On Hecke's decomposition of the regular differentials on the modular curve of prime level

Benedict H. Gross

July 12, 2016

Contents

1 Introduction

In a series of papers [13, 14, 15, 16], Erich Hecke obtained the decomposition of the vector space of regular differentials (or in the language of the day, "Integrale 1. Gattung") on the modular curve $\Gamma(p)\backslash\mathfrak{H}^*$ of prime level p, under the action of the finite group $G = \Gamma(1)/\Gamma(p) = \mathrm{SL}_2(p)/\langle\pm 1\rangle$. Hecke's methods combined the geometric study of the curve with some explicit information contained in the character table of G. This table had been computed by Frobenius [6] in the first paper ever written on group characters, and Hecke's decomposition of the space of regular differentials is one of the first applications of character theory (outside of the study of finite groups). It is also one of the first constructions of linear representations using cohomology. His ideas were immediately extended by Chevalley and Weil to finite group actions on the regular differentials of complex curves [2, Aus einem Briefe an E. Hecke], [29].

When $p \equiv 3 \pmod 4$ and $p > 3$ Hecke described an invariant subspace of differentials of dimension $h.(p-1)/2$, where $h = h(-p)$ is the class number of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-p})$. The group acts on this subspace by h copies of W, one of the two irreducible representations of G of dimension $(p-1)/2$. This subspace is spanned by weighted binary theta series, and Hecke identified the periods of these differentials as the periods of certain elliptic curves with complex multiplication by K. Shimura reconsidered Hecke's argument, adding several ideas of his own [26] [27]. He realized the associated elliptic curves as factors of the Jacobian of the modular curve $X_0(p^2)$, by defining a simple factor $B(p)$ of the Jacobian with real multiplication over $\mathbb{Q}$, which decomposes as a product of h elliptic curves with complex multiplication by K over $\overline{\mathbb{Q}}$. In my PhD thesis [9], I described certain remarkable elliptic curves $A(p)$ with complex multiplicaation over their field of moduli and showed how the abelian variety $B(p)$ decomposes over the Hilbert class field H of K as the product of the h conjugate, isogenous elliptic curves $A(p)^\sigma$. Hida [17] developed Shimura's ideas in a different direction, studying abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves over totally real fields.

In this paper, I will begine by reviewing Hecke's main results. I will prove them using the character theory of G, the Lefshetz fixed point formula [19] (which dates from approximately the same period as Hecke's work), and the holomorphic analog of the fixed point formula (which was later generalized by Eichler [5] in this context). The general line argument is similar to that in Hecke's original papers. I will also give an explanation for the mutilplicity h of the irreducible G-module W occuring in Hecke's invariant subspace, using the algebra generated by the Hecke operators at the primes ℓ away from p, and will reinterpret that result using the language of automorphic representations. I will end with a summary of what we now know about the arithmetic of the abelian varieties $B(p)$ over $\mathbb{Q}$.

2 Representations of $G = \mathrm{SL}_2(p)/\langle \pm 1 \rangle$

Let p be a prime with $p > 3$, and let G be the finite group $\mathrm{SL}_2(p)/\langle \pm 1 \rangle$. The group G is simple of order $p(p^2-1)/2$. Every non-trivial element in G is either contained in a split torus $S = \langle s^a \rangle$, which is cyclic of order $(p-1)/2$, a non-split torus $T = \langle t^b \rangle$, which is cyclic of order $(p+1)/2$, or a unipotent subgroup $U = \langle u^c \rangle$, which is cyclic of order p. Since these orders are relatively prime, the type of subgroup containing a non-trivial element is unique. The normalizers of these subgroups $N(S) = S.2$, $N(T) = T.2$, and $N(U) = U.S$ are maximal subgroups of G.

Every semi-simple class is conjugate to its inverse, but not to any other element in the cyclic group it generates. Hence, for every divisor $d > 2$ of $(p-1)/2$ or $(p+1)/2$, there are $\phi(d)/2$ conjugacy classes of order d in G. When $d = 2$ or $d = 3$, there is a unique conjugacy class of order d.

There are two unipotent conjugacy classes of order p, which are represented by the matrices

$$u = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}. \tag{1}$$

$$v = u^e = \begin{bmatrix} 1 & e \\ 0 & 1 \end{bmatrix}. \tag{2}$$

where e is a non-square $(\mathrm{mod\ p})$. The powers u^{a^2} are conjugate to u and the powers v^{a^2} are conjugate to v.

When $p \equiv 3 \pmod 4$, we may take $c = -1$. Hence $v = u^{-1}$ is **not** conjugate to u in this case, and the two conjugacy classe u and v are not real, in the sense of [23]. All of the semi-simple conjugacy classes are real, and when $p \equiv 1 \pmod 4$, all of the conjugacy classes are real.

The characters of the irreducible, complex representations of G are given explicitly in [6] and repeated in [14]. The corresponding representations are constructed in Lecture 5 of [7]. Two of the characters are easy to describe. The character of the trivial representation takes the value 1 on all conjugacy classes. The Steinberg representation St has dimension p and gives the regular representation when restricted to a unipotent subgroup U. Its restriction to a split torus S is two copies of the regular representation plus the trivial representation, and its restriction to a non-split torus T is two copies of the regular representation minus the trivial representation. Hence its character is given by

$$\chi(1) = p \quad \chi(u^c) = 0 \quad \chi(s^a) = 1 \quad \chi(t^b) = -1.$$

The remaining types of irreducible representations are the principal series of dimension $(p+1)$, corresponding to non-trivial characters α of the split torus S up to inversion, and the discrete series of dimension $(p-1)$, corresponding to non-trivial characters β of the non-split torus T up to inversion. The restriction of a principal series to a non-split torus T is two copies of the regular representation, its restriction to a split torus S is two copies of the regular representation plus the characters α and α^{-1}, and its restriction to a unipotent subgroup U is the regular representation plus the trivial character. The restriction of a discrete series to a split torus S is two copies of the regular representation, its restriction

to a non-split torus T is two copies of the regular representation minus the characters β and β^{-1}, and its restriction to a unipotent subgroup U is the regular representation minus the trivial representation.

When $p \equiv 1 \pmod 4$ and $\alpha = \alpha^{-1}$ is quadratic, the corresponding principal series representation is not irreducible, but decomposes into two irreducible pieces W and W' of dimensions $(p+1)/2$. The characters of W and W' take values in the real quadratic field $\mathbb{Q}(\sqrt{p})$ and are conjugate.

When $p \equiv 3 \pmod 4$ and $\beta = \beta^{-1}$ is quadratic, the corresponding discrete series representation is not irreducible, but decomposes into two irreducible pieces W and W' of dimensions $(p-1)/2$, whose characters take values in the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ and are conjugate. (They are also interchanged by the non-trivial outer automorphism of G, given by conjugation by $\mathrm{PGL}_2(p)$, so are algebraically indistinguishable.) We follow Hecke and use the following convention in the complex numbers to distinguish them. Let $\zeta = e^{2\pi i/p}$ and let $\sqrt{-p}$ be the square root of $-p$ in $\mathbb{C}$ with positive imaginary part. Then the character χ of W is given by the following formula

$$\chi(1) = (p-1)/2 \quad \chi(s^a) = 0 \quad \chi(t^b) = (-1)^b$$

$$\chi(u) = \sum_{a \in QR} \zeta^a = (-1 + \sqrt{-p})/2$$

$$\chi(v) = \sum_{b \in NR} \zeta^b = (-1 - \sqrt{-p})/2$$

Here the sum in $\chi(u)$ is taken over the quadratic residues modulo p and the sum in $\chi(v)$ is taken over the non-residues. The character of W' is the complex conjugate of the character of W, so W' is isomorphic to the dual of W. All of the remaining irreducible characters of G take real values, so are self-dual.

When $p \equiv 1 \pmod 4$, all of the conjugacy classes in G are real and all of the irreducible characters take real values. In general, whenever an irreducible character of G takes values in $\mathbb{R}$, Hecke proved that the corresponding representation of G can be realized over $\mathbb{R}$ [16], so the duality is symmetric.

