Fall Break Number Theory Remix

October 19, 2012

outline:

• Define hecke operators in general.
  – done

• Hecke operators as coset representatives + Fourier coefficients are integral.
  – a couple of paragraphs left

• Modular Equation for $\Gamma_0(N)$
  – couple of paragraphs left

• Hecke operators as Correspondences + Eichler-Shimura
  – done

• Weil Conjectures Elliptic Curves gives zeta function $Z(E; T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$.
  – done

• Zeta function of curve is mellin transform implies strong hasse-weil conjecture
  – need more on mellin transform Euler expansion.

• langlands / tunnel
- not started

- Galois representations
  - not started

- Deformation of Galois representations
  - not started

- Taniyama Weil implies Fermat
  - not started - See Knapp, Elliptic Curves, pp 397
Define Hecke operators in general. For $n \in \mathbb{N}$, let $M$ be the matrices with determinant $n$. Define, for a modular form $f \left( T_n \right) (z) = n^{k-1} \sum_{g \in SL_2(\mathbb{Z}) \setminus M} (cz + d)^{-k} f \left( \frac{az+b}{cz+d} \right)$ where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. In order to shorten this notation, we define $(cz + d)^{-k} f \left( \frac{az+b}{cz+d} \right)$ interchangelably with $f \mid [\gamma]_k$. Note if $\gamma' \in SL_2(\mathbb{Z})$, then we have $f \mid [\gamma']_k = (f \mid [\gamma]_k) \mid [\gamma]_k = f \mid [\gamma]_k$ which shows that $T_n f$ is well-defined.

Note that $T_n f$ is a modular form. To see this first check, from definitions, that $f \in H (\mathbb{H})$ and $(T_n f) \mid [\gamma]_k = T_n f$. After transforming $\gamma$ into an upper triangular element of $SL_2(\mathbb{Z}) \setminus M$, write $(T_n f) (z) = n^{k-1} \sum_{d \mid n} \sum_{b=0}^{d-1} d^{-k} f \left( \frac{(n/d)z+b}{d} \right)$. Using the $q$-expansion, $f \left( \frac{m}{d} \right) = \sum_{m \geq 0} a_f (m) q^m$, at $\infty$ of $f$, this becomes $n^{k-1} \sum_{d \mid n} d^{-k} \sum_{m \geq 0} a_f (m) e^{2\pi i \left( \frac{m(n/d)z+b}{d} \right)}$. When summing roots of unity, we have $\sum_{0 \leq b < d} q^{mb} = \begin{cases} d & d \mid m \\ 0 & \text{else} \end{cases}$. Write $m' = \frac{m}{d}$ and reparametrizing over $m'$ will give $n^{k-1} \sum_{d \mid n} d^{1-k} d^{-k} \sum_{m \geq 0} a_f (m'd) q^{m'd^2}$. Note that the constant coefficient $a_f (0) d$ will vanish at infinity iff $a_f (0) d$ does.

Now consider the $\mathbb{Z}$-algebra generated by Hecke operators $T_n$ acting on the space of cusp forms for some congruence subgroup $\Gamma$. We call this the Hecke Algebra associated to $S_k (\Gamma)$. Tensoring with a ring $R$, gives us the Hecke Algebra over $R$, $T_R (S_k (\Gamma))$. Since we define $T_n$ as a sum over divisors of $n$, we can show that $T_p \circ T_p = \sum_{d \mid \min (r,s)} p^{d(k-1)} T_{p^{d+1-s}}$. Note that $(T_p \circ T_p) (f) = \left( \sum_{d \mid p} \sum_{b=0}^{d-1} d^{-k} \right) \left[ f (pz) + \sum_{b=0}^{p-1} d^{-k} f \left( \frac{(n/d)z+b}{d} \right) \right]$. Writing this out shows $T_p \circ T_p = T_{p^{k+1}} + p^{k-1} T_{p^{k-1}}$. Using induction, and noting that for $(p, q) = 1$ $T_p T_q$ commute, gives that $T_R (S_k (\Gamma))$ is generated by the $T_p$, $p$ prime. This also shows the $T_R (S_k (\Gamma))$ is commutative.

