Part of the power of modular forms comes from the fact that they can be seen as functions on several different spaces. A modular form can be seen as a function on lattices in the complex plane, on the upper half plane, or on a Riemann surface known as the modular curve. We will first give a definition of a modular function as a function on the space of lattices which is not quite correct but is the most intuitive and will then refine it.

A lattice in $\mathbf{C}$, by which we will always mean a rank two lattice embedded in a discrete manner, can be specified by giving a basis (ω_1, ω_2) for it. We will then define a modular form as a holomorphic function of two variables; we will assume that ω_1, ω_2 is an oriented basis, meaning that ω_1/ω_2 has positive imaginary part. A modular form is then a holomorphic funtion $f(\omega_1, \omega_2)$, defined for $\mathrm{Im}(\omega_1/\omega_2) > 0$, which depends only on the lattice spanned by ω_1 and ω_2 and which has the folowing homogenity property: there is an integer k such that $f(\alpha\omega_1, \alpha\omega_2) = \alpha^{-k} f(\omega_1, \omega_2)$ for all complex α. k is called the *weight* iof the modular form.

There two things wrong with this definition: a generality we have not included and a condition we have not imposed. To see the first, note that the requirement that $f(\omega_1, \omega_2)$ depend only on the lattice spanned by ω_1 and ω_2 means explicitly that $f(\omega_1, \omega_2) = f(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbf{Z})$. The generaliztion is to replace $SL_2(\mathbf{Z})$ with a subgroup of $SL_2(\mathbf{Z})$ of the sort known as a congruence subgroup. For convenience, we introduce the notation

$$([\gamma]|_k f)(\omega_1, \omega_2) = f(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$$

where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. $[\gamma]|_k$ is a right action of $GL_2(\mathbf{R})$ on the space of modular forms.

For any positive integer N, define the group

$$\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mathrm{mod} N\}.$$

(By this we mean $a = 1$, $b = 0$, $c = 0$ and $d = 1$.) We will frequently write modular conditions on matrix entries in this shorthand.) A congruence subgroup is a subgroup of $SL_2(\mathbf{Z})$ that contains some $\Gamma(N)$. We now give the expanded defintion: given an integer N, a group Γ with $\Gamma(N) \subseteq \Gamma \subseteq SL_2(\mathbf{Z})$ and an integer k, a modular form is a holomorphic function f of two variables such that

$$f = [\gamma]|_k f \text{ for } \gamma \in \Gamma$$

and

$$f(\alpha\omega_1, \alpha\omega_2) = \alpha^{-k} f(\omega_1, \omega_2).$$

f is called a modular form of weight k for Γ, the least N for which this defintion holds is called the *level* of f.

Just as the symmetry under $SL_2(\mathbf{Z})$ corresponds to requiring that the modular form depend only on the matrix spanned by ω_1 and ω_2, the symmetry under $\Gamma(N)$ has a geometric interpretation as well. Let Λ be the lattice spanned by ω_1 and ω_2. Color the points of Λ with N^2 colors based on which coset of $\Lambda/N\Lambda$ they lie in. Being symmetric under $\Gamma(N)$ means that a function is dependen only on the colored lattice arising from ω_1 and ω_2.

There are two specific subgroups lying in between $\Gamma(N)$ and $SL_2(\mathbf{Z})$ that will be of importance in the future. Set

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mathrm{mod} N\}$$

and

$$\Gamma_1(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mathrm{mod} N\}.$$

Being a modular form for these groups also has coloring interpretations. For $\Gamma_0(N)$, color a point of $\Lambda(N)$ with one color if it lies in the sublattice spanned by $(\omega_1, N\omega_2)$ and another color otherwise; f is a modular form for $\Gamma_0(N)$ if it depends only on the coloring arising from ω_1 and ω_2. For $\Gamma_1(N)$, color Λ in N colors, depending on which coset a point lies in modulo the lattice spanned by $\omega_1, N\omega_2)$.

We are still missing one condition before we give the completely correct definition fo a modular form. In order to easily give this, we now show how to look at a modular form as a function on the upper half plane and then on a Riemann surface. Note that, by our homogenity condition, the values of a modular form of given weight k are determined by its values on points of the form $(z, 1)$. We must now interpret $[\gamma]|_k$ in this context. Writing f both for the function of one and two variables,

$$([\gamma]|_k f)(z) = ([\gamma]|_k f)(z,1) = f(az+b, cz+d) = (cz+d)^{-k} f((az+b)/(cz+d), 1) = (cz+d)^{-k} f((az+b)/(cz+d)). \blacksquare$$

Our requirement that ω_1/ω_2 have positive imaginary part means we can consider functions solely on the upper half plane.