3 Regular differentials on the Riemann surface $PX(p)^+$

Let p be a prime with $p > 3$, and define the subgroup $\Gamma(p)$ of $\mathrm{SL}_2(\mathbb{Z})$ as the kernel of the homomorphism to $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. This homomorphism is surjective, as $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is generated by its unipotent elements. Since $\Gamma(p)$ does not contain the central element $-I$ in $\mathrm{SL}_2(\mathbb{Z})$, the following sequence remains exact:

$$1 \to \Gamma(p) \to \mathrm{SL}_2(\mathbb{Z})/\langle \pm 1 \rangle \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\langle \pm 1 \rangle \to 1.$$

The modular group $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})/\langle \pm 1 \rangle$ acts faithfully on the upper half-plane $\mathfrak{H}$ and on the projective line $\mathbb{P}^1(\mathbb{Q})$ by fractional linear transformations. Let $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$. The two orbit spaces

$$X(1) = \Gamma(1)\backslash\mathfrak{H}^* \quad X = PX(p)^+ = \Gamma(p)\backslash\mathfrak{H}^*$$

have the structure of connected, compact Riemann surfaces [25, Ch 1] and the map

$$X \to X(1)$$

is a covering with Galois group $G = \mathrm{SL}_2(p)/\langle \pm 1 \rangle$. (We use the notation $PX(p)^+$ as this will be a single geometric component of a Shimura variety $PX(p)$ (associated to the group PGL_2 and a specific open compact subgroup of its finite adèlic points) which we will define later in the text.)

The Riemann surface $X(1)$ has genus zero; a specific isomorphism with the projective line is given by the modular function

$$j(\tau) = 1/q + 744 + 196884q + \ldots \quad q = e^{2\pi i \tau}.$$

Using the Riemann-Hurwitz formula, one can show that the Riemann surface $X = X(p)^+$ has genus [25]

$$g = (p^2 - 1)(p - 6)/24 + 1.$$

This is the dimension of the complex vector space of holomorphic differentials

$$V = H^0(X, \Omega^1)$$

on X, which affords a complex linear representation of the group $G = \mathrm{SL}_2(p)/\langle \pm 1 \rangle$.

The problem which Hecke considered was to decompose the representation of the group G on V into irreducible representations. Since the representation theory of G over $\mathbb{C}$ is semi-simple, one knows from the general theory that

$$V = \sum m(U).U$$

where the sum is taken over the irreducible representations U of G, and $m_U \geq 0$ is the multiplicity of the representation U in V. Equivalently, $m(U)$ is the dimension of the complex vector space $\mathrm{Hom}_G(U, V)$. Since Frobenius had identified the irreducible characters, and eventually the irreducible representations U, the problem remaining was to determine the non-negative integers $m(U)$.

For example, in the simplest case when $p = 7$, the curve $PX(7)^+$ has genus 3 and is isomorphic to the Klein quartic with equation $xy^3 + yz^3 + zx^3 = 0$ in $\mathbb{P}^2$. In this case, Hecke shows that $m(W) = 1$, for W the distinguished representation of dimension $3 = (7-1)/2$ of G described above, and $m(U) = 0$ for all other irreducible representations. When $p = 11$ the curve $PX(11)^+$ has genus 26, in this case, Hecke shows that the multiplicity $m(U)$ is 1 for $U = W$ of dimension 5, the Steinberg representation U of dimension 11, and the discrete series representation U of dimension 10 corresponding to a cubic character β of T. We have $m(U) = 0$ for all other irreducible representations U of G.

By Serre's duality theorem, the complex vector space

$$H^1(X, \mathscr{O})$$

affords the dual representation $V^\vee = \sum m(U).U^\vee$ of G. Hence the multiplicity of U in the representation $H^1(X, \mathscr{O})$ of G on cohomology is equal to the integer $m(U^\vee)$. Since we have an exact sequence of G-modules

$$1 \to H^0(X, \Omega^1) \to H^1(X, \mathbb{C}) \to H^1(X, \mathscr{O}) \to 1,$$

we conclude that the multiplicity of the irreducible representation U in the deRham cohomology $H^1(X, \mathbb{C})$ is equal to

$$m(U) + m(U^\vee).$$

Since integration over cycles gives a canonical isomorphism from the deRham cohomology to the singular cohomology of X with complex coefficients, this is also the multiplicity of U in the representation on singular cohomology.

4 Using the Lefschetz fixed point formula

We can determine the trace of any non-trivial element g in G on the alternating sum of singular cohomology using the Lefschetz fixed point formula:

$$\#Fix(g) = \mathrm{Tr}(g|H^0(X)) - \mathrm{Tr}(g|H^1(X)) + \mathrm{Tr}(g|H^2(X)).$$

Since the trace of g on $H^0(X)$ and $H^2(X)$ are both equal to 1, this gives the simple formula:

$$\mathrm{Tr}(g|H^1(X)) - 2 = \#Fix(g).$$

The only non-trivial classes in G which fix points in X are the classes of orders 2, 3, and p, as these elements generate the cyclic inertia subgroups $C(2)$, $C(3)$ and $C(p)$ of the elliptic points of orders 2 and 3 (corresponding to the moduli of elliptic curves with additional automorphisms) and the cusps (corresponding to the moduli of degenerate elliptic curves). Since on the level 1 curve $X(1)$ there is a unique elliptic point of order 2 (corresponding to the point i in the upper half plane), a unique elliptic point of order 3 (correspdonding to the point ρ in the upper half plane) and a unique cusp, the group G permutes the fixed points of a given type transitively. The total G-set of fixed points of each type is therefore identified with the coset space $G/C(2)$, $G/C(3)$, and $G/C(p)$ respectively. This allows us to write the number of fixed points of any such element g as the trace of g on the permutation representation $\mathrm{Ind}_C^G(\mathbb{C})$.

Proposition 3 *Let g be an element of order 2, 3, or p in G, and let C be the cyclic subgroup generated by g. Then the number of fixed points $\#Fix(g)$ of g acting on the curve X is equal to the trace of g on the induced representation* $\mathrm{Ind}_C^G(\mathbb{C})$.

Although we won't need the number of fixed points explicity, we can calculate this number by determining the order of the normalizer $N_G(C)$ of each cyclic subgroup C in G. For the class of order 2, the normalizer of C is the normalizer of a non-split torus, and there are $\#N_G(C)/C = (p+1)/2$ fixed points. For the class of order 3, the normaliser of C is either the nomalizer of a split torus or the nomalizer of a non-split torus, depending on whether $p \equiv \pm 1 \pmod 3$, and there are $\#N(C)/C = (p-1)/3$ or $\#N(C)/C = (p+1)/3$ fixed points. For the class of order p the normalizer of C is the Borel subgroup and there are $\#N(C)/C = (p-1)/2$ fixed points.

This geometric data, together with the genus of X, determines the trace of every element in G on $H^1(X)$. Using this, and the fact that the isomorphism class of a virtual complex representation of G is determined by its character, we can determine the isomorphism class of $H^1(X)$.

Theorem 4.1 *The virtual representations of G*

$$H^1(X) - 2.\mathbb{C}$$

$$\mathrm{Ind}_1^G(\mathbb{C}) - \mathrm{Ind}_{C(2)}^G(\mathbb{C}) - \mathrm{Ind}_{C(3)}^G(\mathbb{C}) - \mathrm{Ind}_{C(p)}^G(\mathbb{C})$$

are isomorphic.

Indeed, the identity element has trace equal to $(2g-2)$ on the first representation, and has trace

$$\#G(1 - 1/2 - 1/3 - 1/p)$$

on the second representation. These integers are equal, by the Riemann-Hurwitz formula [25, §1.5]. A non-trivial class whose order is not equal to 2, 3, or p has trace zero on both representations. The classes of orders 2, 3, and p have non-trivial trace on exactly one of the induced representations, where its trace is given by the above Proposition.