For a modular form $f$, let $(T_n, \lambda_n)_{n \in \mathbb{N}}$ be a sequence of Hecke operators and scalars such that $T_n f = \lambda_n f$ (we call these simultaneous eigenforms / eigenvalues for $f$). Above we found that $(T_n f) (z) = n^{k-1} \sum_{d \mid n} d^{1-k} \sum_{m \geq 0} a_f (m'd) q^{m'd^2}$. In order to get this in the $q$-expansion form $\sum c_f^T (\mu) q^\mu$, write $\mu = m'n/d$. Thus

---

1 Kilford 29, 59
\[ c_{J_n}(m) = \sum_{d|n,m} \left( \frac{n}{d} \right)^{k-1} a_f \left( \frac{\mu d^2}{n} \right). \]

Writing \( n/d = \nu \) gives
\[ \sum_{\nu|n,m} \nu^{k-1} a_f \left( \frac{m}{\nu^2} \right) \]
and we see that \( c_{J_n}(0) = \sigma_{k-1}(n) := \sum_{\nu>0|n} \nu^{k-1} \) and that \( c_{J_n}(1) = a_f(n) \). If \( c_{J}(1) = 0 \) thus \( f \) must be equal to \( c(0) \), hence constant, hence 0. If \( c_{J}(1) = 1 \), then \( c_{J_n}(1) = a_f(n) = \lambda_n a_f(1) = \lambda_n \), since these are coefficients of first powers of \( q \).
Hecke operators as coset representatives + Fourier coefficients are integral. Recall that we earlier transformed an element of \( SL_2(\mathbb{Z}) \setminus M \) into an upper triangular \( \begin{pmatrix} n/d & b \\ 0 & d \end{pmatrix} = A \) with \( 0 \leq b < d \). This was in order to simplify the notation of \( (T_n f) \). Such an \( A \) is uniquely determined so we have a coset decomposition over all such \( A \), \( M = \coprod_A SL_2(\mathbb{Z}) A \). Now any \( \alpha \in M(n) \), has a Smith form, which we may achieve by elementary row and column switches and replacements. Thus \( M = \coprod_{d|n \atop d \geq n/2} SL_2(\mathbb{Z}) \begin{pmatrix} d & 0 \\ 0 & n/d \end{pmatrix} SL_2(\mathbb{Z}) \).

For such a matrix \( \alpha = \begin{pmatrix} d & 0 \\ 0 & n/d \end{pmatrix} \) in smith form, let \( A, B \in \mathbb{N} \) such that \( A\alpha, B\alpha^{-1} \) have integer entries. Then we may see \( \alpha^{-1} SL_2(\mathbb{Z}) \alpha \) is a congruence subgroup, since it will contain \( \Gamma(AB) \). Thus the index \( |SL_2(\mathbb{Z}) : \alpha^{-1} SL_2(\mathbb{Z}) \alpha \cap SL_2(\mathbb{Z})| \) is finite since \( 1 \to \Gamma(AB) \to SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/AB\mathbb{Z}) \) is exact. By group theory, we see \( SL_2(\mathbb{Z}) \setminus SL_2(\mathbb{Z}) \alpha SL_2(\mathbb{Z}) \alpha^{-1} \approx SL_2(\mathbb{Z}) \cap \alpha SL_2(\mathbb{Z}) \alpha^{-1} \) so that \( SL_2(\mathbb{Z}) \setminus SL_2(\mathbb{Z}) \alpha SL_2(\mathbb{Z}) = [SL_2(\mathbb{Z}) : \alpha^{-1} SL_2(\mathbb{Z}) \alpha \cap SL_2(\mathbb{Z})] = \beta \). This gives \( SL_2(\mathbb{Z}) \alpha SL_2(\mathbb{Z}) = \bigoplus_{i=1}^{\beta} SL_2(\mathbb{Z}) \alpha_i \).

Now we see that we may define a Hecke operator for such an \( \alpha \) by \( (T_n f) = \sum_{\beta} f[\alpha_i] \). For any \( T_n \), written in terms of \( M = \coprod_A SL_2(\mathbb{Z}) A \) we may therefore also write it in terms of \( M = \coprod_{d|n \atop d \geq n/2} SL_2(\mathbb{Z}) \begin{pmatrix} d & 0 \\ 0 & n/d \end{pmatrix} SL_2(\mathbb{Z}) \) like \( \sum_{d|n \atop d \geq n/2} T_{\text{diag}(d,n/d)} \).