Now, in the case of forms of weight 0, this definition can be restated by saying that a modular form is a holomorphic function on the Riemann surface produced by taking the quotient of the upper half plane by the action on the upper half plane by Γ by $z \to (az+b)/(cz+d)$. It can be easily shown that this Riemman surface can be uniquely compactifed by adding a finite number of points, known as the cusps. Add to the upper half plane the rational points of the real access and a point at infinity, the neighborhoods of which are of the form $\{z \text{ s.t. } \mathrm{Im}(z) > R\}$. The the quotient map from the upper half plane to the curve extends to a map from the added points to the cusps. We call the resulting curve the modular curve correspoding to Γ and denote it X. (At times it will be denoted $X(N)$, $X_0(N)$, etc. to show what Γ we are considering.) This makes plausible the condition we have previously been missing in the case of weight 0: modular forms should extend to meromorphic functions on the modular curve.

The condition in general is the following. A modular form must have the property that, when viewed as a function in the upper half plane, it must be bounded on any path whose imaginary part approaches infinity. By the general theory of Riemann surfaces, this will mean that in a neighborhood of infinity, it will extend to a holomorphic function on the modular curve. The corresponding condition at the other cusps is messier to state. Perhaps the simplest statement is that, if $\gamma \in GL_2(\mathbf{R})$ maps the cusp in question to infinity, that $[\gamma]f$ should be bounded at infinity. Another statement is that f shuold be bounded on arcs orthogonal to the real axis. A form is called a cusp form if it's value at each of the cusps is 0. If f is a form of weight two, then $f(z)dz$ gives rise to a diffferential form on the modular curve; oddly, it is the cusp forms, and not simply the modular forms, that correspond to holomorphic differential fomrs in this way.

For most purposes we can ignore the meromorphic condition, as it is preserved by every operation we normally perform and most formal identities hiold with out it.. We can thus think of modular forms in three ways. We can think of a modular form simply as a function on lattices with additional structure and the appropriate homogenity. Alternatively, one can view them as objects on the upper half plane with less intuitive symmetries. Finally, one can view a modular form as an object on the modular curve. A weight 0 form is simply a fucntion on the modular curve. Although it is less obvious, a weight 2 worm is a differntial one form. This is because $d((az+b)/(cz+d)) = (cz+d)^{-2}dz$ so, if f is a weight 2 form, then $f(z)dz$ is invariant under the pull back action by members of Γ, so it descends to a one fomr on the modular curve. Modular forms of other weights are sections of less familiar line bundles. (The forms of weight $2k$ correspond to sections of the k-fold tesor product of the cotangent bundle with itself; the odd weight forms are less familiar.)

Especially important are modular forms which, viewed as sections of bundles on the modular curve, are holomorphic at the cusps. These are called cusp forms. The cusp forms of weight k are denoted S_k.

We now introduce a representation of a modular forms known as a q-series. Suppose that Γ contains the matrix $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. Then f is periodic with period 1 and can thus be written as

$$f(z) = \sum a_n e^{2\pi i n z}.$$

We will regularly make the substitution $q = e^{2\pi i z}$ when writing this series. By the meromorphic condition, this sum contains only finitely many negative powers of q. This manner of expressing a modular form will become more important later.

We have one more basic tool to define before we can begin working with modular forms. This is a Hermitian inner product on S_k known as the Peterson inner product. For $k = 2$, the modular forms can be viewed as one forms ω and η on the modular curve and the inner product is simply $<\omega, \eta> = \int_X \omega \wedge \bar{\eta}$.