Corollary 4 *The multiplicity of the trivial representation of G in $H^1(X)$ is zero. The multiplicity of a non-trivial irreducible representation U in $H^1(X)$ is given by the formula*

$$\dim U - \dim U^{C(2)} - \dim U^{C(3)} - \dim U^{C(p)}$$

Indeed, for any irreducible representation U, the multiplicity of U in the permuation representation $\mathrm{Ind}_C^G(\mathbb{C})$ is equal to the dimension U^C of the C invariant subspace, by Frobenius reciprocity[23, Ch].

Since the multiplicity of U in $H^1(X)$ is equal to $m(U)+m(U^\vee)$, with $m(U)$ the multiplicity of U in the representation on the space of regular differentials $H^0(X,\Omega^1)$, we obtain the preliminary multiplicty formulae:

$$m(\mathbb{C}) = 0,$$

and for U irreducible and non-trivial

$$m(U) + m(U^\vee) = \dim U - \dim U^{C(2)} - \dim U^{C(3)} - \dim U^{C(p)}.$$

5 The real case

When the character of the irreducible representation U of G is real, the representation U is isomorphic to its dual representation $U^\vee$ and $m(U) = m(U^\vee)$ in the space of regular differentials. This occurs for all irreducible representations of G when $p \equiv 1 \pmod 4$, and for all irreducible representations except for the two representations W and W' of dimension $(p-1)/2$ when $p \equiv 3 \pmod 4$. So in all but these two cases, we have obtained a final form for the multiplicity of an irreducible, non-trivial representation U in the space of regular differentials:

$$2.m(U) = \dim U - \dim U^{C(2)} - \dim U^{C(3)} - \dim U^{C(p)}.$$

In particular, the right hand side of this identity must be an even integer.

As an example, let us work out the multiplicity of the Steinberg representation $U = St$. Its dimension of the Steinberg representation is p, and the trace of g_2 is equal to 1 when $p \equiv 1 \pmod 4$ and is equal to -1 when $p \equiv 3 \pmod 4$. Hence the dimension of $U^{C(2)}$ is equal to $(p+1)/2$ when $p \equiv 1 \pmod 4$ and is equal to $(p-1)/2$ when $p \equiv 3 \pmod 4$. Similarly, the dimension of $U^{C(3)}$ is equal to $(p+2)/3$ when $p \equiv 1 \pmod 3$ and is equal to $(p-2)/3$ when $p \equiv 2 \pmod 3$. Finally, the dimension of $U^{C(p)}$ is equal to 1 in all cases. Putting these dimensions into the above formula, we find that the multiplicity of the Steinberg representation in the space of regular differentials on $X = PX(p)^+$ is given by the formula

$$\begin{aligned} m(St) &= (p-13)/12 \quad p \equiv 1 \pmod{12} \\ m(St) &= (p-5)/12 \quad p \equiv 5 \pmod{12} \\ m(St) &= (p-7)/12 \quad p \equiv 7 \pmod{12} \\ m(St) &= (p+1)/12 \quad p \equiv 11 \pmod{12} \end{aligned}$$

6 The complex case

For the two representations W and W' of dimension $(p-1)/2$ when $p \equiv 3 \pmod 4$ and $p > 3$, we only obtain the sum

$$m(W) + m(W^\vee) = \dim W - \dim W^{C(2)} - \dim W^{C(3)} - \dim W^{C(p)}$$

from the multiplicity of W in $H^1(X, \mathbb{C})$.

From the character of W tabulated by Frobenius, we find that the dimension of the space of $C(2)$ invariants in W is $(p+1)/4$ when $p \equiv 3 \pmod 8$ and is equal to $(p-3)/4$ when $p \equiv 7 \pmod 8$. The dimension of the space of $C(3)$ invariants in W is equal to $(p-1)/6$ when $p \equiv 1 \pmod 3$ and is equal to $(p-5)/6$ when $p \equiv 2 \pmod 3$. Finally, there are no non-trivial $C(p)$ invariants in W. Hence we find that

$$\begin{aligned} m(W) + m(W^\vee) &= (p+5)/12 \quad p \equiv 7 \pmod{24} \\ m(W) + m(W^\vee) &= (p+1)/12 \quad p \equiv 11 \pmod{24} \\ m(W) + m(W^\vee) &= (p-7)/12 \quad p \equiv 19 \pmod{24} \\ m(W) + m(W^\vee) &= (p+13)/12 \quad p \equiv 23 \pmod{24} \end{aligned}$$

Note that $m(W) + m(W^\vee)$ is always **odd**, so $m(W) \neq m(W^\vee)$.

Hecke completed the determination of $m(W)$ by finding an amazing formula for the difference of multiplicities (which must also be odd).

Theorem 6.1 *The difference $m(W) - m(W^\vee) = h(-p)$, where $h(-p)$ is the class number of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-p})$.*

There are a few cases where one finds that $m(W) + m(W') = m(W) - m(W')$, so $m(W') = 0$ and $m(W) = h(-p)$. These are $p = 7, 11, 19$ where $h(-p) = 1$, $p = 23, 31$ where $h(-p) = 3$, $p = 47$ where $h(-p) = 5$, and $p = 71$ where $h(-p) = 7$ [14]. In all other cases, both W and W' appear with positive multiplicity in V.

In Hecke's argument, the class number of K appears via Dirichlet's class number formula

$$h(-p) = \sum_{a=1}^{p-1} \epsilon(a)(-a/p).$$

Here ϵ is the non-trivial quadratic character of $(\mathbb{Z}/p\mathbb{Z})^*$. Our proof of the theorem also uses this class number formula. Shimura found a different argument [27], which gives a new proof of Dirichlet's class number formula independent of the theory of L-functions.

The character χ of the virtual representation $W - W^\vee$ of G is supported on the non-trivial unipotent elements. It takes the value $\sqrt{-p}$ on the elements conjugate to u in G and the complex conjugate value $-\sqrt{-p}$ on the elements conjugate to v in G. Each unipotent class contains $(p^2-1)/2$ elements. Hence we find [23]

$$m(W) - m(W^\vee) = \langle \chi_V, \chi \rangle = (\mathrm{Tr}(u|V) - \mathrm{Tr}(v|V))/\sqrt{-p}.$$

The trace of u on the representation $V = H^0(X, \Omega^1)$ is an algebraic integer in the imaginary quadratic field K. Its complex conjugate is the trace of u on the dual representation $V^\vee \cong H^1(X, \mathscr{O})$, and we can calculate the latter trace using the holomorphic trace formula:

$$\mathrm{Tr}(g|H^0(X, \mathscr{O})) - \mathrm{Tr}(g|H^1(X, \mathscr{O})) = \sum_{x \in Fix(g)} 1/(1 - dg_x)$$

Since the trace of u on $H^0(X, \mathscr{O})$ is equal to 1, this gives a formula for the trace of u on $H^1(X, \mathscr{O})$ as a sum of local terms, taken over the $(p-1)/2$ cusps fixed by u. It's complex conjugate gives the trace of u on $V = H^1(X, \Omega^1)$.

The $(p-1)/2$ cusps fixed by u and v correspond to the points a/p on the rational projective line, with $a = 1, 2, \ldots, (p-1)/2$. (The orbit of a/p under $\Gamma(p)$ is equal to the orbit of $-a/p$.) At the fixed cusp $x = a/p$, the differential du_x is given by ζ^{a^2}, with $\zeta = e^{2\pi i/p}$. Hence we obtain the formula

$$\mathrm{Tr}(u|H^1(X, \mathscr{O})) = 1 - \sum_{a=1}^{(p-1)/2} (1/1 - \zeta^{a^2}) = 1 - \mathrm{Tr}(1/(1-\zeta)$$

where the trace is taken from the cyclotomic subfield $\mathbb{Q}(\zeta)$ to its quadratic subfield $K = \mathbb{Q}(\sqrt{-p})$.