Note that \( SL_2(\mathbb{Z}) \alpha SL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) \alpha^T SL_2(\mathbb{Z}) \), where \( \alpha^T \) is the transpose. Thus we see that for \( f \in M_k \), \( f[\alpha] = f[\alpha^T] \) is the same as \( f[\alpha^T] \). In order to see that the Fourier coefficients are algebraic integers, we must show normality of eigenforms. The fact that \( f[\alpha]_k = f[\alpha^T]_k \) will help, but first we must define an inner product. Define a measure \( \frac{dx dy}{y^2} \) on \( \mathbb{H} \). For \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \) we may write out \( \gamma \) \( (x + iy) \) as \( u + iv \). Change of variables gives \( \int_{\mathbb{H}} f(\gamma z) \frac{dx dy}{y^2} = \int_{\mathbb{H}} f(u + iv) \left| \frac{\partial x}{\partial u} \frac{\partial y}{\partial v} - \frac{\partial x}{\partial v} \frac{\partial y}{\partial u} \right| \frac{dudv}{y^2} = \int_{\mathbb{H}} f(u + iv) \frac{dudv}{y^2} \). Thus \( \frac{dx dy}{y^2} \) is invariant under \( SL_2(\mathbb{Z}) \).

Suppose that \( f, g \in M_k(\Gamma) \) and one is a cusp form. Our candidate for an inner product is the integral over a fundamental domain \( D \) for \( \Gamma \), \( \langle f, g \rangle_D = \)
Using basic calculus, we may show that the volume of $D$ computed with the invariant measure $\frac{dx\,dy}{y^2}$ is finite. The number of cusps, is $\leq [SL_2(\mathbb{Z}) : \Gamma]$ so we may decompose $D$ into a finite union of neighborhoods of cusps and an open set $U$ whose closure contains no cusp. In one of the sets containing a cusp, the $q$-expansion of the cusp form must vanish to order $e^{-ky}$ which gives convergence of the integral. The integral over $U$ will be finite since $\langle f, g \rangle_U$ is finite. Thus $\langle f, g \rangle_D$ defines a positive definite inner product.

Using a long sequence of elementary variable changing, (See Milne, MF pp 78), we may get that $\langle f| [\alpha]_k, g \rangle = \langle f, g| [\alpha^{-1}]_k \rangle$. (pretty reasonable looks)

Next paragraph is self-adjointness Brubaker pp 86 - looks reasonable.

final paragraph:
Now use Stein pp34 4.4.1 (I proved this - we have a basis of $E^a_4 E^b_6$ with integer coefficients)
matrices of hecke operators have integer entries (stein pp 36)
monic polynomials integer coeffs
roots of polys are real by (4.6.2, stein)
so roots are totally real algebraic integers
Weil Conjectures Elliptic Curves gives \( Z(E; T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} \). Let \( q = p^n \) and \( E/F_q \) be an elliptic curve defined over \( F_q \). Recall we have the frobenius \( T_p : E/F_q \mapsto E^{(p^n)}/F_q \). The algebraic closure of \( F_q \) is \( \mathbb{F} = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n} \) and we may consider \( E/F \). If \( a \in \mathbb{F} \) is a root of \( x^q - x \) then it must lie in \( \mathbb{F}_q \), so we get that the fixed point set of \( T_q \) acting on \( E \) is \( E(\mathbb{F}_q) \). Furthermore, by computing the differential of frobenius, we see that each such fixed point has multiplicity 1.

The \( \ell \)-adic numbers, \( \mathbb{Q}_\ell \), define earlier have a cohomology theory (see appendix) which satisfies the Lefschetz Fixed Point Formula, \( (\Gamma_{T_p} \cdot \Delta) = \sum_n (-1)^n Tr(T_p|H^n(E, \mathbb{Q}_\ell)) \). Here \( \Gamma_{T_p} \) denotes the graph of Frobenius, \( \Delta \) denotes the diagonal and \( Tr \) denotes the trace. Note that the intersection number (see Hartshorne V.1.I) of \( \Gamma_{T_p} \) and \( \Delta \), denoted \( \Gamma_{T_p} \cdot \Delta \) will count the number of fixed points with multiplicity. By the previous paragraph, we have that \( |E(\mathbb{F}_q)| \), the number of \( \mathbb{F}_q \)-rational points of \( E \), must be equal to \( (\Gamma_{T_q} \cdot \Delta) \). In general, we will have \( |E(\mathbb{F}_q^m)/\mathbb{F}_q| = (\Gamma_{T_q^m} \cdot \Delta) = \sum_n (-1)^n Tr(T_{q^m}|H^n(E, \mathbb{Q}_\ell)) \).