More generally, for any k, the Peterson inner product of two weight k forms f and g can be defined as follows. Let $\tilde{X}$ be the space formed by taking the quotient of $\{(\omega_1, \omega_2) \in \mathbf{C}^2 \text{ s.t. } \mathrm{Im}(\omega_1/\omega_2) > 0\}$ by the relevant modular subgroup Γ. Setting

$$\Omega = (\omega_2 d\omega_1 - \omega_1 d\omega_2),$$

we can define a one form $\tilde{f}$ on $\tilde{X}$ by

$$\tilde{f}(\omega_1, \omega_2) = f(\omega_1, \omega_2)\mathrm{Det}(\omega_1, \omega_2)^{k/2-1}\Omega$$

where $\mathrm{Det}(\omega_1, \omega_2)$ means the volume of the fundamental parrallelogram of the lattice spanned by ω_1, ω_2. Note that, although this is a $(1,0)$ form, it is *not* holomorphic unless $k = 2$. It is easy to check that $\tilde{f}$ is invariant under scaling.

Let X be the modular curve assosciated to Γ, X is also the quotient of $\tilde{X}$ by scaling. $\tilde{f}$ descends to a one form on X; if we denote this form again by f we can compute $< f, g >= \int_X f \wedge \bar{g}$. As an integral on the upper half plane, the formula is

$$\int_\Delta f\bar{g}y^{k-2}dz \wedge d\bar{z}$$

where Δ is a fundamental domain for Γ.

We now move to one of the main subjects of this paper, the Hecke operaters. These are linear operaters which act on formal sums of lattices and thus induce a linear action on modular forms. There is a Hecke operater associated with each positive integer, dentoed $T(n)$.

We will first define Hecke operaters for $SL_2(\mathbf{Z})$ on formal sums of lattices. We will then show how this leads them to act on modular forms, including giving explicit formulas in terms of q-series. Of especial importance will be modular forms that are eigenvectors for every Hecke operater; these are caled eigenforms. The Hecke operaters will be deliberately normalized so that, if $f = \sum a_n q^n$ with $a_1 = 1$ is an eigenform then $T(n)f = a_n f$. We will then derive certain relations between the Hecke operaters and between the Hecke operaters and the Peterson inner product. Using these, we will be able to derive relations between the coefficents of the q-expansion of an eigenform and show the eigenforms are a basis for the modular forms.

Finally, we will translate this theory to an arbitrary congruent subgroup. There will be some difficulties, but the sequence of events will be similar. Definition acting on formal sums of colored lattices, resulting action on modular forrms, formulas in terms of q-series, implications for eigenforms, relations between Hecke operaters, relations between Hecke operaters and peters inner product and linear algebra consequences. It will not be true in general that a basis of eigenvectors will exist, but it will be close to true.

We define the nth Hecke operator of weight k, $T(n)$, to act on a lattice Λ by

$$T(n) : \Lambda \to n^{k-1} \sum_{\mathcal{M} \subset \Lambda,\ [\Lambda:\mathcal{M}]=n} \mathcal{M}.$$

(The n^{k-1} is a normalization factor whose importance will emerge later). $T(n)$ is defined on formal sums of lattices by linearity. It is not immediately clear that this sum is finite, but it will follow from other formulas we will derive from this expression that it is. This formula is very useful theoretically, but not computationally; our next task will be to devise a computational form of this formula.

For this, we need a good way to describe all of the index n sublattices of Λ. Let $\mathcal{M}$ be such a sublattice, we know that $\mathcal{M} = [\gamma]\Lambda$ where γ is a member of $GL_2(\mathbf{Z})$ with determinant n. Let ω_1, ω_2 be a basis for Λ. Then $\mathrm{span}(\omega_2) \cap \Lambda = \mathrm{span}(d\omega_2)$ for some $d|n$, and we can take $d\omega_2$ to be one member of a basis for $\mathcal{M}$. Let $a\omega_1 + b\omega_2$ be another member of $\mathcal{M}$ which forms a basis for $\mathcal{M}$ together with $d\omega_2$. As $[\Lambda : \mathcal{M}] = n$, we have $ad = n$. Moreover, we can subtract multiples of ω_2 from $a\omega_1 + b\omega_2$ to make $0 \le b < d$. Thus, every $\mathcal{M}$ is of the form $[\gamma]\Lambda$ where $\gamma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, $ad = n$, $0 \le b < d$ and it is easy to check that none of these are identical. So we get the new formula

$$T(n)\mathrm{span}(\omega_1, \omega_2) = n^{k-1} \sum_{ad=n, 0\le b<d} \mathrm{span}(a\omega_1 + b\omega_2, d\omega_2).$$

To see how this acts on modular forms, viewed as functions on the upper half plane, we just plug in, we get

$$(T(n)f)(z) = n^{k-1} \sum_{ad=n,0\le b<d} \frac{1}{(0z+d)^k} f(\frac{az+b}{0z+d}) = n^{k-1} \sum_{ad=n,0\le b<d} \frac{1}{d^k} f(\frac{az+b}{d}).$$

Since the definition of the operater on lattices depended only on the lattice and not its basis and clearly commutes with scaling, $T(n)f$ will clearly be a modular form of weight k if f was.