Proposition 5 *Let p be a prime with $p > 3$ and $p \equiv 3 \pmod 4$ and let $\zeta = e^{2\pi i/p}$ in $\mathbb{C}$. Then the trace of the element $1/(1-\zeta)$ from the cyclotomic field $\mathbb{Q}(\zeta)$ in $\mathbb{C}$ to its quadratic subfield $K = \mathbb{Q}(\sqrt{-p})$ is equal to the algebraic integer $((p-1)/2 + h(-p)\sqrt{-p})/2$, where $h(-p)$ is the class number of K and $\sqrt{-p}$ has positive imaginary part in $\mathbb{C}$.*

An elegant proof of this result was shown to me by Noam Elkies. First note that

$$(1-\zeta).(\zeta+2\zeta^2+3\zeta^3+\ldots+(p-1)\zeta^{p-1})=\zeta+\zeta^2+\ldots+\zeta^p-p\zeta^p=-p$$

Hence

$$1/(1-\zeta)=(-1/p).(\zeta+2\zeta^2+3\zeta^3+\ldots+(p-1)\zeta^{p-1})$$

The trace of each ζ^{QR} to K is equal to $(-1+\sqrt{-p})/2$ and the trace of each ζ^{NR} to K is equal to $(-1-\sqrt{-p})/2$, by Gauss's calculation of the quadratic Gauss sum. Hence the trace of $1/(1-\zeta)$ to K has the form $(A+B\sqrt{-p})/2$ with

$$A=(p-1)/2 \qquad B=\sum_{a=1}^{(p-1)}\epsilon(a)(-a/p).$$

The latter sum is equal to $h(-p)$ by Dirichlet's class number formula.

Collecting our formulae, we have shown that

$$\mathrm{Tr}(u|V)=\overline{\mathrm{Tr}(u|H^1(X,\mathscr{O})}=1-\overline{\mathrm{Tr}(1/(1-\zeta)}=((1-p)/2+h(-p)\sqrt{-p})/2.$$

The trace of v on V is the complex conjugate ot the trace of u, so

$$m(W)-m(W^\vee)=(\mathrm{Tr}(u|V)-\mathrm{Tr}(v|V))/\sqrt{-p}=h(-p).$$

This completes the proof of the theorem.

Since their multiplicities $m(W)$ and $m(W')$ in the representation of G on $V=H^0(X,\Omega^1)$ are non-negative and satisfy

$$m(W)-m(W')=h(-p),$$

the multiplicity of W in V is greater than or equal to $h(-p)$. Hecke explained this by exhibiting an explicit G-invariant subspace V_0 in V of dimension $h(-p).(p-1)/2$ on which the group acts by $h(-p)$ copies of the representation W [13].

If we identify the space V of regular differentials on the curve X with the space of cusp forms of weight 2 for the congruence subgroup $\Gamma(p)$, then Hecke's subspace V_0 is spanned by weighted binary theta series, associated to the Euclidean lattices of rank 2 and discriminant $-p$. A typical modular form in this subspace has the Fourier expansion

$$\theta(r,\tau)=\sum\mu.e^{2\pi i\mu\overline{\mu}\tau/p}=\sum\mu q^{N(\mu)/p}$$

where the sum is taken over all elements μ in the ring of integers of $K=\mathbb{Q}(\sqrt{-p})$ which are congruent to a fixed non-zero class r modulo $(\sqrt{-p})$. One can also sum over all μ in an ideal $\mathfrak{a}$ with non-trivial class, replacing the term $N(\mu)$ in the exponent by $N(\mu)/N(\mathfrak{a})$. We will return to this subspace after introducing the curve $PX(p)$ over $\mathbb{Q}$.

7 The Shimura variety $PX(p)$

Henceforth in this paper, we let G be the reductive group scheme PGL_2 over $\mathbb{Z}$ and let p be an odd prime. The group $\mathrm{SL}_2(p)/\langle\pm 1\rangle$ that we have previously called by this letter is a subgroup of index two in the points $G(p) = \mathrm{PGL}_2(p)$ of G over the field of p elements.

Let $h : \mathbb{C}^*/\mathbb{R}^* \to G(\mathbb{R})$ be an inclusion onto a non-split torus. Then the conjugacy class of the homomorphism h can be identified with the union $\mathfrak{H}^{\pm}$ of the upper and lower half planes in $\mathbb{C}$. For a prime $\ell \neq p$ let $K_\ell = G(\mathbb{Z}_\ell) = \mathrm{PGL}_2(\mathbb{Z}_\ell)$ be a hyperspecial maximal compact subgroup of $G(\mathbb{Q}_\ell)$. At the prime p, we let K_1 be the first congruence subgroup of $G(\mathbb{Z}_p)$, so $G(\mathbb{Z}_p)/K_1 = \mathrm{PGL}_2(p)$. Let $\mathbb{A}_f$ be the ring of finite adèles of $\mathbb{Q}$. Then the orbit space

$$S(\mathbb{C}) \;=\; G(\mathbb{Q})\backslash\mathfrak{H}^{\pm} \times G(\mathbb{A}_f)/\prod K_\ell \times K_1$$

has the structure of a Riemann surface with two connected components.

Indeed, by the strong approximation theorem for SL_2 and the fact that $\mathbb{Q}$ has class number 1, we have

$$G(\mathbb{A}_f) = G(\mathbb{Q}).\prod G(\mathbb{Z}_\ell) \times G(\mathbb{Z}_p)$$

The intersection of $G(\mathbb{Q})$ and $\prod G(\mathbb{Z}_\ell) \times G(\mathbb{Z}_p)$ is the group $G(\mathbb{Z}) = \mathrm{PGL}_2(\mathbb{Z})$.

When $p \equiv 3 \pmod 4$, the homomorphism $\mathrm{PGL}_2(\mathbb{Z}) \to \mathrm{PGL}_2(p)$ is surjective, and we still have only one double coset: $G(\mathbb{A}_f) = G(\mathbb{Q}).\prod G(Z_\ell) \times K_1$. The intersection is now the subgroup $\Gamma(p)$ of $\mathrm{SL}_2(\mathbb{Z})/\langle\pm 1\rangle$, and $S(\mathbb{C})$ is isomorphic to the orbit space $\Gamma(p)\backslash\mathfrak{H}^{\pm}$ (which can be compactified by the addition of a finite number of cusps). In this case, the two components are anti-isomorphic over $\mathbb{C}$.

When $p \equiv 1 \pmod 4$, the homomorphism $\mathrm{PGL}_2(\mathbb{Z}) \to \mathrm{PGL}_2(p)$ is not surjective, but has image the subgroup $\mathrm{SL}_2(p)/\langle\pm 1\rangle$ where the determinant is a square modulo p. In this case we have two double cosets of $G(\mathbb{Q})$ and $\prod G(\mathbb{Z}_\ell) \times K_1$ in $G(\mathbb{A}_f)$, with each discrete subgroup Γ in the intersection containing elements of determinant ± 1. Here each component $\Gamma\backslash\mathfrak{H}^{\pm}$ of $S(\mathbb{C})$ has an anti-holomorphic involution and descends to $\mathbb{R}$.

The theory of canonical models of Shimura varieites shows that the algebraic curve S and its compactification descend to $\mathbb{Q}$ as the coarse moduli space $PX(p)$ of (generalized) elliptic curves with a full level p structure, up to scaling [3] [4]. We use the notation $PX(p)$ as $X(p)$ is the moduli space of (generalized) elliptic curves with a full level p structure. The curve $X(p)$ is defined over $\mathbb{Q}$ and has an action of the group $\mathrm{GL}_2(p)/\langle\pm 1\rangle$ [10]. It is not geometrically connected: the $(p-1)$ geometric components of $X(p)$ are defined over the p^{th} cyclotomic field $\mathbb{Q}(\zeta)$ The curve $PX(p)$ is the quotient of $X(p)$ by the central subgroup $(\mathbb{Z}/p\mathbb{Z})^*/\langle\pm 1\rangle$ of $\mathrm{GL}_2(p)/\langle\pm 1\rangle$, and the quotient group $\mathrm{PGL}_2(p)$ acts on $PX(p)$ over $\mathbb{Q}$. The two geometric components of $X(p)$ are defined over the real quadratic field $\mathbb{Q}(\sqrt{p})$ when $p \equiv 1 \pmod 4$ and over the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-p})$ when $p \equiv 3 \pmod 4$. In the latter case, which is of primary interest to us, $PX(p)(\mathbb{C})$ is the compactification of the quotient $\Gamma(p)\backslash\mathfrak{H}^{\pm}$, and complex conjugation gives an anti-isomorphism from the component $X = \Gamma(p)\backslash\mathfrak{H}^*$ to the component Y uniformized by the lower half plane. Hence the action of $\mathrm{SL}_2(p)/\langle\pm 1\rangle$ on the regular differentials of Y is gives the dual of the module studied by Hecke on the regular differentions of X.