Now we define the zeta function of \( E \), \( Z(E, t) = \exp \left( \sum_m |E(\mathbb{F}_q^m)/\mathbb{F}_q| \frac{tm}{m} \right) \).

By the previous paragraph, this may be rewritten \( \prod_{r=0}^{2d} \left( \exp \left( \sum_m Tr(T_{q^m}|H^r(E, \mathbb{Q}_\ell)) \frac{tm}{m} \right) \right)^{-1} \). If we write the characteristic polynomial of \( T_{q^m} \) over \( H^r(E, \mathbb{Q}_\ell) \) as \( f(x) = x^n + c_{n-1}x^{n-1} + ... + c_0 \), then \( c_{n-1} \) is equal to \( Tr(T_{q^m}) \), which is the sum \( \sum \lambda_i \) of roots of \( f \). As formal power series, we have \( \log \frac{1}{1-\lambda_i} = \sum_{m=1}^{\infty} \lambda_i^m \frac{tm}{m} \) and so

\[
\log \left( \frac{1}{\det(1-T_{q^m}t)} \right) = \log \left( \frac{1}{\prod(1-\lambda_i t)} \right) = \sum_{m=1}^{\infty} Tr(T_{q^m}|H^n(E, \mathbb{Q}_\ell)) \frac{tm}{m} \].

Finally, we have the product formula, \( Z(E, t) = \prod_{r=0}^{2d} (1 - T_q t |H^r(E, \mathbb{Q}_\ell))^{-1/r} \).

This argument will apply more generally to a nonsingular, complete, algebraic variety (See Milne, Etale Cohomology).

We can be more explicit when just dealing with an elliptic curve. While exploring Eichler-Shimura theory we defined a mapping \( \phi_\ell \) induced on the Tate modules of \( E \) by Frobenius. Assume \( \phi_\ell \) is in Jordan form as a two-dimensional \( \mathbb{Q}_\ell \)-vector space map, we have \( \det(1 - T_q t) = t^2 - tr(T_q) t + \det(T_q) \). Silverman III.8.6, II.4.10 give that \( \det(\phi_\ell) = \deg(T_q), tr(\phi_\ell) = 1 + \deg(T_q) - \deg(1 - T_q) \), and that for a separable morphism, the degree is the size of the kernel. The frobenius is separable since it’s differential is the identity, hence \( |E(\mathbb{F}_q)| = \deg(1 - T_q) = \det(\phi_\ell) \), and in general \( |E(\mathbb{F}_q^m)| = \deg(1 - T_q^m) = \det(\phi_\ell^m) \).

We obtain an explicit expression for the determinant as \( \det(1 - t\phi_\ell) = t^2 - (1 + \deg(T_q) + |E(\mathbb{F}_q)|) t + \deg(T_q) = (t - \alpha)(t - \beta) \) for \( \alpha, \beta \in \mathbb{C} \). Writing out the \( \det(1 - \phi_\ell) \) gives \( |E(\mathbb{F}_q)| = 1 - \alpha^n - \beta^n + (\alpha\beta)^n \).
Using logarithms again, \( \log Z(E,t) = \sum_{m \geq 1} \left( \frac{t^n}{n} - \frac{\alpha t^n}{n} - \frac{\beta t^n}{n} + \frac{(\alpha \beta)^n t^n}{n} \right) \).