Translating the previous formulae into a formula for q-series is also easy, although it gets complicated. Let $q = e^{2\pi i z}$ and write $f = \sum_j a_j q^j$. Then

$$T(n)f = n^{k-1} \sum_{ad=n, 0 \leq b < d} \frac{1}{d^k} \sum_j a_j e^{2\pi i \frac{az+b}{d} j} = n^{k-1} \sum_{ad=n, 0 \leq b < d} \frac{1}{d^k} \sum_j a_j q^{\frac{a}{d} j} e^{2\pi i \frac{b}{d} j}.$$

(Which (a/d)-th root of 1 is chosen is not important as long as the same one is used every time, because the sum on b has the effect of causing the expression $q^{a/d} e^{2\pi i b/d}$ to take each possible value once.)

Significant simplification can be obtained by regrouping to sum first on b to give

$$n^{k-1} \sum_{ad=n} \sum_j a_j q^{aj/d} \sum_{0 \leq b < d} \frac{1}{d^k} e^{2\pi i bj/d}.$$

The inner sum, $\sum_{0 \leq b < d} e^{2\pi i bj/d}$ is 0 unless $d|j$, in which case it is d. Writing $j = dl$ and using the above observation, we get

$$n^{k-1} \sum_{ad=n} \frac{1}{d^k} \sum_l a_{dl} q^{al} d = \sum_{ad=n} a^{k-1} \sum_l a_{dl} q^{al}.$$

This can be used to find an expression for the coefficent of q^j, it is

$$\sum_{al=j, ad=n} a^{k-1} a_{dl}.$$

(The sum is over all ordered triples (a, l, d) such that $a = j$ and $ad = n$.)

This formula is not especially worth remembering, but some aspects of it are. The first is that the coefficents of the new q-series are integer combinations of the coefficents of the old one. The second is that, if the previous q-series contains no terms with negative exponent, neither does the new and if the old series has constant term 0 so does the new. Thus, $T(n)$ preserves modular forms and cusp forms.

Finally, the special case $j = 1$ is very important. In this case, the formula simplifies to just a_n. (This was the point of the n^{k-1} normalization.) This has several important consequences. Suppose that f is a cuspform and is an eigenform for every $T(n)$. Then the complete sequence of $T(n)$ determine f up to scaling. If (with the same assumptions on f) a_1 is 0, then every a_n is 0. For $f \neq 0$ and meeting the above conditions, we can assume therefore than $a_1 = 1$. Such an f will be called a normalized eigenform. For such an f, we have

$$T(n)f = a_n f.$$

We will now derive two important relations between the $T(n)$. To experss them, we will need the operater $R(n)$, which acts on formal sums of lattices by sending $\Lambda \to n^{2k-2}(n \cdot \Lambda)$. (The simplest way to remember these peculiar factors up front is that $T(n)$ has an image consisiting of lattices of index n, so there is an n^{k-1} in front; $R(n)$ has an image of latttices of index n^2 so it has a $n^{2(k-1)}$.) By definition, this induces an action on modular forms by $R(n)f = n^{2k-2} \cdot n^{-k} f = n^{k-1} f$. The two relations are

$$T(m) \circ T(n) = T(mn) \ (m, n) = 1$$

and

$$T(p^{\alpha+1}) = T(p) \circ T(p^\alpha) - pR(p) \circ T(p^{\alpha-1}).$$

We will delay proving these because it will be better to prove them at the same time as proving the slightly more complicated relations obeyed by Hecke operaters for general congruence subgroups. Instead, we note several consequences.