Since the group $\mathrm{PGL}_2(p)$ acts on the curve $PX(p)$ over $\mathbb{Q}$, one can ask for the structure of the representation on the $\mathbb{Q}$-vector space $H^0(PX(p), \Omega^1)$. To determine the multiplicities of irreducible represetations, it suffices to do this over $\mathbb{R}$, where all of the irreducible complex representations V of $\mathrm{PGL}_2(p)$ can be defined.

Every irreducible representation U of the subgroup $\mathrm{SL}_2(p)/\langle \pm 1 \rangle$ which is defined over the real numbers extends to $\mathrm{PGL}_2(p)$ in two ways: R and $R \otimes \chi$, where χ is the non-trivial quadratic character of $\mathrm{PGL}_2(p)$ with kernel $\mathrm{SL}_2(p)/\langle \pm 1 \rangle$. The two irreducible representations W and W' of dimensions $(p-1)/2$ of $\mathrm{SL}_2(p)/\langle \pm 1 \rangle$ which cannot be defined over the real numbers combine to give a single irreducible representation R of dimension $(p-1)$ of $\mathrm{PGL}_2(p)$. This representation R is the discrete series corresponding to a character ψ of order 4 of a non-split torus of $\mathrm{PGL}_2(p)$ and can be defined over $\mathbb{Q}$. The restriction of R to the subgroup $\mathrm{SL}_2(p)/\langle \pm 1 \rangle$ decomposes as the direct sum of the conjugate irreducibles $W + W'$ over K.

For any irreducible complex representation U of $\mathrm{SL}_2(p)/\langle \pm 1 \rangle$, let $m(U)$ denote the multiplicity of U in Hecke's module $H^0(X, \Omega^1)$.

Proposition 6 *The multiplicity of an irreducible representation R of $\mathrm{PGL}_2(p)$ over $\mathbb{R}$ in the module $H^0(PX(p), \Omega^1) \otimes \mathbb{R}$ is equal to $m(U)$, if the restriction of R to $\mathrm{SL}_2(p)/\langle \pm 1 \rangle$ is isomorphic to the irreducible representation U, and is equal to $m(W) + m(W')$, if the restriction of R to $\mathrm{SL}_2(p)/\langle \pm 1 \rangle$ is isomorphic to the direct sum $W + W'$ over $\mathbb{C}$.*

In particular, Hecke's distinguished subspace of $H^0(X, \Omega^1)$ of dimension $h.(p-1)/2$ which is spanned by weighted binary theta series gives a distinguished subspace V of dimension $h.(p-1)$ in $H^0(PX(p), \Omega^1)$ over $\mathbb{Q}$. The group $\mathrm{PGL}_2(p)$ acts on the distinguished subspace by $h = h(-p)$ copies of the unique irreducible representation R of dimension $(p-1)$ over $\mathbb{Q}$ which decomposes over K. We will give some explanation for this multiplcity in the next section.

8 An irreducible module for the Hecke algebra

Let ℓ be a prime with $\ell \neq p$. The Hecke operator T_ℓ is defined by a correspondence on the modular curve $PX(p)$ over $\mathbb{Q}$, which maps an elliptic curve E with a level p structure up to scaling to the $(\ell+1)$ elliptic curves E' which are isogenous to E by an isogeny of degree ℓ. Since ℓ is prime to p, and ℓ isogeny maps a level p structure up to scaling on E to a level p structure up to scaling on E'. This correspondence induces an endomorphism of the Jacobian of $PX(p)$, as well as a linear endomorphism of the rational vector space $H^0(PX(p), \Omega^1)$ of regular differentials on $PX(p)$. We denote the linear endomorphism of regular differentials by $T(\ell)$.

The operators T_ℓ for different primes commute with each other, and we let $\mathbb{T}$ be the commutative $\mathbb{Q}$-algebra that they freely generate. The algebra $\mathbb{T}$ acts on the regular differentials through the quotient algebra generated by the $T(\ell)$, and commutes with the action of the group $\mathrm{PGL}_2(p)$. It therefore acts on each isotypic component. We shall see that it also preserves Hecke's distinguished subspace, which lies the the isotypic component where $\mathrm{PGL}_2(p)$ acts through the representation R.

We now define a CM field E, which is an extension of $K = \mathbb{Q}(\sqrt{-p})$ of degree $h(-p)$. Write the class group of K as a direct sum of cyclic groups, and for each summand, let $\mathfrak{a}$ be an ideal prime to p whose class gives the generator of order m. Then $(\mathfrak{a})^m = (\alpha)$ is a principal ideal, with a unique generator α which is a square modulo $(\sqrt{-p})$. Indeed, the two generators of this ideal are α and $-\alpha$, and -1 is not a square modulo p. We obtain the field E from K by adjoining an m^{th} root β of α, for each cyclic summand $\mathbb{Z}/m\mathbb{Z}$ of the class group. For example, if the class group is cyclic and $\mathfrak{a}$ is a generator which is prime to p, then $E = K(\beta)$, where β^h is an element of K^* which generates the ideal $\mathfrak{a}^h$.

Since $h(-p)$ is odd, for every prime ideal $\mathfrak{l}$ of K which is not equal to $(\sqrt{-p})$, there is a unique generator α of $\mathfrak{l}^h$ in K^* which is a square modulo $(\sqrt{-p})$, and a unique element β in E^* with $\beta^h = \alpha$ in K^*. The homomorphism from fractional ideals of K which are prime to p to the multiplicative group E^* which takes $\mathfrak{l}$ to the element $\chi(\mathfrak{l}) = \beta = \beta_{\mathfrak{l}}$ is a Hecke character. Indeed, on principal ideals $\mathfrak{a} = (\alpha)$ with a generator congruent to $1(\mathrm{mod}\ \sqrt{-\mathrm{p}})$, we have $\chi(\mathfrak{a}) = \alpha$. If $\mathbb{A}_K$ denotes the ring of adèles of K, then χ gives rise to a continuous homomorphism

$$\rho : \mathbb{A}_K^* \to E^*$$

which is the identity on the subgroup K^*. The number field E has an involutive automorphism, given by complex conjugation. On the elements β with $\beta^h = \alpha$ a square modulo $(\sqrt{-p})$, the conjugate $\overline{\beta}$ the unique h^{th} root of $\overline{\alpha}$ in E. The homomorphism ρ is equivariant for complex conjugation on K and E, and E is a CM field.

Let E^+ be the totally real subfield of E fixed by complex conjugation, which is an extension of $\mathbb{Q}$ of degree $h(-p)$. For a prime ℓ of $\mathbb{Q}$ which splits in K, we define an element t_ℓ in E^+ as follows. Let $\mathfrak{l}$ be a factor of the ideal (ℓ) in K and let $\beta = \chi(\mathfrak{l})$. Then $t_\ell = \beta + \overline{\beta}$ in E^+. If the prime ℓ of $\mathbb{Q}$ is inert in K, we define $t_\ell = 0$. Then the Euler product with coefficients in E^+

$$L(\chi, s) = \prod_{\ell \neq p} (1 - t_\ell \ell^{-s} + \ell^{1-2s})^{-1} = \sum a_n n^{-s}$$

is equal to the finite part of the L-series of the Hecke character χ.

Theorem 8.1 *The map taking T_ℓ to the elements $\phi(T_\ell) = t_\ell$ in the totally real field E^+ gives a surjective homomorphism of $\mathbb{Q}$-algebras $\phi : \mathbb{T} \to E^+$, which factors through the quotient algebra generated by the linear endomorphisms $T(\ell)$ on the regular differentials on $PX(p)$.*

Let $M(E^+)$ be a vector space over E^+ of dimension 1 (which is a simple $\mathbb{T}$ - module via the homomorphism ϕ). Then Hecke's invariant subspace in $H^0(PX(p), \Omega^1)$ is isomorphic to the simple module $M(E^+) \otimes R$ of dimension $h(-p).(p-1)$ over $\mathbb{Q}$, under the action of $\mathbb{T} \times \mathbb{Q}[\mathrm{PGL}_2(p)]$.