We get \( Z(E,t) = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-\alpha \beta)} \). Since \( (t - \alpha)(t - \beta) \) is \( \deg (1 - \mathbb{T}_q t) \geq 0 \), we see the roots must have the same absolute value, which is the Riemann Hypothesis for Elliptic curves. Unfortunately, the Riemann hypothesis for nonsingular varieties of arbitrary dimension requires a Lefschetz Formula which works for nonconstant sheaves so I won’t do it here.
2.5. Modular Equations and Models  I will follow Milne, Modular Forms closely. We defined \( \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \mod N \right\} \). Recall that \( \Delta \) was defined as the elliptic curve \( g_3^2 - 27g_2^3 \) and \( j = \frac{(12g_2)^3}{\Delta} \). Let \( X_0(N) = \Gamma_0(N) \setminus \mathbb{H} \). We have the following theorem from Milne, 6.1:

1. The field, \( \mathbb{C}(X_0(N)) \), of modular functions for \( \Gamma_0(N) \) is generated over \( \mathbb{C} \) by \( j(z) \) and \( j(Nz) \).
2. The minimum polynomial \( F_N(j,Y) \in \mathbb{C}(j)[Y] \) of \( j(Nz) \) over \( \mathbb{C}(j) \) has degree \( \mu \).
3. \( F_N(j,Y) \) is a polynomial in \( j \) with coefficients in \( \mathbb{Z} \).
4. When \( N > 1 \), \( F_N(X,Y) \) is symmetric in \( X \) and \( Y \), and when \( N = p \) is prime:
   \[
   F_N(X,Y) = X^{p+1} + Y^{p+1} - X^pY^p - XY \mod p.
   \]

By the theorem, we have \( \mathbb{C}(X_0(N)) \approx \mathbb{C}(j(z), j(Nz)) \approx \mathbb{C}[X,Y] / (F_N) \). Using Hartshorne I.6.12, we have an equivalence of categories between function fields of dimension 1 over \( \mathbb{C} \) and nonsingular projective curves over \( \mathbb{C} \). Thus we may find a “model” projective nonsingular curve \( \overline{C_0} \) for \( X_0(N) \) over \( \mathbb{C} \).

Over \( \mathbb{Q} \), \( F_N \) is irreducible with rational coefficients, so \( \mathbb{Q}[X,Y] / (F(X,Y)) \) is an affine \( \mathbb{Q} \)-algebra. By the nullstellensatz, \( \text{Spec} A \) is the curve \( F(X,Y) = 0 \) which we denote by \( C \). Recall \( F(X,Y) \) will be nonsingular when the partials are 0. Therefore, let \( C' \) be the subset of \( \text{Spec} A \) which has no intersection with \( \left( \frac{\partial F_N}{\partial x}, \frac{\partial F_N}{\partial y} \right) \mod F(X,Y) \). We can then embed \( C' \) into a complete regular curve \( \overline{C} \) and identify it with \( \overline{C_0} \) by identifying generators of the two function fields. We call \( \overline{C} \) the canonical model of \( X_0(N) \) over \( \mathbb{Q} \).

We define a moduli problem over \( k \) to be a contravariant functor \( F \) from varieties over \( k \) to sets. A solution to a moduli problem is a variety and a bijection \( (V, \alpha : F(k) \to V(k)) \) which satisfies:

1. For any variety \( T \) over \( k \), let \( f \in F(T) \). For a point \( t \in T(k) \) mapping \( t : \text{Specm}(k) \to T \), \( F \) gives a map \( F(T) \to F(k) \) in the other direction, where \( f \mapsto f_t \). We require that \( t \mapsto \alpha(f_t) \) be defined by a morphism of algebraic varieties.
2. \( \alpha \) must be universal with respect to 1.

For example, Hartshorne IV.4.1 gives a one-to-one correspondence between the set of elliptic curves over \( k \) and the elements of \( k \), given by mapping a curve \( E \) to its \( j \)-invariant in \( k \). As another example, we have a bijection between
$Y_0(N)$ and the set of isomorphism classes of morphisms $E \to E'$ with kernel $(\mathbb{Z}/N\mathbb{Z}, +)$ given by identifying a point $(x, y) \in E$ with $(j(E), j(E'))$.

finish $Y_0(N)$ as moduli problem / solutions.
Hecke Correspondences + Eichler-Shimura  We define a correspondence $T$ between two curves $X,X'$ as a pair of finite surjective morphisms, $\xi_X : Y \to X$, $\xi_{X'} : Y \to X'$. The correspondence $T$ defines a map $\text{Div} (X) \to \text{Div} (X')$, $P \mapsto \sum_{i \in \xi_X^{-1}(P)} \xi_{X'}(Q_i)$. The ring of correspondences will be the the maps generated by correspondences in $\text{End} (C_0(X))$ where $C_0$ is the kernel of the degree map from the divisor class group.