By recursively using the two formulas, we say that every Hecke operater can be expressed as a polynomial in $R(p)$ and $T(p)$. The first relation shows that $T(p)$ and $T(q)$ commute where p and q are distinct primes and it is onbiovus that the $R(p)$ commute with each other and with all $T(p)$. Therefore, the Hecke operaters all commute with each other. Also, if f is an normalized eigenform for all of the $T(n)$, plugging in the formulae $T(n)f = a_n f$ and $R(n)f = n^{k-2}f$ give

$$a_{mn} = a_m a_n \ (m,n) = 1$$

and

$$a_{p^{\alpha+1}} = a_p a_{p^\alpha} - p^{k-1} a_{p^{\alpha-1}}.$$

These can be regrouped into the simpler identity

$$\sum_n \frac{a_n}{n^s} = \prod_p \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}.$$

(Note: historically, this was how the Hecke operaters were discovered. Ramanujan observed the above identities in the case of a normalized eigenform of weight 12 and Hecke invented his operaters to prove Ramanujan's observations.)

We now state the important relation between the Hecke operaters and the Peterson inner product:

$$< T(n)f, g >=< f, T(n)g > .$$

The term for this behavior is that $T(n)$ is self-adjoint. This is important because it is known that a commuting ring of self-adjoint operaters on a finite dimensional vector space always decomposes into a sum of simultaneous eigenspaces for all of the operaters. Applying this result to the space of cusp forms, we see that the eigenforms we have proved results about above do exist. Moreover, since we showed that the set of eigenvalues of a normalized eigenform deterines it, we know that each of these spaces is one-dimensional.

We now define the Hecke operaters on modular forms for $\Gamma_0(N)$. We can interpret the members of $\Gamma_0(N)$ as functions on lattices with a cyclic sublattice of index N being colored in a different color from the other points. Let (Λ, C) represent such a lattice and its coloring. Then we can define the $T(n)$ as a formal sum on such pairs (Λ, C) by

$$T(n)(\Lambda, C) = \sum_{\mathcal{M} \subset \Lambda, [\Lambda:\mathcal{M}]=n, D=C|_{\mathcal{M}}} (\mathcal{M}, D).$$

We work out the formula explicitly. In this case, a ponit $a\omega_1 + b + \omega_2$ is colored one color, say blue, if $a = 0 \bmod N$ and another, say red, otherwise. A sublattice $\mathcal{M}$ of index n will have the appropriate coloring induced iff there are points in $\mathcal{M}$ with ω_1 coordinate relatively prime to N. (Otherwise, the blue points of $\mathcal{M}$ will have index $N/(N,n) < N$ in $\mathcal{M}$.) We have seen before that every index n sublattice of $\mathcal{M}$ has a unique basis of the form $a\omega_1 + b\omega_2$, $d\omega_2$, $ad = n$, $0 \leq b < d$. It is clear that the opssible ω_1 coefficents in such a lattice are the multiples of a, so this lattice is aceptable iff $(a, N) = 1$ in which case this basis is a compatible one with the coloring. Thus we get

$$T(n)(\omega_1, \omega_2) = n^{k-1} \sum_{ad=n, 0 \leq b < d, (a,N)=1} (a\omega_1 + b\omega_2, d\omega_2).$$

As before, this gives an action on the upper half plane and on q-series. As 1 is relatively prime to everything, we still get all the $q^{1/n}$ terms and thus again get that the coefficent of q in $T(n)f$ is the coefficent of q^n in f.

In general, congruence subgroups for which the $\binom{1\,b}{0\,n}$ are not acceptable sublattices do not have interesting behavior with respect to the Hecke operaters as this property no longer holds and we thus can not use the eigenforms of the Hecke operaters to extract coefficents of the q-series. Requiring that these matrices be acceptible basis changes amounts to requiring we consider colorings in which lines parallel to ω_2 recieve the same color, and thus congruence subgroups containing some $\Gamma_1(N)$. For any Γ containing a $\Gamma_1(N)$, we have that the coefficent of q in $T(n)f$ is that of q^n in f by computations similar to the above.

We will now prove the relations

$$T(mn) = T(m) \circ T(n)$$

$$T(p^{\alpha+1}) = T(p) \circ T(p^\alpha) - pR(p) \circ T(p^{\alpha-1}),\ (p,N) = 1$$
$$T(p^{\alpha+1}) = T(p) \circ T(p^\alpha)$$

where $R(n)(\Lambda, C)$ now means $n^{2k-2}(n\Lambda, C|_{n\Lambda})$ if $C|_{n\Lambda}$. Note that, for a normalized eigenform $\sum a_n q^n$, these give

$$\sum \frac{a_n}{n^s} = \prod_p \frac{1}{1 - a_p p^s + \delta_p p^{k-1-2s}}$$

where $\delta_p = 0$ if $p|N$, 1 otherwise.