We will prove this result in the two sections, after reviewing the relationship between the regular differentials on the curves $PX(p)$ and $X_0(p^2)$ over $\mathbb{Q}$. Here we note that just as we have an action of the subgroup $\mathrm{SL}_2(p)/\langle \pm 1 \rangle$ of $\mathrm{PGL}_2(p)$ on each component $X^{\pm}$ of $PX(p)$ over $K = \mathbb{Q}(\sqrt{-p})$, we note that the Hecke operator $T(\ell)$ preserves the regular differentials on each component whenever ℓ is a square modulo p. Since the Hecke operators T_ℓ at all primes ℓ which are not squares modulo p act as zero on the module $M(E^+)$ defined above, we find that $M(E^+)$ is also a simple module for the subalgebra of the Hecke algebra that preserves each component of the curve, and Hecke's invariant subspace in the regular differentials on the complex curve $X(p)^+ = \Gamma(p) \backslash \mathfrak{H}^*$ is isomorphic to the simple module $M(E^+) \otimes W$ of dimension $h.(p-1)/2$ over $\mathbb{C}$.

9 The modular curve $X_0(p^2)$ as a quotient of $PX(p)$

In this section, we show how the Hecke module $M(E^+)$ appears (with multiplicity one) in the regular differentials on the modular curve $X_0(p^2)$ over $\mathbb{Q}$. Recall that the curve $X_0(N)$ classifies (generalized) elliptic curves together with a cyclic N-isogeny. [4] The regular differentials on $X_0(N)$ correspond to the cusp forms of weight 2 for the group $\Gamma_0(N)$ with rational Fourier coefficients.

By a theorem of Weil (cf. [24]) the Dirchlet series $\sum a_n n^{-s}$ determined by the Hecke character χ is the L-function of a cusp form $\sum a_n q^n$ of weight 2 for the group $\Gamma_0(p^2)$ with coefficients in the totally real field E^+. Taking the distinct embeddings of E^+ into $\mathbb{R}$, we obtain an $h(-p)$ dimensional subspace of $H^0(X_0(p^2), \Omega^1) \otimes \mathbb{R}$. This subspace descends to $\mathbb{Q}$ and consists of the forms of weight 2 and level p^2 with complex multiplication by $\mathbb{Q}(\sqrt{-p})$. Indeed, by a theorem of Serre [24] this Hecke module is determined by the condition that $T_\ell = 0$ for all primes ℓ which are inert in $\mathbb{Q}(\sqrt{-p})$. This realizes the simple Hecke module $M(E^+)$ in the space of regular differentials on $X_0(p^2)$ over $\mathbb{Q}$. To realize $M(E^+)$ in the regular differentials on $PX(p)$, we need to recognize $X_0(p^2)$ as a quotient of $PX(p)$ over $\mathbb{Q}$, by the action of a split torus in the group $\mathrm{PGL}_2(p)$.

Let T be a split torus in the group $\mathrm{GL}_2(p)$ and let $B = TU$ be a Borel subgroup containing T. These groups act on the curve $X(p)$ over $\mathbb{Q}$, and we let $X(p)/B$ and $X(p)/T$ be the quotient curves. Since both subgroups contain the center Z of $\mathrm{GL}_2(p)$, both curves are also quotients of the curve $X(p)$, by the subgroups (B/Z) and (T/Z) in $\mathrm{PGL}_2(p)$ respectively,and $X(p)/T$ is a cyclic cover of $X(p)/B$ of degree p. Since both subgroups map surjectively to $(\mathbb{Z}/p\mathbb{Z})^*$ under the determinant homomorphism, both of the quotient curves are geometrically connected over $\mathbb{Q}$. We will identify them with the modular curves $X_0(p)$ and $X_0(p^2)$, which classify pairs $E \to E'$ of elliptic curves with a cyclic isogeny of degree p and p^2 respectively. [4]

Since $X(p)$ is the moduli of generalized elliptic curves with a full level structure at p, the quotient curve $X(p)/B$ is the moduli of generalized elliptic curves E with a fixed line C in the p-torsion $E[p]$. Then C is the kernel of a cyclic p-isogeny $\phi : E \to E' = E/C$, which identifies $X(p)/B$ with $X_0(p)$.

To identify $X(p)/T$ with $X_0(p^2)$, we observe that the former curve is the moduli of elliptic curves E with a decomposition of the p-torsion into two lines: $E[p] = C \oplus D$. Let $\phi_C : E \to E/C$ and $\phi_D : E \to E/D$ be the corresponding cyclic isogenies of degree p and let $\phi_C^\vee : E/C \to E$ be the dual isogeny. Consider the composition

$$\phi = \phi_D \circ \phi_C^\vee : E/C \to E/D.$$

This isogeny has degree p^2 but is not equal to multiplication by p, so its kernel is cyclic. The map taking the modular data $(E, E[p] = C \oplus D)$ to the modular data $(\phi : E/C \to E/D)$ gives an isomorphism from the curve $X(p)/T$ to the curve $X_0(p^2)$ over $\mathbb{Q}$.

With these identifications, we obtain the following.

Proposition 7 *The space regular differentials $H^0(X_0(p), \Omega^1)$ on the curve $X_0(p)$ is isomorphic to the subspace of $H^0(PX(p), \Omega^1)$ which is fixed by (B/Z).*

The space of regular differentials $H^0(X_0(p^2), \Omega^1)$ on the curve $X_0(p^2)$ is isomorphic with the subspace of $H^0(PX(p), \Omega^1)$ which is fixed by (T/Z).

In fact, since the action of the group $\mathrm{PGL}_2(p)$ commutes with Hecke correspondences T_ℓ at primes $\ell \neq p$, the isomorphisms above are not just as rational vector spaces, but as $\mathbb{T}$-modules. If we decompose the regular differentials on $PX(p)$ over $\mathbb{R}$ using the (absolutely) irreducible representations U of $\mathrm{PGL}_2(p)$:

$$H^0(PX(p), \Omega^1) \otimes \mathbb{R} \cong \oplus_U U \otimes M(U)$$

where $M(U)$ is a module for $\mathbb{T}$ of dimension $m(U)$ as a real vector space, we have isomorphisms of $\mathbb{T}$-modules

$$H^0(X_0(p), \Omega^1) \otimes \mathbb{R} \cong \oplus_U \dim(U^B) \otimes M(U)$$
$$H^0(X_0(p^2), \Omega^1) \otimes \mathbb{R} \cong \oplus_U \dim(U^T) \otimes M(U)$$

The Steinberg and the trivial representation of $PGL_2(p)$ are the only two representations with $\dim U^B \neq 0$. Since the Steinberg representation S satisfies $\dim S^B = 1$ and the trivial representation $\mathbb{C}$ does not occur in the action on regular differentials of $PX(p)$, the formula obtained for $m(St)$ at the end of §5 gives the genus of the curve $X_0(p)$. (The Steinberg representation St of dimension p of the subgroup $\mathrm{SL}_2(p)/\langle \pm 1 \rangle$ has two extensions to $\mathrm{PGL}_2(p)$: the Steinberg representation S and its ramified twist $S \otimes \chi$. Both have multiplicity $m(St)$ in the regular differentials on $PX(p)$). Similarly, the Hecke module associated to the Steinberg representation S on the curve $PX(p)$ gives the action of the Hecke operators on the regular differentials of $X_0(p)$.