For $\alpha \in GL_2(\mathbb{R})^+$ and $\Gamma \leq SL_2(\mathbb{Z})$ of finite index, then $\alpha \Gamma z = \{ \alpha g z | g \in \Gamma \}$ is not in general an element of $\Gamma \backslash \mathbb{H} = \{ \Gamma z | z \in \mathbb{H} \}$. However, we wish to define Hecke operators in terms of an action $\alpha : \Gamma \backslash \mathbb{H} \to \Gamma \backslash \mathbb{H}$. If $\exists g A \in \Gamma A \cap \alpha \Gamma$, $A \in GL_2(\mathbb{R})^+$, then $A \in \alpha \Gamma$. We may write $\alpha \Gamma = \bigsqcup \Gamma \alpha \beta_i$ so that $\alpha \Gamma z = \bigsqcup \Gamma \alpha \beta_i z$. Now if we define $\alpha : \Gamma \backslash \mathbb{H} \to \Gamma \backslash \mathbb{H}, \Gamma z \mapsto \{ \Gamma \alpha \beta_i z \}$ we will have something that is well-defined (not necessarily an action), since $\Gamma \alpha \Gamma = \bigsqcup \Gamma \alpha \beta_i$ is the union of orbits meeting $\alpha \Gamma z$.

Recall we showed that $[SL_2(\mathbb{Z}) : \alpha^{-1} SL_2(\mathbb{Z}) \cap SL_2(\mathbb{Z})]$ is finite and $SL_2(\mathbb{Z}) \alpha SL_2(\mathbb{Z}) = \bigsqcup SL_2(\mathbb{Z}) \alpha \beta_i$, where $SL_2(\mathbb{Z}) \alpha SL_2(\mathbb{Z}) = \bigsqcup (SL_2(\mathbb{Z}) \alpha^{-1} SL_2(\mathbb{Z}) \alpha \beta_i)$. In a similar manner, we may show for $\alpha \in GL_2(\mathbb{R})^+$ a scalar multiple of an integer matrix that $\Gamma \alpha \Gamma = \bigsqcup \Gamma \alpha \beta_i$ where $\Gamma = \bigsqcup \Gamma \alpha \beta_i$, $\Gamma_\alpha = \Gamma \cap \alpha^{-1} \Gamma \alpha$.

Let $Y(\Gamma_\alpha) = \Gamma_\alpha \backslash \mathbb{H}$, and $X(\Gamma),X'(\Gamma) = \Gamma \backslash \mathbb{H}$. Then the map $\alpha : Y \to X'$, $\alpha : \Gamma_\alpha x \mapsto \Gamma \alpha x$ is well-defined. We still wish to get a well-defined action $X \to X'$ and in fact by defining by for modular function $f \in X'$, $(T_\alpha f)(z) = \sum f \circ \alpha \circ \beta_i(z)$ we have recover our earlier notion of a Hecke operator via a correspondence. This is equivalent to pulling back $f$ via $\alpha$ and then summing over $\beta_i$ in the preimage of $Y \to X$.

Fix $\Gamma = \Gamma_0(N)$ and define $T_p$ to be the Hecke operator associated to $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. We work over the characteristic 0 field $\mathbb{Q}_p$. Recall we defined the structure of a curve on $Y_0(N) = \Gamma \backslash \mathbb{H}$. Recalling the moduli solution for $Y_0(N)$, we may identify a point $(j(E),j(E'))$ on $Y_0(N)$ with a class $\beta$ of morphisms for two elliptic curves. The map $T_\alpha$ will act on the points of $E$, and specifically, order dividing $p$, $E[p]$, which via Hartshorne IV.4.16, is $\approx (\mathbb{Z}/p\mathbb{Z})^2$. By counting the number of distinct subspaces of dimension 1 over $\mathbb{Z}/p\mathbb{Z}$, we will find there are $p+1$ subgroups, $(\beta_i)$ of order $p$ in $(\mathbb{Z}/p\mathbb{Z})^2$. Label the quotient of $E$ by the $i^{th}$ such, $E_i$, which will be an elliptic curve since it is the quotient by a finite subgroup. Our correspondence $T_\alpha$ should map $[z] \mapsto \sum [\alpha \beta_i z]$ (we can write $T_\alpha(j(E),j(E')) = \{(j(E_i),j(E'_i))\}$ where