Aply each side of the formula to (Λ, C). In both cases, the extra factors of n^{k-1} and n^{2k-2} cancel out. The first formula thus becomes

$$\sum_{\Lambda'' \subset \Lambda, [\Lambda:\Lambda''] = mn, C'' = C|_{\Lambda''}} (\Lambda'', C'') = \sum_{\Lambda'' \subset \Lambda', [\Lambda':\Lambda''] = m, C'' = C'|_{\Lambda''}} \sum_{\Lambda' \subset \Lambda, [\Lambda:\Lambda'] = n, C' = C|_{\Lambda'}} (\Lambda'', C'')$$

In other words, we are being asked to show that each (Λ'', C'') on the left arises from a unique chain $\Lambda \supset \Lambda' \supset \Lambda''$ on the right. If we disregard the colorings, this is easy. Λ/Λ'' is an abelian group of order mn. It follows from the classification fo abelian groups that Λ/Λ'' contains a unique subgroup of order m (using that $(m,n) = 1$). This corresponds to a unque lattice Λ' with $\Lambda \supset \Lambda' \supset \Lambda''$ and $[\Lambda' : \Lambda''] = n$. We now must see that Λ' is appropriately colored. But this is simple. A sublattice of Λ will have an apropriate subcoloring induced iff it contains points with ω_1 coordinate relatively prime to N. If Λ'' has this property, then so must Λ' which contains it.

For the second property, regroup this equation as $T(p^{\alpha+1}) + pT(p^{\alpha-1}R(p)) = T(p)T(p^\alpha)$. Note that, as $(p,N) = 1$, any sublattice of Λ with index a power of p will automatically be appropriately colored, so we just need to check that the same lattices appear with the same multiplicities on each side. For any lattice $\Lambda'' \subset \Lambda$ of index $p^{\alpha+1}$, the number of times Λ'' appears on the right is 1 if Λ'' is not a sublattice of $p\Lambda$ and $p+1$ if it is.

On the right, the number of times Λ'' appears is the number of lattices Λ' such that $\Lambda \subset \Lambda' \subset \Lambda''$ and $[\Lambda' : \Lambda''] = p$. Using the equivalence between lattices in between Λ and Λ'' and subgroups of Λ'', the right hand side is the number of subgroups of order p in Λ/Λ''. Now, Λ/Λ'' is an abelian group of order $p^{\alpha+1}$. Moreover, it can be generated by two elements, as it is a quotient of $\Lambda = \mathbf{Z}^2$. So $\Lambda/\Lambda'' = (\mathbf{Z}/p^{\alpha+1})$ or $(\mathbf{Z}/p^\beta) \oplus (\mathbf{Z}/p^\gamma)$ for $\beta, \gamma > 0$, $\beta + \gamma = \alpha + 1$. In the first case, there is one subgroup of order p. In the second, there are $p+1$. Moreover, in the first case, $p\Lambda$ is not a sublattice of Λ'' and in the second it is, so the conclusion is proven.

To show the result where $p|N$, we use the same proof as the above, except that we now have to consider whether the coloring will be appropriate. Any sublattice of $p\Lambda$ can not be correctly colored, as $p|N$. On the other hand, if Λ'' is correctly colored, so is any Λ' containing it. Thus we get that each side is simply the correctly colored subleattices of Λ of index $p^{\alpha+1}$.

We now need to discuss the relation between the Hecke operaters and the Peterson inner product. Specifically, we shall prove that $< f, T(n)g > = < T(n)f, g >$ when $(n,N) = 1$. In order to see where such relations come from, we need to set up some geometry. Let $H = \{(\omega_1, \omega_2) \in \mathbf{C}^2,\ \mathrm{Im}(\omega_1/\omega_2) > 0\}$. and let Γ act on H in the usual way with $\tilde{X}$ the quotient. Let X in turn be the modular curve. We saw before that we could write the Peterson inner product as

$$\int_X f(\Lambda)\bar{g}(\Lambda)\Omega(\Lambda)\bar{\Omega}(\Lambda)\mathrm{Det}(\Lambda)^{k-2}$$

where Λ is short for (ω_1, ω_2) and $\Omega = \omega_2 d\omega_1 - \omega_1 d\omega_2$. Note that this can also be seen as the integral in $\tilde{X}$ over any section of the projection map to X. Teh advaantage of this second form is that we have a simlpe way of thinking of $T(n)$ as acting on formal sums of points in $\tilde{X}$.