The case of $X_0(p^2)$ is more interesting, as *every* irreducible representation U of $\mathrm{PGL}_2(p)$ has a non-zero fixed vector under the split torus T. In fact, it follows easily from an examination of the character table of $\mathrm{PGL}_2(p)$ that every irreducible representation has $\dim U^T = 1$, except for the Steinberg representation S which has $\dim S^T = 2$. Since every irreducible representation U of $\mathrm{PGL}_2(p)$ has at least one non-zero fixed vector under the split torus, the Hecke modules $M(U)$ which occur in the decomposition $\oplus_U U \otimes M(U)$ of regular differentials on $PX(p)$ must all occur in the decomposition of regular differentials of $X_0(p^2)$: $\oplus_U \dim U^T \otimes M(U)$.

In particular, the Hecke module $M(E^+)$, which we saw occured on the regular differentials of $X_0(p^2)$, occurs in the action of the Hecke algebra $\mathbb{T}$ on the regular differentials of $PX(p)$. Moreover, since the simple Hecke module $M(E^+)$ occurs with multiplicity one on the differentials of the curve $X_0(p^2)$ [1], there is a unique irreducible representation U of $\mathrm{PGL}_2(p)$ (which is not the trivial or the Steinberg representation) such that $U \otimes M(E^+)$ occurs as a simple submodule of the differentials on the curve $PX(p)$. To finish the proof of Theorem 9.1, we need to show that U is isomorphic to R, the unique discrete series associated to a quartic character of the non-split torus, which decomposes as $W \oplus W'$ when restricted to the subgroup $\mathrm{SL}_2(p)/\langle \pm 1 \rangle$. This follows from the fact that Hecke's distinguished subspace of dimension $h.(p-1)$ in $R \otimes M(R)$ contains the forms with complex multiplication by $K = \mathbb{Q}(\sqrt{-p})$. Hence it is isomorphic to $M(E^+) \otimes R$ as claimed.

10 Local components of some automorphic representations of $\mathrm{PGL}_2(\mathbb{A})$

The identification of the simple module $M(E^+) \otimes R$ in the regular differentials on $PX(p)$ over $\mathbb{Q}$ has a nice interpretation in the language of automorphic representations. We present this here.

Recall the Euler product defined by the Hecke character of K:

$$L(\chi, s) = \prod_{\ell \neq p} (1 - t_\ell \ell^{-s} + \ell^{1-2s})^{-1} = \sum a_n n^{-s}.$$

For each real embedding $\iota : E^+ \to \mathbb{R}$, the q-expansion

$$F(q) = \sum_{n \geq 1} \iota(a_n) q^n$$

defines an newform of weight 2 for $\Gamma_0(p^2)$. This newform corresponds to a new vector in an irreducible automorphic representation $\pi = \otimes \pi_v$ of the adèlic group $\mathrm{PGL}_2(\mathbb{A})$ which occurs in the space of cusp forms. The local components π_v are irreducible complex representations of the locally compact groups $\mathrm{PGL}_2(\mathbb{Q}_v)$.

Since $F(q)$ has weight 2, the local component π_∞ is the discrete series for $\mathrm{PGL}_2(\mathbb{R})$ of weight 2 and infinitesimal character ρ. For all $\ell \neq p$ the local component π_ℓ has a vector fixed by the maximal compact subgroup $\mathrm{PGL}_2(\mathbb{Z}_\ell)$. Since it is an unramified representation of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$, its isomorphism class is determined by its Frobenius-Hecke parameter under the Satake isomorphism [11]. If we use the "Hecke nomalization" of this isomorphism, the parameter of π_ℓ is the semi-simple conjugacy class in $\mathrm{GL}_2(\mathbb{C})$ with characteristic polynomial $x^2 - \iota(a_\ell)x + \ell$. The one local representation that is difficult to read off of the classical data is the representation π_p of $\mathrm{PGL}_2(\mathbb{Q}_p)$. This has conductor p^2, so has a vector fixed by the congruence subgroup $\Gamma_0(p^2)$ of $\mathrm{PGL}_2(\mathbb{Z}_p)$.

Since the Langlands parameter of the automorphic representation π is induced from the Hecke character χ of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-p})$ (choosing an embedding $E \to \mathbb{C}$ extending the real embedding $\iota : E^+ \to \mathbb{R}$), the local Langlands parameter of π_p is obtained by inducing the local character χ_p of K_p^*. That character is tamely ramified, and its restriction to the units has order 2. Since -1 is not a square modulo p, we must have $\chi_p(-1) = -1$. Since the character χ_p is conjugate symplectic, $\chi_p(p) = 1$, as p is a norm from the quadratic extension $\mathbb{Q}_p(\sqrt{-p})$. Hence $\chi(-p) = -1$ and $\chi(\sqrt{-p})$ is a fourth root of unity. This determines χ_p completely, as it is trivial on the squares of units. The corresponding cyclic extension of degree 4 over K_p is Galois over $\mathbb{Q}_p$ with Galois group the quaternion group of order 8. The Langlands parameter of π_p is the 2-dimensional symplectic representation of this quaternion group.

From the local Langlands correspondence, which is known explicitly for PGL_2, we obtain the following (which explains the appearance of the representations R and W in Hecke's invariant subspace of forms with complex multiplication). Note that the local representations π_∞ and π_p are independent of the choice of embedding $\iota : E^+ \to \mathbb{R}$.

Theorem 10.1 *The local component π_p of π is the depth zero supercuspidal representation compactly induced from the irreducible representation R of $\mathrm{PGL}_2(\mathbb{Z}_p)$, where R is the discrete series of dimension $(p-1)$ of $\mathrm{PGL}_2(p)$ associated to a quartic character of the non-split torus.*

The finite dimensional space of K_1-invariants in π_p (where K_1 is the first congruence subgroup of $\mathrm{PGL}_2(\mathbb{Z}_p)$) is isomorphic to the representation R of $\mathrm{PGL}_2(p)$.

Since the representations π_∞ and π_p are both in the discrete series, the global Jacquet-Langlands correspondence [18] shows that (for each real embedding ι of E^+) there is an automorphic representation $\pi^* = \prod \pi_v^*$ of the adèlic group $(D \otimes \mathbb{A})^*/\mathbb{A}^*$, with D the quaternion algebra over $\mathbb{Q}$ ramified at ∞ and p. The local components π_ℓ^* are all unramified, and isomorphic to the components π_ℓ. The local component π_∞^* is the trivial representation of the compact group $D_\infty^*/\mathbb{R}^*$. The local component π_p^* is the 2-dimensional representation of the finite dihedral group $D_p^*/\mathbb{Q}_p^*(1+P)$ of order $2(p+1)$, induced from a quartic character of the cyclic subgroup [21, Appendix].

Note that the dimension of the space V_0^+ in [21, Prop 12] is equal to the integer $m(W) + m(W^\vee)$ in section 6. This is the number of irreducible automorphic representations π of $\mathrm{PGL}_2(\mathbb{A})$ with local components π_∞ isomorphic to the discrete series of weight 2, π_p isomorphic to the depth zero supercuspidal representation which is compactly induced from the representation R of $\mathrm{PGL}_2(\mathbb{Z}_p)$, and π_ℓ unramified for all $\ell \neq p$.

11 Elliptic curves with complex multiplication

As Shimura observed in [26], certain regular differentials in Hecke's distinguished subspace give elliptic curve quotients of the Jacobian $J_0(p^2)$ of $X_0(p^2)$ over $\mathbb{C}$, which have complex multiplication by $K = \mathbb{Q}(\sqrt{-p})$. He defined an abelian variety $B(p)$ of dimension $h = h(-p)$ which was a quotient of $J_0(p^2)$ over $\mathbb{Q}$ and had complex multiplication over K. In my PhD thesis [9], I showed that, over the Hilbert class field H of K, the variety $B(p)$ decomposes as a product of h conjugate elliptic curves $A(p)^\sigma$ with complex multiplication by the ring of integers of K. Here is a definition of the abelian varieties $A(p)$ and $B(p)$.