\footnote{Or Silverman 6.4.b, char 0 case}

\footnote{See Vélu's Formulae}
\[
\Gamma \left( \begin{array}{cc} 1 & 0 \\ 0 & p \end{array} \right) \Gamma = \prod \Gamma \left( \begin{array}{cc} 1 & 0 \\ 0 & p \end{array} \right) \beta_i.
\]
Since it should do the same thing to each subgroup of order \( p \) in \( E[p] \), we may identify \((\beta_i)\) with \( \beta_i \).

Suppose now that \( p \) is a prime where \( Y_0(N) \), has good reduction. multiplication \( \times p \) in characteristic \( p \) will not have separable degree 0 (you should be able to find some polynomial such that \( f(pX), f'(pX) \) have common roots), using Silverman, II.2.1.2, if \( \times p \) is purely inseparable, we have the factorization of multiplication, over characteristic \( p \), as \( \times p : E \rightarrow E^{(p^2)} \approx \rightarrow E \) and so \( j(E) = j(E)^{p^2} \). There are only finite many such point, which we ignore, and on the dense complement, we have inseparable degree \( p \), so \( \tilde{E}[p] \approx \mathbb{Z}/p\mathbb{Z} \). Let \((\beta_0) \approx \mathbb{Z}/p\mathbb{Z} \) be the kernel of \( E[p] \rightarrow \tilde{E} [p] \).

We may factor \( \times p \), differently this time, as \( \times p : \tilde{E} \xrightarrow{\phi} \tilde{E}_i \xrightarrow{\psi} \tilde{E} \). For \( i = 0 \) we are modding out by the kernel of the reduction so \( \times p \) remains inseparable, degree \( p \) so purely inseparable, and again using Silverman II.2.1.2, we get that \( \tilde{E}^{(p)} \approx \tilde{E}_0 \). Thus \( j(\tilde{E}_0) = j(\tilde{E}^{(p)}) = j(\tilde{E})^p = T_p \left( j \left( \tilde{E} \right) \right) \) where \( T_p \) is denoting the frobenius. Similarly for \( E' \). If \( i \neq 0 \), then \( \tilde{E} \rightarrow \tilde{E}/S_i \) has order \( p \) kernel so \( \psi \) is purely inseparable. So \( j \left( \tilde{E}_i^{(p)} \right) = j \left( \tilde{E}_i \right) \), and similarly for \( E'_i \) (Silv. II.2.1.2). Summing from \( i = 0, \ldots, p \), and recalling that \( T_\alpha (j(E_i), j(E'_i)) = \{ j(E_i), j(E'_i) \} \), we get that \( T_p + T_q^{-1} = T_\alpha \), which is called Eichler-Shimura’s theorem. Note that the same argument essentially works for \( X_0 = \Gamma_0(N) \setminus \mathbb{H}^* \), since you may ignore a finite number of reductions of cusp points.
For a fixed continuous function $\phi$ on $(0, \infty)$, define $\hat{\phi}(s) = \int_{0}^{\infty} \phi(y) y^{s-1} dy$, which we call the Mellin transform of $\phi$. There is an interval $(a, b)$ such that the Mellin transform converges absolutely when $\text{Re}(s) \in (a, b)$ and Fourier inversion will give a “Mellin inversion formula”:

$$\phi(y) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \hat{\phi}(s) y^{-s} ds$$

for $t \in (a, b), y \in (0, \infty)$. We may also define a similar Mellin transform for $...$ CONTINUE HERE And describe the L-function euler expansion, see page 70 Milne

Recall $X_0(N) = \Gamma_0(N) \backslash \mathbb{H}^*$ has the structure of a curve. We defined before the dimension of the space of cusp forms for $SL_2(\mathbb{Z})$. In a similar manner we can find dimensions of the space of weight $k$ cusp forms for $\Gamma_0(N)$. For $k = 2$ it is true that $\text{dim} \ S_k(\Gamma_0(N)) = g(N)$. Let $N$ be such that $X_0(N)$ has genus $= g(N) = 1$. Then up to a constant, there is one cusp form such with fourier coefficient $a_f(1) = 1$.

