we ask: "how to construct the modular elliptic curve associated to a newform $f \in \mathcal{S}_2(N)$, when all we know is the q-expansion of f?" Well, the newform $f \in \mathcal{S}_2(N)$, which is a Hecke eigenform with integer eigenvalues a_p, corresponds to the two-dimensional eigenspace in $H(N)$ spanned by A, B. Set

$$\begin{aligned} \omega_1 &:= \langle A, f\rangle, \\ \omega_2 &:= \langle B, f\rangle. \end{aligned}$$

Thus ω_1 and ω_2 are complex numbers. Consider the lattice $\Lambda = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2$. Then we know from the theory that $E_f := \mathbf{C}/\Lambda$ is defined over $\mathbf{Q}$, and has conductor N.

For example, consider again the case $N = 11$. Then we can compute

$$\begin{aligned} \omega_1 &= 1.2692..., \\ \omega_2 &= \frac{\omega_1}{2} + 1.4588... \times i. \end{aligned}$$

Using 100 terms of the q-expansion, we can compute

$$\begin{aligned} c_4 &= 496 \text{ (to } 10^{-11} \text{ decimal places)}, \\ c_6 &= 20008 \text{ (to } 10^{-8} \text{ decimal places)}. \end{aligned}$$

From the theory, we know that these are in fact integers. We can then argue that

$$E_f : y^2 + y = x^3 - x^2 - 10x - 20.$$

Again from the theory, we have

$$L(E_f, s) = L(f, s).$$

Our previous computations then give

$$\frac{L(E_f, 1)}{\omega_1} = \frac{1}{5} \overset{?}{=} \frac{5}{5^2} \left| Ш(E_f) \right|,$$

where the final proposed equality comes from the Birch and Swinnerton-Dyer conjecture. In fact, it is known in this case that Ш(E) is trivial.