Let $F = \mathbb{Q}(j)$ be the numberfield of degree $h = h(-p)$ which is generated by the modular invariant $j = j((1+\sqrt{-p})/2)$ of an elliptic curve with complex multiplication by the ring of integers of K. In [9] I defined an elliptic curve $A(p)$ over F having this j-invariant and having minimal discriminant $\Delta = -p^3$. We can obtain an explicit model for $A(p)$ over F by solving the two equations

$$(c_4)^3/\Delta = j \quad (c_6)^2/\Delta = j - 1728.$$

The former has a unique solution in F and the latter has a unique solution in F whose sign at the real place is equal to the quadratic symbol $\left(\frac{2}{p}\right)$ [12]. The curve $A(p)$ is defined over F by the cubic equation

$$y^2 = x^3 - (c_4/48)x - (c_6/864).$$

The elliptic curve $A(p)$ has a number of agreeable propeties. Over the Hilbert class field $H = K(j) = F(\sqrt{-p})$ of K, it acquires complex multiplication by the ring of integers of K, and is isogenous to all of its Galois conjugates $A(p)^\sigma$. The L-function of $A(p)$ over F is equal to the L-function of the algebraic Hecke character of H defined by composing the algebraic Hecke character χ with the norm map from H to K: $\chi \circ N : \mathbb{A}_H^* \to K^*$ [9, §].

The abelian variety $B(p) = \mathrm{Res}_{F/\mathbb{Q}}\, A(p)$ is obtaained from $A(p)$ by restriction of scalars. It has real multiplication by an order in E^+ over $\mathbb{Q}$ and complex multiplication by an order in E (generated by the h^{th} roots of algebraic integers of K whose principal ideal is an h^{th} power).[9, §]. Since $B(p)$ is obtained by restriction of scalars, the L-function of $B(p)$ over $\mathbb{Q}$ is equal to the L-function of $A(p)$ over F. It factors into a product of h L-series of modular forms as follows. Recall the Euler product of the eigenform f of weight 2 and coefficients in E^+

$$L(f,s) = \prod_{\ell \neq p} (1 - t_\ell \ell^{-s} + \ell^{1-2s})^{-1}.$$

The $L(B(p)/\mathbb{Q}, s)$ is obstained by composing this Euler product with the h different embeddings $\iota : E^+ \to \mathbb{R}$ and taking their product:

$$L(B(p)/\mathbb{Q}, s) = \prod L(\iota \circ f, s).$$

The completed L-function

$$\Lambda(s) = p^{hs}.\Gamma_{\mathbb{C}}(s)^h.L(B(p)/\mathbb{Q}, s)$$

is entire, and satisfies the functional equation

$$\Lambda(s) = \epsilon.\Lambda(2-s)$$

with sign $\epsilon = \left(\frac{2}{p}\right)$ [9, §]. Thus $\epsilon = +1$ when $p \equiv 7 \pmod 8$ and $\epsilon = -1$ when $p \equiv 3 \pmod 8$.

The curve $B(7) = A(7)$ was the first elliptic curve for which the full conjecture of Birch and Swinnerton-Dyer was proved. I showed that $A(7)(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ had rank 0 and that $L(A(7)/\mathbb{Q}, 1)$ was non-zero. I also proved that $Ш[2] = Ш[7] = 0$ [9, §]. In the fall of 1986, Rubin [22] proved that $Ш[\ell] = 0$ for all primes $\ell \neq 2, p$. Hence $Ш = 0$ and the conjecture of Birch and Swinnerton-Dyer is true. In the general case it is known that [20]:

- The order of vanishing of $L(B(p/\mathbb{Q}, s)$ at the point $s = 1$ is equal to 0 if $p \equiv 7 \pmod 8$ and is equal to $h = h(-p)$ if $p \equiv 3 \pmod 8$.
- The Mordell-Weil group $B(p)(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if $p \equiv 7 \pmod 8$ and is isomorphic to $\mathbb{Z}^h$ if $p \equiv 3 \pmod 8$.
- The Tate-Shafarevich group $Ш(B(p)/\mathbb{Q})$ is finite.

The entire conjecture of Birch and Swinnerton-Dyer for the abelian varieties $B(p)$ over $\mathbb{Q}$ should be within reach, using the results of [28] and [30].

References

[1] A. O.L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$. *Math. Ann.* **185** (1970), 134-160.

[2] C. Chevalley and A. Weil, Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers. *Abh. Math. Sem. Univ. Hamburg* **10** (1934), 358–361.

[3] P. Deligne Travaux de Shimura. In: Sminaire Bourbaki, Exp. No. 389, *Springer Lecture Notes* **244**, (1971), 123-165

[4] P. Deligne and M. Rapoport. Les schmas de modules de courbes elliptiques. In: Modular functions of one variable, II. *Springer Lecture Notes* **349** (1973), 143–316.

[5] M. Eichler, Eine Spurformel für Korrespondenzen von algebraischen Funktionenkörpern mit sich selber. *Invent. Math.* **2** 1967 274-300.

[6] G. Frobenius, Über Gruppencharaktere. *S'bar. Akad. Wiss. Berlin* (1896), 985–1021.

[7] W. Fulton and J. Harris, Representation Theory. Springer GTM 129 (1991).

[8] B. Gross, Group representations and lattices. *Journal AMS* **3** (1990), 929–960.

[9] B. Gross, Arithmetic on elliptic curves with complex multiplication *Springer Lecture Notes* **776** (1980).

[10] B. Gross Representation theory and the cuspidal group of $X(p)$. *Duke Math. J.* **54** (1987), 67-75.

[11] B. Gross On the Satake isomorphism. In: Galois representations in arithmetic algebraic geometry, *London Math. Soc. Lecture Notes* **254** (1998), 223–237.

[12] B. Gross Minimal models for elliptic curves with complex multiplication. *Compositio Math.* **45** (1982), 155–164.

[13] E. Hecke, Bestimmung der Perioden gewisser Integrale durch die Theorie der Klassenkörper. *Math. Zeitschrift* **28** (1928), 707–727.

[14] E. Hecke, Über ein Fundalmentalproblem aus der Theorie der elliptischen Modulfunktionen. *Abh. Math. Sem. Univ. Hamburg* **6** (1928), 235–257.

[15] E. Hecke, Über das Verhalten der Integrale 1. Gattung bei Abbildungen, insbesondere in der Theorie der elliptischen Modulfunktionen. *Abh. Math. Sem. Univ. Hamburg* **8** (1930), 271–281.

[16] E. Hecke, Grundlagen einer Theorie der Integralgruppen und der Integralperioden bei den Normalteilern der Modulgruppe. *Math. Annalen* **116** (1939), 469–510.

[17] H. Hida, On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves. *Amer. J. Math.* **103** (1981), 727–776.

[18] H. Jacquet and R. Langlands, Automorphic forms on $\mathrm{GL}(2)$. *Springer Lecture Notes* **114** (1970).

[19] S. Lefshetz, On the fixed point formula. *Ann. of Math.* **8** (1937) 819-822.

[20] S. Millller and T. Yang. Non-vanishing of the central derivative of canonical Hecke L-functions. *Math. Res. Lett.* **7** (2000), 263-277.

[21] A. Pacetti and F. Rodriguez-Villegas, with an appendix by B. Gross, Computing weight 2 modular forms of level p^2. *Math. of Computation* **74** (2004), 1545–1557.

[22] K. Rubin, Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. *Invent. Math.* **89** (1987), no. 3, 527-559.

[23] J-P. Serre, Linear representations of finite groups. Springer GTM, 1977.

[24] J-P. Serre Quelques applications de théorème de Chebotarev. *Publ. Math. IHES* **54** (1981), 123–201.

[25] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan, No. 11, 1971.

[26] G. Shimura, On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. *Nagoya Math. J.* **43** (1971), 199–208.

[27] G. Shimura, On the factors of the Jacobian variety of a modular function field. *J. Math. Soc. Japan* **25** (1973), 523–5

[28] C. Skinner and E. Urban, The Iwasawa main conjectures for GL_2. *Invent. Math.* **195** (2014), 1-277.

[29] A. Weil, Über Matrizenringe auf Riemannschen Flächen und den Riemann-Rochsen Satz. *Abh. Math. Sem. Univ. Hamburg* **11** (1935), 110–115.

[30] W. Zhang, Selmer groups and the indivisibility of Heegner points. *Cambridge Journal of Math.* **2** (2014), 191–253.