Recall that we found a product representation for $Z(C/\mathbb{F}_p; T)$, the zeta function of an elliptic curve $C$ over $\mathbb{F}_p$. Define the Hasse-Weil L function of $C$ to be $L(C, s) = \prod_p L_p(E, p^{-s})^{-1}$ where $L_p(E, p^{-s})$ depends on the type of reduction of $p$:

$$L_p(E, p^{-s}) = \begin{cases} \frac{\text{numerator } Z(C/\mathbb{F}_p; T)}{(1-T)} & \text{good, split, mult.} \\ \frac{1}{(1+T)} & \text{split, mult.} \\ 1 & \text{additive} \end{cases}$$

Using the Riemann hypothesis for elliptic curves, which we did above, the series will converge. For a prime of good reduction,

While exploring Hecke Operators, we noted that for $f$ normalized, $f$ satisfies $T_p f = a_f(p) f$ (it is an eigenfunction) where $a_f(p)$ will be real algebraic integers. Recall the Frobenius action on the Tate module $T_{\ell}(E)$ induces a homomorphism $\rho_{\ell} : \text{End}(E) \rightarrow \text{End}(T_{\ell}(E))$. Recall $T_{\ell}(E)$ has the structure of a 2-dimensional free $\mathbb{Z}_\ell$-module.

Now $$(I_2 - \rho_{\ell}(T_p)) (I_2 - \rho_{\ell}(T_p')) x = I_2 - \rho_{\ell}(T_p + T_p') x + \rho_{\ell}(T_p T_p') x^2.$$

Using Silverman III.6.2, we get that $T_p \circ T_p = \text{deg } [T_p] = p$. The above becomes $I_2 - \rho_{\ell}(T_p + T_p') x + px^2$. Using Eichler-Shimura, and assuming $p$ has good reduction, this is $I_2 - \rho_{\ell}(T_p) x + px^2 = I_2 - \begin{pmatrix} a_p & 0 \\ 0 & a_p \end{pmatrix} x + px^2$ where equality
is because for reduction mod $p \neq \ell$ we have same eigenvalues for $T_p$ as $\tilde{T}_p$. We may rewrite this as $\begin{pmatrix} 1 - a_p x + px^2 & 0 \\ 0 & 1 - a_p x + px^2 \end{pmatrix}$. Then $det(1 - T_p x)^2 = (1 - a_p x + px^2)^2$ so $det(1 - \rho_t (T_p) x) = 1 - a_p x + px^2 \star$. Thus we will have an equality between $p$-factors of the Euler-expansion of the Hasse-Weil $L$-function $L(X_0(N), s)$, corresponding to the LHS of $\star$, and the Euler expansion of the Mellin transform, $L(f, s)$ of $f$, corresponding to the right side.

Milne states the following: In the general case, Taniyama-Weil states: Let $E$ an elliptic curve over $\mathbb{Q}$. Then $L(E, s) = L(f, s)$ for some normalized eigenform of weight 2 for $\Gamma_0(N)$, where $N$ is the conductor of $E$. This conjecture is subsumed by the Langlands program which predicts that all Dirichlet series arising from algebraic varieties occur among those arising from automorphic representations for reductive algebraic groups.
Biblio

Integrality of Eigenform Coefficients:
Brubaker Lecture Notes, Automorphic Forms / Milne
Peterson inner product:
algebraic closure of finite field:
http://planetmath.org/encyclopedia/AlgebraicClosureOfAFiniteField.html
Weil Conjectures:
Milne, Etale Cohomology
Riemann Hypothesis, Elliptic Curves:
Silverman
Homework:
Elliptic Curve genus 1. Let $c_n = \{ f | \text{div}(f) - nP \geq 0 \}$.
1. Derive Weierstrass: See Silverman chap III

2. If $\dim c_1 = 1$, then curve is rational.
   Confused... An elliptic curve is never rational (birational to $\mathbb{P}^1$) see Hartshorne chapter 1.
0.0.1 After Fall break
Complex Multiplication