Let $\tilde{\Pi}_n \subset \tilde{X} \times \tilde{X}$ be

$$\{(\Lambda_1, \Lambda_2) | \Lambda_2 \text{ appears in } T(n)\Lambda_2\}$$

and Π_n be the image of $\tilde{\Pi}_n$ under the projection to $X \times X$. Then we can write

$$< f, T(n)g > = \int_{\text{any section of } X \text{ in} \tilde{X}} f(\Lambda)\Omega(\Lambda)\mathrm{Det}(\Lambda)^{k/2-1} T(n)\bar{g}(\Lambda)\bar{\Omega}(\Lambda_2)\mathrm{Det}(\Lambda)^{k/2-1}.$$

Now, any for any $\mathcal{M}$ appearing in $T(n)\Lambda$, $[\Lambda : \mathcal{M}] = n$ and therefore $\mathrm{Det}(\mathcal{M}) = n\mathrm{Det}(\Lambda)$ and $\Omega(\mathcal{M}) = n\Omega(\Lambda)$ so we can rewrtie the above as

$$\int_{\text{any section of } X \text{ in} \tilde{X}} f(\Lambda)\Omega(\Lambda)\mathrm{Det}(\Lambda)^{k/2-1} n^{k-1} \sum_{\mathcal{M}\in T(n)\Lambda} \bar{g}(\mathcal{M})\frac{1}{n}\bar{\Omega}(\mathcal{M})\frac{1}{n^{k/2-1}}\mathrm{Det}(\mathcal{M})^{k/2-1} =$$

$$n^{k/2-1}\int_{\text{any section of } \Pi_n \text{ in } \tilde{\Pi}_n} f(\Lambda)\Omega(\Lambda)\mathrm{Det}(\Lambda)^{k/2-1}\bar{g}(\mathcal{M})\frac{1}{n}\bar{\Omega}(\mathcal{M})\frac{1}{n^{k/2-1}}\mathrm{Det}(\mathcal{M})^{k/2-1}.$$

This integrand is symmetric under scaling and vainshes on the fibers of $\tilde{\Pi}_n \to \Pi_n$ so it can be rewritten as

$$n^{k/2-1}\int_{\Pi_n} f(\Lambda)\Omega(\Lambda)\mathrm{Det}(\Lambda)^{k/2-1}\bar{g}(\mathcal{M})\frac{1}{n}\bar{\Omega}(\mathcal{M})\frac{1}{n^{k/2-1}}\mathrm{Det}(\mathcal{M})^{k/2-1}.$$

Now, the integrand is clearly conjugate-symmetric in Λ and $\mathcal{M}$, so if we prove that Π_n is symetric under the interchange of Λ and $\mathcal{M}$, we will have $< f, T(n)g >=< T(n)f, g >$ as promised. We will prove this by showing that $\mathcal{M}$ appears in $T(n)\Lambda$ iff $n\Lambda$ apears in $T(n)\mathcal{M}$ when $(N, n) = 1$.

As $(N, n) = 1$, the colorings on $\mathcal{M}$ and $n\Lambda$ will auotmatiaclly be correct so we just need to check that we get the same sets of lattices. If $\mathcal{M} \subset \Lambda]$, $[\Lambda : \mathcal{M}] = n$, then $\Lambda/\mathcal{M}$ is a group of order n, so every element in it has order dividing n which means $n\Lambda \subset \mathcal{M}$. THe indices work out becuase $[\mathcal{M} : n\Lambda] = [\Lambda : n\Lambda]/[\mathcal{M} : \Lambda] = n^2/n = n$. Similarly, if $n\Lambda \subset \mathcal{M}$, $[\mathcal{M} : n\Lambda] = n$, then by the above logic $n\mathcal{M} \subset n\Lambda$ so $\mathcal{M} \subset \Lambda$ and the indices work out as before.

We now investigate the structure of the space of cusp forms under all the $T(n)$. We know that the cusp forms, which we will refer to S, form a finite dimensional vector space, that the $T(n)$ are commuting linear operaters and that the $T(n)$ are self adjoint with respect to $<, >$ for $(N, n) = 1$. Now, it is known that any linear operater A gives rise to a canonical decomposition of $S = \bigoplus_\Lambda S_\Lambda$ where $S_\Lambda = \bigcup_n \mathrm{Ker}((A - \Lambda)^n)$. Moreover, we claim that if B commutes with A, then B preserves the S_Λ. This is because $(A - \Lambda)^n Bv = 0B(A - \Lambda)^n v = 0$. Proceeding inductively, we get that S breaks down into a direct sum of spaces on which, for each n, there is an a_n such that $T(n) - a_n$ is nilpotent.

For $(n, N) = 1$, we have moreover that $T(n)$ is self adjoint and hence diagonalizable, so we actually have $T(n) = a_n$ on each subspace. For general n, we don't know that, but we do knwo that $T(n) - a_n$ has a kernel and we can show that the other $T(m)$ oreserve the kernel. (Because if $(T(n) - a_n)v = 0$ then $(T(n)-a_n)T(m)v = T(m)(T(n)-a_n)v = 0$.) So there is some nonzero subsace on which we have $T(n) = a_n$. As we showed that the a_n determine the coefficents of the q-series, this space is one dimensional. Thus, we know that there will be eigenforms.

We now will investigate, in the special case of weight 2 forms, the relation between the eigen forms found above and the cohomolgy of the modular curve. Recall that weight 2 cusp forms are equivalent to holomorphic differential forms on the modular curve. It is standard from the theory of Riemann surfaces that these form a complex vector space of dimension g, where g is the genus of the curve, and that the integral cohomology of the cruve has a natural embedding in this space as a discrete lattice of rank $2g$.

The Hecke operaters act on formal sums of points on the modular curve; this can easily be seen to induce an action on the homology of the curve. (Given any chain in the curve, applying the Hecke operater to it pointwise gives a formal sum of chains, it is easy to see this commutes with boundary maps.) By duality we also have a map on cohomolgy. We thus have

$$\begin{array}{ccc} \mathbf{Z}^{2g} & \overset{T(n)}{\Rightarrow} & S_2 \\ \Downarrow & & \Downarrow \\ \mathbf{Z}^{2g} & \overset{T(n)}{\Rightarrow} & S_2 \end{array}$$

and this is easily seen to commute. Thus, in a basis given by generaters for H^1, all the $T(n)$ are given by matrices with integer entries.

Now, let f be an eigenform for all the $T(n)$, with sequence of eigenvalues a_n. As the a_n aer eigenvalues of operaters that can be written as integer matrices, they are algebraic integers. Moreoevr, if $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, then we must also have that there is an eigenform with sequence of eigenvalues $\sigma(a_n)$. Now, S is a finite dimensional space so there are only finitely many possible distinct sequences of the form $\sigma(a_n)$, meaning that all the a_n lie in some finite extension of $\mathbf{Q}$.

Now, $f = \sum a_n q^n$ be a normalized eigenform and let K be the normal closure of the number field generated by the a_i, the above shows K is finite. Let $G = \mathrm{Gal}(K/\mathbf{Q})$ and let $V = \mathrm{span}_{\sigma\in K}\sigma(f)$ where $\sigma(f) = \sum \sigma(a_n)q^n$. We claim that V has a basis which lies in $H^1(\mathbf{Q})$. Proof:

$$V = \bigcap_n \mathrm{span}_{\sigma\in G}\{f|T(n)f = \sigma(a_n)F\}.$$

It is enough to show that each space in the intersection has a basis of the claimed form. But

$$\mathrm{span}_{\sigma\in G}\{f|T(n)f = \sigma(a_n)F\} = \ker(\prod_{\sigma\in G}(T(n) - \sigma(a_n)).$$

The operater on the right is a polynomial in $T(n)$ with integer coefficents and $T(n)$ acts on $H^1(\mathbf{Q})$, so the operater takes $H^1(\mathbf{Q})$ to itself and thus has a kernel with basis in $H^1(\mathbf{Q})$.

Since $H^1(\mathbf{Q}) = \mathbf{Q}\otimes H^1(\mathbf{Z})$, we have that $H^1(\mathbf{Z})\cap V$ is a discrete lattice of the same rank as the dimension of V over $\mathbf{R}$, so $V/(V\cap H^{\mathbf{Z}})$ is an abelian variety. At the moment, this seems like a fairly arbitrary object of study, but it will turn out that in fact this abelian variety has number theoretic properties which are tightly bound to the a_n.